

Command Reference

vRX Amazon EC2 Edition

Rev. 19.00.08

vRX VMware ESXi Edition

Rev. 19.01.06

vRX Sakura Cloud Edition

Rev. 19.02.10

RTX840 Rev. 23.02.02

RTX3510 Rev. 23.01.03

RTX1300 Rev. 23.00.17

RTX1220 Rev. 15.04.07

RTX830 Rev. 15.02.33

RTX1210 Rev. 14.01.42

RTX5000 Rev. 14.00.34

RTX3500 Rev. 14.00.34

Yamaha Corporation

October 2025

Version 12.01

Table of Contents

Preface: Introduction

Chapter 1: How to Read This Command Reference

- 1.1 Supported Program Revisions
- 1.2 How to Use This Command Reference
- 1.3 Interface Names
- 1.4 Input Format for Commands Beginning with “no”
- 1.5 Number of Characters Required for Command Input and Escape Sequences
- 1.6 Differences in Peer Information Numbers by Model
- 1.7 Default Settings at Factory Shipment or Initial State After Deployment

Chapter 2: How to Use Commands

- 2.1 Console
 - 2.1.1 Configuration Procedure Using the Console
 - 2.1.2 Configuration via CONSOLE or SERIAL Port
 - 2.1.3 Configuration via Virtual Machine Console
 - 2.1.4 Configuration via TELNET
 - 2.1.5 Configuration via SSH
 - 2.1.6 Remote Setup
- 2.2 SSH Server
 - 2.2.1 Notes on Using the SSH Server Function
 - 2.2.2 SSH Server Configuration
- 2.3 TFTP
 - 2.3.1 Configuration Procedure Using TFTP
 - 2.3.2 Reading Configuration Files
 - 2.3.3 Writing Configuration Files
- 2.4 Keyboard Operations When Using the Console
- 2.5 Commands Beginning with “show”
 - 2.5.1 Extracting Only Lines Matching Search Patterns
 - 2.5.2 Improving Readability of Output
 - 2.5.3 Redirecting Output to External Memory or Storage

Chapter 3: Help

- 3.1 Displaying Brief Explanations on the Console
- 3.2 Displaying the Command List

Chapter 4: Device Configuration

- 4.1 Setting the Administrator Password
- 4.2 Encrypted Storage of the Administrator Password
- 4.3 Setting General Usernames and Login Passwords
- 4.4 Using RADIUS for Password Authentication at Login
- 4.5 Using RADIUS for Password Authentication When Switching to Administrator
- 4.6 Setting User Attributes
- 4.7 Forcibly Disconnecting Other Users
- 4.8 Security Class Configuration
- 4.9 Time Zone Configuration
- 4.10 Setting the Current Date
- 4.11 Setting the Current Time
- 4.12 Setting the Clock via a Remote Host
- 4.13 Clock Configuration Using NTP
- 4.14 Setting the Source IP Address for NTP Packets
- 4.15 Allowing Time Synchronization with Stratum 0 NTP Servers
- 4.16 Console Prompt Display Settings

- 4.17 Console Language and Encoding Settings
- 4.18 Console Display Character Width
- 4.19 Console Display Line Count
- 4.20 Displaying System Messages on the Console
- 4.21 SYSLOG Host IP Address Configuration
- 4.22 SYSLOG Packet Format
- 4.23 SYSLOG Facility Configuration
- 4.24 SYSLOG Header Hostname
- 4.25 Output of NOTICE-type SYSLOG
- 4.26 Output of INFO-type SYSLOG
- 4.27 Output of DEBUG-type SYSLOG
- 4.28 Source IP Address for SYSLOG Transmission
- 4.29 Source Port Number for SYSLOG Packets
- 4.30 Outputting Executed Commands to SYSLOG
- 4.31 Outputting Interface Packet Dumps to SYSLOG
- 4.32 TELNET Server ON/OFF
- 4.33 TELNET Server Listen Port
- 4.34 Hosts Allowed to Access TELNET Server
- 4.35 Maximum Concurrent TELNET Connections
- 4.36 CPU Usage Threshold
- 4.37 Memory Usage Threshold
- 4.38 Fast Path Function
- 4.39 Transmission Suppression Time After LAN Link-Up
- 4.40 Port Mirroring
- 4.41 LAN Interface Operation Type
- 4.42 Static Link Aggregation
- 4.43 LAN Interface Receive Packet Buffer Size
- 4.44 Login Timer
- 4.45 Hosts Allowed to Access via TFTP
- 4.46 Relaying Magic Packets to LAN
- 4.47 Interface/System Description
- 4.48 Outputting TCP Connection-Level SYSLOG
- 4.49 Allowing HTTP Firmware Revision Upgrade
- 4.50 URL for HTTP Firmware Revision Upgrade
- 4.51 Proxy Server for HTTP Firmware Revision Upgrade
- 4.52 Timeout for HTTP Firmware Revision Upgrade
- 4.53 Allowing Firmware Downgrade
- 4.54 Allowing Firmware Upgrade via DOWNLOAD Button
- 4.55 Scheduling Firmware Upgrade
- 4.56 SSH Server ON/OFF
- 4.57 SSH Server Listen Port
- 4.58 Hosts Allowed to Access SSH Server
- 4.59 Maximum Concurrent SSH Connections
- 4.60 SSH Server Host Key Configuration
- 4.61 Displaying SSH Server Host Keys
- 4.62 Available Encryption Algorithms for SSH Server
- 4.63 SSH Client Keepalive
- 4.64 Hiding OpenSSH Version Information in SSH Server Responses
- 4.65 Authentication Methods Available on SSH Server
- 4.66 File for Storing Public Keys Used for SSH Public Key Authentication
- 4.67 SSH Public Key Configuration
- 4.68 Displaying SSH Public Keys
- 4.69 Hosts Allowed to Access SFTP Server
- 4.70 SSH Client
- 4.71 SCP Client
- 4.72 Available Encryption Algorithms for SSH Client
- 4.73 File for Storing SSH Server Public Key Information

4Command reference.

4.74 Modifying Packet Buffer Parameters

4.75 Alarm Sound Settings (Enable/Disable)

Chapter 5: Yamaha Router File System (RTFS)

5.1 Formatting RTFS

5.2 Garbage Collection of RTFS

Chapter 6: IP Configuration

6.1 Common Interface Settings

6.1.1 Enabling/Disabling IP Packet Handling

6.1.2 IP Address Configuration

6.1.3 Secondary IP Address Configuration

6.1.4 Interface MTU Configuration

6.1.5 Enabling/Disabling Loopback Packets on the Same Interface

6.1.6 Enabling/Disabling echo, discard, and time Services

6.1.7 Static IP Route Configuration

6.1.8 Automatically Adding Default Routes When IP Address Is Obtained via DHCP

6.1.9 Automatically Adding Implicit Routes When IP Address Is Obtained via DHCP

6.1.10 IP Packet Filter Configuration

6.1.11 Filter Set Definition

6.1.12 Filtering IP Packets with Source-Route Options

6.1.13 Filtering Directed Broadcast Packets

6.1.14 Dynamic Filter Definition

6.1.15 Dynamic Filter Timeout Configuration

6.1.16 Cache Timer Configuration for FQDN Filters

6.1.17 Intrusion Detection Operation Configuration

6.1.18 Notification Frequency Configuration for Intrusion Detection (per Second)

6.1.19 Suppression of Duplicate Intrusion Detection Notifications

6.1.20 Maximum Display Count for Intrusion Detection Information

6.1.21 TCP Session MSS Limitation Configuration

6.1.22 TCP Window Scale Option Configuration

6.1.23 Configuration of Maximum TCP Sessions Terminated at the Router

6.1.24 Logging Configuration When IPv4 Route Information Changes

6.1.25 Security Configuration Using Filtering

6.1.26 Rewriting the DF Bit to 0 for Matching IP Packets

6.1.27 TOS Field Rewrite Configuration

6.1.28 Proxy ARP Configuration

6.1.29 ARP Entry Lifetime Configuration

6.1.30 Static ARP Entry Configuration

6.1.31 Controlling the Number of Packets Queued Until ARP Resolution

6.1.32 Logging Configuration for ARP Entry Changes

6.1.33 Priority Configuration for Implicit Routes

6.1.34 Flow Table Entry Lifetime Configuration

6.1.35 Flow Table Entry Count Configuration

6.1.36 Retention Time for Fragment Packet Reassembly

6.1.37 DS Field Rewrite Configuration

6.2 PP-Side Configuration

6.2.1 PP-Side IP Address Configuration

6.2.2 Remote IP Address Pool Configuration

6.2.3 Keepalive Interval Configuration over PP

6.2.4 Enabling/Disabling Keepalive over PP

6.2.5 Logging Configuration for PP Keepalive

6.3 RIP Configuration

6.3.1 Enabling/Disabling RIP

6.3.2 Trusted Gateway Configuration for RIP

6.3.3 RIP Route Priority Configuration

6.3.4 RIP Packet Transmission Settings

- 6.3.5 RIP Packet Reception Settings
- 6.3.6 RIP Filtering Configuration
- 6.3.7 Hop Count Addition Configuration for RIP
- 6.3.8 Authentication Configuration for RIP2
- 6.3.9 Authentication Key Configuration for RIP2
- 6.3.10 Advertisement Mode Configuration for RIP2
- 6.3.11 Route Retention on Line Disconnection
- 6.3.12 RIP Operation on PP Side When Line Connects
- 6.3.13 RIP Transmission Interval on PP Side When Line Connects
- 6.3.14 RIP Operation on PP Side When Line Disconnects
- 6.3.15 RIP Transmission Interval on PP Side When Line Disconnects
- 6.3.16 Source Interface Switching During Backup Operation
- 6.3.17 Forced Route Advertisement in RIP
- 6.3.18 Filter Comparison Method in RIP2
- 6.3.19 RIP Timer Adjustment
- 6.4 VRRP Configuration
 - 6.4.1 VRRP Configuration per Interface
 - 6.4.2 Shutdown Trigger Configuration
- 6.5 Backup Configuration
 - 6.5.1 PP Backup Destination When Provider Connection Goes Down
 - 6.5.2 Wait Time Before Returning from Backup
 - 6.5.3 Backup Destination When LAN-Based Provider Connection Goes Down
 - 6.5.4 Wait Time Before Returning from Backup
 - 6.5.5 Enabling/Disabling LAN-Based Keepalive
 - 6.5.6 LAN-Based Keepalive Interval Configuration
 - 6.5.7 Logging Configuration for LAN-Based Keepalive
 - 6.5.8 Network Monitoring Function Configuration
- 6.6 Packet Forwarding Filter Configuration
 - 6.6.1 Packet Forwarding Filter Definition
 - 6.6.2 Applying Packet Forwarding Filters to Interfaces
- 6.7 LAN Pass-Through Function Configuration
 - 6.7.1 EtherType Configuration for LAN Pass-Through
 - 6.7.2 Interface Configuration for LAN Pass-Through

Chapter 7: Ethernet Filter Configuration

- 7.1 Filter Definition Configuration
- 7.2 Application to Interfaces
- 7.3 Displaying Ethernet Filter Status

Chapter 8: URL Filter Configuration

- 8.1 Filter Definition Configuration
- 8.2 Applying URL Filters to Interfaces
- 8.3 HTTP Port Number Configuration for URL Filtering
- 8.4 Enabling/Disabling URL Filtering
- 8.5 HTTP Response Behavior for Dropped Packets
- 8.6 Logging Configuration for Filter Matches

Chapter 9: PPP Configuration

- 9.1 Peer Username and Password Configuration
- 9.2 Accepted Authentication Type Configuration
- 9.3 Requested Authentication Type Configuration
- 9.4 Local Username and Password Configuration
- 9.5 Enabling/Disabling Duplicate Connections from the Same Username
- 9.6 LCP-Related Configuration
 - 9.6.1 Address and Control Field Compression
 - 9.6.2 Magic Number Option
 - 9.6.3 Maximum Receive Unit Option

- 9.6.4 Protocol Field Compression
- 9.6.5 lcp-restart Parameter Configuration
- 9.6.6 lcp-max-terminate Parameter Configuration
- 9.6.7 lcp-max-configure Parameter Configuration
- 9.6.8 lcp-max-failure Parameter Configuration
- 9.6.9 Immediate Configure-Request Transmission
- 9.7 PAP-Related Configuration
 - 9.7.1 pap-restart Parameter Configuration
 - 9.7.2 pap-max-authreq Parameter Configuration
- 9.8 CHAP-Related Configuration
 - 9.8.1 chap-restart Parameter Configuration
 - 9.8.2 chap-max-challenge Parameter Configuration
- 9.9 IPCP-Related Configuration
 - 9.9.1 Van Jacobson Compressed TCP/IP
 - 9.9.2 PP-Side IP Address Negotiation
 - 9.9.3 ipcp-restart Parameter Configuration
 - 9.9.4 ipcp-max-terminate Parameter Configuration
 - 9.9.5 ipcp-max-configure Parameter Configuration
 - 9.9.6 ipcp-max-failure Parameter Configuration
 - 9.9.7 WINS Server IP Address Configuration
 - 9.9.8 Enabling/Disabling IPCP MS Extension Options
 - 9.9.9 Acceptance of Peer IP Addresses with Existing Host Routes
- 9.10 MSCBCP-Related Configuration
 - 9.10.1 mscbcpr-restart Parameter Configuration
 - 9.10.2 mscbcpr-maxretry Parameter Configuration
- 9.11 CCP-Related Configuration
 - 9.11.1 Compression Type Configuration for All Packets
 - 9.11.2 ccp-restart Parameter Configuration
 - 9.11.3 ccp-max-terminate Parameter Configuration
 - 9.11.4 ccp-max-configure Parameter Configuration
 - 9.11.5 ccp-max-failure Parameter Configuration
- 9.12 IPV6CP-Related Configuration
 - 9.12.1 Enabling/Disabling IPV6CP
- 9.13 PPPoE-Related Configuration
 - 9.13.1 LAN Interface Selection for PPPoE
 - 9.13.2 Access Concentrator Name Configuration
 - 9.13.3 Automatic Session Connection Configuration
 - 9.13.4 Automatic Session Disconnection Configuration
 - 9.13.5 Maximum Retransmissions for PADI Packets
 - 9.13.6 Retransmission Interval for PADI Packets
 - 9.13.7 Maximum Retransmissions for PADR Packets
 - 9.13.8 Retransmission Interval for PADR Packets
 - 9.13.9 PPPoE Session Disconnect Timer
 - 9.13.10 Service Name Configuration
 - 9.13.11 TCP MSS Limitation Configuration
 - 9.13.12 Forcibly Disconnecting Unknown PPPoE Sessions
 - 9.13.13 Interface Configuration for PPPoE Frame Relay

Chapter 10: DHCP Configuration

- 10.1 DHCP Server / Relay Agent Function
 - 10.1.1 DHCP Operation Configuration
 - 10.1.2 RFC2131-Compliant Operation Configuration
 - 10.1.3 Duplicate IP Address Check Configuration
 - 10.1.4 DHCP Scope Definition
 - 10.1.5 DHCP Reserved Address Configuration
 - 10.1.6 DHCP Address Allocation Behavior
 - 10.1.7 Generating Reservations from DHCP Lease Information

- 10.1.8 DHCP Option Configuration
- 10.1.9 Manual Addition of DHCP Lease Information
- 10.1.10 Manual Deletion of DHCP Lease Information
- 10.1.11 DHCP Server Specification
- 10.1.12 Source Port Configuration for DHCP Relay Agent
- 10.1.13 DHCP Server Selection Method
- 10.1.14 DHCP BOOTREQUEST Relay Criteria
- 10.1.15 DHCP Operation Configuration per Interface
- 10.2 DHCP Client Function
 - 10.2.1 DHCP Client Hostname Configuration
 - 10.2.2 Requested IP Address Lease Duration
 - 10.2.3 Retransmission Count and Interval for IP Address Requests
 - 10.2.4 DHCP Client ID Option Configuration
 - 10.2.5 DHCP Options Included in Client Requests
 - 10.2.6 Releasing Information on Link Down

Chapter 11: ICMP Configuration

- 11.1 IPv4 Configuration
 - 11.1.1 Enabling/Disabling ICMP Echo Reply
 - 11.1.2 Sending ICMP Echo Reply When Link Is Down
 - 11.1.3 Enabling/Disabling ICMP Mask Reply
 - 11.1.4 Enabling/Disabling ICMP Parameter Problem
 - 11.1.5 Enabling/Disabling ICMP Redirect
 - 11.1.6 Behavior on Receiving ICMP Redirect
 - 11.1.7 Enabling/Disabling ICMP Time Exceeded
 - 11.1.8 Enabling/Disabling ICMP Timestamp Reply
 - 11.1.9 Enabling/Disabling ICMP Destination Unreachable
 - 11.1.10 Sending ICMP Errors for Packets Decrypted by IPsec
 - 11.1.11 Logging Configuration for Received ICMP
 - 11.1.12 Stealth Mode Configuration
 - 11.1.13 Enabling/Disabling ARP-Based MTU Discovery
 - 11.1.14 Sending ICMP Destination Unreachable for Truncated Packets
- 11.2 IPv6 Configuration
 - 11.2.1 Enabling/Disabling ICMPv6 Echo Reply
 - 11.2.2 Sending ICMPv6 Echo Reply When Link Is Down
 - 11.2.3 Enabling/Disabling ICMPv6 Parameter Problem
 - 11.2.4 Enabling/Disabling ICMPv6 Redirect
 - 11.2.5 Behavior on Receiving ICMPv6 Redirect
 - 11.2.6 Enabling/Disabling ICMPv6 Time Exceeded
 - 11.2.7 Enabling/Disabling ICMPv6 Destination Unreachable
 - 11.2.8 Logging Configuration for Received ICMPv6
 - 11.2.9 Enabling/Disabling ICMPv6 Packet Too Big
 - 11.2.10 Sending ICMP Errors for Packets Decrypted by IPsec
 - 11.2.11 Stealth Mode Configuration
 - 11.2.12 Sending ICMP Errors (Packet Too Big) for Truncated Frames

Chapter 12: Tunneling

- 12.1 Enabling Tunnel Interfaces
- 12.2 Disabling Tunnel Interfaces
- 12.3 Tunnel Interface Connection Type Configuration
- 12.4 Tunnel Interface Type Configuration
- 12.5 Tunnel Interface IPv4 Address Configuration
- 12.6 Remote IPv4 Address Configuration for Tunnel Interface
- 12.7 Remote Tunnel Endpoint IP Address Configuration
- 12.8 Local Tunnel Endpoint IP Address Configuration
- 12.9 Tunnel Endpoint IP Address Configuration
- 12.10 Tunnel Endpoint Name Configuration

- 12.11 Multipoint Tunnel Server Configuration
- 12.12 Local Name Configuration for Multipoint Tunnel
- 12.13 Maximum Number of Peers for Multipoint Tunnel
- 12.14 MAP-E Type Configuration for Tunnel Interface
- 12.15 Translation Type Configuration for Tunnel Interface
- 12.16 Username and Password Configuration for Domestic Standard IPv6 Migration Provisioning
- 12.17 Provisioning Server Name Configuration for IPv6 Migration

Chapter 13: IPsec Configuration

- 13.1 IPsec Operation Configuration
- 13.2 IKE Version Configuration
- 13.3 IKE Authentication Method Configuration
- 13.4 Automatic Route Addition Based on Received IKE ID
- 13.5 Pre-Shared Key Registration
- 13.6 PKI File Configuration for IKEv2 Authentication
- 13.7 Username and Password Configuration for EAP-MD5 Authentication
- 13.8 User Authentication Configuration Using EAP-MD5
- 13.9 Sending Certificate Request Payload in EAP-MD5 Authentication
- 13.10 Initiating IKE Key Exchange
- 13.11 Rejecting Key Exchange When Configuration Differs
- 13.12 Continuing Key Exchange Without Suspension on Failure
- 13.13 Retransmission Count and Interval for Key Exchange
- 13.14 Remote Security Gateway Name Configuration
- 13.15 Remote Security Gateway IP Address Configuration
- 13.16 Remote ID Configuration
- 13.17 Local Security Gateway Name Configuration
- 13.18 Local Security Gateway IP Address Configuration
- 13.19 Local ID Configuration
- 13.20 IKE Keepalive Configuration
- 13.21 SYSLOG Output Configuration for IKE Keepalive
- 13.22 Encryption Algorithm Configuration for IKE
- 13.23 Receive Queue Length Configuration for IKE Packets
- 13.24 Diffie-Hellman Group Configuration
- 13.25 Hash Algorithm Configuration for IKE
- 13.26 Logging Configuration for Invalid SPI Values
- 13.27 IKE Payload Type Configuration
- 13.28 IKEv1 Key Exchange Type Configuration
- 13.29 Sending IKE Informational Payloads
- 13.30 Perfect Forward Secrecy (PFS) Configuration
- 13.31 XAUTH Configuration
- 13.32 User ID Configuration for XAUTH / EAP-MD5 Authentication
- 13.33 User ID Attribute Configuration for XAUTH / EAP-MD5
- 13.34 User Group Configuration for XAUTH / EAP-MD5
- 13.35 User Group Attribute Configuration for XAUTH / EAP-MD5
- 13.36 User Authentication Using XAUTH
- 13.37 Internal IP Address Pool Configuration
- 13.38 IKE XAUTH Mode-Cfg Method Configuration
- 13.39 Internal IP Address Pool Assignment for IPsec Clients
- 13.40 Registration of Concurrent VPN Client License
- 13.41 Applying Concurrent VPN Client License
- 13.42 IKE Log Type Configuration
- 13.43 UDP Encapsulation Configuration for ESP
- 13.44 Negotiation Parameter Restriction Configuration
- 13.45 IKE Message ID Management Configuration
- 13.46 CHILD SA Creation Method Configuration
- 13.47 Accepting Key Exchange Initiation Packets
- 13.48 SA-Related Configuration

- 13.48.1 SA Lifetime Configuration
- 13.48.2 SA Policy Definition
- 13.48.3 Manual SA Update
- 13.48.4 Dangling SA Behavior Configuration
- 13.48.5 IPsec NAT Traversal Configuration
- 13.48.6 SA Deletion
- 13.49 Tunnel Interface–Related Configuration
 - 13.49.1 Fragment Handling for Outer IPv4 Packets
 - 13.49.2 DF Bit Control for Outer IPv4 Packets
 - 13.49.3 SA Policy Selection
 - 13.49.4 IPComp Compression Configuration
 - 13.49.5 Tunnel Backup Configuration
 - 13.49.6 Tunnel Template Configuration
- 13.50 Transport Mode–Related Configuration
 - 13.50.1 Transport Mode Definition
 - 13.50.2 Transport Mode Template Configuration
- 13.51 PKI-Related Configuration
 - 13.51.1 Certificate File Configuration
 - 13.51.2 CRL File Configuration

Chapter 14: L2TP Function Configuration

- 14.1 Enabling/Disabling L2TP
- 14.2 L2TP Tunnel Authentication Configuration
- 14.3 L2TP Tunnel Disconnect Timer Configuration
- 14.4 L2TP Keepalive Configuration
- 14.5 L2TP Keepalive Logging Configuration
- 14.6 SYSLOG Output Configuration for L2TP Connection Control
- 14.7 Always-On Configuration for L2TPv3
- 14.8 L2TP Tunnel Hostname Configuration
- 14.9 L2TPv3 Local Router ID Configuration
- 14.10 L2TPv3 Remote Router ID Configuration
- 14.11 L2TPv3 Remote End ID Configuration

Chapter 15: IPIP Tunneling Function Configuration

- 15.1 IPIP Keepalive Configuration
- 15.2 IPIP Keepalive Logging Configuration

Chapter 16: SIP Function Configuration

- 16.1 Common Configuration
 - 16.1.1 Enabling/Disabling SIP
 - 16.1.2 SIP Session-Timer Value Configuration
 - 16.1.3 IP Protocol Selection for SIP Outbound Calls
 - 16.1.4 Enabling/Disabling 100rel Support for SIP Outbound Calls
 - 16.1.5 Adding User-Agent Header to SIP Packets
 - 16.1.6 Behavior When Incoming INVITE Lacks Refresher Specification
 - 16.1.7 Supporting P-N-UAType Header for Incoming SIP
 - 16.1.8 Session Timer Request Configuration for Incoming SIP
 - 16.1.9 Username Verification for Incoming SIP
 - 16.1.10 SIP Response Code When No Available Incoming Ports
 - 16.1.11 SIP IP Address Configuration
 - 16.1.12 SIP Message Logging Configuration

Chapter 17: SNMP Configuration

- 17.1 Host Configuration Permitted for SNMPv1 Access
- 17.2 Read-Only Community Name Configuration for SNMPv1
- 17.3 Read/Write Community Name Configuration for SNMPv1
- 17.4 SNMPv1 Trap Destination Configuration

- 17.5 Community Name Configuration for SNMPv1 Traps
- 17.6 Host Configuration Permitted for SNMPv2c Access
- 17.7 Read-Only Community Name Configuration for SNMPv2c
- 17.8 Read/Write Community Name Configuration for SNMPv2c
- 17.9 SNMPv2c Trap Destination Configuration
- 17.10 Community Name Configuration for SNMPv2c Traps
- 17.11 SNMPv3 Engine ID Configuration
- 17.12 SNMPv3 Context Name Configuration
- 17.13 User Configuration Managed by SNMPv3 USM
- 17.14 Host Configuration Permitted for SNMPv3 Access
- 17.15 MIB View Family Configuration Managed by SNMPv3 VACM
- 17.16 Access Policy Configuration Managed by SNMPv3 VACM
- 17.17 SNMPv3 Trap Destination Configuration
- 17.18 Source Address Configuration for SNMP Packets
- 17.19 sysContact Configuration
- 17.20 sysLocation Configuration
- 17.21 sysName Configuration
- 17.22 Enabling/Disabling Standard SNMP Traps
- 17.23 SNMP Trap Configuration for CPU Usage Monitoring
- 17.24 SNMP Trap Configuration for Memory Usage Monitoring
- 17.25 Delay Time Configuration for SNMP Trap Transmission
- 17.26 linkDown Trap Control Configuration
- 17.27 Displaying PP Interface Information Within MIB2 Scope
- 17.28 Displaying Tunnel Interface Information Within MIB2 Scope
- 17.29 Displaying Switch Interface Information Within MIB2 Scope
- 17.30 Forced Display Configuration for PP Interface Addresses
- 17.31 Trap Transmission Configuration for LAN Port Link Up/Down
- 17.32 Trap Transmission Configuration for Radio Signal Strength
- 17.33 Static Interface Number Assignment for Switches
- 17.34 Static Switch Number Assignment
- 17.35 SNMP Trap Condition Configuration Based on Switch Status
- 17.36 Common SNMP Trap Condition Configuration for Switches

Chapter 18: RADIUS Configuration

- 18.1 Enabling/Disabling Authentication Using RADIUS
- 18.2 Enabling/Disabling Accounting Using RADIUS
- 18.3 RADIUS Server Specification
- 18.4 RADIUS Authentication Server Specification
- 18.5 RADIUS Accounting Server Specification
- 18.6 UDP Port Configuration for RADIUS Authentication Server
- 18.7 UDP Port Configuration for RADIUS Accounting Server
- 18.8 RADIUS Shared Secret Configuration
- 18.9 RADIUS Retransmission Parameter Configuration

Chapter 19: NAT Function

- 19.1 NAT Operation Type Configuration
- 19.2 Applying NAT Descriptors to Interfaces
- 19.3 NAT Descriptor Operation Type Configuration
- 19.4 Outside IP Address Configuration for NAT Processing
- 19.5 Inside IP Address Configuration for NAT Processing
- 19.6 Static NAT Entry Configuration
- 19.7 Enabling/Disabling rlogin, rcp, and ssh in IP Masquerade
- 19.8 Static IP Masquerade Entry Configuration
- 19.9 NAT Address Mapping Cleanup Timer Configuration
- 19.10 Behavior When No Matching Translation Table Exists for Incoming Packets
- 19.11 Port Range Configuration for IP Masquerade
- 19.12 FTP Port Recognition Configuration

- 19.13 Port Range Exclusion Configuration for IP Masquerade
- 19.14 Logging Configuration for NAT Address Assignment
- 19.15 SIP IP Address Rewrite Configuration
- 19.16 Removing DF Bit During IP Masquerade Translation
- 19.17 Session Limit Configuration per Host for IP Masquerade
- 19.18 Total Session Limit Configuration for IP Masquerade

Chapter 20: DNS Configuration

- 20.1 Enabling/Disabling DNS
- 20.2 DNS Server IP Address Configuration
- 20.3 DNS Domain Name Configuration
- 20.4 Peer Information Number Configuration for DNS Server Notification
- 20.5 Interface Configuration for Obtaining DNS Server Addresses
- 20.6 DNS Server Notification Order Configuration via DHCP / DHCPv6 / IPCP MS Extension
- 20.7 Enabling/Disabling Queries for Private Addresses
- 20.8 Restricting AAAA Record Queries to DNS Servers
- 20.9 Enabling/Disabling Name Resolution in SYSLOG Display
- 20.10 DNS Server Selection Based on Query Content
- 20.11 Static DNS Record Registration
- 20.12 Source Port Configuration for DNS Query Packets
- 20.13 Host Configuration Permitted to Access DNS Server
- 20.14 Enabling/Disabling DNS Cache
- 20.15 Maximum DNS Cache Entry Configuration
- 20.16 Unified DNS Fallback Operation Configuration

Chapter 21: NAT46 / DNS46 Function

- 21.1 IPv4 Address Pool Configuration for NAT46
- 21.2 IPv6 Prefix Configuration for NAT46
- 21.3 Static Destination Address Mapping Configuration for NAT46
- 21.4 Displaying NAT46 Entries

Chapter 22: Priority Control / Bandwidth Control

- 22.1 Interface Speed Configuration
- 22.2 Filter Configuration for Traffic Classification
- 22.3 Queueing Algorithm Type Selection
- 22.4 MP Interleave Configuration
- 22.5 Applying Classification Filters
- 22.6 Queue Length Configuration per Class
- 22.7 Default Class Configuration
- 22.8 Class Attribute Configuration
- 22.9 Dynamic Class Control Configuration

Chapter 23: OSPF

- 23.1 Enabling OSPF
- 23.2 OSPF Usage Configuration
- 23.3 Route Priority Configuration Using OSPF
- 23.4 OSPF Router ID Configuration
- 23.5 Reflecting OSPF Routes in the Routing Table
- 23.6 External Route Redistribution
- 23.7 Filtering Configuration for Handling Received OSPF Routes
- 23.8 Filter Definition for External Route Redistribution
- 23.9 OSPF Area Configuration
- 23.10 Route Advertisement to Areas
- 23.11 Advertisement of Stub Connections
- 23.12 Virtual Link Configuration
- 23.13 OSPF Area Configuration for Specified Interfaces

- 23.14 Designating OSPF Routers on Non-Broadcast Networks
- 23.15 Handling Network Routes When Stubs Exist
- 23.16 Logging Configuration for OSPF State Transitions and Packet Exchange
- 23.17 Interval Configuration for Reflecting Interface State Changes in OSPF

Chapter 24: BGP

- 24.1 BGP Startup Configuration
- 24.2 Route Aggregation Configuration
- 24.3 Filter Configuration for Route Aggregation
- 24.4 Autonomous System (AS) Number Configuration
- 24.5 Router ID Configuration
- 24.6 Route Priority Configuration Using BGP
- 24.7 Applying Filters to Routes Received via BGP
- 24.8 Filter Configuration for Routes Received via BGP
- 24.9 Applying Filters to Routes Advertised via BGP
- 24.10 Enabling BGP Configuration
- 24.11 Filter Configuration for Routes Advertised via BGP
- 24.12 Peer Connection Configuration for BGP
- 24.13 Pre-Shared Key Configuration for TCP MD5 Authentication
- 24.14 BGP Logging Configuration
- 24.15 Forced Route Advertisement in BGP
- 24.16 Interval Configuration for Reflecting Interface State Changes in BGP
- 24.17 Default MED Value Configuration for Routes Without MED Attribute
- 24.18 Route Selection Priority Rule Configuration in BGP

Chapter 25: IPv6

- 25.1 Common Configuration
 - 25.1.1 Enabling/Disabling IPv6 Packet Handling
 - 25.1.2 IPv6 Interface Link MTU Configuration
 - 25.1.3 TCP Session MSS Limitation Configuration
 - 25.1.4 TCP Window Scale Option Configuration
 - 25.1.5 Discarding IPv6 Packets with Type 0 Routing Headers
 - 25.1.6 IPv6 Fast Path Function Configuration
 - 25.1.7 Packet Queue Count Until Address Resolution Completes (ICMPv6)
 - 25.1.8 Maximum Neighbor Cache Entry Configuration
 - 25.1.9 Retention Time for IPv6 Fragment Reassembly
 - 25.1.10 DS Field Rewrite Configuration for IPv6 Packets
- 25.2 IPv6 Address Management
 - 25.2.1 Dynamic Prefix Assignment Definition via DHCPv6
 - 25.2.2 IPv6 Address Configuration for Interfaces
 - 25.2.3 IPv6 Address Configuration Based on Interface Prefix
 - 25.2.4 Logging Configuration for IPv6 Prefix Changes
 - 25.2.5 DHCPv6 Operation Configuration
 - 25.2.6 Duplicate Address Detection (DAD) Transmission Count
 - 25.2.7 Maximum Number of Automatically Configured IPv6 Addresses
 - 25.2.8 Source IPv6 Address Selection Rules
- 25.3 Neighbor Discovery
 - 25.3.1 Prefix Definition Distributed via Router Advertisement
 - 25.3.2 RDNSS Option Definition via Router Advertisement
 - 25.3.3 Router Advertisement Transmission Control
 - 25.3.4 Router Solicitation Retransmission Configuration
 - 25.3.5 DNSSL Option Definition via Router Advertisement
 - 25.3.6 Route Information Option Definition via Router Advertisement
- 25.4 Route Control
 - 25.4.1 Adding IPv6 Route Information
 - 25.4.2 Logging Configuration for IPv6 Route Changes
- 25.5 RIPng

- 25.5.1 Enabling RIPng
- 25.5.2 RIPng Transmission Policy Configuration per Interface
- 25.5.3 RIPng Reception Policy Configuration per Interface
- 25.5.4 Hop Count Addition Configuration for RIPng
- 25.5.5 Trusted RIPng Gateway Configuration per Interface
- 25.5.6 Filtering Configuration for Routes Transmitted and Received via RIPng
- 25.5.7 RIPng Operation on PP Side When Line Connects
- 25.5.8 RIPng Transmission Interval on PP Side When Line Connects
- 25.5.9 RIPng Operation on PP Side When Line Disconnects
- 25.5.10 RIPng Transmission Interval on PP Side When Line Disconnects
- 25.5.11 Retaining RIPng Routes on Line Disconnection
- 25.5.12 Route Priority Configuration Using RIPng
- 25.6 VRRPv3
 - 25.6.1 VRRPv3 Configuration per Interface
 - 25.6.2 Shutdown Trigger Configuration
- 25.7 Filter Configuration
 - 25.7.1 IPv6 Filter Definition
 - 25.7.2 Applying IPv6 Filters
 - 25.7.3 IPv6 Dynamic Filter Definition
- 25.8 IPv6 Multicast Packet Forwarding
 - 25.8.1 MLD Operation Configuration
 - 25.8.2 Static MLD Configuration
- 25.9 Neighbor Solicitation
 - 25.9.1 Triggering Neighbor Solicitation by Duplicate Address Detection

Chapter 26: OSPFv3

- 26.1 Enabling OSPFv3
- 26.2 OSPFv3 Usage Configuration
- 26.3 OSPFv3 Router ID Configuration
- 26.4 OSPFv3 Area Configuration
- 26.5 Route Advertisement to Areas
- 26.6 OSPFv3 Area Configuration for Specified Interfaces
- 26.7 Virtual Link Configuration
- 26.8 Route Priority Configuration Using OSPFv3
- 26.9 Reflecting OSPFv3 Routes in the Routing Table
- 26.10 Filtering Configuration for Handling Received OSPFv3 Routes
- 26.11 External Route Redistribution
- 26.12 Filter Definition for External Route Redistribution
- 26.13 OSPFv3 Logging Configuration

Chapter 27: HTTP Server Function

- 27.1 Enabling/Disabling the HTTP Server Function
- 27.2 Host Configuration Permitted to Access the HTTP Server
- 27.3 HTTP Server Session Timeout Configuration
- 27.4 HTTP Server Listen Port Configuration
- 27.5 Naming Configuration for PP Interfaces and Tunnel Interfaces

Chapter 28: Netvolante DNS Service Configuration

- 28.1 Enabling/Disabling Netvolante DNS Service
- 28.2 Manual Update to Netvolante DNS Server
- 28.3 Deleting Entries from Netvolante DNS Server
- 28.4 Port Number Configuration for Netvolante DNS Service
- 28.5 Retrieving the List of Registered Hostnames from Netvolante DNS Server
- 28.6 Hostname Registration
- 28.7 Communication Timeout Configuration
- 28.8 Enabling/Disabling Automatic Hostname Generation
- 28.9 Hostname Registration Command Configuration Using Serial Number

- 28.10 Netvolante DNS Server Configuration
- 28.11 Enabling/Disabling Netvolante DNS Server Address Update Function
- 28.12 Port Number Configuration for Netvolante DNS Server Address Update
- 28.13 Retry Interval and Count Configuration for Failed Automatic Updates
- 28.14 Periodic Update Interval Configuration for Netvolante DNS Registration
- 28.15 File Configuration for Saving Settings on Successful Automatic Registration

Chapter 29: UPnP Configuration

- 29.1 Enabling/Disabling UPnP
- 29.2 Interface Configuration for Obtaining IP Address Used by UPnP
- 29.3 Erase Timer Type Configuration for UPnP Port Mapping
- 29.4 Erase Timer Configuration for UPnP Port Mapping
- 29.5 SYSLOG Output Configuration for UPnP

Chapter 30: USB Configuration

- 30.1 Enabling/Disabling USB Host Function
- 30.2 Time Configuration Until Overcurrent Protection Activates on USB Bus

Chapter 31: Schedule

- 31.1 Schedule Configuration

Chapter 32: VLAN Configuration

- 32.1 VLAN ID Configuration
- 32.2 VLAN Interconnection Interface Group Configuration
- 32.3 Logging Configuration for Traffic Control by VLAN Interconnection Interface Groups

Chapter 33: Alive Notification Function

- 33.1 Shared Key Configuration for Alive Notification
- 33.2 Enabling/Disabling Alive Notification Reception
- 33.3 Executing Alive Notification

Chapter 34: Alive Notification Function – Release 2

- 34.1 Notification Name Configuration
- 34.2 Notification Definition Configuration
- 34.3 Enabling Notification Definitions
- 34.4 Notification Interval Configuration
- 34.5 Logging Configuration When Notifications Are Sent
- 34.6 Reception Definition Configuration
- 34.7 Enabling Reception Definitions
- 34.8 Monitoring Configuration for Reception Intervals
- 34.9 Logging Configuration When Notifications Are Received
- 34.10 Maximum Number of Alive Information Entries That Can Be Stored Simultaneously
- 34.11 Displaying Alive Notification Status
- 34.12 Clearing Alive Notification Status

Chapter 35: SNTP Server Function

- 35.1 Enabling/Disabling the SNTP Server Function
- 35.2 Host Configuration Permitted to Access the SNTP Server

Chapter 36: External Memory Function

- 36.1 Enabling/Disabling the microSD Card Slot
- 36.2 Operating Mode Configuration for Cache Memory Used with External Memory
- 36.3 Cache Memory Size Configuration for High-Speed File Access
- 36.4 Filename Prefix Configuration for Statistical Information Stored in External Memory
- 36.5 SYSLOG Filename Configuration for Storage in External Memory
- 36.6 Enabling/Disabling Copy Operation of Configuration and Firmware Files by Simultaneous Press of External

Memory Button and DOWNLOAD Button

- 36.7 Enabling/Disabling Boot from Files Stored in External Memory
- 36.8 Timeout Configuration for Detecting External Memory at Router Startup
- 36.9 Firmware Filename Configuration Loaded at Startup or by Simultaneous Button Press
- 36.10 Configuration Filename Configuration Loaded at Startup or by Simultaneous Button Press
- 36.11 Timeout Configuration for File Search
- 36.12 Executing Batch Files
- 36.13 Configuration of Batch Files and Execution Result Files
- 36.14 External Memory Performance Measurement Command
- 36.15 Function Configuration Executed When DOWNLOAD Button Is Pressed
- 36.16 Enabling/Disabling Batch File Execution by DOWNLOAD Button

Chapter 37: HTTP Upload Function

- 37.1 File Configuration for HTTP Upload
- 37.2 URL Configuration for HTTP Upload Destination
- 37.3 Enabling/Disabling HTTP Upload
- 37.4 Timeout Configuration for HTTP Upload
- 37.5 Retry Interval and Count Configuration for HTTP Upload
- 37.6 Proxy Server Configuration for HTTP Upload
- 37.7 Executing HTTP Upload
- 37.8 Alarm Sound Configuration Related to HTTP Upload Function

Chapter 38: Bridge Interface (Bridge Function)

- 38.1 Interface Assignment to Bridge Interface
- 38.2 Enabling/Disabling Automatic Learning
- 38.3 Aging Timer Configuration for Learned Bridge Information
- 38.4 Static Learning Information Configuration

Chapter 39: Lua Script Function

- 39.1 Enabling/Disabling Lua Script Function
- 39.2 Executing Lua Scripts
- 39.3 Executing the Lua Compiler
- 39.4 Displaying Lua Script Execution Status
- 39.5 Forcibly Terminating Lua Scripts
- 39.6 Alarm Sound Configuration Related to Lua Script Function

Chapter 40: Custom GUI

- 40.1 Enabling/Disabling Custom GUI
- 40.2 User Configuration for Custom GUI
- 40.3 Enabling/Disabling Custom GUI API
- 40.4 Password Configuration for Accessing Custom GUI API

Chapter 41: L2MS

- 41.1 Common Configuration
 - 41.1.1 Enabling/Disabling L2MS
 - 41.1.2 Monitoring Interval Configuration for Agents
 - 41.1.3 Monitoring Interval Configuration for Device Information
 - 41.1.4 Enabling/Disabling Snapshot Function
 - 41.1.5 Creating Snapshot Files
 - 41.1.6 SYSLOG Output Configuration for LAN Map
 - 41.1.7 Device Name Configuration Used in LAN Map
- 41.2 Switch Control
 - 41.2.1 Selecting a Switch
 - 41.2.2 Function Configuration Supported by the Switch
 - 41.2.3 Retrieving Switch Function Settings and Operational Status
 - 41.2.4 Executing Specific Operations on a Switch

- 41.2.5 Deleting Switch Configuration
- 41.2.6 Updating Switch Firmware
- 41.2.7 LAN Cable Redundancy Function Configuration
- 41.2.8 Directory Configuration for Storing Switch Configuration Files
- 41.2.9 Filename Configuration for Storing Switch Configuration
- 41.2.10 Retrieving Switch Configuration
- 41.2.11 Restoring Switch Configuration
- 41.3 Switch Functions
 - 41.3.1 System
 - 41.3.2 Ports
 - 41.3.3 MAC Address Table
 - 41.3.4 VLAN
 - 41.3.5 QoS
 - 41.3.6 Mirroring
 - 41.3.7 Counters
 - 41.3.8 Loop Detection
 - 41.3.9 PoE Power Supply
- 41.4 Access Point Control
 - 41.4.1 Selecting an Access Point
 - 41.4.2 Directory Configuration for Storing Access Point Configuration Files
 - 41.4.3 Filename Configuration for Storing Access Point Configuration
 - 41.4.4 Executing Backup of Access Point Configuration
 - 41.4.5 Executing Restore of Access Point Configuration
 - 41.4.6 Deleting Access Point Configuration
 - 41.4.7 Enabling/Disabling Zero-Configuration Function for Access Point
 - 41.4.8 Executing HTTP Firmware Revision Upgrade for Access Point
 - 41.4.9 Using HTTP Proxy for Access Point Control
 - 41.4.10 Timeout Configuration for HTTP Proxy Used in Access Point Control

Chapter 42: YNO Agent

- 42.1 Enabling/Disabling YNO Agent Function
- 42.2 Access Code Configuration for Connecting to YNO Manager
- 42.3 Additional SYSLOG Output Configuration for YNO Agent Function
- 42.4 Device Description Configuration Displayed in YNO Manager
- 42.5 HTTPS Proxy Server Configuration Used by YNO
- 42.6 Timeout Configuration for GUI Forwarder Connection
- 42.7 Zero-Configuration Setting for YNO
- 42.8 Displaying Operational Status of YNO Agent
- 42.9 LAS (Log Analysis Service)
 - 42.9.1 SYSLOG Transmission Queue Length Configuration
 - 42.9.2 Timeout Configuration for Waiting for LAS Server Response
 - 42.9.3 Retry Count Configuration for LAS Client Requests
 - 42.9.4 Keepalive Configuration for Connection to LAS Server
 - 42.9.5 Displaying LAS Operational Status
- 42.10 Keepalive Interval Configuration for XMPP Server Connection

Chapter 43: Diagnostics

- 43.1 Diagnosing Port Open/Close Status
- 43.2 Diagnosing Reachable Access Range to Ports
- 43.3 Maximum Number of Pass-Through Packets Detectable in Port Status Diagnostics
- 43.4 Number of Stored Diagnostic Result Histories
- 43.5 Displaying Port Open/Close Diagnostic Results
- 43.6 Displaying Reachable Access Range Diagnostic Results
- 43.7 Clearing Diagnostic Results

Chapter 44: Statistics

- 44.1 Enabling/Disabling Statistics Function

Chapter 45: Flexible LAN/WAN Ports

- 45.1 Port Mapping Configuration for LAN Interfaces
- 45.2 Displaying Ports Mapped to LAN Interfaces
- 45.3 LAN Port Operation Type Configuration
- 45.4 MAC Address Aging Function Configuration
- 45.5 LAN Port Operation Settings

Chapter 46: LBO

- 46.1 Enabling/Disabling LBO
- 46.2 Primary Destination List Retrieval Source Configuration
- 46.3 Secondary Destination List Retrieval Source Configuration
- 46.4 Manual Execution of Destination List Retrieval
- 46.5 Displaying LBO Operational Status
- 46.6 Displaying Traffic Volume with Modified Routes
- 46.7 Clearing Traffic Volume with Modified Routes

Chapter 47: Operations

- 47.1 Selecting Peer Information Number
- 47.2 Selecting Tunnel Interface Number
- 47.3 Configuration Operations
 - 47.3.1 Switching to Administrator Mode
 - 47.3.2 Exit
 - 47.3.3 Saving Configuration
 - 47.3.4 Duplicating Configuration Files
 - 47.3.5 Copying Firmware Files to Internal Storage (Built-in Flash ROM, etc.)
 - 47.3.6 Deleting Configuration Files
 - 47.3.7 Deleting Executable Firmware Files
 - 47.3.8 Setting Default Configuration Files
 - 47.3.9 Setting Default Firmware Files
 - 47.3.10 Serial Port Baud Rate Configuration
 - 47.3.11 Initializing Configuration
 - 47.3.12 Restrictions on Remote Configuration
- 47.4 Clearing Dynamic Information
 - 47.4.1 Clearing Account Information
 - 47.4.2 Clearing PP Account Information
 - 47.4.3 Clearing Tunnel Account Information
 - 47.4.4 Clearing Data Connect Account Information
 - 47.4.5 Clearing ARP Table
 - 47.4.6 Clearing Dynamic IP Route Information
 - 47.4.7 Clearing Peak Values of Connections Managed by Dynamic Filters
 - 47.4.8 Clearing Bridge Learning Information
 - 47.4.9 Clearing Logs
 - 47.4.10 Clearing DNS Cache
 - 47.4.11 Clearing Interface Counter Information
 - 47.4.12 Clearing NAT Address Table
 - 47.4.13 Clearing NAT Address Table per Interface
 - 47.4.14 Clearing Session Statistics Managed by IP Masquerade
 - 47.4.15 Clearing Peak Session Values Managed by IP Masquerade
 - 47.4.16 Clearing Information Learned by PPPoE Pass-Through
 - 47.4.17 Clearing Dynamic IPv6 Route Information
 - 47.4.18 Clearing Peak Values of Connections Managed by IPv6 Dynamic Filters
 - 47.4.19 Clearing Neighbor Cache
 - 47.4.20 Deleting Startup Information History
 - 47.4.21 Clearing SYSLOG Files Stored in External Memory and Deleting Backup Files
- 47.5 File and Directory Operations
 - 47.5.1 Creating Directories
 - 47.5.2 Deleting Files or Directories

47.5.3 Duplicating Files or Directories

47.5.4 Renaming Files or Directories

47.6 Other Operations

47.6.1 Enabling Peer Usage

47.6.2 Disabling Peer Usage

47.6.3 Reboot

47.6.4 Restarting Interfaces

47.6.5 Dial

47.6.6 Disconnect

47.6.7 ping

47.6.8 ping6

47.6.9 traceroute

47.6.10 traceroute6

47.6.11 nslookup

47.6.12 Deleting Connection Management Information for IPv4 Dynamic Filters

47.6.13 TELNET Client

47.6.14 Deleting Connection Management Information for IPv6 Dynamic Filters

47.6.15 Clearing MAC Address Table of Switching Hub

47.6.16 Sending Magic Packets

47.6.17 Executing Firmware Check and Revision Upgrade via HTTP

47.6.18 Clearing URL Filter Statistics

47.6.19 Executing Mail Notification

47.6.20 Rotating (Backing Up) SYSLOG Files Stored in External Memory

47.6.21 Executing License Authentication

47.6.22 Retry Interval and Count Configuration for License Authentication

47.6.23 Bulk Configuration Update

47.6.24 Starting Rollback Timer

47.6.25 Verifying Configuration

47.6.26 Executing Files as Macros

47.6.27 echo

Chapter 48: Displaying Configuration

48.1 Displaying Device Configuration

48.2 Displaying All Configuration Settings

48.3 Displaying Configuration for a Specified Access Point

48.4 Displaying Configuration for a Specified PP

48.5 Displaying Configuration for a Specified Switch

48.6 Displaying Configuration for a Specified Tunnel

48.7 Displaying Configuration Differences

48.8 Displaying Configuration File List

48.9 Displaying File Information List

48.10 Displaying IPv6 Addresses Assigned to Interfaces

48.11 Displaying SSH Server Public Keys

48.12 Displaying Filter Settings for a Specified Interface

48.13 Displaying IPv6 Filter Settings for a Specified Interface

48.14 Displaying Firmware File List

48.15 Displaying Environment Variables

48.16 Displaying Aliases

48.17 Displaying Macros

Chapter 49: Displaying Status

49.1 Displaying ARP Table

49.2 Displaying Interface Status

49.3 Displaying Peer Status

49.4 Displaying IP Routing Table

49.5 Displaying RIP Routing Table

49.6 Displaying IPv6 Routing Table

- 49.7 Displaying IPv6 RIP Table
- 49.8 Displaying Neighbor Cache
- 49.9 Displaying Bridge Learning Information
- 49.10 Displaying IPsec SA Information
- 49.11 Displaying Certificate Information
- 49.12 Displaying CRL File Information
- 49.13 Displaying VRRP Information
- 49.14 Displaying Address Maps of Dynamic NAT Descriptors
- 49.15 Displaying Active NAT Descriptor Application Lists
- 49.16 Displaying NAT Address Maps for LAN Interfaces
- 49.17 Displaying Number of Ports Used by IP Masquerade
- 49.18 Displaying Number of Sessions Used by IP Masquerade
- 49.19 Displaying Session Statistics Managed by IP Masquerade
- 49.20 Displaying Peak Session Values Managed by IP Masquerade
- 49.21 Displaying L2TP Status
- 49.22 Displaying PPTP Status
- 49.23 Displaying IPIP Tunnel Status
- 49.24 Displaying OSPF Information
- 49.25 Displaying BGP Status
- 49.26 Displaying DHCP Server Status
- 49.27 Displaying DHCP Client Status
- 49.28 Displaying DHCPv6 Status
- 49.29 Displaying Backup Status
- 49.30 Displaying Connections Managed by Dynamic Filters
- 49.31 Displaying Peak Connection Values Managed by Dynamic Filters
- 49.32 Displaying IPv6 Dynamic Filter Connections
- 49.33 Displaying Peak Values of IPv6 Dynamic Filter Connections
- 49.34 Displaying Network Monitoring Status
- 49.35 Displaying Intrusion Detection History
- 49.36 Displaying Information Learned by PPPoE Pass-Through
- 49.37 Displaying Netvolante DNS Service Configuration
- 49.38 Displaying Switching Hub MAC Address Table
- 49.39 Displaying UPnP Status Information
- 49.40 Displaying Tunnel Interface Status
- 49.41 Displaying VLAN Interface Status
- 49.42 Displaying Trigger-Based Mail Notification Status
- 49.43 Displaying MLD Group Management Information
- 49.44 Displaying IPv6 Multicast Routing Information
- 49.45 Displaying Logged-In User Information
- 49.46 Displaying Login History of Logged-In Users
- 49.47 Displaying Packet Buffer Status
- 49.48 Displaying QoS Status
- 49.49 Displaying Cooperative Operation Status
- 49.50 Displaying OSPFv3 Information
- 49.51 Displaying URL Filter Information
- 49.52 Displaying Alive Notification Status
- 49.53 Displaying USB Host Function Status
- 49.54 Displaying Connection Information for Remote Setup Function
- 49.55 Displaying Technical Information
- 49.56 Displaying microSD Slot Status
- 49.57 Displaying External Memory Status
- 49.58 Displaying RTFS Status
- 49.59 Displaying Startup Information
- 49.60 Displaying Detailed Startup History
- 49.61 Displaying Startup History List
- 49.62 Displaying Agent List
- 49.63 Displaying LAN Cable Redundancy Status
- 49.64 Displaying DNS Cache

49.65 Displaying License Information

49.66 Displaying License Authentication Status

49.67 Displaying CPU Scheduling (Packet Forwarding) Status

49.68 Displaying STATUS LED Information

49.69 Displaying LAN Map Status

49.70 Displaying Copyright Information for Third-Party Software

49.71 Displaying SFP Module Information

49.72 Displaying Domestic Standard IPv6 Migration Provisioning Status

Chapter 50: Logging

50.1 Displaying Logs

50.2 Displaying Account Information

50.3 Displaying PP Account Information

50.4 Displaying Tunnel Account Information

50.5 Displaying Data Connect Account Information

50.6 Displaying Command History

INDEX

Preface

Introduction

- Unauthorized reproduction of part or all of this document is prohibited.
- The contents of this document are subject to change without prior notice.
- Yamaha Corporation assumes no responsibility for losses such as data loss resulting from the use of this product. Warranty coverage is limited to physical damage to the product.
- Every effort has been made to ensure accuracy; however, if you find omissions or unclear points, please contact us.
- Company names and product names appearing in this document are registered trademarks or trademarks of their respective owners.

CHAPTER 1

How to read the command reference

1.1 Revision of the corresponding program

This command reference supports Yamaha routers with firmware or images Rev.14.00.34, Rev.14.01.42, Rev.15.02.33, Rev.15.04.07, Rev.19.00.08, Rev.19.01.06, Rev.19.02.10, Rev.23.00.17, Rev.23.01.03, and Rev.23.02.02.

For information on the latest firmware or images released after the printing of this command reference, as well as manuals and differences, please refer to the information available on the WWW server at the following URL:

<https://www.rtpro.yamaha.co.jp>

1.2 How to read the command reference

This command reference describes commands to enter from the router console.

Each command is described by a combination of the following items.

[Format]	Describes the command input format. You can use either uppercase or lowercase letters when entering keys.
	The name part of the command is shown in bold (Bold face).
	The parameter part is shown in italic.
	Keywords are shown in standard characters.
	Parameters enclosed in parentheses ([]) are optional.
[Setting value]	Describes the types of command setting values and their meanings.
Description	Describes the command.
Notes	Here are some things to be aware of when using the command.
[Configuration Example]	Specific examples of commands are shown below.
Extended license support	Features that are extended when an extended license is imported.
Applicable models	Describes model names to which the command can be applied.

1.3About interface names

In the command input format, interface names are used to specify each interface of the router. Interface names are shown with interface types and interface numbers in between, without spaces.

Physical interface types include "lan", "bri", and "pri", and the interface numbers are assigned to each type in the order they were detected at startup.

Regarding the lan interface, divided LANs are connected by periods (.) when the LAN division function is applied. Tag VLANs are connected by slashes (/).

When a module has multiple interfaces, such as a BRI extension module, the interface number is in the form of a period (.) connecting the number assigned to the module and the number in the module.

Interface types	Interface names	Models equipped with them
LAN on the main module	LAN1	All models
Tags: VLAN	LAN1/1, LAN1/2, ...	Models except vRX series
LAN division function LAN	LAN1.1, LAN1.2, ...	Models except vRX series and RTX1300

Interface types	Interface names	Models equipped with them
LAN division function LAN	vlan1,vlan2, ...	Models except vRX series and RTX1300
BRI on the main module	bri1	RTX1210
The first BRI module	bri2.1, bri2, ...	BRI expansion modules were installed. RTX5000 and RTX3500
The second BRI module	bri2.1, bri2.2, ...	BRI expansion modules were installed. RTX5000 and RTX3500
The first PRI module.	pri1	PRI expansion modules are installed. RTX5000 and RTX3500

Virtual interfaces can be specified as LOOPBACK, NULL, or BRIDGE.

Interface types	Interface names	Equipped models
LOOPBACK	loopback1, loopback2, ...loopback9	All models
NULL	null	All models
BRIDGE	bridge1	All models except vRX Amazon EC2 version (*1)

*1 RTX5000 / RTX3500 Rev. 14.00.11 and earlier are excluded.

1.4 Input formats for commands starting with no

There are many commands in which the input format of the command starts with a form starting with no. If you use a form starting with no, the setting of the command will be deleted and returned to the initial value unless otherwise specified.

Also, it will not be displayed in the show config command. In other words, unless you use a form starting with no, the entered command will be displayed in the show config command, even if you set the initial value as it is.

Optional parameters may be listed for command input formats starting with no. These mean that specifying a parameter does not cause an error, and the value given as a parameter has no effect on the behavior of the no command.

1.5 About input characters and escape sequences of commands

The maximum number of characters that can be entered as one command is 4095 characters or less, including the command body, parameter parts, and spaces.

Also, when entering the following special characters in the parameter part of the command, enter them by the method shown in the table.

Special characters	Input
?	\?, '?', "?"
#	\#, '#', "#"
	\ , ' ', " "
>	\>, '>', ">"
\	\\
\	\', "'"
"	\", ""
Blank	Blanks behind \, ", "'"

1.6 Differences in destination information numbers by model

The range of numerical values that can be used for destination information numbers differs depending on the model.

Model name	Range of destination information numbers
vRX series, RTX5000, RTX3510, RTX3500	1-150
RTX1300, RTX1220, RTX1210	1-100
RTX840, RTX830	1-30

1.7 Setting values in the factory default state or the default state after deployment

In the case of RTX1300, RTX1220, RTX1210, RTX840, and RTX830, the initial values of the commands described in this manual are not applied to the purchased state or the state immediately after executing the cold start command, and the factory default settings are shown below.

```
iplan1address192.168.100.1/24 dhcp
service server
dhcpserverrfc2131compliantexceptremain-silent dhcp
scope 1 192.168.100.2-192.168.100.191/24
```

The following models also have the telnetd host lan command set.

Models	Revisions
RTX1300, RTX1220, RTX840	All revisions
RTX830	Rev.15.02.03 or later
RTX1210	Rev.14.01.26 or later

In vRX Amazon EC2 version, the following settings are applied in the initial state after deployment and in the state immediately after executing the cold start command.

```
iprouteDefaultgatewaydhcplan2 ip lan1 address
dhcp
iplan2addressdhcp telnetd
service off
dnsserverdhcplan2 sshd
service on
sshdhostkeygenerate*
```

In vRX Sakura cloud version, the following settings are applied in the initial state after deployment and in the state immediately after executing the cold start command.

```
telnetdserviceoff
```

CHAPTER 2

How to use commands

Two types of methods are supported: one is to send commands directly to a Yamaha router one by one to set and operate functions, and the other is to send and configure a file describing a set of necessary commands. If the LAN interface is not available, you can execute commands using the CONSOLE or SERIAL port or the virtual machine console to perform necessary operations such as recovery.

The means for setting interactively is called the console, and you can execute commands one by one to set and operate. A file describing a set of necessary commands is called a configuration file (Config), and it is possible to send and receive configuration files from an environment that can access the Yamaha router by TFTP.

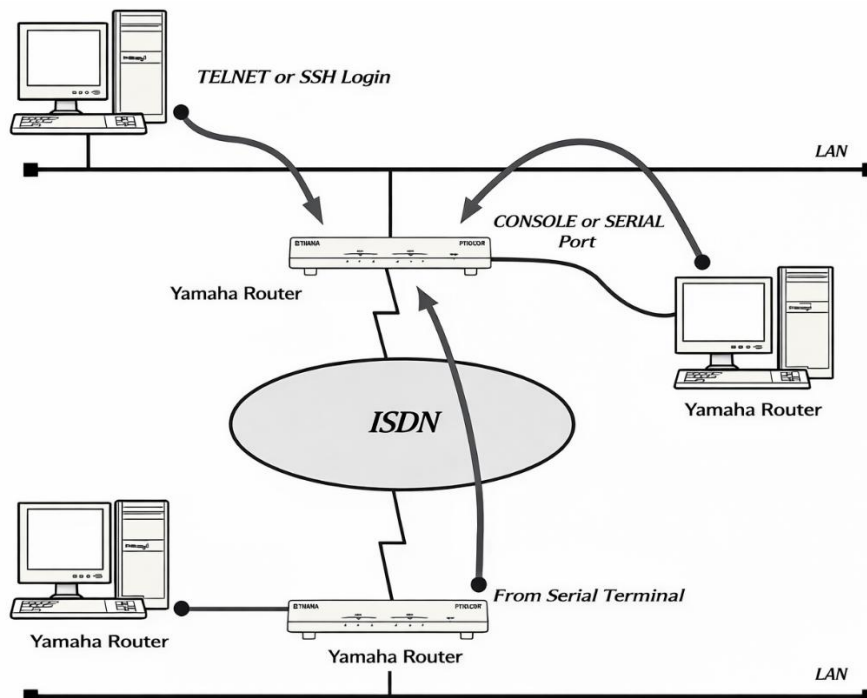
2.1 About consoles

To perform various settings, access the Yamaha router by one of the following methods.

How to access the Yamaha router	Compatible models
Access from a terminal connected to the CONSOLE or SERIAL port	All models except the vRX series
Log in with the virtual machine console	vRX vRX series except Amazon EC2 version
Log in with TELNET or SSH from a host on the LAN	All models
Log in from another Yamaha router via an ISDN line or leased line	RTX5000, RTX3500, RTX1210

One user can access each of the Yamaha routers. Also, only one user can be an administrative user at a time. For example, if a user accessing the serial terminal is setting as an administrative user, another user can access as a general user, but cannot become an administrative user and perform settings.

For models that support the TELNET multiple session function and the SSH server function, simultaneous access by TELNET or SSH is possible for up to eight users. Also, multiple users can become administrative users at the same time, and settings can be performed from different hosts at the same time. In addition, each user can check the access status of all users who are currently accessing the router, and if it is an administrative user, it is possible to force disconnection of other users.



2.1.1 Setting procedure by console

To set from the CONSOLE or SERIAL port, first connect the CONSOLE or SERIAL port of the Yamaha router to a personal computer with a cross type serial cable. Use a type suitable for a personal computer for connectors at both ends of the serial cable.

Use terminal software on a personal computer. If you are using Windows, prepare software with terminal functions. If you are using macOS, use the Terminal application that comes with the OS.

To configure settings in the virtual machine console, use the console functions provided by the management software of the hypervisor running vRX series.

If you want to configure settings in TELNET, use the TELNET application on a personal computer. If you are using macOS, use the "TELNET" software that comes with the OS. If you are using macOS, run the telnet command in the "Terminal" application that comes with the OS.

For specific contents of console commands, see Chapter 3 and later in this manual.

Please understand the operation of commands before using console commands. Please be sure to check whether it behaves as intended after setting.

The initial value of the character set displayed in the console is as follows. This can be selected according to the ability of terminal character display using console character command. Note that the input characters of commands are common in ASCII in either case.

- vRX series
 - UTF-8
- Other models
 - Shift JIS

The general flow of the setup procedure is as follows.

1. After logging in as a general user, access it as an administrative user with administrator command. If a management password is set at this time, you need to enter the management password.
2. If you want to change the destination information of an unconnected party, change the destination information after executing pp disable command. If the line is connected, manually disconnect the line first with the disconnect command.
3. Use various commands to change the destination information.
4. **Run the pp enable command.**
5. **Run the save command to save settings to non-volatile memory.**



Note : Pressing Ctrl + S will pause console output. If you press a key in this state, it looks unresponsive on the screen, but key input is processed. Press Ctrl + Q to resume console output.

For security reasons, the console is set to automatically log out in 300 seconds (default) when there is no key input for a certain period of time. This time can be changed using the login timer command.

When you become an administrative user and execute a configuration command, the contents are immediately reflected in the operation, but it will not be written to non-volatile memory unless you execute the save command.



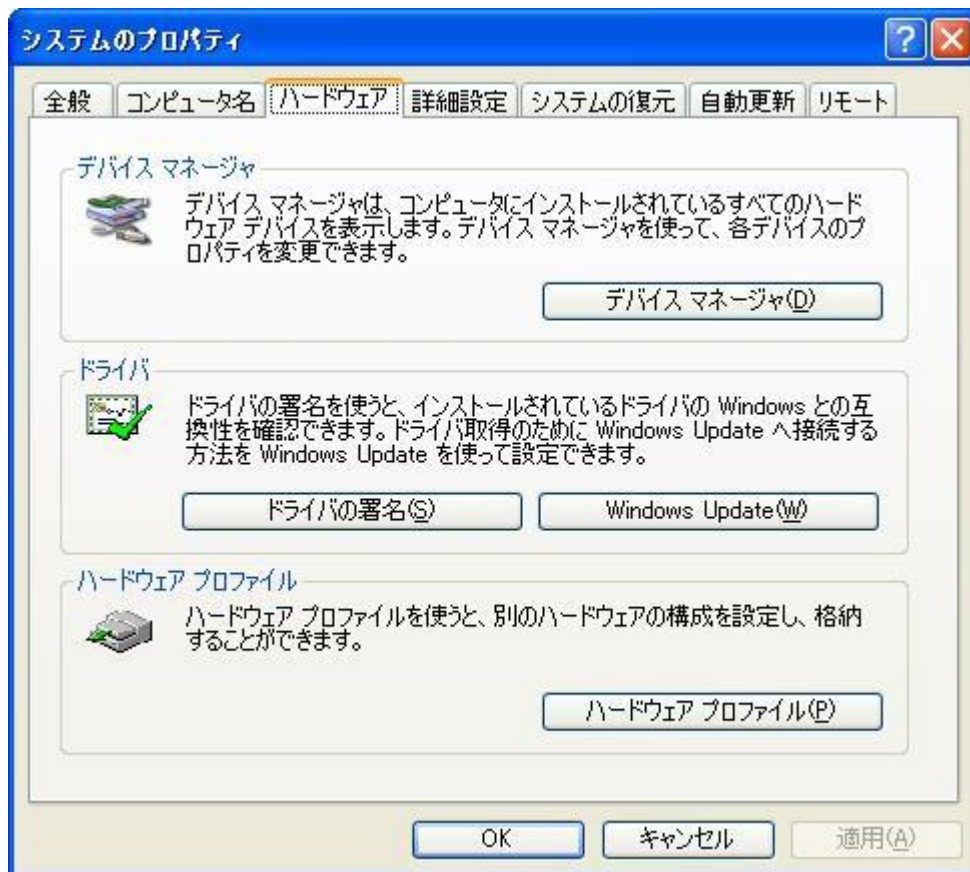
Note : There is no login password or administrative password set immediately after purchase or after cold start. For security reasons, we recommend setting a login password and an administrative password.

- Various settings can be made from the console by starting immediately after purchasing a Yamaha router, but the operation to actually deliver packets is not performed.
- Regarding security settings and additional settings such as detailed parameters, please follow the operation policy of each network.

2.1.2 Configuration from CONSOLE or SERIAL port.

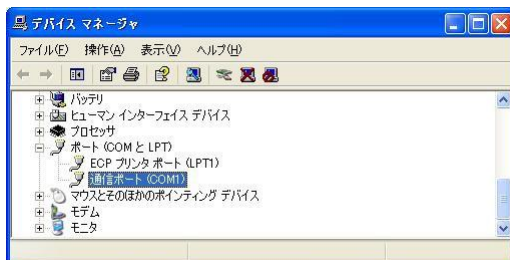
Here, we will explain using the case of using "HyperTerminal" of Windows XP as an example. The serial cable connection will be closed in advance.

1. From the Start menu, select "My Computer", and then select "Show system information" in the "System Tasks" column. When the "System Properties" window opens, press the Hardware tab.



2. Click Device Manager.

Double-click the "Port (COM and LPT)" icon to open it, and examine the expression "COMx" in the "Communication Ports". It will usually be "COM1". Remember this COM port number as you will need it in step 5.



3. Close the "Device Manager" window.

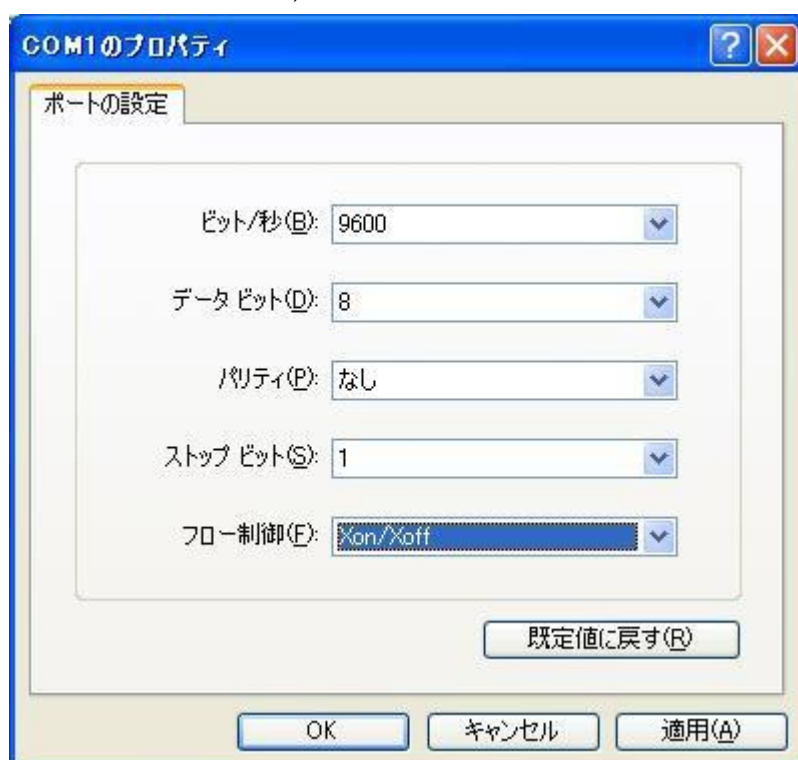
4. From the Start menu, select "All Programs" - "Accessories" - "Communications" - "HyperTerminal". When the "Connection Settings" window opens, enter the appropriate name in the name field and click OK.



5. From the "Connection Method" column, select the COM port you checked in step 2 and click OK.



6. When the "COMx Properties" window opens, set Bits per Second to 9600, Data Bits to 8, Parity to 1, Stop Bits to 1, Flow Control to Xon/Xoff, and click OK.



7. When "Password:" appears, enter the login password and press Enter.

* If you log in as a user with a name set in a model that supports TELNET multiple session functions, press Enter without entering anything. Next, "Username:" is displayed, and you are waiting for the user name to be entered. Now, enter the configured user name and press Enter, followed by the user password.

If nothing is displayed, press Enter once.

When "Password:" appears, you can enter console commands. The following example shows when you log in to RTX1200.


```

test - ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)
[Icons]

Password:
RTX1200 Rev.10.01.08 (build 4) (Fri Dec 12 10:15:18 2008)
Copyright (c) 1994-2008 Yamaha Corporation.
Copyright (c) 1991-1997 Regents of the University of California.
Copyright (c) 1995-2004 Jean-loup Gailly and Mark Adler.
Copyright (c) 1998-2000 Tokyo Institute of Technology.
Copyright (c) 2000 Japan Advanced Institute of Science and Technology, HOKURIK
U.
Copyright (c) 2002 RSA Security Inc. All rights reserved.
Copyright (c) 1997-2004 University of Cambridge. All rights reserved.
Copyright (C) 1997 - 2002, Makoto Matsumoto and Takuji Nishimura, All rights r
eserved.
Copyright (c) 1995 Tatu Ylonen , Espoo, Finland All rights reserved.
Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.
Copyright (c) 2006 Digital Arts Inc. All Rights Reserved.
00:a0:de:37:b5:04, 00:a0:de:37:b5:05, 00:a0:de:37:b5:06
Memory 128Mbytes, 3LAN, 1BRI
> -
接続 0:02:36 自動検出 9600 8-N-1 SCROLL CAPS NUM キー コーシ

```

**Note:**

- Type **help** and press **Enter** to see a list of key operations.
- Type **show command** and press **Enter** to display a list of commands.

8. Type **administrator** and press **Enter**.

9. When "Password:" appears, enter the administrative password.

When "#" appears, you can enter various console commands.

10. Type console commands to configure them.

11. When you are done, type **save** and press **Enter**.

The settings made in the console commands are saved in the machine's non-volatile memory.

12. To finish the configuration, type **quit** and press **Enter**.

13. To exit the console screen, type **quit** again and then press **Enter**.

2.1.3 Virtual Machine Console Configuration

The virtual machine console can be used with vRX series except for vRX Amazon EC2 edition. In this section, vRX VMware ESXi

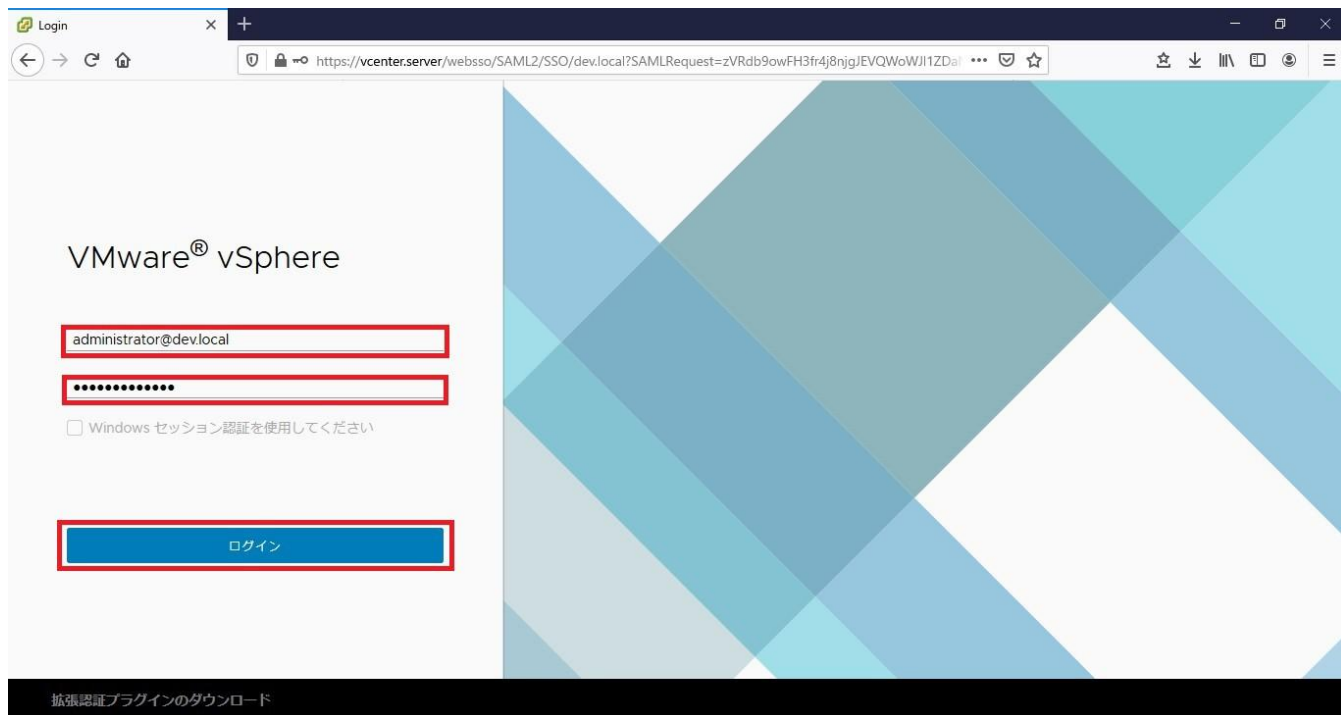
An example of the setting procedure in the version is explained.

- The vRX has been deployed to VMware ESXi and started up.
- The vCenter Server is installed and the deployed vRX is managed.

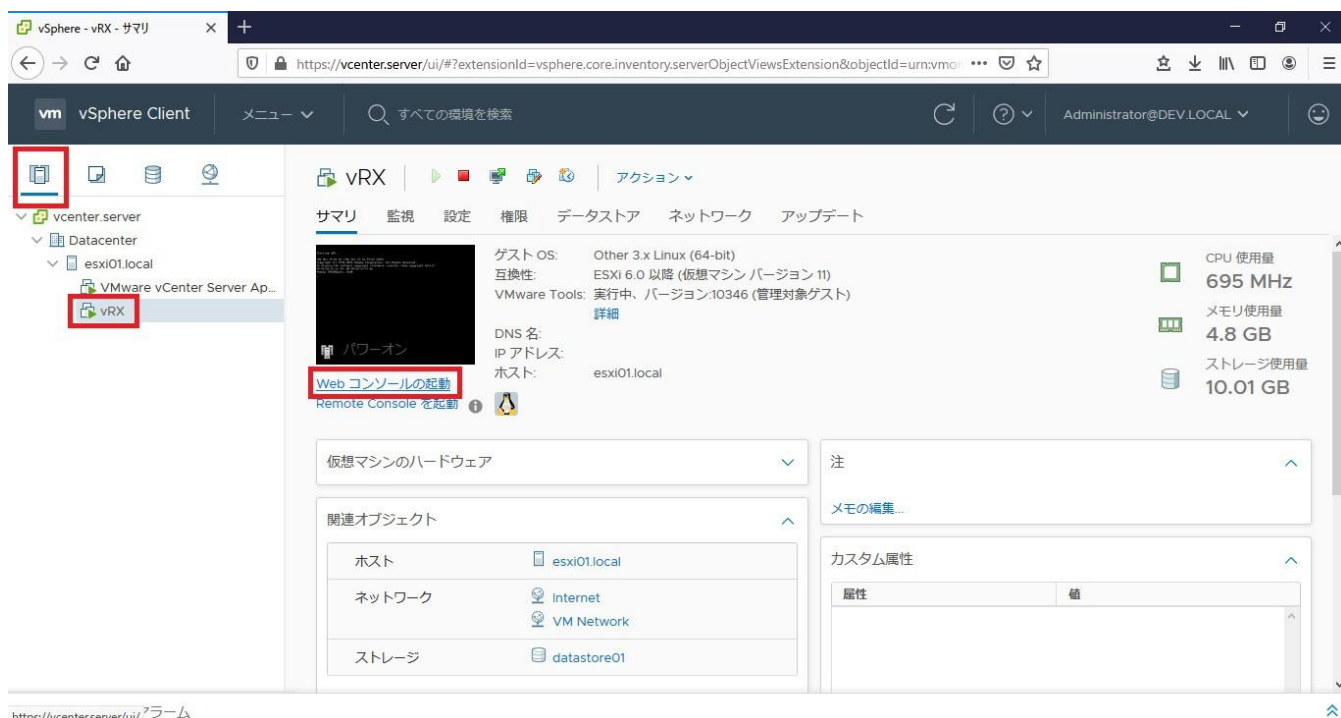
1. Open a web browser and launch VMware Vsphere.

2. When the login screen appears, enter your ID@domain and password, then press **Enter**. The image ID, domain, and password are examples.

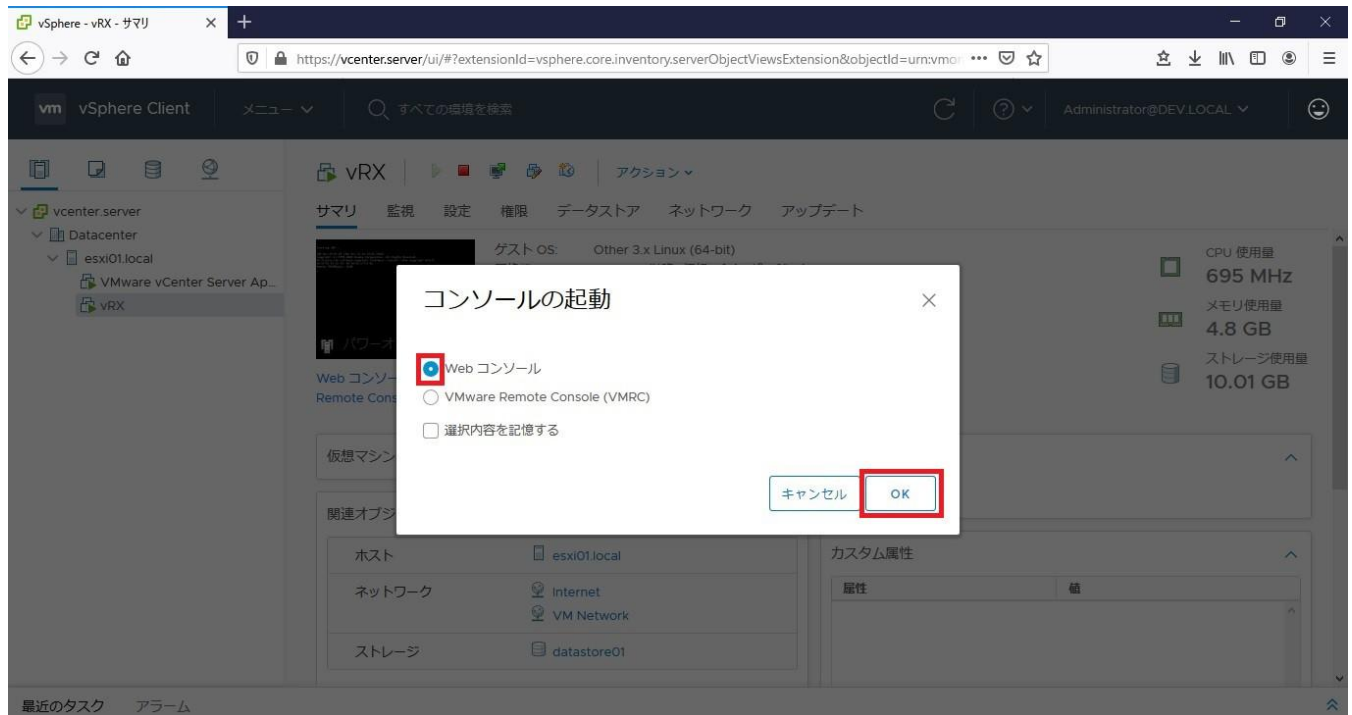
Actually, use the credentials of a user who has authority over the vCenter Server to which you are connected.



3. From the Hosts and Clusters screen, select the deployed vRX and select Launch Web Console.



4. When the "Start Console" popup appears, check "Web Console" and then press Enter.

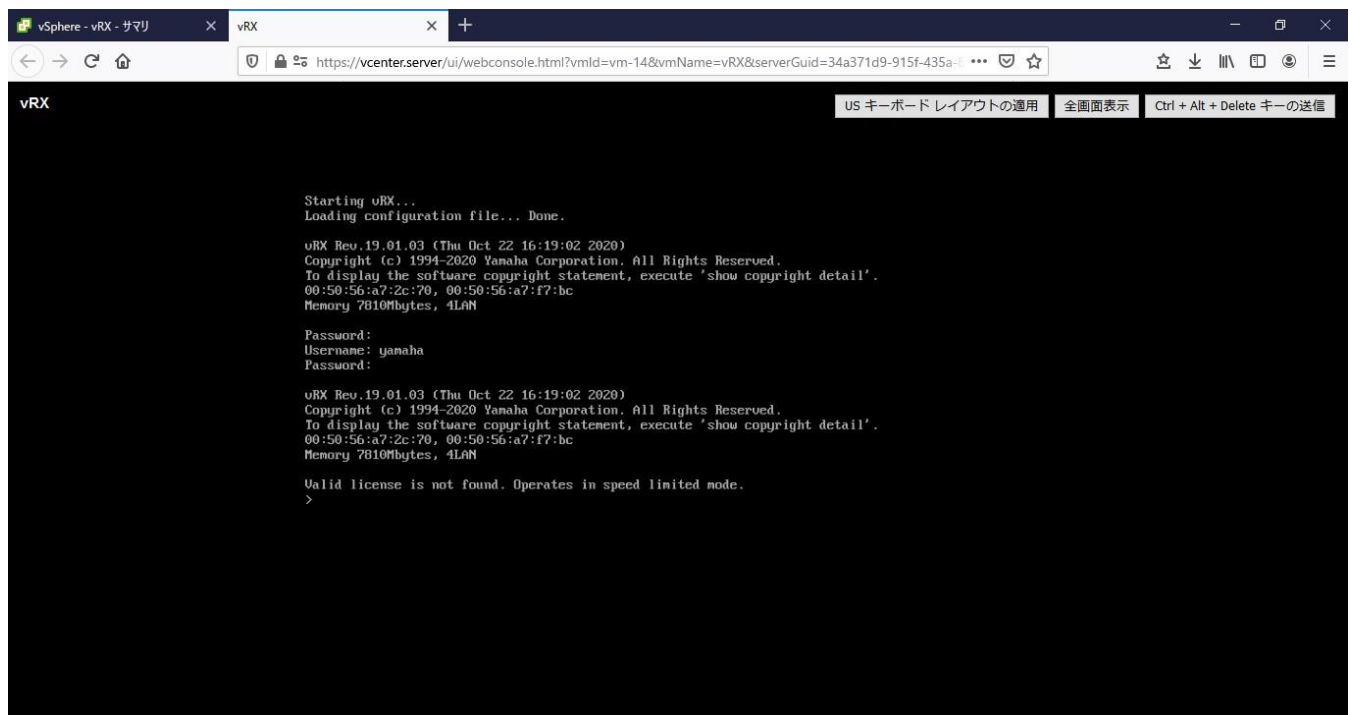
**Note:**

- To use VMware Remote Console, you need to install it separately.

5. When "Password:" appears, enter your login password and then press Enter.

Note: When logging in as a user with the set name, press Enter without entering anything. Next, "Username:" appears and you are waiting for the user name to be entered. Now, enter the configured user name and press Enter, followed by the user password.

If nothing appears, press Enter once. When "Password:" appears, you can enter console commands.

**Note:**

- When you type help and then press Enter, a list of key operations will appear.
- When you type show command and then press Enter, a list of commands will appear.

6. Type administrator and then press Enter.

7. When "Password:" appears, enter your administrative password.

When "#" appears, you can enter various console commands.

8. Type console commands to configure the settings.

9. When you are done, type save and then press Enter.

The settings made in the console commands are saved in the machine's non-volatile memory.

10. To finish the configuration, type quit and then press Enter.

11. To exit from the virtual machine console, type quit again and then press Enter.

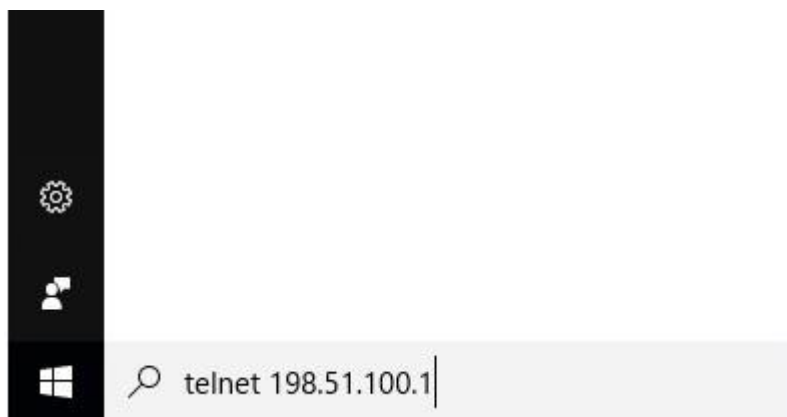
2.1.4 Settings via TELNET

Here, we will explain using a case of using TELNET on Windows as an example. This is an example where the IP address of a Yamaha router is 198.51.100.1.

On Windows, you need to enable TELNET by the following method in advance. In the "Windows functions" screen that appears when you select "Enable or disable Windows functions" in "Control Panel" - "Programs" - "Programs and Functions", check "Telnet client" and then click OK.

1. From the Start menu, type "telnet 198.51.100.1".

Actually, instead of "198.51.100.1", enter the IP address set on this machine.



2. When "Password:" is displayed, enter the login password and then press Enter.

* If you log in as a named user set on a model that supports TELNET multiple sessions, press Enter without entering anything. Next, "Username:" is displayed and you are waiting for the user name to be entered. Here, type the configured user name and press Enter, followed by the user password.

If nothing is displayed, press Enter once. When ">" is displayed, you can enter console commands.

```

Telnet 198.51.100.1
Password:
RTX1200 Rev. 10.01.78 (Wed Nov 13 16:29:42 2019)
Copyright (c) 1994-2019 Yamaha Corporation. All Rights Reserved.
Copyright (c) 1991-1997 Regents of the University of California.
Copyright (c) 1995-2004 Jean-loup Gailly and Mark Adler.
Copyright (c) 1998-2000 Tokyo Institute of Technology.
Copyright (c) 2000 Japan Advanced Institute of Science and Technology, HOKURIKU.
Copyright (c) 2002 RSA Security Inc. All rights reserved.
Copyright (c) 1997-2010 University of Cambridge. All rights reserved.
Copyright (C) 1997 - 2002, Makoto Matsumoto and Takuji Nishimura, All rights reserved.
Copyright (c) 1995 Tatu Ylonen , Espoo, Finland All rights reserved.
Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.
Copyright (c) 2006 Digital Arts Inc. All Rights Reserved.
Copyright (C) 1994-2012 Lua.org, PUC-Rio.
Copyright (c) 1988-1992 Carnegie Mellon University All Rights Reserved.
Copyright (C) 2004-2007 Diego Nehab. All rights reserved.
Copyright (c) 2005 JSON.org
00:a0:de:68:13:ce, 00:a0:de:68:13:cf, 00:a0:de:68:13:d0
Memory 128Mbytes, 3LAN, 1BRI

The login password is factory default setting. Please request an administrator to change
the password by the 'login password' command.
> administrator
Password:
The administrator password is factory default setting. Please change the password by the
'administrator password' command.
# quit
>

```

**Note:**

- When you type **help** and then press **Enter**, a list of key operations will appear.
- When you type **show command** and then press **Enter**, a list of commands will appear.

3. Type administrator and then press Enter.

4. When "Password:" is displayed, enter the administrative password.

When "#" is displayed, you can enter various console commands.

5. Type console commands to configure settings.

6. When you are done, type save and then press Enter.

The settings made in the console commands are saved in the machine's non-volatile memory.

7. To exit the settings, type quit and then press Enter.

8. To exit the console screen, type quit again and then press Enter.

2.1.5 Setting via SSH

Here, we will explain using Windows SSH as an example. The user name set on a Yamaha router is yamaha, this is an example where the IP address is 198.51.100.1.

1. From the Start menu, type `ssh yamaha@198.51.100.1`.

Actually, instead of "yamaha@198.51.100.1", enter the user name set on this machine @ IP address.



2. When 「Are you sure you want to continue connecting (yes/no)?」 displays input 「yes」 and press Enter Key
When "yamaha@198.51.100.1's password:" is displayed, type the login password and then press Enter.
If nothing is displayed, press Enter once. When the ">" is displayed, you can enter console commands.

```

OpenSSH SSH client
The authenticity of host '198.51.100.1 (198.51.100.1)' can't be established.
RSA key fingerprint is SHA256:eVyHM2yrjKxEFIPgn9Iplqq99nfZBxWwToTcjpokdBEY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '198.51.100.1' (RSA) to the list of known hosts.
yamaha@198.51.100.1's password:

vRX Rev.19.00.01 (Fri Sep 13 12:13:56 2019) ** Compact Mode **
Copyright (c) 1994-2019 Yamaha Corporation. All Rights Reserved.
To display the software copyright statement, execute 'show copyright detail'.
00:50:56:92:6b:a7, 00:50:56:92:01:f1
Memory 3787Mbytes, 4LAN
> administrator
Password:
The administrator password is factory default setting. Please change the password by
the 'administrator password' command.
#
# quit
>

```



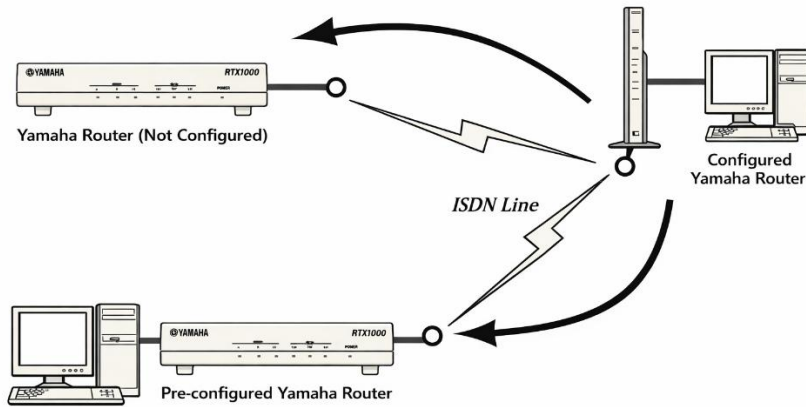
Note:

- If you type help and then press Enter, a list of key commands will be displayed.
- If you type show command and then press Enter, a list of commands will be displayed.

3. If you type administrator and then press Enter.
4. If "Password:" is displayed, enter the management password.
If "#" is displayed, you can enter various console commands.
5. Enter console commands to configure settings.
6. When you are done, type save and then press Enter.
The settings made by the console commands are saved in the unit's nonvolatile memory.
7. To exit the console screen, type quit and then press Enter.
8. To exit the console screen, type quit again and then press Enter.

2.1.6 Remote setup

If you already use a Yamaha router, you can configure a remote router via an ISDN line or leased line. This is called remote setup. Since it connects directly to the other router via an ISDN line or leased line, it can be set up even if you do not have a contract with a provider and cannot connect to the Internet.



Since it can be configured to deny remote setup, setting it to deny prevents intrusion from unspecified parties. Remote setup is done from the console. Refer to "Settings from CONSOLE or SERIAL ports" or "Settings with TELNET" in the previous section for how to use the console. The remote setup command is remote setup. When you have logged in to the other party's Yamaha router, you can configure the router you want to set with console commands.



Note:

- Remote setup from a router other than a Yamaha router is not possible.
- Remote setup via a WAN port such as FTTH, CATV, ADSL, etc. is not possible.

2.2 About SSH Servers

If your model supports the SSH server function, you can log in via SSH from a host on a LAN and configure it. At this time, the SSH client used by the host side is included and can be run as standard in macOS "Terminal" applications and UNIX environments, but it is not included as standard in Windows 10 version 1803 or earlier. If your environment does not include an SSH client, prepare free software that has the SSH client function.

2.2.1 Notes on using the SSH server function

Note that the following features are not supported by the SSH server function.

- SSH Protocol Version 1
- User authentication other than password authentication and public key authentication (host-based authentication, challenge-response authentication, GSSAPI authentication)

*Public key authentication is not supported by the following models and revisions.

- RTX5000 / RTX3500 Rev.14.00.31 or later
- RTX1210 Rev.14.01.34 以前
- RTX830 Rev.15.02.13 or earlier
- Port forwarding (X11/TCP forwarding)
- Gateway Ports
- Allow blank passwords

2.2.2 SSH Server Settings

In vRX Amazon EC2 version, you can use the SSH server function in the initial state after deployment. In user authentication, public key authentication is performed using a key pair specified at deployment.

On other models, the SSH server function cannot be used in the factory default state. The following is the setting procedure until you can use the SSH server function.

1. **Register a named user with the login user command. Since it is mandatory to enter a user name at login, you must register a named user beforehand.**
2. Next, generate the host key of the SSH server with the `sshd host key generate` command. This command generates a public key and a private key pair for DSA or RSA. However, depending on the model, it may take several tens of seconds to process this command.
3. Finally, enable the SSH server function with the `sshd service on` command.

```

Telnet 198.51.100.1
> administrator
Password:
The administrator password is factory default setting. Please change the password by the 'administrator password' command.
# login user RTuser himitsu
Password Strength : Weak
# sshd host key generate
Update to new host key ? (Y/N)Y
Generating public/private dsa key pair ...
|*****
Generating public/private rsa key pair ...
|*****
# sshd service on
# save
Saving ... CONFIG Done .
# quit
>

```

2.3 About TFTP

Items set in Yamaha router can be read as a configuration file from the host on the LAN by TFTP. Also, you can load the configuration file on the host into this machine and configure it.

TFTP is standard on Windows and macOS "Terminal" applications and in UNIX environments, and can be run. In an environment where TFTP is not installed, prepare free software that has the TFTP client function. At this time, Yamaha router operates as a TFTP server.

The configuration file describes the overall settings, and it is not possible to read only specific settings or write only difference points. The configuration file is a text file (Shift JIS, CRLF line feed) that can be edited directly in Windows Notepad.

TFTP can handle plaintext configuration files and encrypted configuration files. Supported encryption formats are AES128 and AES256. Files encrypted with a password cannot be used. RT-Tftp Client does not support encryption.

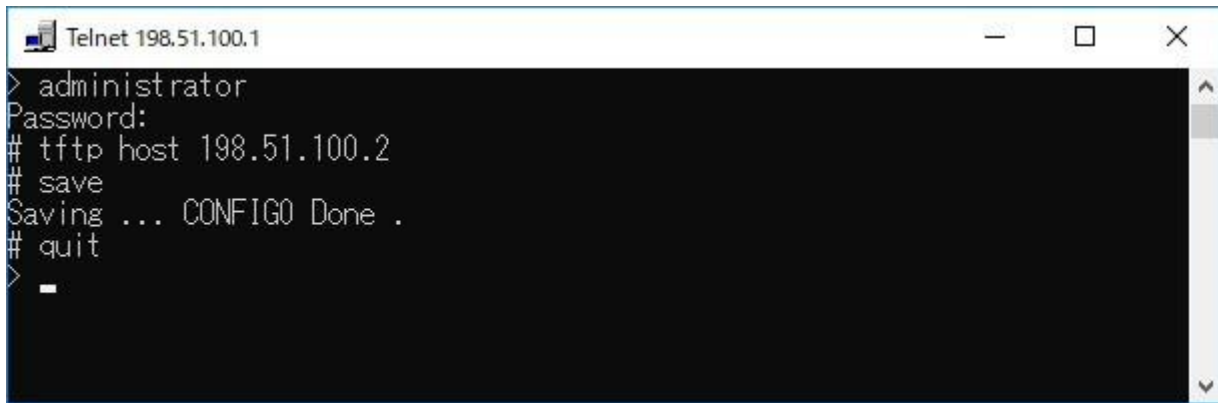


Note:

- The contents of the configuration file must be described correctly, such as specifying the command format and parameters. If there is an incorrect format or content, the content will not be reflected in the operation and will be ignored.
- Note that if you make a configuration change that requires a restart, such as the line type command, when reading a configuration file by TFTP, you need to use the restart command at the end of the configuration.

2.3.1 Setting procedure by TFTP

To exchange a configuration file by TFTP, it is necessary to make settings to allow access on the Yamaha router side in advance. First, use the `tftp host` command to set a host that can access this machine. Note that the factory default setting is such that it cannot be accessed from any host.



```

Telnet 198.51.100.1
> administrator
Password:
# tftp host 198.51.100.2
# save
Saving ... CONFIG0 Done .
# quit
>

```

Next, run the TFTP command from the host on the LAN. The command format used depends on the OS of the host. Please pay attention to the following points when you execute it.

- IP address of this machine
- The transfer mode should be "ASCII", "ascii" or "character".
If you want to handle an encrypted configuration file, use "binary" or "binary".
- If the management password is set for this machine, you need to specify the management password after the file name.
- If you want to read or write a running configuration file, specify the configuration file name as "config".

2.3.2 Reading a configuration file

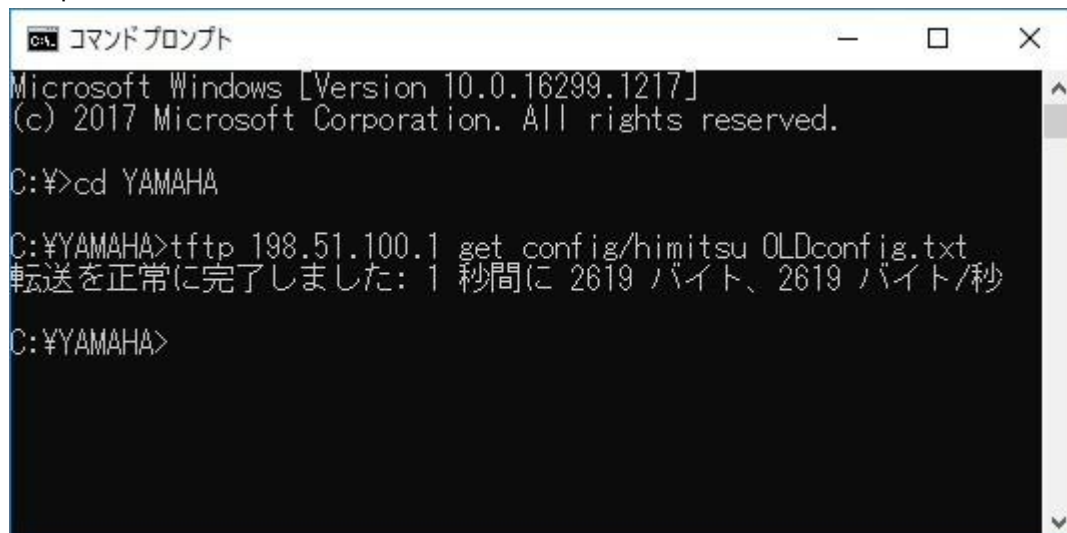
Here is an example of reading a configuration file from Windows. Note that this is not a Yamaha router console operation. In this example, the IP address of the Yamaha router is 198.51.100.1, the management password is "himitsu", and the name of a file that can be newly created on Windows is "OLDconfig.txt".

1. From the Start menu, select Windows System Tools - Command Prompt.
2. Navigate to the directory where you want to save a configuration file.
3. Input **tftp 198.51.100.1 get config/himitsu OLDconfig.txt** and Press Enter Key

If you want to read a configuration file encrypted, specify the "-encryption" option after the file name. If you want to specify an encryption format, specify "-aes128" or "-aes256" after "-encryption". If you omit the encryption format, AES256 is used as the encryption format. If you want to read a configuration file encrypted with the encryption format AES128, specify

tftp -i 198.51.100.1 get config-encryption-aes128/himitsu OLDconfig.txt

and press Enter.



```

コマンドプロンプト
Microsoft Windows [Version 10.0.16299.1217]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\>cd YAMAHA

C:\YAMAHA>tftp 198.51.100.1 get config/himitsu OLDconfig.txt
転送を正常に完了しました: 1 秒間に 2619 バイト、2619 バイト/秒

C:\YAMAHA>

```

2.3.3 Writing a configuration file

Here is an example of reading a configuration file from Windows. Note that this is not a Yamaha router console operation. In this example, the IP address of the Yamaha router is 198.51.100.1, the management password is "himitsu", and the name of the file on Windows to be written is "NEWconfig.txt".

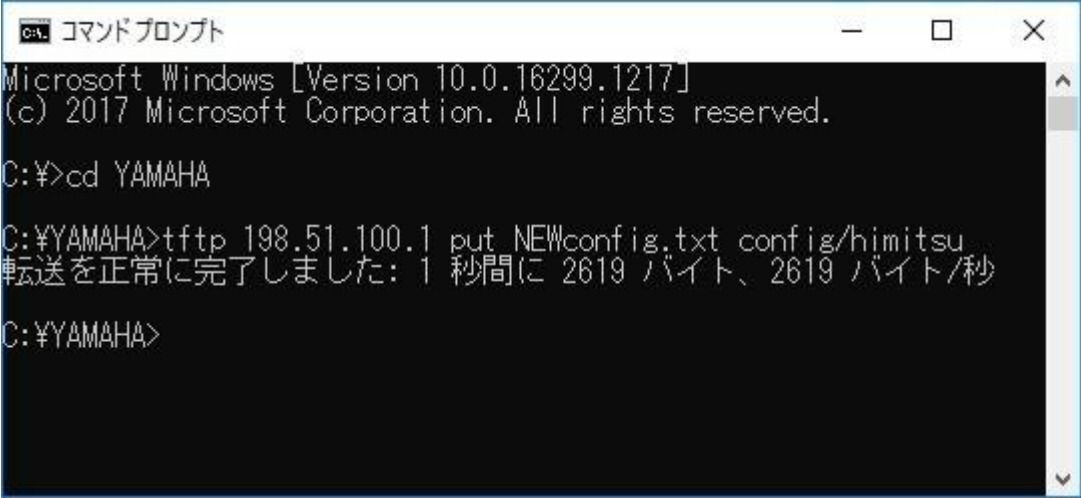
1. From the Start menu, select Windows System Tools - Command Prompt.
2. Navigate to the directory where you want to save a configuration file.

3. Type `tftp 198.51.100.1 put NEWconfig.txt config/himitsu` and press Enter.

If you want to write an encrypted configuration file "NEWconfig.rtf" to a configuration file, just like writing a normal configuration file,

`tftp -i 198.51.100.1 put NEWconfig.rtf config/himitsu`

and press Enter.



2.4About keyboard operation when using the console

If you want to display information on the number of lines that do not fit on one screen, stop the display when the number of lines set by the console lines command is displayed, and "--- Continued ---" is displayed at the bottom of the screen.

To display the rest from this state, press the space key. Press Enter to display a new line. Repeat these operations to display it until the end, and you will be able to enter commands automatically.

If you want to finish displaying it at this stage without displaying it until the end, press q. After that, you will be able to enter commands.

If you do not want to stop displaying information on the number of lines that do not fit on one screen, run the console lines infinity command.

Keyboard operation	Description and remarks
SPACE	Advance one screen
ENTER	Advance one line
RETURN	
q	End
Ctrl-C	

Use the commands `less config`, `less config list`, `less config pp`, `less config tunnel`, `less config switch`, `less config ap`, `less file list`, and `less log` if you want to display the same content as in the `less` style of a UNIX command.

Keyboard operation	Description and remarks
{n}f	{n}go ahead
{n} Ctrl-F	
{n} SPACE	
{n}f	{n}go back
{n}Ctrl-B	

Keyboard operation	Description and remarks
{n}j	Advance to the {n} destination
{n} Ctrl-J	
{n}Ctrl-E	
{n}Ctrl-M	
{n} ENTER	
{n}RETURN	
{n}k	Move back to the {n} destination
{n} Ctrl-K	
{n}y	
{n} Ctrl-Y	
{n} Ctrl-P	
{n}d	Move back to the {n} half-screen
{n}Ctrl-M	
{n}u	Move back to the {n} half-screen
{n}Ctrl-U	
{n}g	Move to the {n} destination
	{n}]If omitted, start line
{n}g	Move to the {n} destination
	If omitted, tail tail
{n}r	Rewriting the current screen
{n} Ctrl-R	
{n} Ctrl-L	
q	End
Ctrl-C	

Description

- n: Numeric key input represents an integer value. If omitted, it is '1'.
- Ctrl-X: Indicates holding down the [Ctrl] key and pressing the [X] key.

2.5Commands that start with "show"

From the contents displayed by the command that starts with "show", only the contents that match the specified search pattern can be extracted and displayed. Alternatively, you can display the contents displayed by the command that starts with "show" on a page-by-page basis, and then go back or search for the contents that match the specified search pattern.

These features are available for all commands that start with "show".

2.5.1 Extract only the contents that match the search pattern from the contents displayed by the show command.

[Format]

show [...] | grep [-i] [-v] [-w] pattern

[Setting value and initial value]

- -i: Search without distinguishing between uppercase and lowercase letters in pattern
 - Initial value: -
- -v: Display only the lines that do not match the pattern
 - Initial value: -

- **-w:** Display only when the pattern matches a word
 - Initial value: -
- **pattern**
 - Setting value: Search pattern
 - Initial value: -

[Description]

Only the lines that match the search pattern, pattern, are extracted and displayed from the contents displayed by the show command.

When the **-i** option is specified, search without distinguishing between uppercase and lowercase letters in pattern. For example, when the **-i** option is present, the pattern 'abc' matches 'abc', 'ABC', 'aBc', 'ABc', etc. On the other hand, without the **-i** option, 'abc' matches only 'abc'.

When the **-v** option is present, lines that do not match the pattern are displayed.

When the **-w** option is present, only the words match the pattern. For example, when the **-w** option is present, the pattern 'IP' does not match 'IPv4' or 'IPv6', but matches 'IP' (with a trailing space) and '[IP]'. On the other hand, when the **-w** option is absent, all of the examples given above match.

Pattern is a restricted regular expression. Although general regular expressions can construct various search patterns using many special characters, only the following special characters are implemented.

Characters	Meaning	Examples	Examples of matching strings
...	Matches any one character	a.b	aab, aXb, a-b
?	Matches a pattern in which the preceding character repeats zero or once	b?c	ac, abc
*	Matches a pattern in which the preceding character repeats zero or more times	ab*c	ac, abc, abbc, abbbbbbbbc
+	Matches a pattern in which the preceding character repeats one or more times	ab+c	abc, abbc, abbbbbbbbc
	Matches any of the preceding or following characters	ab cd	abd, acd
[]	Matches any of the characters in []	a[bc]d	abd, acd
[^]	Matches anything other than the characters in []	a[^bc]d	aad, axd
^	Matches the beginning of a line	^abc	Lines ending in abc
\$	Matches the end of a line	abc\$	Lines ending in abc
()	Treating strings as groups	(ab cd)	ab, cd
\	Cancels the effect of following special characters	a[^bc]d	a.c

Also, **grep** can be specified repeatedly on a line. Furthermore, it can be used simultaneously with the **less** command. If '\', '?' or '|' are used as characters in a pattern, one more '\' must be placed before those characters.

"Searching ..." is displayed when the command is executed. is displayed, and the display can be canceled by entering **Ctrl+C** while searching for the target character string.

```
Examples ( )
#showcommand|grepmat
Searching ...
clearnatThe descriptor dynamic:Delete information.NATDelete information.
^C
#
```

[Configuration Example]

```
showconfig|grepip|greplan show
config | grep ip | less
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

2.5.2 Make the display contents of the show command easy to see.**[Format]**

show [...] |

less

[Explanation]

The display contents of the show command are displayed in one screen unit, and the command is accepted in the last line. When the display contents are less than one screen, all contents are displayed and finished.

The command is executed by inputting a numerical prefix and a command character. The numerical prefix can be optionally omitted. If the numerical prefix is omitted, it is regarded as 1. In the search command, a search character string can be entered after the command character.

There are the following types of commands.

Commands	Contents (where N is the numerical prefix)
q	Finish less.
Space	Go to N screen.
b	Go back to N screen.
ENTER	Go to N destination.
Go to k	Go back to N line.
G	Jump to N line.
G	Jump to N line. However, if the numerical prefix is omitted, it jumps to the last line.
/	Search patterns entered after the command character are searched backward. Search patterns are the same as those of the grep command.
?	Search patterns entered after the command character are searched backward. Search patterns are the same as those of the grep command.
N	Search patterns are the same as those of / or ? entered at the end, and search directions are the same.
N	Search patterns are the same as those of / or ? entered at the end, and search directions are the same.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

2.5.3 Redirection to external memory or storage**Format**

show [...] > name

show [...] >> name

Set value and initial value

- *name* : file name
- [Setting value]:

Setting value	Description
usb1:filename (filename must be within 99 single-byte characters)	Files in a USB memory (filename must be within 99 single-byte characters)
sd1:filename	Files in a microSD card
<i>prefix:path</i>	Files in an external storage (prefix specifies the prefix set by the mount command)

- [Initial value]: -

Description

The execution result of a show command can be saved in an external memory or storage. It does not correspond to encryption of saved files.

Only necessary lines can be saved as a file by using it in conjunction with a pipe ('|').

```
#showlog|GrepIke>usb1:log.txt
```

Also, the execution result of a command can be added to an existing file by using a redirect symbol '>>' for an existing file in the external memory or storage.

```
#showlog>usb1:log.txt #
#showlog>usb1:log.txt)log.txt...Add to end of file
```

Also, when the redirect symbol '>' is used and the existing file name is specified for an output destination file, a confirmation message whether the file can be overwritten is displayed.

```
#showlog>usb1:(Existing)log.txt
#The specified file already exists. Do you want to overwrite it??(Y/N)
```

However, if you specify a file in an external storage, or if you specify a command input page of a GUI, a custom GUI, or Lua

If executed from rt.command, the confirmation message is not displayed and it is forcibly overwritten.

[Notes]

The external memory cannot be used with the vRX series. The external storage can be used with the vRX series.

A pipe ('|') cannot be specified after a redirect. A redirect cannot be specified multiple times.

Commands starting from other than show and commands starting from less are not applicable.

This function cannot be executed in the following conditions for the external memory.

- Not connected
- Button pressed
- Not connected

If the external storage capacity is insufficient, a file equal to the size succeeded in writing is generated. If the external storage capacity is insufficient, a file equal to the size succeeded in writing is generated.

[Configuration Example]

Save the contents of the show log to a USB memory

```
#showlog>usb1:log.txt
```

Show techinfo on a microSD card

```
#showtechinfo>sd1:techinfo.txt
```

[Applicable model]

vRX VMware ESXi Edition, vRX Sakura Cloud Edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 3

Help

3.1 Display of simple explanation to console

[Format]

help

[Explanation]

Display a brief description of how to use console

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

3.2 Display of command list

[Format]

show command

[Explanation]

Names of commands and their simple explanations are listed.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 4

Device Setting

4.1 CONFIGURATION OF ADMINISTRATIVE PASSWORD

[FORMAT]

administrator password

[Explanation]

A management password for changing a setting of a router is set as an administrative user. There is no parameter, and the password is input again according to a prompt after command input.

Characters that can be used for the password are half-width alphanumeric characters and symbols (displayable in 7-bit ASCII Code). vRX series

1 to 32 characters for RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, and RTX830; other models
Then, a character string of 8 to 32 characters is input.

When an enter key is pressed without inputting anything to the password, the administrative password is deleted.

[APPLICATION MODEL]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

4.2 Encrypted storage of administrative password

[FORMING]

administrator password

encrypted [説明]

The password of the administrative user is set, encrypted and stored. There is no parameter, and the password is input again according to a prompt after command input.

Characters that can be used for the password are half-width alphanumeric characters and symbols (displayable in 7-bit ASCII Code). vRX series

1 to 32 characters for RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, and RTX830; other models
Then, a character string of 8 to 32 characters is input.

When an enter key is pressed without inputting anything to the password, the administrative password is deleted.

[Notes]

This command is used when the password is encrypted and stored, and the administrator password command is used when it is saved in plain text.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

4.3 Setting a general user name and login password

[FORMING]

login user user [password]

login user user encrypted password

no login user user [password]

[Setting value and initial value]

- *user*
 - [Setting value]: User name (up to 32 characters)
 - [Initial value]: -
- *password*
 - [Setting value]: Password
 - [Initial value]: -

[Description]

Setting a general user name and password. Up to 32 users can be registered.

Characters that can be used for the user name are half-width alphanumeric characters, hyphens (-), and underscores (_).

In the first format, the password is entered in plain text and encrypted and stored. When the password is omitted, the password is input again according to a prompt after command input. Characters that can be used for the password are half-width alphanumeric characters and symbols (displayable in 7-bit ASCII Code). Enter character strings of 1 to 32 characters for the vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, and RTX830, and 8 to 32 characters for other models.

In the second format, the encrypted password is entered in password.

When the setting is acquired by TFTP, it is always displayed in the form of the second format because the password is encrypted and stored.

[Notes]

Multiple identical user names cannot be registered.

When the setting is performed with a user name that has already been registered, the original setting is overwritten.

When syslog execute command is set to on, it is desirable to enter the password in a format that omits the password, set syslog execute command to off temporarily, or execute clear log to prevent the setting password from being recorded in the log.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.4 Setting whether to use RADIUS for password authentication at login

[Format]

login radius use use

no login radius use

[Setting value and initial value]

- Use
 - [Setting value]

Setting value	Explanation
on	To use
off	Not used

- [Initial value]: off

[Explanation]

Whether to use RADIUS for password authentication at login is set.

[Notes]

The following commands related to the RADIUS authentication server must be set correctly.

- radius auth
- radius auth server
- radius auth port
- radius secret

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.5 Whether to use RADIUS for password authentication when transitioning to an administrative user

[Format]

administrator radius auth use

no administrator radius auth [use]

[Setting value and initial value]

- Use

- [Setting value]: off

Setting value	Description
on	Using local authentication and RADIUS authentication together
only	Only RADIUS authentication is used
off	Not used

- [Initial value]: off

[Explanation]

Whether to use RADIUS for password authentication when transitioning to an administrative user by an administrator command is set.

When on, comparison with the administrative password set by the administrator password command is performed first, and if there is no match, inquiry to the RADIUS server is performed. When only, inquiry to the RADIUS server is performed only.

[Notes]

The following commands related to the RADIUS authentication server must be set correctly.

- radius auth
- radius auth server
- radius auth port
- radius secret

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.6Set user attributes

[Format]

user attribute [user] attribute=value [attribute=value...]

no user attribute [user...]

[Setting value and initial value]

- user
- [Setting value]: off

Setting value	Description
Registered user name	Registered user name
*radius	Any user who logs in with RADIUS authentication
*	All users

- [Initial value]: off
 - attribute=value : User attribute
 - [Setting value]: off
 - administrator : attribute indicating whether to use administrator mode
- vRX Amazon EC2 version, vRX VMware ESXi version, RTX5000, RTX3500, RTX1220, RTX1210, RTX830

Setting value	Description
on	It is possible to be promoted to an administrative user by the administrator command. Also, it is possible to connect to an administrator page of a GUI. It is possible to perform an SFTP connection using an administrator password.
off	It is not possible to be promoted to an administrative user by the administrator command. Also, it is not possible to connect to an administrator page of a GUI. It is not possible to perform an SFTP connection using the administrator password.

Other models

Setting value	Description
2	It is possible to be promoted to an administrative user without entering a password of the administrator command. Also, it is possible to connect to an administrator page of a GUI. It is possible to perform an SFTP connection using the administrator password.
1	It is possible to be promoted to an administrative user by the administrator command. Also, it is not possible to connect to an administrator page of a GUI. It is possible to perform an SFTP connection using the administrator password.
off	It is not possible to be promoted to an administrative user by the administrator command. Also, it is not possible to connect to an administrator page of a GUI. It is not possible to perform an SFTP connection using the administrator password.

- connection : attribute indicating how to access a router.

Setting value	Description
off	All connections are prohibited.
all	All connections are prohibited.
serial	Connection via a serial console is permitted.
vm-console	Connection via a virtual machine console is permitted.
telnet	Connection via a TELNET is permitted.
ssh	Connection via an SSH is permitted.
sftp	Connection via an SFTP is permitted.
remote	Connection via a remote setup is permitted. (Cannot be specified in the vRX series)
http	Connection via a GUI setting screen is permitted. (Cannot be specified in the vRX series, RTX5000, RTX3510, and (Cannot be specified in the RTX3500)

- gui-page : attribute indicating the type of GUI screen that allows a logged-in user to browse.

Setting value	Description
all	Browsing of all screens accessible by the logged-in user is permitted.
dashboard	Browsing of a dashboard screen is permitted.
lan-map	Browsing of a LAN map screen is permitted.
config	Browsing of a simple setting screen, a detailed setting screen, a management screen, a CONFIG screen and a TECHINFO screen is permitted.

- Can be specified in RTX840 and RTX830 after Rev. 14.01.11 for RTX1300, RTX1220, RTX1210
- host : attribute specifying an access host to a router

Setting value	Description
IP address	Connection via a specified interface is permitted.
Any	Connection via a specified interface is permitted.
Interface name	Connection via a specified interface is permitted.

- multi-session : Attribute indicating whether multiple connections are allowed.

Set value	Description
on	Multiple connections by TELNET, SSH, and HTTP with the same user name are allowed.

Set value	Description
off	Multiple connections by TELNET, SSH, and HTTP with the same user name are prohibited.

- login-timer : Specifying a login timer

Set value	Description
120..21474836	The number of seconds before automatically logging out when there is no key input.
clear	Do not set a login timer.

- [Initial value]:
 - administrator=on (vRX Amazon EC2 Version、 vRX VMware ESXi Version RTX5000、 RTX3500、 RTX1220、 RTX1210、 RTX830)
 - administrator=1 (models other than the above)
 - connection=all
 - gui-page=all
 - host=any
 - multi-session=on
 - login-timer=300

Description

User attributes are set.

If user is omitted, attributes of anonymous users are set.

*If *radius is specified for user, attributes of all users who log in with RADIUS authentication are set.*

If user is specified with an asterisk (), the setting is valid for all users. However, if a setting specifying a user name is made, the setting takes precedence.*

Even if an administrator attribute is changed to off by this command for a user who has already been promoted to an administrative user, the user can be demoted to a general user by the exit command or remain as an administrative user until logging out.

In the connection attribute, values other than off and all can be specified with commas (,).

Even if a connection is prohibited by this command for a user who has already been connected by the connection attribute or host attribute, the user can continue to maintain the connection until disconnection.

In the gui-page attribute, values other than all can be specified with commas (,). The setting contents set in this attribute are valid only when the user logs in as a logged-in user. When a user logs in as an administrative user, he/she has authority to browse all screens on the GUI regardless of the setting of this attribute. If the setting of this attribute is changed by this command for a user who has already been connected to the GUI, the new setting is reflected from the next access to the page on the GUI.

In the host attribute, hosts that can be connected by TELNET, SSH, SFTP, and HTTP can be specified. IP addresses that can be specified are one IP address or an IP address (range specification) with a hyphen (-) in between, and these can be specified with commas (,).

In the multi-session attribute, multiple connections by TELNET, SSH, and HTTP can be specified. Even if this attribute is changed to off, if the connection method is different such as serial and TELNET or remote setup and SSH, the user can continue to connect with the same user name.

Even if the multi-session attribute is changed to off by this command for a user who has already had multiple connections, the user can continue to maintain the connection until disconnection.

For an unknown user, connection by SSH and SFTP cannot be permitted. However, vRX for Amazon EC2 and vRX for VMware ESXi version allows connection only when public key authentication

is used. For an unknown user, connection by TELNET cannot be made multiple times.

When connecting by TELNET, SSH, SFTP, and HTTP, the timer value is treated as 300 seconds even if the login-timer attribute value is set to clear.

The setting value of the login-timer attribute of this command takes precedence over the setting value of the login timer command.

[Notes]

For each model except for vRX for Amazon EC2, vRX for VMware ESXi, RTX5000, RTX3500, RTX1220, RTX1210, and RTX830, the user parameter cannot be omitted because an unknown user cannot be registered. One or more users with administrator attribute of 2 must be set.

When connecting to the administrator page of the GUI, RTX1300 uses a user password and other models use an administrator password.

It should be noted that if this command prohibits all users from connecting or all users cannot be promoted to administrative users, it is impossible to change the router settings or check the status.

The 'vm-console' of the connection attribute can be specified for vRX Sakura cloud version.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

4.7 Forced disconnection of other users

[Format]

disconnect user user [/connection[no]]

disconnect user [user]/connection[no]

[Setting value and initial value]

- *user*
 - [Setting value]: User name
 - [Initial value]: -
- *Connection: Connection type*
 - [Setting value]:

Setting value	Description
telnet	Connection via SFTP
serial	Connection via Serial Console
vm-console	Connection via Virtual Machine Console
remote	Connection via Remote Setup (Cannot be specified in vRX series)
ssh	Connection via SSH
sftp	Connection via SFTP
http	Connection via GUI Setup (vRX series, RTX5000, RTX3510, and RTX3500 cannot be specified in

- [Initial value]: -
- *no*
 - [Setting value]: Connection number
 - [Initial value]: -

Description

Connections of other users are disconnected.

Parameters are specified from the connection status displayed by the show status user command. When disconnecting an anonymous user, specify the user in a form that omits the specified parameter in the second format.

When the parameter is omitted, all connections that match the specified parameter are disconnected.

[Notes]

You cannot disconnect your own session.

The 'vm-console' of the connection parameter can be specified in vRX Sakura Cloud Edition.

[Configuration Example]

Example 1) Disconnect all connections logged in with the user name "test".

```
#disconnect user Test
```

Example 2) Disconnect all users connected via TELNET.

#disconnect user /telnet

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.8 Setting security class

Format**security class level forget [telnet [ssh]]****no security class [level forget [telnet [ssh]]]****[Setting value and initial value]**

- *level*
- [Setting value]:

Setting value	Description
1	Login via serial, TELNET, SSH, and remote setup functions
2	Login via serial, TELNET, and SSH, but not via remote setup functions
3	Login via serial only

- [Initial value]: 1
- *forget*
- [Setting value]:

Setting value	Description
on	You can log in with "w,lXlma" (double, comma, el, x, el, m, a) instead of the password you set, and you can change the setting. However, only serial (vRX Amazon EC2 version, vRX VMware ESXi version, vRX 5000, RTX 3500, RTX 1220, RTX 1210, and (Can be specified with RTX 830)
off	You can't log in unless you enter your password

- [Initial value]:
 - off (RTX 3510, RTX 1300, RTX 840)
 - on (other than above)
- *telnet*

- [Set value]:

Set value	Description
on	Telnet command can be used as a TELNET client
off	Telnet command can not be used

- [Initial value]: off
- *ssh*

- [Set value]:

Set value	Description
on	ssh command can be used as an SSH client
off	ssh command cannot be used

- [Initial value]: off

Description

Set a security class.

However, Web GUI is not applicable to the setting by this command.

[Notebook]

Remote setup function refers to the following functions.

- **Ability to configure a remote router via an ISDN line or leased line using the remote setup command**
- **Ability to specify an NGN network phone number as host in the telnet command and configure a remote router via the NGN network**

By the remote setup accept command, login by the remote setup function can be finely restricted. If more users are connected than the changed value when the setting is changed, a connected user can maintain it, but new connections are not allowed until the number of connected users is less than the set value.

If the level parameter is set to 3 in vRX Amazon EC2 version, access to vRX disappears. To restore to an accessible state, this command must be reconfigured with CONFIG (user data) at startup.

In models where the SSH client function is not implemented, the ssh keyword cannot be used

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.9Time zone setting

Format

timezone timezone

no timezone [timezone]

Setting value and initial value

- *timezone*: Difference between the area and global standard time
- [Setting value]:

Setting value	Description
jst	(+09:00)
utc	(+09:00)
Any time: minutes	Time: minutes (-12:00.+11:59)

- jst

Description

Setting time zone

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.10Setting current date setting

[Format]

date date

[Setting value and initial value]

- *date*
- [Setting value]: yyyy-mm-dd or yyyy/mm/dd
- [Initial value]: -

[Explanation]

Set the current date.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.11Set the current time

[Format]

time time

[Setting value and initial value]

- *time*
 - [Setting value]: hh:mm:ss
 - [Initial value]: -

[Explanation]

Set the current time.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.12 Clock setting by remote host

[Format]

rdate host [syslog]

[Setting value and initial value]

- *host*
 - [Setting value]:

Setting value	Explanation
IP address	IP address of remote host (xxx.xxx.xxx.xxx (xxx is a decimal number))
Name	Host name

- [Initial value]: -
- syslog: Keyword indicating output result to SYSLOG
 - [Initial value]: -

[Explanation]

Clock of router is set to the time of host specified by parameter. When this command is executed, it connects to TCP port 37 of host.

[Notebook]

Yamaha router series and many UNIX computers can be designated as remote hosts.

If syslog keyword is specified, output result of command is output to SYSLOG at the INFO level.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.13 Clock setting by NTP

[Format]

ntpdate ntp_server [syslog]

[Setting value and initial value]

- *ntp_server*
 - [Setting value]:

Setting value	Explanation
IP address	IP address of NTP server (xxx.xxx.xxx.xxx (xxx is a decimal number))
IPv6 address	IPv6 address of NTP server (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (xxxx is a hexadecimal number))
Name	Name of NTP server

- [Initial value]: -

- **syslog**: Keyword indicating output result to SYSLOG
 - [Initial value]: -

[Explanation]

Clock of router is set using NTP. When this command is executed, it connects to the host's UDP port 123.

[Notes]

When connected to the Internet, more precise clock adjustment is possible than when using the `rdate` command. It is better to specify an NTP server as close as possible. Contact your provider for available NTP servers.

When the `syslog` keyword is specified, the output result of the command is output to SYSLOG at the INFO level.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.14 Setting the start IP address when sending an NTP packet

[Format]

ntp local address ip_address

no ntp local address

[Setting value and initial value]

- *ip_address*
 - [Setting value]: IP address
 - [Initial value]: -

[Explanation]

Setting the start IP address when sending an NTP packet

When the start IP address is not set, the time synchronization with the Stratum 0420 with respect to the normal transmission rule of UDP packet is allowed.

Using the address

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.15 Setting to allow time synchronization with Stratum 0's NTP server

[Format]

ntp backward-compatibility comp

no ntp backward-compatibility [comp]

[Setting value and initial value]

- *Comp*
 - [Setting value]:

Setting value	Explanation
accept-stratum-0	Setting the time synchronization with Stratum 0's NTP server

- [Initial value]: -

[Explanation]

Setting the time synchronization with Stratum 0's NTP server

[Notes]

It does not become Stratum 0 unless it is an NTP server synchronized with an external clock.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.16 Setting the prompt display of the console

[Format]

console prompt prompt
no console prompt [prompt]

[Setting value and initial value]

- *prompt*
 - Setting value: The first string of the prompt of the console (64 characters or less)
 - [Initial value]: -

[Explanation]

Setting the prompt display of the console Empty character string can also be set.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.17 Setting the language and code of the console

[Format]

console character code
no console character [code]

[Setting value and initial value]

- *code*
 - [Setting value]:

Setting value	Explanation
en.ascii (after Rev.14.01), ascii (other than above)	Displayed in English, character code is ASCII
ja.sjis (Rev.14.01 series or later), sjis (other than the above)	Displayed in Japanese, character code is shift JIS
ja.euc (Rev.14.01 series or later), euc (other than the above)	Displayed in Japanese, character code is EUC
ja.utf8 (Rev.14.01 系以降)	Displayed in Japanese, character code is UTF-8

- [Initial value]:
 - ja.sjis (Rev.14.01 series or later)
 - en.utf8 (vRX series)
 - sjis (other than the above)

[Explanation]

Set the language and code to be displayed on the console. This command can be executed by a general user.

In the virtual machine console of the vRX series, the display language is English regardless of the setting of this command.

[Notes]

The setting of this command is displayed by the show config command even if it is not saved by the save command. Character code UTF-8 is not available for RTX5000 and RTX3500.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.18 Setting the number of characters to be displayed on the console

[Format]

Console columns col
no console columns [col]

[Setting value and initial value]

- *Set the number of characters to be displayed on the*

- Setting value: The number of characters to be displayed on the console
- Setting value:
 - 80..200 (RTX5000、RTX3500、RTX1210 Rev.14.01.34 以前、RTX830 Rev.15.02.13 以前)
 - 80..4096 (models and revisions other than the above)
- Setting value: 80

[Explanation]

Set the number of characters to be displayed per line on the console. This command can be executed by a general user.

[Notes]

The setting of this command is displayed by the show config command even if it is not saved by the save command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.19 Set the number of lines to be displayed on the console

[Format]

console lines lines

no console lines [lines]

Setting value and initial value

- *lines*
- Setting value:

Setting value	Explanation
10..100	Number of lines to be displayed
infinity	Don't stop scrolling

- Initial value: 24

[Explanation]

Set the number of lines to be displayed on the console. This command can be executed by a general user.

[Notes]

The setting of this command is displayed by the show config command even if it is not saved by the save command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.20 Setting whether to display a system message on the console

[Format]

console info info

no console info [info]

Setting value and initial value

- *info*
- [Setting value]: off

Setting value	Description
on	Display
off	Do not display

- [Initial value]: off

[Explanation]

Set whether or not to display a system message on the console.

[Notes]

If there is a system message during keyboard input, the display screen is disturbed, but the character string being input can be displayed again by pressing [Ctrl] + r.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.21 Set IP address of host to receive SYSLOG

[Format]

syslog host host
no syslog host [host]

[Setting value and initial value]

- *host*
 - [Setting value]: IP address or host name of host to receive SYSLOG (can be set up to 4 places separated by spaces)
 - [Initial value]: -

[Explanation]

Set IP address or host name of host to receive SYSLOG.
Any IPv4/IPv6 address can be set as IP address.
If the syslog debug command is set to on, a large number of debug messages will be sent, so it is desirable to have enough disk space for the host configured with this command.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.22 Set format of SYSLOG packet

[Format]

syslog format type type
no syslog format type [type]

[Setting value and initial value]

- *type*
 - [Setting value]:

Setting value	Description
rfc3164	Sending SYSLOG packets in RFC3164 format
rfc5424	Sending SYSLOG packets in RFC5424 format
yamaha	Sending SYSLOG packets in conventional format (PRI+MSG)

- [Initial value]: yamaha

[Explanation]

Set the format of SYSLOG packets sent by this unit.
Timestamps are set automatically, and the host name is the one set by the syslog format hostname command.
RFC3164 format consists of the following elements:

Elements	Contents
PRI	Facility+Severities
TIMESTAMP	Timestamps in "Mmm dd hh:mm:ss" format

Elements	Contents
HOSTNAME	Hostname (1..63 characters)
MSG	SYSLOG messages (maximum 231 characters)

RFC5424 format consists of the following elements:

Elements	Contents
PRI	Facility+Severities
VERSION	Fixed with "1"
TIMESTAMP	Timestamp of the format "yyyy-mm-ddThh:mm:ss±offset"
Hostname	Hostname (1..63 characters)
APP-NAME	Fixed with "-"
PROCID	Fixed with "-"
MSGID	Fixed with "-"
STRUCTURED-DATA	Fixed with "-"
MSG	SYSLOG message (maximum 231 characters)

The yamaha form consists of the following elements:

Elements	Contents
PRI	Facility+Severities
MSG	SYSLOG message (maximum 231 characters)

[Notes]

RTX1300 can be used with Rev. 23.00.14 or later. RTX1220 can be used with Rev. 15.04.07 or later. RTX1210 can be used with Rev. 15.02.31 or later. RTX830 can be used with Rev. 15.02.31 or later.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.23 SYSLOG facility configuration

Format

syslog facility facility

no syslog facility [facility]

Setting value and initial value

- *facility*
 - Setting value:

Setting value	Explanation
0..23	facility 値
user	1
local0..local7	16..23

- [初期値] : user

Explanation

Setting facility of SYSLOG

[Notes]

Meaning of facility number is uniquely performed by each SYSLOG server.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.24Setting hostname of SYSLOG header

Format

syslog format hostname text name
no syslog format hostname [text [name]]

Setting value and initial value

- name
 - Setting value: Hostname (one-byte characters)
 - [Initial value]: "Model name - serial number"

Explanation

Setting hostname of SYSLOG header transmitted by this machine

When syslog format type command is set to rfc3164 or rfc5424, the value set by this command is used.

Only alphabets, numbers, and hyphens are allowed in the name parameter.

[Notes]

RTX1300 can be used in Rev. 23.00.14 or later. RTX1220 can be used in Rev. 15.04.07 or later. RTX830 can be used in Rev. 15.02.31 or later. RTX830 can be used in Rev. 15.02.31 or later.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.25Setting whether to output NOTICE type SYSLOG

[Format]

syslog notice notice
no syslog notice [notice]

[Setting value and initial value]

- Notice
 - [Setting value]:

Setting value	Description
on	Output
off	Do not output

- [Initial value]: off

[Explanation]

Whether to output packet information detected by various filter functions or the like by SYSLOG is set.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.26Setting SYSLOG output of type INFO

[Format]

syslog info info
no syslog info [info]

[Setting value and initial value]

- info
 - [Setting value]:

Setting value	Description
on	Output
off	Output, but not send to SYSLOG host

- [Initial value]: on

[Explanation]

Setting SYSLOG output related to router operation status.

[Notes]

Logs of type INFO are stored in the router regardless of whether the info parameter is on or off. Transmission to the host configured by the syslog host command is performed only when the info parameter is on.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.27 Setting whether to output SYSLOG of type DEBUG

[Format]

syslog debug debug

no syslog debug [debug]

[Setting value and initial value]

- *debug*
- [Setting value]:

Setting value	Description
on	Output
off	Not output

- [Initial value]: off

[Explanation]

Setting whether to output router debug information by SYSLOG.

[Notes]

If the debug parameter is set to on, a large number of debug messages will be sent, so secure enough disk space on the host side set by the syslog host command, and turn it off as soon as necessary data is obtained.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.28 Setting the starting IP address when sending a SYSLOG

[Format]

syslog local address address

no syslog local address [address]

[Setting value and initial value]

- *address*
- [Setting value]: Starting IP address
- [Initial value]: -

[Explanation]

Setting the starting IP address when sending a SYSLOG packet When the starting IP address is not set, the normal Using the IP address of the output interface according to the UDP packet transmission rule.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.29 Setting the starting port number of a SYSLOG packet

[Format]

syslog srcport port

no syslog srcport [port]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number (1..65535)
 - [Initial value]: 514

[Explanation]

Setting the starting port number of a SYSLOG packet sent by this unit

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.30 Setting whether to output an execution command to SYSLOG

[Format]

syslog execute command switch

no syslog execute command [switch]

[Setting value and initial value]

- *switch*
 - [Setting value]:

Setting value	Explanation
on	Log executed commands
off	Do not log executed commands

- [Initial value]: off

[Explanation]

Whether to output the executed command by SYSLOG or not is set.

[Notes]

If command execution is successful, the command input is output to a log.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.31 Setting whether to output interface packet dump to SYSLOG

[Format]

packetdump interface count

packetdump pp peer_num count

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *peer_num*
 - [Setting value]:
 - Counterpart information number
 - anonymous
 - [Initial value]: -

- *count*
 - [Setting value]:

Setting value	Description
1..21474836	Number of times
off	No dumping
infinity	No limit on the number of times

- [Initial value]: off

Description

Only when syslog debug on is set, packets of the specified interface are dumped.

[Notes]

The setting of this command is not displayed by the show config command.

The setting of this command is not saved by the save command. The setting of this command is cleared by power cycle or restart.

When the count parameter is set to infinity, a large number of packet dump messages are output, which increases the load on the equipment. Not all packets are dumped. Packets may be lost.

Packets processed by fast path are not output.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.32 TELNET server function ON/OFF setting

[Format]

telnetd service service

no telnetd service

[Setting value and initial value]

- *service*
 - [Setting value]:

Setting value	Description
on	TELNET server function enable
off	TELNET server function disable

- [Initial value]: on

Description

Use of the TELNET server function is selected.

[Notes]

TELNET server does not respond to any access requests if the TELNET server is disabled.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.33 TELNET server function listen port setting

[Format]

telnetd listen port

no telnetd listen

[Setting value and initial value]

- *port*
 - setting value: TELNET server function listen port number (1..65535)
 - [Initial value]: 23

Description

TELNET server function listen port setting

[Notes]

telnetd listens on TCP port 23, and can change the listening port by this command. However, when changing the listening port, it is necessary to use a TELNET client that can negotiate the TELNET option even if the port number is changed.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.34 TELNET server access host setting**[Format]**

telnetd host ip_range [ip_range...]

telnetd host

any telnetd

host none

telnetd host lan

no telnetd host

[Setting value and initial value]

- *ip_range* : IP address or mnemonic of the host to allow access to the TELNET server
- [Setting value]:

Setting value	Description
One IP address or an IP address (range) with a hyphen (-) in between, and any number of these	Allow access from a specified host
lanN	Allow access from a WAN interface
wan1	Allow access from a WAN interface (Cannot be specified for vRX series, RTX5000, and RTX3500)
bridge1	Allow access from a bridge interface
vlanN	Allow access from a VLAN interface (Cannot be specified for vRX series)
lanN/M	Allow access from a tag VLAN interface (Cannot be specified for vRX series)

- [Initial value]: -
- *any*
 - [Setting value]: Allow access from all hosts
 - *any*.
- *None*
 - [Setting value]: Allow access from all hosts
 - [Initial value]: -
- *lan*
 - [Setting value]: Allow access from all LAN side networks
 - [Initial value]: -

Description

Set the host to allow access to the TELNET server

[Notes]

It is applied from a new TELNET connection after setting.

Bridge interface cannot be specified for vRX Amazon EC2 version and RTX5000/RTX3500 Rev.14.00.11 or earlier
The lan keyword cannot be specified for RTX5000/RTX3500 Rev.14.00.25 or earlier and RTX1210 Rev.14.01.15 or earlier

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.35 Setting the number of users who can connect to the TELNET server at the same time

[Format]

telnetd session num
no telnetd session

[Setting value and initial value]

- *num*
 - [Setting value]: Number of simultaneous connections (1...8)
 - [Initial value]: 8

Description

Setting the number of users who can connect to the TELNET at the same time

[Notes]

If more users are connected than the changed value when the setting is changed, the connected user can maintain it, but new connections are not allowed until the number of connected users is less than the set value.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.36 Setting CPU utilization threshold

[Format]

system cpu threshold off
system cpu threshold cpu1 cpu2 [duration=duration]
no system cpu threshold [cpu1 [cpu2 [duration=duration]]]

[Setting value and initial value]

- *off*
 - [Setting value]: No warning
 - [Initial value]: -
- *cpu1*
 - [Setting value]: Upper limit of CPU utilization threshold for warning (0..100 %)
 - [Initial value]: -
- *cpu2*
 - [Set value] : Lower limit of CPU usage threshold to warn (0..100 %)
 - [Initial value] : -
- *duration*
 - [Set value] : Judgment time (1..300 seconds)
 - [Initial value] : 1

[初期設定]

system cpu threshold off

[Explanation]

CPU usage is monitored, and a warning is issued by SYSLOG or SNMP trap when the usage is equal to or greater than *cpu1* or equal to or less than *cpu2*.

It is necessary to set snmp trap cpu threshold on in order to send SNMP trap.

RTX5000 and RTX3500 can be used after Rev.14.00.29. RTX1210 can be used after Rev.14.01.34. RTX830 is It can be used after Rev.15.02.10.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.37 Setting memory usage threshold

[Format]

system memory threshold off

system memory threshold memory1 memory2 [duration=duration]

no system memory threshold [memory1 [memory2 [duration=duration]]]

[Set value and initial value]

- **off**
 - [Set value] : Warning is not issued
 - [Initial value] : -
- **memory1**
 - [Set value] : Upper limit of memory usage threshold to warn (0..100 %)
 - [Initial value] : -
- **memory2**
 - [Set value] : Lower limit of memory usage threshold to warn (0..100 %)
 - [Initial value] : -
- **duration**
 - [Set value] : Judgment time (1..300 seconds)
 - [Initial value] : 1

[初期設定]

system memory threshold off

[Explanation]

It monitors memory usage and issues a warning by SYSLOG or SNMP trap when the usage is equal to or greater than memory1 or equal to or less than memory2.

It is necessary to set snmp trap memory threshold on in order to send SNMP trap.

RTX5000 and RTX3500 can be used after Rev.14.00.29. RTX1210 can be used after Rev.14.01.34. RTX830 is available after Rev.15.02.10

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.38 Fastpass function setting

[Format]

ip routing process process

no ip routing process

[Set value and initial value]

- **process**
 - [Set value] :

Set value	Explanation
fast	Fastpass function is used
normal	Process all packets by normal path without using fastpass function

- [Initial value] : fast

[Explanation]

Whether packet transfer is processed by fastpass function or normal path function is set.

[Note]

Fastpass does not limit usable functions, but it may be processed by normal path instead of fastpath depending on the type of packet to be handled.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.39 Setting transmission suppression time after link-up of LAN interface

[Format]

lan linkup send-wait-time interface time
no lan linkup send-wait-time interface [time]

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *time*
 - [Setting value]: Transmission suppression seconds (0..10)
 - [Initial value]: 0 (Do not suppress)

[Explanation]

The transmission suppression time after link-up is set to suppress packet transmission. Packets whose transmission is suppressed are stored in a queue and are transmitted after the elapse of the set number of seconds from link-up. The queue length of the save destination follows the setting of the queue interface length command.

[Notes]

When packets such as Gratuitous ARP and IPv6 neighbor solicitation are transmitted from a router immediately after link-up, but cannot be received on the opposite device side because the transmission is too early, the suppression time is set appropriately and transmission is delayed to enable reception on the opposite device side.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.40 Port mirroring function setting

[Format]

lan port-mirroring interface mirror direction port ... [direction port ...]
lan port-mirroring mirror direction port ... [direction port ...]
no lan port-mirroring interface
no lan port-mirroring

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *mirror*
 - [Setting value]: Port number to send mirroring packets
 - [Initial value]: -
- *direction : direction of the packet to be observed*
 - [Setting value]:

Setting value	Explanation
in	Direction to enter
out	Direction to enter

- [Initial value]: -
- *port*
 - [Setting value]: Port number to be observed
 - [Initial value]: -

[Explanation]

In the switching hub interface, a function that allows observation of communication on a specific port by other ports is set.

Only interfaces with switching hubs can be specified in the LAN interface name.

[Notebook]

Combined use with the LAN division function is not possible.

It is necessary that the transmission rate of packets sent from a sniffer port does not exceed the line speed. If mirroring packets cannot be sent from a sniffer port, communication between other ports may be affected.

The second format and the fourth format are valid only for models corresponding to flexible LAN/WAN ports. In models corresponding to flexible LAN/WAN ports, mirroring can be performed across multiple LAN interfaces. If it is desired to exclude communication packets other than mirroring packets, a port belonging to a LAN interface for which an IP address is not set may be set as a sniffer port.

When this command is executed on RTX5000 and RTX3500, only the target LAN interface is reset.

When this command is executed on RTX1220 and RTX1210, only the lan1 interface is reset.

When this command is executed on RTX840 and RTX830, all lan1 and lan2 interfaces are reset simultaneously.

When this command is executed on RTX3510 and RTX1300, all LAN interfaces are reset simultaneously. [設定例]

定例]

Example 1) Observe port 1 received packet on port 4.

```
#Lanport-mirroringLan14in1
```

Example 2) On port 4, observe packets sent/received on port 1 and sent/received on port 2.

```
#Lanport-mirroringLan14in1out12
```

Example 3) On RTX1300, observe packets sent/received on LAN2 (port 9) on LAN8 (port 8).

```
#Lanflexible-portLan1=1-7Lan2=9Lan3=10lan8=8 # lan  
port-mirroring 8 in 9 out 9
```

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.41 Setting the operation type of the LAN interface

[Format]

lan type interface_with_swhub speed [port] [speed [port]...] [option=value...]

Lan type interface_with_swhub option=value [option=value...]

lan type interface_without_swhub speed [option=value...]

Lan type interface_with_swhub option=value [option=value...]

lan type interface

mtu=mtu no lan type

interface [...]

[Setting value and initial value]

- *interface_with_swhub*
 - Setting value: Name of the LAN interface with a switching hub
 - Initial value: -
- *interface_without_swhub*
 - Setting value: Name of the LAN interface without a switching hub
 - Initial value: -
- *interface*
 - Setting value: Name of the LAN interface
 - Initial value: -
- *speed: LAN speed and operation mode*
 - Setting value:

Setting value	Description	Notes
Auto	Automatic speed discrimination	-

Setting value	Explanation	Notes
10g-fdx	100BASE-T full duplex	Can be specified only on RTX3510
5g-fdx	5GBASE-T full duplex	
2.5g-fdx	2.5GBASE-T full duplex	
1000-fdx	1000BASE-T full duplex	Cannot be specified on the vRX series
100-fdx	100BASE-TX full duplex	
100-hdx	100BASE-TX half-duplex	
10-fdx	10BASE-T half-duplex	
10-hdx	10BASE-T half-duplex	
Omitted	Auto if omitted	-

- [Initial value]: -
- *port*
 - [Setting value]: Port number of the switching hub
 - [Setting value]:
 - All ports if omitted
 - [Initial value]: -
- *option=value: Optional feature*
 - [Setting value]:
 - mtu
 - Maximum data length that can be transmitted and received at the interface
 - auto-crossover
 - Auto crossover function

Setting value	Description
on	Enable auto crossover function
off	Disable auto crossover function

- *macaddress-aging*
 - MAC address aging function

Setting value	Description
Seconds	Aging time
on	Enable MAC address aging function
off	Disable MAC address aging function

- Cannot be specified for vRX series and RTX3510
- *port-based-option*
 - LAN division function, port separation function

Setting value	Description
divide-network	Enable LAN division function
split-into-split_pattern	Enable port separation function (basic function)
X1, X2, X3, X4 (X1..X4 is a list of numbers 1..4 with "+" or "-")	Enable port separation function (extended function)
off	Disable LAN division function and port separation function

- Cannot be specified for vRX series
- *speed-downshift*
 - Speed downshift function

Setting value	Description
on	Enable speed downshift function
off	Disable speed downshift function

- Cannot be specified for vRX series
- energy-saving
- Power saving function

Setting value	Description
on	Enable power saving function
off	Disable power saving function

- Cannot be specified for vRX series, RTX5000, and RTX3500
- [Initial value]:
 - mtu=1500
 - auto-crossover=on
 - macaddress-aging=300 (models that can not specify the number of seconds)
 - macaddress-aging=300 (models that can specify the number of seconds)
 - port-based-option=off
 - speed-downshift=on
 - energy-saving=off

[Explanation]

Speed and operation mode types of a specified LAN interface, and optional functions are set. For a LAN interface with a switching hub, speed and operation mode can be specified for each port.

○ *mtu*

The maximum data length that can be transmitted and received by the interface is specified. The data length does not include the MAC header and FCS, and the tag length (4 bytes) at tag VLAN is also not included.

The range of data length that can be specified differs depending on the LAN interface. For a LAN interface that does not support jumbo frames, the range is 64 to 1500. For a LAN interface that does not support jumbo frames, the following is shown.

Model	Interface	Setting range
RTX3510	LAN1, LAN2, LAN3, LAN4	64 to 10218
RTX3500, RTX5000	LAN1, LAN2, LAN3, LAN4	64 to 9578
RTX1300	LAN1 to LAN8	64 to 10218

When the mtu of the interface is set and the setting of the ip mtu command or the ipv6 mtu command is left at the initial value, the mtu of the interface is used for MTU in IPv4 or IPv6. On the other hand, when the ip mtu command or the ipv6 mtu command is set and its setting value is smaller than the mtu of the interface, the setting value of the ip mtu command or the ipv6 mtu command is used as MTU. When all values including the mtu of the interface are not set, the initial value of 1500 is used.

○ Auto crossover function

A function to automatically determine whether a LAN cable is a straight cable or a cross cable and connect them. When this function is effective, there is no need to worry about the type of the cable.

In RTX1300, the switching-hub macaddress-aging command is used instead of this command.

○ MAC address aging function

It can be used only for a LAN interface with a switching hub.

In RTX3510 and RTX1300, the switching-hub macaddress-aging command is used instead of this command to set it.

A function to erase the entries in the MAC address table held by the switching hub in a fixed time. Turn off this function.

Then, once the MAC address stored by the switching hub is not automatically erased, even if the clear switching-hub macaddress command is executed, it is not erased. The entry is erased only when this function is reset to on.

In the following models, the number of seconds can be specified in the setting value. However, there may be an error between the setting value of the command and the time until it is actually erased.

In RTX1220 and RTX1210, it is erased from the set value to twice the time.

In RTX840 and RTX830, even if a value of less than 13 seconds is set, the time actually erased is not shorter than 13 seconds.

Model	Setting range
RTX5000, RTX3500, RTX840, RTX830	1-3825
RTX1220, RTX1210	10-630

When on is input in a model that can specify the number of seconds, it is converted to the initial value of 300.

The size of the MAC address table is as follows.

Model	Maximum number of entries
RTX5000, RTX3500, RTX1220, RTX1210, RTX840, RTX830	8192

○ LAN division function

It can be used only with a LAN interface having a switching hub.

There are basic function and extended function in the LAN division function.

In the basic function, each port of the switching hub operates as an individual LAN interface. Each interface can be assigned an individual IP address, and routing between them is also possible.

For example, RTX830 is a router which normally has two LAN interfaces, but if the LAN division function is used, five LAN interfaces can be used.

In the extended function, each port of the switching hub can be freely combined to form one LAN interface (VLAN interface).

Ports belonging to the same VLAN interface operate as switches.

The interface name used in the LAN division is different between the basic function and the extended function.

The interface name of the LAN interface in the basic function is expressed by connecting a period and a port number to the original LAN interface name.

For example, since RTX830 is a LAN interface in which lan1 has a four-port switching hub, the following LAN interfaces can be used.

Port number	Interface name
1	lan1.1
2	lan1.2
3	lan1.3
4	lan1.4

In the extended function, vlan1, vlan2, vlan3 ... (VLAN interface) are used as the interface name of the LAN interface. Unlike the basic function, the VLAN interface is not associated with a specific port. By using the vlan port mapping command, it is possible to freely change the division method by setting which VLAN interface each port of the switching hub belongs to.

The number of VLAN interfaces that can be used at the same time is different for each model, and is as follows.

Model	VLAN interface that can be configured
RTX5000, RTX3510, RTX3500	vlan1-vlan4 (LAN1), vlan5-vlan8 (LAN2)
RTX1220, RTX1210	vlan1-vlan8
RTX840, RTX830	vlan1-vlan4

If the LAN division function is enabled, the setting for the lan1 interface is either lan1.1 (for basic function) or vlan1 (for extended function) takes over.

The MAC address of the LAN interface used in the LAN division matches the MAC address of the original LAN interface. Therefore, in the above example, the MAC addresses of lan1.1-lan1.4 and vlan1-vlan4 are all the same as those of lan1.

○ Port separation function

It can be used only with a LAN interface that has a switching hub.

Normally, each port of a switching hub can communicate with other ports without restriction, but the port separation function can restrict communication between ports.

The port separation function has a basic function and an extended function, and in the basic function, it is possible to communicate via a router while restricting communication between ports, and in the extended function, it is also possible to restrict communication via a router from a designated port.

In the basic function, it is possible to separate ports into groups and limit communication with ports of other groups while allowing communication within the groups and with routers.

Unlike the LAN division function, the port separation function does not increase or decrease the LAN interface. All separated ports are recognized as the same LAN interface and have the same IP address.

The port separation pattern is described by putting "":" in the part to be separated by the order of port numbers.

Examples are shown below. If the number of ports of a switching hub is four

split_pattern	Port				Explanation
	1	2	3	4	
1:234	←	↔			Port one and others
1:2:34	←	←	↔		Port one, port two and others
1:2:3:4	↔	↔	↔	↔	Separate all ports

In RTX 1220 and RTX 1210, the description of the last group can be omitted. In the following table, abbreviations are shown in parentheses.

split_pattern	Port								Explanation
	1	3	3	4	5	6	7	8	
123:45678 (123)	4	4	→	4	5	6	7	→	Port 1 3 and others
1:23:567 8 (1:234)	2	4	6	→	7	8	9	→	Port 1 and ports 2-4 and others
12:34:56:7 8 (12:34:56)	7	→	8	9	9	10	9	10	Ports 1 and 2 and others Ports 3 and 4 and ports 5 and 6 and others
1:2:3:4:5:6 :7:8 (1:2:3:4:5: 6:7)	9	9	12	12	12	12	↔	←	Separate all ports

Even if a command is entered in the abbreviated form, it is displayed in the output of show config without abbreviating.

Communication between a primary address network and a secondary address network in the same LAN interface is via a router, so that communication with other groups is also possible.

In an extended function, by specifying a port for transferring received packets for each port, it is possible to restrict communication between ports, the router itself, and through the router. Concretely, the following settings are made.

```
lantypelanlport-based-option=X1,X2,X3,X4
```

Xn (n = 1..4) is a list of port numbers for forwarding packets received on port n, and "+" is added at the end to allow communication with the router itself and communication via the router, and "-" is added at the end to prohibit it. However, "+" can be omitted.

If "-" is specified, packets received on that port will not be routed, and devices connected to that port will not be able to communicate with the router.

For example, in the following settings, packets received on ports 1 to 3 are forwarded to port 4 and the router, and received on port 4.

Packets received on ports 1 to 3 are forwarded but not to the router. Ports 1 and 4, ports 2 and 4.

Ports 1 to 3 are separated into three groups, ports 3 and 4, and cannot communicate with each other's ports.

Ports 1 to 3 can communicate with the router, but port 4 cannot communicate and received packets are not routed.

```
lantypelanlport-based-option=4,4,4,123-
```

○Speed downshift function

When set to on, when a cable that cannot be used with 1000BASE-T is connected, it will attempt to link at a reduced speed.

In RTX1300, the lan port type command is used instead of this command.

○Power saving function

When set to on, power consumption of a non-communicating LAN port can be suppressed by EEE (Energy Efficient Ethernet). Connected devices must also support EEE.

In RTX1300, the lan port type command is used instead of this command.

[Notes]

After this command is executed, the LAN interface is reset automatically, and then the setting becomes valid. In RTX3510 and RTX1300, when this command is executed, all LAN interfaces are reset simultaneously. In RTX840 and RTX830, when this command is executed for lan1 or lan2, the lan1 and lan2 interfaces are reset simultaneously.

In other models, when this command is executed, only the specified LAN interface is reset.

Formats 1,2, and 4 are not available in VRX series and RTX1300. Format 3 is not available in RTX1300.

Format 5 is not available in VRX series.

In RTX1300, only the fifth format is available. The macaddress-aging option can be set with the switching-hub macaddress-aging command. Among port-based-options, divide-network (LAN partitioning function) can be substituted with the lan flexible-port command. Split-into (port separation function) cannot be used. Other options can be set with the lan port type command.

[設定例]

1. It is a LAN interface with a switching hub, ports 1 and 2 are connected by 100BASE-TX full duplex, and the other ports are connected by auto-negotiation.

```
#LantypeLan1100-fdx12
```

2. It is a LAN interface with a switching hub, port 1 is connected by 100BASE-TX full duplex, and the other ports are connected by auto-negotiation, and the LAN partitioning function is used.

```
#LantypeLan1100-fdx1port-based-option=divide-network
```

3. It is a LAN interface with a switching hub, and all ports are connected by auto-negotiation. Ports are separated by the port separation function.

- To separate 1,2 and 3,4 of a switching hub with four ports

```
#Lantypelanlport-based-option=split-into-12:34
```

- To separate 1,2,3,4,5,6 and others of a switching hub with eight ports

```
#Lantypelan1port-based-option=split-into-123:456:78
```

- To omit the separation pattern

```
#Lantypelan1port-based-option=split-into-123:456
```

4. Jumbo frames (9000 bytes) can be used in LAN1.

```
#Lantypelan1automtu=9000
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840 and RTX830

4.42 Setting up static link aggregation

[Format]

```
lan link-aggregation static link_id interface:port interface:port [interface:port ...]
```

```
no lan link-aggregation static link_id [interface:port ...]
```

[Setting value and initial value]

- *link_id*
 - Setting value: Link identifier (1..10)
 - [Initial value]: -
- *interface*
 - Setting value: Name of the LAN interface with the switching hub
 - [Initial value]: -
- *port*
 - Setting value: Port number to be aggregated
 - [Initial value]: -

[Explanation]

Physical links of a plurality of ports in a LAN interface with the switching hub are aggregated to form one logical link. A plurality of LAN cables connected to the ports to be aggregated are virtually regarded as one LAN cable. The ports to which packets are actually output among the ports to be aggregated are determined based on the destination MAC address and the source MAC address of the packets.

Ports belonging to the same LAN interface can be aggregated. A port cannot be subordinated to multiple logical links (multiple link identifiers).

The learned MAC addresses of each port to be aggregated are shared by all ports belonging to the same logical link and are always stored in the MAC address table of the largest port number. This is the same even when the physical link of the largest port number is down. Therefore, in the show status switching-hub macaddress command, a MAC address is always displayed in the column of the largest port number. Similarly, a port number displayed in the show arp command and an ARP log is always the largest port number when the port whose MAC address is learned is to be aggregated.

It can be used together with a LAN division function, a port separation function, and a port mirroring function. However, when it is used together with a LAN division function or a port separation function, only ports belonging to the same segment as the divided or separated switch ports can be aggregated.

In a model that supports flexible LAN/WAN ports, if the port to be aggregated specified in port is not mapped to the LAN interface specified in interface, an input error does not occur, but link aggregation does not function properly. Before setting this command, it is necessary to set the lan flexible-port command so that the ports to be aggregated are mapped to the same LAN interface.

In the RTX1300, up to eight ports can be aggregated in one logical link. Also, if output ports of packets are distributed on a logical link, the available bandwidth of the logical link as a whole is increased by the number of ports aggregated.

[Notes]

To avoid packet looping, it is necessary to set up link aggregation before connecting a LAN cable, including setting up link partner devices.

When this command is executed on the RTX1220 and RTX1300, only the target LAN interface is reset. When this command is executed on the RTX1220 and RTX1300, all LAN interfaces are reset. When this command is executed on the RTX1220 and RTX1210, only the target LAN interface is reset. The RTX1300 can be used after Rev.23.00.04.

[Configuration Example]

- Ports 1 and 2 of a LAN1 are aggregated.

```
#Lanlink-aggregationstatic1Lan1: 1Lan2: 1
```

- Ports 3 and 4 of a LAN1 are aggregated.

```
#Lanlink-aggregationstatic2Lan1: 3Lan1: 4
```

- Four ports of a LAN2 are aggregated.

```
#Lanlink-aggregationstatic3Lan2: 1Lan2: 2Lan2: 3Lan2: 4
```

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210

4.43 Setting the received packet buffer size of a LAN interface

[Format]

lan receive-buffer-size size

no lan receive-buffer-size [size]

[Setting value and initial value]

- size*
 - [Setting value]: Received packet buffer size (1..16384)
 - [Initial value]:
 - 8 (vRX Amazon EC2 version with QoS)
 - 64 (RTX3510 and RTX1300 with QoS)
 - 128 (RTX5000 and RTX3500 with QoS)
 - 1024 (other than the above)

[Description]

The received packet buffer size (receive queue length) of a LAN interface is set by the number of packets.

The size set by this command is applied to all CPU cores performing reception processing, and cannot be set for each LAN interface.

The initial value changes depending on whether or not QoS is set, but if the size is explicitly set using this command, the setting value is always applied regardless of whether or not QoS is set.

[Notes]

RTX5000 and RTX3500 can be used after Rev.14.00.18.

RTX1300 can be used after Rev.23.00.18.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300

4.44 Login timer setting

[Format]

login timer time

no login timer [time]

[Setting value and initial value]

- time*
 - [Setting value]:

Setting value	Description
120..21474836	The number of seconds it takes to automatically log out if there is no key input
clear	Do not set a login timer

- [Initial value]: 300

[Explanation]

Time until automatic logout when there is no key input is set.

[Notes]

When connecting by TELNET, SSH, SFTP, or HTTP, the timer value is treated as 300 seconds even if clear is set.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.45 Setting up hosts that can be accessed by TFTP

[Format]

tftp host ip_range [ip_range...]

tftp host any

tftp host

none tftp

host lan no

tftp host

[Setting value and initial value]

- *ip_range* : IP address or mnemonic of the host that allows access to the TFTP server
- [Setting value]:

Setting value	Description
One IP address or IP address (ranged) with a hyphen (-) in between, and any of these	Allow access from a specified host
lanN	Allow access from a WAN interface
Wan1	Allow access from a WAN interface (Not specified for vRX series, RTX5000, and RTX3500) Allow access from a WAN interface
bridge1	Allow access from a bridge interface
vlanN	Allow access from a VLAN interface (Not specified for vRX series)
lanN/M	Allow access from a tag VLAN interface (Not specified for vRX series)

- [Initial value]: -
- *any*
 - [Setting value]: Allow access from all hosts
 - [Initial value]: -
- *none*
 - [Setting value]: Prohibit access from all hosts
 - none.
- *lan*
 - [Setting value]: Allow access from within a network on the LAN side
 - [Initial value]: -

[Explanation]

Set up hosts that allow access to the TFTP server

[Notes]

For security reasons, set to none as soon as revisions of programs and reading/writing of configuration files are completed.

Specifying a range of IP addresses and multiple keywords, and specifying a LAN interface, a WAN interface, a VLAN interface, a tag VLAN interface, and a lan keyword are not possible with RTX5000, RTX3500, and RTX1210 Rev. 14.01.15 or earlier.

Bridge interfaces are not possible with vRX Amazon EC2 version, RTX5000, RTX3500, and RTX1210 Rev. 14.01.15 or earlier.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

4.46 Setting whether or not to relay Magic Packet to the LAN

[Format]

ip interface wol relay relay

no ip interface wol relay

[Setting value and initial value]

- *interface*
 - [Setting value]: Name of the LAN interface
 - [Initial value]: -
- *relay*
 - [Setting value]:

Setting value	Description
broadcast	Relaying Magic Packet as a broadcast packet
unicast	Relaying Magic Packets as Unicast Packets
off	Do not check if they are Magic Packets

- [Initial value]: off

[Explanation]

MagicPackets configured as IPv4 packets sent from a remote location and addressed to a directed broadcast are relayed to a specified LAN interface. The endpoint IP address of an IPv4 packet must be addressed to the directed broadcast of the specified LAN interface.

If broadcast or unicast is specified, the content of the received packet is checked and the packet is relayed only if a Magic Packet data sequence exists.

If broadcast is specified, the Magic Packet is transmitted to the LAN interface as a broadcast packet.

If unicast is specified, the MAC address is extracted from the Magic Packet data sequence and it is sent as a unicast packet with the endpoint MAC address.

If off is specified, whether it is a Magic Packet or not is not checked.

[Notes]

In either case, packets that are not relayed as Magic Packets are processed based on the setting of the ip filter directed-broadcast command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.47 Setting the description of the interface or system

[Format]

description id description

no description id [description]

description interface description

no description interface [description]**[Setting value and initial value]**

- *id*
 - Setting value: ID for describing the description of the entire system (1..21474836)
 - [Initial value]: -
- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - pp
 - tunnel
 - [Initial value]: -
- *description*
 - Setting value: Description string (up to 64 characters/ASCII, 32 characters/shift JIS)
 - [Initial value]: -

[Explanation]

Set the description of the entire system or the description of the interface.
The setting content is only for explanation and does not affect operation.

In the case of the description of the entire system, a description of multiple lines can be set by changing the value of ID. The description of the interface is limited to one line.

When 'pp' or 'tunnel' is specified as an interface, the description of the interface selected by pp select or tunnel select respectively.

The setting content is displayed by the show config command. The setting content for the interface is

It is also displayed by the show status command.

The description of the entire system is displayed in ID order before all settings in the show config command.

Not only ASCII characters but also Japanese characters (excluding half-width katakana) within the range that can be expressed by shift JIS can be used for description. However, it can be set and displayed correctly only when the console character command is set to sjis, and characters may become garbled in other settings.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.48 Setting whether to output syslog of TCP connection level

[Format]

```
tcp log switch [src_addr[/mask] [dst_addr[/mask] [tcpflag[src_port_list [dst_port_list]]]]]
no tcp log [...]
```

[Setting value and initial value]

- *switch*
 - [Setting value]:

Setting value	Description
on	Output syslog of TCP connection
off	Do not output syslog of TCP connection

- [Initial value]: off
- *src_addr*: Starting address
 - [Setting value]:
 - IP address
 - xxx.xxx.xxx.xxx

- Decimal number
- *(The corresponding bit of the netmask is the same as 0 for all 8 bits.)
- Two top items with a minus sign in between, a top item with a minus sign in front, and a top item with a minus sign in back, specifying ranges.
- Multiple values can be set as separators.
- FQDN
 - Arbitrary character string (Up to 255 single-byte characters. / : cannot be used. , cannot be used because it is used as a separator.)
 - FQDNs starting with * will judge strings after * as backward matching conditions. For example, *.example.co.jp
It matches www.example.co.jp, mail.example.co.jp, etc.
 - Multiple values can be set as separators.
- *(All IP addresses)
- [Initial value]: -
- *dst_addr*: End address
 - [Setting value]:
 - Same format as *src_addr*
 - If omitted, it is the same as a single *
 - [Initial value]: -
- *mask*: Bitmask of the IP address. Can be specified only if *src_addr* and *dst_addr* are network addresses.
 - [Setting value]:
 - Hexadecimal notation such as "0xffffffff"
 - Bitwise notation such as "/24"
 - Same as 0xffffffff if omitted
 - [Initial value]: -
- *tcpflag*: TCP packet type to filter
 - [Setting value]:
 - Decimal number representing protocol (6 only)
 - Mnemonic representing protocol

Mnemonic	Decimal number	Description
tcp	6	All TCP packets
tcpfin	-	Packets with the SYN flag
tcpfin	-	Packets with the SYN flag
tcpfin	-	Packets with the RST flag
established	-	Packets with the ACK flag

- *tcpflag=flag_value/flag_mask* or *tcpflag!=flag_value/flag_mask*
 - Flag_value and flag_mask are in hexadecimal notation
 - Reference flag value

0x0001	FIN
0x0002	SYN
0x0004	RST
0x0008	PSH
0x0010	ACK
0x0020	URG

- * (All TCP packets, same as when tcp is specified for mnemonic)
- Same as * if omitted.
- [Default]: -
- *src_port_list*: Source port number of TCP

- [Setting value]:
 - Port number, decimal number indicating type
 - Mnemonic indicating port number

Mnemonic	Port number
ftp	20,21
ftpdata	20
telnet	23
smtp	25
domain	53
gopher	70
finger	79
www	80
pop3	110
sunrpc	111
Ident	113
NTTP	123
NTTP	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540
submission	587

- Two top items with - in between, top items with - in front, top items with - in back, these specify ranges.
- Comma-separated rows of top items (up to 10)
- *(All ports, types)
- Same as * if omitted.
- [Default]: -
- *dest_port_list* : Destination port number of TCP
 - Setting value: Same format as src_port_list
 - [Default]: -

Description

Output TCP syslog. Syslog debug on must also be set. Supports IPv4 only. It is recommended only for temporary use such as troubleshooting, etc., because of the load on the system.

Notebook

Specifying FQDN to src_addr and dest_addr can be specified in RTX5000 Rev.14.00.26 or later, RTX3500 Rev.14.00.26 or later, RTX1210 Rev.14.01.26 or later, RTX830 Rev.15.02.03 or later, and Rev.15.04 series or later.

[Configuration Example]

```
tcplogon**tcpsyn*1723(PPTP)SYNis it coming?)
tcplogon**tcpflag!=0x0000/0x0007(FIN,RST,SYNstandsTCPpacket) tcp log on
(AllTCPTCPtcp log on * * * * **)
```

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.49 Setting whether to allow HTTP revision upgrade

Format

```
http revision-up permit permit
no http revision-up permit [permit]
```

[Setting value and initial value]

- *permit*
- [Setting value]:

Setting value	Description
on	Allow
off	Do not allow

- [Initial value]: on

Description

Setting whether to allow HTTP revision upgrade

[Notes]

The setting of this command affects direct HTTP revision upgrade by command, revision upgrade by easy setting page, and revision upgrade by DOWNLOAD button.
RTX5000 and RTX3500 can be used after Rev.14.00.26.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.50 Setting URL for HTTP revision upgrade

Format

```
http revision-up url url
no http revision-up url [url]
```

[Setting value and initial value]

- *url*
- Setting value: Set URL where firmware is placed
- [初期値]: `http://www.rtpro.yamaha.co.jp/firmware/revision-up/(機種名).bin`

Description

Setting URL where firmware is placed as HTTP revision upgrade

The input format is "http://server's IP address or hostname/pathname".

If the server's port number is other than 80, it must be specified in the URL in the form of "http://server's IP address or hostname: port number/pathname".

[Notes]

RTX5000 and RTX3500 can be used after Rev.14.00.26.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.51 Configuring Proxy Server for HTTP Revision Up

[Format]

```
http revision-up proxy proxy_server [port]
no http revision-up proxy [proxy_server [port]]
```

[Setting value and initial value]

- *proxy_server*

- [Setting value]: Proxy server used for HTTP revision up
- [Initial value]: -
- *port*
 - [Setting value]: Proxy server's port number
 - [Initial value]: -

[Explanation]

Specify the proxy server's hostname or IP address and port number.

[Notes]

RTX5000 and RTX3500 can be used after Rev.14.00.26.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.52 Timeout setting for HTTP revision up process

[Format]

http revision-up timeout time
no http revision-up timeout [time]

[Setting value and initial value]

- *time*
 - [Setting value]: Timeout time (seconds)
 - [Initial value]: 30

[Explanation]

Timeout time for HTTP revision up process is set.

[Notes]

RTX5000 and RTX3500 can be used after Rev.14.00.26.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.53 Setting whether to allow revision down

[Format]

http revision-down permit permit
no http revision-down permit [permit]

[Setting value and initial value]

- *permit*
 - [Setting value]:

Setting value	Explanation
on	Do not allow revision down to a revision older than the current revision
off	Do not allow revision down to a revision older than the current revision

- [Initial value]: off

[Explanation]

In the HTTP revision up function, set whether to allow revision down of firmware to a revision older than the current revision.

[Notes]

RTX5000 and RTX3500 can be used after Rev.14.00.26.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.54 Setting whether to allow revision up operation by DOWNLOAD button**[Format]****operation http revision-up permit permit****no operation http revision-up permit [permit]****[Setting value and initial value]**

- *permit*

- [Setting value]:

Setting value	Description
on	Do not allow the DOWNLOAD button to perform revision-up operation.
off	Do not allow the DOWNLOAD button to perform revision-up operation.

- [Initial value]: off

Description

Use the DOWNLOAD button to set whether or not to use the firmware revision-up function.

Notes

The revision-up function conforms to the HTTP revision-up function.

If this command is set to off while the STATUS lamp is displaying an error, the error display is canceled.

Applicable model

RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.55 Schedule for executing revision-up**Format****http revision-up schedule period time1 time2****http revision-up schedule startup****no http revision-up schedule [period time1 time2]****http revision-up schedule**

startup [Setting value and initial value]

- *period* : Set a schedule to attempt the revision-up of the firmware.

- [Setting value]:

Setting value	Description
daily	Daily
weekly day	Weekly day is a string representing the day of the week, either sun,mon,tue,wed,thu,fri,sat
monthly date	毎月 date is a number from 1 to 31 and represents the day within a month.

- [Initial value]: -
- *time1,time2* : Set a time zone to attempt the revision-up.
 - time1,time2 are set to 24-hour format and specified in HH:MM format.
 - [Initial value]: -

- Description

Set a schedule to attempt the revision-up of the firmware.

period specifies an interval to attempt the revision-up. Daily, weekly, and monthly specifications are specified as daily, weekly, and monthly, respectively. In the case of weekly and monthly, it is necessary to specify the day of the week and day, respectively.

In the case of monthly, if the specified day does not exist in that month, the revision-up is not attempted in that month. For example, if 'monthly 31' is specified, the revision-up is not attempted in February, April, June, September, and November when there is no 31 day.

time1 and time2 set a time zone to attempt the revision-up. The revision-up is attempted only once at a random time between the time specified in time1 and the time specified in time2. If the revision-up cannot be performed there, the revision-up is not performed until the next day/week/month.

If the time specified in time1 is later than the time specified in time2, time2 is interpreted as the next day's time.

The http revision-up schedule startup command attempts the revision-up only once at startup. If the revision-up cannot be performed there, the revision-up is not performed until the next startup.

When the HTTP revision-up is not permitted by the http revision-up permit command, the firmware is not rewritten.

When the revision-down is permitted by the http revision-down permit command, the firmware is rewritten even if a certain firmware is older than the current firmware in the WEB server.

If a certain firmware in the WEB server has the same revision as the current firmware, the firmware is not rewritten.

- Note

RTX5000 and RTX3500 can be used with Rev.14.00.26 or later.

Startup is RTX5000, RTX3500 is Rev.14.00.29 or later, RTX1210 Rev.14.01.34 or later, RTX830 Rev.15.02.10 or later, and

Can be used with Rev.15.04 or later firmware.

[設定例]

```
httprevision-upscheduledaily23:0002:00          #Every day23From time to next day2From
time to time
httprevision-upscheduleweeklySun12:0013:00      #Sunday lunch12From time to time13From
time to time
```

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.56 **Setting the SSH server function ON/OFF**

[Format]

sshd service service

no sshd service [service]

[Setting value and initial value]

- *service*
- [Setting value]:

Setting value	Description
on	Enabling the SSH server function
off	Stopping the SSH server function

- [Initial value]: off

Explanation

Select to use the SSH server function.

Notebook

If the SSH server function is stopped, the SSH server does not respond to any access requests.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.57 Setting the listen port of the SSH server function

[Format]

sshhd listen port
no sshhd listen [port]

[Setting value and initial value]

- *port*
 - [Setting value]: Listen port number for the SSH server function (1..65535)
 - [Initial value]: 22

[Explanation]

Select the listen port of the SSH server.

[Notes]

The SSH server listens on TCP port 22, and can change the listen port by this command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.58 Setting up hosts that can access the SSH server

[Format]

sshhd host ip_range [ip_range...]
sshhd host
any sshhd
host none
sshhd host
lan no sshhd
host

[Setting value and initial value]

- *ip_range*: IP address or mnemonic of the host that allows access to the SSH server
 - [Setting value]:

Setting value	Description
One IP address or IP address (range specification) with a hyphen in between, and optionally arranged	Allow access from specified hosts
lanN	Allow access from WAN interface
wan1	Allow access from WAN interface (Not specified for vRX series, RTX5000, and RTX3500)
bridge1	Allow access from bridge interface
vlanN	Allow access from VLAN interface (Not specified for vRX series)
lanN/M	Allow access from tag VLAN interface (Not specified for vRX series)

- [Initial value]: -
- *any*
 - [Setting value]: Allow access from all hosts
 - [Initial value]: any
- *None*
 - [Setting value]: Prohibit access from all hosts
 - [Initial value]: -

- *lan*
 - [Setting value]: Allow access from all LAN side networks
 - [Initial value]: -

[Explanation]

Set the hosts that allow access to the SSH server.

[Notes]

Applies from a new SSH connection after configuration.

Bridge interface cannot be specified for vRX Amazon EC2 version and RTX5000 / RTX3500 Rev.14.00.11 or earlier.
The lan keyword cannot be specified for RTX5000 / RTX3500 Rev.14.00.31 or earlier and for RTX1210 Rev.14.01.15 or earlier

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.59 Set the number of users who can connect to the SSH server at the same time

[Format]

sshd session num
no sshd session [num]

[Setting value and initial value]

- *num*
 - [Setting value]: Number of simultaneous connections (1..8)
 - [Initial value]: 8

[Explanation]

Set the number of users who can connect to the SSH at the same time.

[Notes]

If more users are connected than the changed value when the setting is changed, the connected users can maintain it, but new connections are not permitted until the number of connected users is less than the set value.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.60 SSH server host key setting

[Format]

sshd host key generate [bit=bit]
no sshd host key generate [...]

[Setting value and initial value]

- *bit*
 - [Setting value]: Key bit length (1024, 2048)
 - [Initial value]:
 - 1024 (RTX5000, RTX3500, RTX1210)
 - 2048 (models other than the above)

[Description]

SSH server host key setting

The bit parameter specifies the number of bits of the key to be generated.

[Notes]

When using the SSH server function, it is necessary to generate a host key by executing this command in advance.
When this command is executed in a state where the host key has already been set, it is confirmed whether or not to update the host key to the user.

The generation of the host key takes from several seconds to several minutes for a 1024-bit key, and from several minutes to ten minutes for a 2048-bit key, depending on the model.

If the setting is obtained by TFTP, it is saved in the format of sshd host key generate [bit=bit] KEY1 KEY2 KEY3. *Keys 1 to 3 are strings obtained by encrypting a private key in a device-specific manner.*

[Notes]

The bit keyword is not available for RTX5000/RTX3500 Rev.14.00.20 and earlier and RTX1210 Rev.14.01.10 and earlier.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.61 Display of SSH server host key

[Format]

show sshd host key [type=fingerprint [hash_algorithm]]

[Setting value and initial value]

- *Fingerprint: Key keyword indicating display of fingerprint.*
 - [Initial value]: -
- *hash_algorithm: Hash function algorithm used to display the key fingerprint.*
 - [Setting value]:

Setting value	Explanation
MD5	MD5
sha256	SHA-256

- [Initial value]: Sha256

Explanation

Displays the host key of the SSH server.

When a fingerprint keyword is specified, the key length and the key fingerprint of the public key are displayed.

[Notes]

RTX8300 can be used with Rev.14.02.14 or later. RTX500 can be used with Rev.15.02.14 or later. RTX8300 can be used with Rev.15.02.14 or later. RTX830 can be used with Rev.15.02.14 or later.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.62 Setting cryptographic algorithms available on the SSH server

[Format]

sshd encrypt algorithm algorithm [algorithm ...]

no sshd encrypt algorithm [...]

[Setting value and initial value]

- *algorithm: cryptographic algorithm (can be specified in multiple spaces)*
 - [Setting value]:

Setting value	Explanation
aes128-ctr	AES128-CTR
aes192-ctr	AES192-CTR
aes256-ctr	AES256-CTR
aes128-cbc	AES128-CBC

Set value	Description
aes192-cbc	AES192-CBC
aes256-cbc	AES256-CBC
3DES-CBC	DES-CBC
blowfish-cbc	Blowfish-CBC (RTX5000、RTX3500、RTX1210 Rev.14.01.33 or before and RTX830 Rev.15.02.09 or earlier)
cast128-cbc	CAST-128-CBC (RTX5000、RTX3500、RTX1210 Rev.14.01.33 or before and RTX830 Rev.15.02.09 or earlier)
arcfour	Arcfour (RTX5000、RTX3500、RTX1210 Rev.14.01.33 or before and RTX830 Rev.15.02.09 or earlier)

- [Initial value]: aes128-ctr aes192-ctr aes256-ctr

Description

Set the cryptographic algorithm available on the SSH server.

Proposes a list of cryptographic algorithms specified by algorithm to the client at the time of SSH connection.

[Notes]

If the client does not support the cryptographic algorithm specified by algorithm, it cannot be connected to the client by SSH.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.63 Checking the survival of the SSH client

[Format]

sshd client alive switch [interval [count]]

no sshd client alive [switch ...]

[Set value and initial value]

- *switch*
- [Set value]:

Set value	Description
on	Checking the survival of the client
off	Do not check the survival of the client

- [Initial value]: off
- *Interval*
 - Set value: Number of seconds between transmissions (1..2147483647)
 - [Initial value]: 100
- *count*
 - Set value: Number of attempts (1..2147483647)
 - [Initial value]: 3

Description

Set whether to check the survival of the client

Sends a message requesting a response at intervals set by interval to the client. If there is no response for the number of consecutive times specified by count, disconnects from this client and terminates the session.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.64 Hide OpenSSH version information included in the SSH server response

[Format]**sshd hide openssh version use****no sshd hide openssh version [use]****[Set value and initial value]**• *Use*

• [Set value]:

Setting value	Description
on	Show no SSH version information
off	Showing SSH version information

• [Initial value]: off

[Explanation]

Sets whether to display OpenSSH version information included in a server response at the time of SSH connection. This command is used when you want to hide OpenSSH version information for security purposes. When this command is set to on, "SSH-2.0-OpenSSH" is notified.

[Notes]

This version information is used to adjust the compatibility of server and client protocols during SSH connection. Depending on the client software, connection may not be possible by setting this command to on.

In that case, change the client software or set this command to off.

RTX5000 and RTX3500 can be used with Rev.14.00.18 or later.

RTX1210 can be used with Rev.14.01.09 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.65 Configuring authentication methods available on an SSH server

[Format]**sshd auth method all****sshd auth method method [method]****no sshd auth method [...]****[Setting value and initial value]**• *all: Accept password authentication and public key authentication*

• [Initial value]: all (vRX Sakura cloud version, other than RTX840)

• *method*

• [Setting value]:

Setting value	Description
password	Accept password authentication
publickey	Accept public key authentication

• [Initial value]: publickey (vRX Sakura cloud version, RTX840)

[Explanation]

Configuring authentication methods available on an SSH server

Public key authentication is a more secure authentication method than password authentication.

[Notes]

In farms where this command cannot be used, the behavior is equivalent to sshd auth method password. RTX5000 can be used with Rev.14.00.32 or later. RTX830 can be used with Rev.14.01.35 or later. RTX1210 can be used with Rev.15.02.14 or later. RTX830 can be used with Rev.15.02.14 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.66 **Setting up a file to store public key information used for public key authentication on an SSH server**

[Format]

```
sshd authorized-keys filename [user] path=path
no sshd authorized-keys filename [user] [path=path]
```

[Setting value and initial value]

- *user*: Registered user name
 - [Initial value]: -
- *path*: File name that stores the public key of the SSH client
 - [Initial value]:
 - /ssh/authorized_keys/username (for registered users)
 - /ssh/authorized_keys/no.name (In the case of an anonymous user)

[Explanation]

Set up a file (authorized_keys file) that stores the public key of the SSH client. It is used when a user authenticates the public key.

When setting up this command, it is necessary to register a user with the login user command in advance except for an unknown user. If this command is set for an unregistered user, an error will occur.

If user is omitted, the setting is for an unknown user.

The external storage mounted by mount command can be specified in path. The path of the external storage is specified by adding the prefix set at mounting to the beginning. For example, if you specify "/dir/sample" of external storage whose prefix is "storage:", specify "storage:/dir/sample".

When using public key authentication, it is necessary to store the public key of SSH client which is permitted in advance in a file. The supported file formats are as follows.

- One public key is stored in each line.
- One public key is described in the order of "(public key type) (base64 encoded key body) (key comment)".
- Up to 33 public keys can be registered in the file. The 34th and subsequent public keys are ignored.
- Blank lines and lines starting with # are ignored.
- The length of one line corresponds to up to 4094 characters (excluding line feed codes). Lines longer than 4094 characters are ignored.
- The line feed codes correspond to CR+LF, LF, and CR. In the case of the last line, there is no need for a line feed.
- The character code of the file corresponds to ASCII.
- For the public key type, you can set ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519, ssh-dss, and ssh-rsa (*).
 - * The key length of ssh-rsa corresponds to 1024bit, 2048bit, and 4096bit.
- In the authorized_keys file of OpenSSH, you can specify an option, but it is not supported. Ignore the description of the option.

[Note] Sample [Note]

ExampleRSA2048bitFor public keys of ssh-

```
rsaAAAAB3NzaC1yc2EAAAABIwAAQEA3eK3sk60fhHP9zsRgI39tqAoNfljbnCNiJ7horhwu6lZyaK
DKf8BiiCsKnvFsLI fSgcOejllflBtrFX3bN8iu+me2Ggh52vuIWDS/SUEQNWcYCalY0Ign8u8O
zVxldx1QABzuAKEKA654gkhQA40iaCKbKD5RGp4zujqDA6p8Y9o06pC/Ns7GzkgegrMxg40feB+0hJS
+K2eY49uqqwqYUYCdNw6bTIJiH6nAgsXSUDjbo3N+b9CY/9/7txKBykt1zt04WCXepngxVRw2ss+JOV k
PisDmt10//Q7Xdi+MxiLKhjeZk3jpqrSHiLon6D30xU/5/FY0cwcRBwrj4Uuw== user1
```

Example:ECDSA256bitFor public keys of

```
IP8Bg+r8rZhNmRq+ber0+sOaYCsvm5TN1CGt5WpCNkpwkV3c3rxwA6GAgGxuJsSn4J6Bo1mABhHg+YHM
= user2
```

If connected by a user who is not registered by the login user command, public key authentication is attempted as an anonymous user.

[Note]

For each model except for vRX Amazon EC2 version, vRX VMware ESXi version, RTX5000, RTX3500, RTX1220, RTX1210, and RTX830, the user cannot be omitted because an anonymous user cannot be registered.

Specifying external storage to the path parameter is possible for vRX series except for vRX Amazon EC2 version.

RTX1210 can be used with Rev. 14.00.32 or later. RTX3500 can be used with Rev. 14.00.32 or later. RTX1210 can be used with Rev. 15.02.14 or later. RTX830 can be used with Rev. 15.02.14 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.67 Setting public keys used for public key authentication of SSH servers

[Format]

```
import sshd authorized-keys [user]
```

[Setting value and initial value]

- *user*
- [Setting value]: Registered user name
- [Initial value]: -

[Description]

Add settings to the `authorized_keys` file that stores the public key of an SSH client.

When executing this command, it is necessary to register users with the login user command in advance except for anonymous users. If this command is set for a user who is not registered, an error will occur.

If user is omitted, the setting is for an anonymous user.

Add settings to the `authorized_keys` file specified by the `sshd authorized-keys filename` command.

If the `authorized_keys` file or directory does not exist, create a new one.

Enter one public key according to a prompt after command input. The entered public key is additionally written to the `authorized_keys` file. The public key is described in the order of "(public key type) (base64 encoded key body) (key comment)". Up to 4094 characters can be entered.

The format of the public key is similar to the `sshd authorized-keys filename` command.

If you want to delete or initialize an `authorized_keys` file, use the delete command.

[Notes]

Except for vRX Amazon EC2 version, vRX VMware ESXi version, RTX5000, RTX3500, RTX1220, RTX1210, and RTX830, an unknown user cannot be registered and the user cannot be omitted.

RTX5000 can be used with Rev. 14.00.32 or later. RTX1210 can be used with Rev. 14.01.32 or later. RTX1210 can be used with Rev. 14.01.35 or later. RTX830 can be used with Rev. 15.02.14 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.68 Display of public key used for public key authentication of SSH server

[Format]

```
show sshd authorized-keys [user] [type=fingerprint [hash_algorithm]]
show sshd authorized-keys * [type=fingerprint [hash_algorithm]]
```

[Setting value and initial value]

- *user*: Registered user name
 - [Initial value]: -
- *fingerprint*: Keyword indicating display of fingerprint
 - [Initial value]: -
- *hash_algorithm*: Hash function algorithm used to display key fingerprint
 - [Setting value]:

Setting value	Explanation
MD5	MD5
sha256	SHA-256

- [Initial value]: sha256
- * *All users*
 - [Initial value]: -

[Explanation]

Displays a file (authorized_keys file) that stores the public key of SSH client.
When fingerprint is specified, the key length and the key fingerprint of public key are displayed.
In the first format, an authorized_keys file corresponding to user is displayed. When user is omitted, information on an unknown user is displayed.
In the second format, an authorized_keys file for all users is displayed.

[Notebook]

Except for vRX Amazon EC2 version, vRX VMware ESXi version, RTX5000, RTX3500, RTX1220, RTX1210 and RTX830, unknown users cannot be registered, so user cannot be omitted.

RTX1210 is available in Rev. 14.02.32 or later. RTX500 is available in Rev. 14.02.32 or later. RTX830 is available in Rev. 15.02.14 or later. RTX830 is available in Rev. 15.02.14 or later.

[設定例]

Example: Displaying an RSA 2048bit public key
show sshd authorized-keys user1
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA... user1

Example: Displaying an RSA 2048bit public key fingerprint with SHA-256
show sshd authorized-keys user1 type=fingerprint sha256
2048 SHA256:uk2janKfeZXBsUniTMdNwL2fhdcAdfY0MsGSsCtpg8E user1 (RSA)

Example: Displaying an RSA 2048bit public key fingerprint with MD5
show sshd authorized-keys user1 type=fingerprint md5
2048 MD5:6e:fe:21:cc:d2:a4:55:78:07:7f:7f:f7:59:17:56:3a user1 (RSA)

Example: Displaying all users
There are unknown users and users1, user2 and user3.
user2 changes the file location with the sshd authorized-keys filename command.
user3 does not have an authorized_keys file.

show sshd authorized-keys * type=fingerprint sha256 (noname)
/ssh/authorized_keys/no.name
2048 SHA256:fMIGwY5YIQvz9xEObkDXaO7TuvllgFIakmV0K2MGbyU (RSA)

user1 /ssh/authorized_keys/user1
2048 SHA256:uk2janKfeZXBsUniTMdNwL2fhdcAdfY0MsGSsCtpg8E user1 (RSA)

```
# user2/pub-key
2048SHA256:U17sScopCUNPA5IndPWzHhkANqr3PkD2k3GMv0qS5NAuser2 (RSA)

user3/ssh/authorized_keys/user3
/ssh/authorized_keys/user32048Failed to read file data2048Nosuch file or
directory
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.69 Setting up a host that can access an SFTP server

[Format]

sftpd host ip_range [ip_range...]

sftpd host

any sftpd

host none

sftpd host lan

no sftpd host

[Setting value and initial value]

- *ip_range*: IP address or mnemonic of the host that allows access to the SFTP server
 - [Setting value]:

Setting value	Description
one IP address or IP addresses (ranged) with a hyphen (-) in between, and optionally arranged	Allow access from a specified host
lanN	Allow access from a LAN interface
wan1	Allow access from a WAN interface (Not available for vRX series, RTX5000, and RTX3500)
bridge1	Allow access from a bridge interface
vlanN	Allow access from a VLAN interface (Not available for vRX series)
lanN/M	Tag Allow access from a VLAN interface (Not available for vRX series)

- [Initial value]: -
- *any*
 - [Setting value]: Allow access from all hosts
 - [Initial value]: -
- *none*
 - [Setting value]: Forbid access from all hosts
 - none.
- *lan*
 - [Setting value]: Allow access from within a network on the LAN side
 - [Initial value]: -

[Description]

Set up a host that allows access to an SFTP server

[Notes].

The target host must also be allowed access with the `sshd host` command. It is applied from a new SFTP connection after configuration.

Bridge interface cannot be specified for vRX Amazon EC2 version and RTX5000 / RTX3500 Rev.14.00.11 or earlier.
The lan keyword cannot be specified for RTX5000 / RTX3500 Rev.14.00.31 or earlier and for RTX1210 Rev.14.01.15 or earlier.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.70 SSH clients

[Format]

ssh [-p port] [-e escape] [user@]host

[Setting value and initial value]

- *port*
 - [Setting value]: Port number of a remote host
 - [Initial value]: 22
- *escape*
 - [Setting value]: Character code of escape character (0 ... 255)
 - [Initial value]: 126 (~)
- *user*
 - [Setting value]: User name used to log in to the remote host
 - [Initial value]: -
- *host*
 - [Setting value]: Host name or IP address of the remote host
 - [Initial value]: -

[Explanation]

Execute SSH and log in remotely to the specified host.

*If user is omitted, access to the SSH server is attempted using the user name entered when logging in to the router.
When specifying an IPv6 address for host, enclose the IP address with "[","]".*

The escape character specified by escape is recognized as an escape character only when it is entered at the beginning of a line. If a period (.) is entered after the escape character, the connection is forcibly closed. If an escape character is entered twice consecutively from the beginning of a line, this character is sent to the server only once.

An execution example is as follows.

Remote host (192.168.1.1Port10022)Access to

```
#ssh-p10022user@192.168.1.1
```

Remote host (2001:1::1)Access to

```
#ssh user@[2001:1::1]
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.71 SCP client

[Format]

scp [[user@]host:]file1 [[user@]host:]file2 [port]

[Setting value and initial value]

- *user*
 - [Setting value]: User name used to log in to the remote host
 - [Initial value]: -
- *host*
 - [Setting value]: Host name or IP address of the remote host
 - [Initial value]: -
- *file1*
 - [Setting value]: Source file name

- [Initial value]: -
- *file2*
 - [Setting value]: Source file name
 - [Initial value]: -
- *port*
 - [Setting value]: Remote host port number
 - [Initial value]: 22

[Description]

Execute SCP.

Either file1 or file2 specifies a file on the remote host, and the other specifies a file in the file system of the router. The remote host's file cannot be specified in both file1 and file2.

Similarly, files in the file system of the router cannot be specified in both file1 and file2.

When specifying a file in RTFS, external memory, and external storage, user and host are omitted and only file is specified as an absolute path.

When specifying a router's configuration file (config, config0 to config4) or firmware (exec, exec0, exec1), specify only the file name as "config" or "exec0".

When specifying external storage, specify by adding a prefix set at mounting. For example, if you specify "/dir/sample.txt" for external storage whose prefix is "storage:", use "storage:/dir/sample.txt".

If you specify an IPv6 address as host, enclose the IP address with "[", "]".

[Notes]

Specifying a file on external storage is possible with vRX series except for vRX Amazon EC2 version.

[設定例]

Remote host (192.168.1.1) from the router

```
exec0Copy the file to
```

```
#scpuser@192.168.1.1:rtx1300.binexec0
```

Files on routerusb1:/log.txtRemote host (2001:1::1)Copy the file to

```
#scpusb1:/log.txtuser@[2001:1::1]:log.txt
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.72 Setting up cryptographic algorithms available for SSH clients

[Format]

ssh encrypt algorithm algorithm [algorithm...]

no ssh encrypt algorithm [algorithm...]

[Setting value and initial value]

- *algorithm* : cryptographic algorithms (multiple can be specified separated by spaces)
- [Setting value]

Setting value	Description
aes128-ctr	AES128-CTR
aes192-cbc	AES192-CTR
aes256-ctr	AES256-CTR
aes128-cbc	AES128-CBC
aes192-cbc	AES192-CBC
aes256-cbc	AES256-CBC
3des-cbc	3DES-CBC

Setting value	Description
blowfish-cbc	Blowfish-CBC (RTX5000、RTX3500、RTX1210 Rev.14.01.33 以前、 and RTX830 Rev.15.02.09 or earlier)
cast128-cbc	CAST-128-CBC (RTX5000、RTX3500、RTX1210 Rev.14.01.33 以前、 and RTX830 Rev.15.02.09 or earlier)
arcfour	Arcfour (RTX5000、RTX3500、RTX1210 Rev.14.01.33 以前、 and RTX830 Rev.15.02.09 or earlier)

- [Initial value]: aes128-ctr aes192-ctr aes256-ctr

[Explanation]

Set the cryptographic algorithm available in the SCP client.

A list of cryptographic algorithms specified by algorithm is proposed to the server at the time of SSH connection.

[Notes]

If the server does not support the cryptographic algorithm specified by algorithm, it is not possible to connect to the server by SSH.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.73 Setup a file to store the public key information of the SSH server

[Format]

ssh known hosts file

no ssh known hosts [file]

[Setting value and initial value]

- *file*
 - [Setting value]: File name to store the public key information of the SSH server
 - [初期値] : /ssh/known_hosts

[Explanation]

Specify a file to store the public key information of the SSH server.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.74 Changing parameters of packet buffers

[Format]

system packet-buffer group parameter=value [parameter=value ...]

no system packet-buffer group [parameter=value ...]

[Setting value and initial value]

- *group*: Specify a group of packet buffers.
 - [Setting value]: Group name (small, middle, large, jumbo, huge)
 - [Initial value]: -
- *parameter*: Specify parameters to be changed.
 - [Setting value]:

Setting value	Explanation
max-buffer	Maximum number of packet buffers allocated

Setting value	Explanation
max-free	Maximum number of free lists (Not specified for vRX series, RTX3510, and RTX1300)
min-free	Minimum number of free lists (Not specified for vRX series, RTX3510, and RTX1300)
buffer-in-chunk	Number of packet buffers in a chunk (Not specified for vRX series, RTX3510, and RTX1300)
init-chunk	Number of chunks to be reserved at startup (Not specified for vRX series, RTX3510, and RTX1300)

- [Initial value]: -
- *value*
- [Setting value]: Specify a value to be changed.
- [Initial value]:

vRX series

group	max-buffer		
	Other than the above	vRX Amazon EC2 version	vRX VMware ESXi version
small	45000	10000	45000
middle	120000	26664	120000
large	180000	40000	180000
huge	20	532	532

RTX1220, RTX1210, RTX840, RTX830

group	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
small	2500	937	62	625	1
middle	6664	2499	166	1666	1
large	10000	2812	62	625	4
huge	20	0	0	1	0

RTX5000, RTX3500

group	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
small	10000	3750	250	2500	1
middle	26664	9999	666	6666	1
large	40000	11250	250	2500	4
jumbo	40000	11250	250	2500	4
huge	20	0	0	1	0

RTX1300

group	max-buffer
small	5000
middle	13332
large	20000
jumbo	5000

group	max-buffer
huge	20

RTX3510

group	max-buffer
small	10000
middle	26664
large	40000
jumbo	5000
huge	20

Explanation

Management parameters of packet buffers are changed. Values that can be specified for parameters are as follows.

- vRX Series
 - The following ranges can be specified.

group	max-buffer		
	Other than those listed on the right	vRX Amazon EC2 Edition	vRX VMware ESXi Edition
small	45000..75000	1..40000	45000..75000
middle	120000..20000	1..106656	120000..20000
large	180000..300000	1..160000	180000..300000
huge	20..80	1..2128	532

- Other models (except RTX3510 and RTX1300)
 - The values that can be specified are different between huge blocks and others.
 - In blocks other than huge blocks, integers of 1 or more can be specified as parameters. At the same time, each parameter must satisfy all of the following conditions.
 - $\text{max-buffer} \geq \text{max-free}$
 - $\text{max-free} > \text{min-free}$
 - $\text{max\_free} \geq \text{buffer-in-chunk}$
 - $\text{max\_free} \geq \text{buffer-in-chunk} \times \text{init-chunk}$
 - In a huge block, integers of 0 or more can be specified for max-free, min-free, and init-chunk, and integers of 1 or more can be specified for max-buffer and buffer-in-chunk. When zero is specified for max-free, min-free, and init-chunk, all three parameters must be zero. When max-free, min-free, and init-chunk are 1 or more, each parameter must satisfy the above conditions like other groups.

[Notes]

A jumbo group can be used only in models that support a 1000BASE-T interface as a LAN interface and can send and receive jumbo packets.

To reflect configuration changes by this command on vRX series, RTX3510, and RTX1300, it is necessary to restart the router.

[設定例]

```
#systempacket-buffersmallmax-buffer=1000max-free=500 #
system packet-buffer large min-free=100
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.75Setting whether an enabled alarm sound is played or not at all.

[Format]

- alarm entire switch
- no alarm entire

[Setting value and initial value]

- *switch*
- [Setting value]

Setting value	Explanation
on	Ring
off	Not sounding

- [Initial value]: on

[Description]

Select whether an enabled alarm sound is played or not at all.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.76 Setting whether an alarm sound related to a USB host function is played or not.

[Format]

alarm usbhost switch
no alarm usbhost

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Explanation
on	Ring
off	Not sounding

- [Initial value]: on

[Explanation]

Setting whether to sound an alarm sound related to a USB host function.

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.77 Setting whether to sound an alarm related to a microSD function.

[Format]

alarm sd switch
no alarm sd [switch]

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Description
on	Ring
off	Don't ring

- [Initial value]: on

Explanation

Sets whether to sound an alarm related to the microSD function.

[Applied model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.78 Setting whether to sound an alarm related to the batch file execution function

[Format]

alarm batch switch
no alarm batch

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Explanation
on	Ring
off	Don't ring

- [Initial value]: on

Explanation

Select whether to sound an alarm related to the batch file execution function.

[Applied model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.79 Setting whether to sound an alarm at startup

[Format]

alarm startup switch [pattern]
no alarm startup [switch]

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Explanation
on	Ring
off	Don't ring

- [Initial value]: off
- *pattern*
 - [Setting value]: Alarm sound pattern (1...3, 1 if omitted)
 - [Initial value]: -

Explanation

Select whether to sound an alarm at startup.

[Applied model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.80 Setting whether to sound an alarm related to the HTTP revision upgrade function

[Format]

alarm http revision-up switch
no alarm http revision-up [switch]

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Explanation
on	To sound.
off	Not to sound.

- [Initial value]: on

[Explanation].

Set whether to sound an alarm related to the HTTP revision up function.

[Applied model].

RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.81 Setting environment variables.

[Format].

set name=value

no set name[=value]

[Setting value and initial value].

- *name*
 - [Setting value]: Environment variable name.
 - [Initial value]: -
- *value*
 - [Setting value]: Setting value.
 - [Initial value]: -

[Explanation].

Setting environment variables of a router.

Naming rules for environment variable names are as follows.

Half-width alphanumeric characters and underscore '_' can be used, and must start with an English character.

There is no limit to the length of variable names, but the set command cannot be executed longer than the maximum command line length (4095 characters). English characters are distinguished between uppercase and lowercase letters. For example, abc and Abc are treated as separate environment variables.

If value contains special characters such as spaces, the entire value must be enclosed in quotation marks.

[Applied model].

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.82 Setting aliases

[Format].

alias name=value

no alias name[=value]

[Setting value and initial value].

- *name*
 - [Setting value]: Alias name.
 - [Initial value]: -
- *value*
 - [Setting value]: Setting value.
 - [Initial value]: -

[Explanation].

Setting aliases.

Naming rules for aliases are as follows.

Half-width alphanumeric characters and underscore '_' can be used, and must start with an English character.

English characters are distinguished between uppercase and lowercase letters. For example, abc and Abc are treated as separate aliases.

If value contains special characters such as spaces, the entire value must be enclosed in quotation marks.

[Notes].

RTX5000 and RTX3500 can be used with Rev.14.00.26 or later.

RTX1210 can be used with Rev.14.01.26 or later.

RTX830 can be used with Rev.15.02.03 or later.

[Applied model].

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.83 Setting macros

[Format].**macro [-v] [-x] name <<eom****no macro [-v] [-x] name [<<eom]****[Setting value and initial value].**

- **-x**
 - [Setting value]: Execute while displaying the contents before expansion.
 - [Initial value]: -
- **-x**
 - [Setting value]: Execute while displaying the expanded line.
 - [Initial value]: -
- **name**
 - [Setting value]: Macro name
 - [Initial value]: -
- **eom**
 - [Setting value]: Terminating string of macro
 - [Initial value]: -

[Explanation]

Set macro.

Since it becomes macro input state after this command input, the contents of macro are inputted. At the end of macro, only the terminating string specified by eom is inputted to finish macro input. The command can be interrupted by inputting Ctrl-C even during macro input.

When -v option is specified, for each line executed when executing macro, environment variable and contents before expansion of alias are displayed.

The -x option executes macro while displaying the line after environment variable and expansion of alias.

Characters which can be used for name are only half-width uppercase letters, lowercase letters, numbers, underscore (_), and the first character must always be an English character.

An execution example is as follows.

```
#macro sample<<EOM
show ip route
show ip connectionEOM
#
```

[Notes]

Since it does not correspond to a command which consists of multiple lines, it cannot be executed from schedule at command.

When executing a command which consists of multiple lines in `rt.command()` of Lua script, a character string in which each line is concatenated by a newline character (`"\n"`) is passed as a command. The newline character must be `'\n'`, and an error occurs with `'\r'` or `'\r\n'`.

An execution example is as follows.

```
rtn,err=rt.command("macro sample<<EOM\nshow ip route\nshow ip connection\nEOM")
```

RTX5000 and RTX3500 can be used in Rev.14.01.26 or later.

RTX1210 can be used in Rev.14.01.26 or later.

RTX830 can be used in Rev.15.02.03 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.84 EMFS file creation and deletion

[Format]**embedded file [-b] filename <<eof****no embedded file [-b] filename [<<eof]****[Setting value and initial value]**

- *-b*
 - [Setting value]: Specify BASE64 format
 - [Initial value]: -
- *filename*
 - [Setting value]: File name
 - [Initial value]: -
- *EOF*
 - [Setting value]: Terminating string
 - [Initial value]: -

[Description]

EMFS file creation and deletion

When the embedded file command is input, the console enters a mode of inputting the contents of the file. EOF specified by eOF

The contents of the file are until a character string is input. The no embedded file command can delete the file.

If the -b option is specified, the contents of the input file are processed as if they were in BASE64 format. An error occurs if the contents are invalid as BASE64 format. When saving a binary file, it must be in BASE64 format. If the -b option is omitted, the input contents are saved as a text file.

Character types that can be used as an EOF character string are only half-width alphanumeric characters (A-Z, a-z, 0-9). English capital letters and lowercase letters are distinguished.

An execution example is as follows.

```
#embeddedfilesample.txt<<EOF show
ip route
showipconnectionEOF
#
```

[Notes]

Since it does not correspond to a command consisting of multiple lines, it cannot be executed from a schedule at command.

When executing a command consisting of multiple lines with `rt.command()` of Lua script, pass a character string obtained by concatenating each line with a newline character ('\n') as a command. The newline character must be '\n', and '\r' or '\r\n' causes an error.

An execution example is as follows.

```
rtn,err=rt.command("embeddedfilesample<<EOF\nnechoThisissample\nEOF")
```

RTX5000 and RTX3500 can be used with Rev.14.00.26 or later.

RTX1210 can be used with Rev.14.01.26 or later.

RTX830 can be used with Rev.15.02.03 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

4.85 Setting CPU Scheduling Method

Format

system packet-scheduling mode

no system packet-scheduling [mode]

Setting Value and Initial Value

- *mode* : CPU Scheduling Method
- Setting Value

Setting Value	Explanation
hash	Hashing Method
Load Balance Method	Load Balance Method (Cannot be specified in vRX Sakura Cloud Version)
lan-based	LAN Interface Method (Cannot be specified in vRX Sakura Cloud Version, RTX3510, and Cannot be specified in RTX1300)
fixed	Fixed Method (Cannot be specified in vRX Sakura Cloud Version, RTX5000, RTX3510, Cannot be specified in RTX3500 and RTX1300)

- Initial Value: hash

Description

CPU Scheduling Method is set.

When hash is selected, a CPU core executing packet transfer processing is determined based on a hash value calculated from received packets.

When load-balance is selected, the CPU core executing packet transfer processing is changed in packet units so that the load of each CPU core is equalized.

When lan-based is selected, the CPU core executing transfer processing by the LAN interface receiving packets is determined as follows (VRX series is an example when the number of CPU cores is four and the number of NICs is four).

Receiving LAN Interface	The vRX series	Other models
LAN1	CPU1	CPU0
CPU2	CPU3	CPU1
CPU3	CPU3	CPU3
LAN4	CPU1	CPU3

When fixed is selected, the transfer processing is always executed by CPU1 regardless of the LAN interface that received the packet.

[Notes]

Packets received by BRI/PRI interface are not subject to the setting of this command.

When this command is executed, initialization processing of all LAN interfaces is executed, so link down occurs temporarily in all LAN interfaces. In order to reflect the setting change by this command in the vRX Amazon EC2 version, it is necessary to restart the router.

As for packets to be processed in a normal path, only reception processing is executed on CPU cores determined according to the setting of this command, and transfer processing is always executed by CPU0 (for vRX series) or CPU1 (for other models). When normal is set in the ip routing process command, all packets are subject to this.

When hash is selected as the CPU scheduling method, the transfer processing of received packets that do not have IPv4/IPv6 headers is executed by CPU1.

(for vRX series) or CPU0 (for RTX5000 and RTX3500). In RTX3510 and RTX1300, the following occurs.

RTX3510 and RTX1300

Protocol	CPU core that executes transfer processing
ARP	CPU0

Protocol	CPU core that executes transfer processing
Other than the above	CPU2

When load-balance is selected as the CPU scheduling method, packets may be switched in order. If packets are switched in order, problems may occur in applications using UDP. In models that can use the system packet-scheduling filter command, packets can be switched in order by fixing CPU cores that execute transfer processing of corresponding packets. In addition, TCP does not normally cause problems even if packets are switched in order.

In IPsec, since ESP packets may not be transmitted according to the order of an ESP sequence number regardless of which CPU scheduling method is used, an ESP sequence error may occur in reception processing of an opposing router, and the ESP packets may be discarded. An ESP sequence error can be avoided by turning off anti-replay-check with the ipsec sa policy command of the opposing router, so that the ESP sequence number is not checked.

RTX5000 and RTX3500 can be used after Rev.14.00.13.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500 and RTX1300

CHAPTER 5

RTFS file system for Yamaha routers

RTFS is a file system built into the internal storage of a router (internal flash ROM, etc.). As with the general PC file system, arbitrary data can be stored in the internal storage and managed with a file name. A directory structure is also realized. Various data such as firmware (exec) and configuration files (config) are stored in the internal storage, but a specific area independent of them is used as RTFS.

For commands to specify files and directories, you can reference the RTFS area by entering a path starting with an unprefixd "/".

Use RTFS for storing read-only data such as script files for Lua scripting functions and HTML files for custom GUIs. Periodic writing to the RTFS area, such as recording log files, accelerates flash ROM consumption. If the flash ROM fails due to frequent writing, it is not covered by the warranty for free repair even within the warranty period.

5.1 Formatting RTFS

Formatting

rtfs format

[Explanation]

Format the RTFS area of the internal storage (internal flash ROM, etc.) and delete all data. Formatting is also performed when returning to a factory shipping state.

[Notes]

When formatting is performed, the data is completely deleted and cannot be restored.

Applicable Models

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

5.2 Garbage Collect for RTFS

Formatting

rtfs garbage-

collect [説明]

Delete unnecessary data in the RTFS area of the internal storage (internal flash ROM, etc.) and increase free space.

Garbage collect is executed automatically when it is normally necessary, but since it takes several tens of seconds to process, this command is executed when you want to do it in advance.

[Notes]

Garbage collect does not delete or overwrite files.

Applicable Models

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 6

Setting IP

6.1 Setting Common to Interfaces

6.1.1 Setting whether to handle IP packets

Formatting

ip routing *routing*

no ip routing [*routing*]

Setting Values and Initial Values

- *routing*
- Setting Values

Setting Values	Explanation
on	Treat IP packets as processing targets
off	Do not treat IP packets as processing targets

- Initial Values: on

Explanation

Setting whether to route IP packets

[Notes]

Setting by TELNET, access by TFTP, PING, etc. are possible even when off.

Applicable Models

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.2 Setting IP Addresses

Formatting

ip interface address *ip_address/mask* [broadcast *broadcast_ip*]

ip interface address dhcp

ip wan address dhcp

ip pp address *ip_address/mask*

ip loopback address *ip_address/mask*

ip bridge_interface address *ip_address/mask* [broadcast *broadcast_ip*]

ip bridge_interface address dhcp [autoip=switch]

no ip interface address [*ip_address/mask* [broadcast *broadcast_ip*]]

no ip interface address [dhcp]

no ip wan address [dhcp]

no ip pp address [*ip_address/mask*]

no ip loopback address [*ip_address/mask*]

no ip bridge_interface address [*ip_address/mask* [broadcast *broadcast_ip*]]

no ip bridge_interface address [dhcp]

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Setting value]: -
- *wan*
 - [Setting value]:
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500

- [Setting value]: -
- *Loopback*
 - [Setting value]: LOOPBACK interface name
- [Setting value]: -
- *bridge_interface*
 - [Setting value]: Bridge interface name
 - [Setting value]: -
- *ip_address*
 - [Setting value]: IP address xxx.xxx.xxx.xxx (where xxx is a decimal number)
 - [Setting value]: -
- *dhcp*: Keyword indicating that you want to get an IP address as a DHCP client
 - [Setting value]: -
- *mask*
 - [Setting value]:
 - xxx.xxx.xxx.xxx (where xxx is a decimal number)
 - Hexadecimal numbers following 0x
 - Number of mask bits
 - [Setting value]: -
- *broadcast_ip*
 - [Setting value]: Broadcast IP address
 - [Setting value]: -
- *switch*
 - [Setting value]:

Setting value	Description
on	Using AutoIP function
off	Do not use AutoIP function

- [Setting value]: off

[Explanation]

Set the IP address and netmask of the interface. When “broadcast *broadcast_ip*” is specified, a broadcast address can be specified. When omitted, in models that support RFC3021, a limited broadcast address is used if the number of mask bits in the netmask is 31 bits, and a directed broadcast address is used otherwise.

When *dhcp* is specified, an IP address is obtained as a DHCP client immediately after setting. When **no ip interface address** is specified, an open message of the obtained IP address is sent to a DHCP server. If the number of retry times of *dhcp* is set to be finite in the **ip bridge_interface dhcp retry** setting, an address of 169.254.0.0/16 is automatically determined if the address allocation in *dhcp* fails.

[Notes]

If an IP address is not set in a LAN interface, an IP address is obtained by RARP.

If an IP address is not set in a PP interface, the interface behaves as unnumbered. The client ID obtained when operating as a DHCP client can be confirmed by the **show status dhcpc** command.

A bridge interface cannot be specified in vRX Amazon EC2 version and RTX5000/RTX3500 Rev.14.00.11 or earlier.

For the setting values of this command after executing the factory default and **cold start command**, refer to "Setting value in factory default or initial state after deployment".

The following models are compatible with RFC3021.
RTX1300 Rev.23.00.17 or later

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.3 Setting a secondary IP address

[Format]

```
ip interface secondary address ip_address[mask]
ip interface secondary address dhcp
no ip interface secondary address [ip_address[mask]
```

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *ip_address*
 - [Setting value]: Secondary IP address xxx.xxx.xxx.xxx (where xxx is a decimal number)
 - [Initial value]: -
- *dhcp*: Keyword indicating that you want to get an IP address as a DHCP client
 - [Initial value]: -
- *mask*
 - [Setting value]:
 - xxx.xxx.xxx.xxx (where xxx is a decimal number)
 - Hexadecimal numbers following 0x
 - Number of mask bits
 - [Initial value]: -

[Explanation]

Set the secondary IP address and netmask on the LAN side.

Specifying dhcp acquires an IP address as a DHCP client immediately after setting.

[Notes]

Broadcast addresses in secondary networks always use directed broadcast addresses.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.4 Setting the MTU of an interface

[Format]

```
ip interface mtu mtu0
IP PP MTU MTU1
ip tunnel mtu mtu2
no ip interface mtu [mtu0]
no ip pp mtu [mtu1]
no ip tunnel mtu [mtu2]
```

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *MTU0, MTU1, MTU2*
 - [Setting value]: Value of MTU (64..1500; LAN interface of RTX5000, RTX3500 is 64..9578, RTX3510, RTX1300 LAN interface of is 64..10218)
 - [Initial value]:
 - MTU0=1280
 - mtu1=1500

- MTU2=1280

[Explanation]

Value of MTU of each interface is set.

[Notes]

In practice, this setting applies only to IP packets. It does not apply to other protocols, and they leave the default value at 1500 MTU.

In an L2TP connection, the MTU setting of tunnel interface or PP interface is ignored and encapsulated, and packets after encapsulation are fragmented according to the MTU setting of the sending physical interface.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.5 Setting whether packets to wrap around to the same interface are sent or not

[Format]

```
ip interface rebound switch
ip pp rebound switch
ip tunnel rebound switch
no ip interface rebound [switch]
no ip pp rebound [switch]
no ip tunnel rebound [switch]
```

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *switch*
 - [Setting value]:

Setting value	Description
on	Send a wrapping packet
off	Do not send a wrapping packet

- [Initial value]:
 - off (for PP interface)
 - on (for other interfaces)

[Explanation]

Sets whether to send a wrapping packet to the same interface.

If it does not send a wrapping packet, discard the packet and send an ICMP Destination Unreachable to the sender.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.6 Echo, discard, time Set whether to run the service

[Format]

```
ip simple-service service
no ip simple-service [service]
```

[Setting value and initial value]

- *service*
 - [Setting value]:

Setting value	Description
on	Operate various services of TCP/UDP

Setting value	Description
off	Stop the service

- [Initial value]: off

[Explanation]

Sets whether to run various services of echo (7), discard (9), and time (37) of TCP/UDP. When the service is stopped, the corresponding port is also closed.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.7 Set static routing information of IP

[Format]

ip route *network* *gateway gateway1* [*parameter*] [*gateway gateway2* [*parameter*]...]

no ip route *network* [*gateway*...]

[Setting value and initial value]

- *network*

- [Setting value]:

Setting value	Description
Default	Default route
IP address	Number of destination host/mask bits (default is 32)

- [Initial value]: -
- *gateway1*, *gateway2*
- [Setting value]:
 - IP address
 - xxx.xxx.xxx.xxx (where xxx is a decimal number)
 - pp *peer_num* [*dlci=dlci*] : Route to PP interface. If "dlci=dlci" is specified, the frame relay Route to DLCI
 - *peer_num* : Destination number
 - pp anonymous *name=name*

Setting value	Description
<i>name</i>	Name by PAP/CHAP

- dhcp *interface*

Setting value	Description
<i>interface</i>	LAN interface name, WAN interface name, bridge interface name that operates as a DHCP client when using the default gateway given by DHCP

- *tunnel_num*: Route to tunnel interface
- LOOPBACK interface name, NULL interface name
- [Initial value]: -
- *parameter*: The following parameters can be set multiple times separated by spaces
- [Setting value]:

Setting value	Description
filter <i>number</i> [<i>number..</i>]	Specifying filter-type routes • <i>number</i> • Filter number (1..21474836) (separated by spaces can be set multiple times)

Setting value	Description
<code>dpi number [number..]</code>	Specifying filter-type routes <code>number</code> - DPI filter number (1..2147483647) (separated by spaces can be set multiple times)
<code>metric metric</code>	Metric specification <code>metric</code> - Metric value (1..15) - If omitted, 1
<code>hide</code>	This option is valid only when the output interface is a LAN interface, or a WAN interface, PP interface, or TUNNEL interface, meaning that the route is valid only when the other destination is connected
<code>weight weight</code>	A value representing the ratio between different routes <code>weight</code> - Weight to route (0..2147483647) - If omitted, 1
<code>keepalive keepalive_id</code>	Only valid when <code>gateway1</code> has reachability <code>keepalive_id</code> - Keep-alive identifiers (1..100; vRX Normal mode for Amazon EC2, vRX Normal mode for VMware ESXi, and vRX Cloud version are 1..6000; RTX5000, RTX3510 are 1...3000; vRX 1...1000 for Amazon EC2 Compact mode, vRX Compact mode for VMware ESXi, and RTX3500)

- [Initial value]: -

[Explanation]

Set a static route for IP.

When a filter-type route is specified as a `gateway` parameter, filters are applied in the order described, and a suitable gateway is selected.

When there is no matching gateway or when no gateway for which a filter-type route is specified is described, a gateway for which a filter-type route is not specified is selected.

When there is also no gateway for which a filter-type route is not specified, processing is continued assuming that the route does not exist.

When multiple gateways for which a filter-type route is not specified are described, selection of the route is determined by round robin at the time when those routes are used.

When multiple gateways for which no filter is specified are described, which one to use when using those routes is determined by the stream identified by the start/end point IP address, protocol, and start/end point port number. Packets of the same stream are always sent to the same gateway. When a value (e.g., a ratio of line speed) is specified in `weight`, the ratio of streams sent to the route increases in proportion to the ratio of that value to the `weight` value of other gateways.

In either case, a gateway for which a `hide` keyword is specified is valid only when the line is connected, and is not evaluated when the line is not connected. Note that since the LOOPBACK interface and null interface are always in the up state, the `hide` option can be specified, but it has no meaning.

When multiple gateways are set, preferentially using only a specific gateway without load balancing is performed. Set to 0 in the `weight` option.

[Notes]

Routes that already exist can be overwritten.

Bridge interfaces cannot be specified in vRX Amazon EC2 version and RTX5000/RTX3500 Rev.14.00.11 or earlier.

WAN interfaces cannot be specified in vRX series, RTX5000, and RTX3500.

The `dpi` keyword of the `parameter parameter parameter` can be specified in RTX1300, RTX840, and RTX830

Rev.15.02.13 or later. Keywords and parameters after the first gateway keyword can be set up to 129 in total.

[Configuration Example]

- The default gateway is 192.168.0.1.

```
# ip route default gateway 192.168.0.1
```

- The network connected by PP1 is 192.168.1.0/24.

```
# ip route 192.168.1.0/24 gateway pp 1
```

- Load distribution by multihoming is performed. It has two default gateways, and PP1 has a leased line of 128k. It is connected to PP2 by a leased line of 64k, and the route when each leased line is down is invalidated to prevent packet loss.

The NAT function and leased line keepalive must be used together.

```
# ip route default gateway pp 1 weight 2 hide gateway pp 2 weight 1 hide
```

- When PP1 is enabled, only PP1 is used. When PP1 goes down, PP2 is used.

```
# ip route 192.168.0.1/24 gateway pp 1 hide gateway pp 2 weight 0
```

- Packets related to software updates are sent via the PP1 interface, and others are sent via TUNNEL1.

```
# dpi group set 100 name=sw_update
windows_update,apple_update,ios_ota_update,adobe_update
# ip dpi filter 1 pass * * 100
# ip route default gateway pp 1 dpi 1 gateway tunnel 1
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.8 Set whether to automatically add a default route when an IP address is obtained by DHCP**[Format]**

```
ip interface dhcp auto default-route-add switch
```

```
no ip interface dhcp auto default-route-add [switch]
```

[Setting value and initial value]

- `interface`
 - [Setting value]
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series
 - Bridge interface name
 - [Initial value]: -
- `switch`
 - [Setting value]:

Setting value	Description
on	Automatically add a default route when an IP address is obtained by DHCP
off	Do not automatically add a default route when an IP address is obtained by DHCP

- [Initial value]: on

Description

Whether to automatically add an implicit route when an IP address is obtained by DHCP while using the specified interface is set.

If the setting of this command is changed for an interface that has already obtained an IP address by DHCP, The new setting is reflected from the time when the IP address is obtained by DHCP.

[Notebook]

Bridge interface cannot be specified for vRX Amazon EC2 version.

RTX1210 can be used with Rev.14.01.28 or later.

RTX830 can be used with Rev.15.02.03 or later.

[Applicable model]

vRX series, RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.9 Whether to automatically add an implicit route when an IP address is obtained by DHCP

[Format]

ip interface dhcp auto interface-route-add switch

no ip interface dhcp auto interface-route-add [switch]

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - LAN interface name
 - WAN interface name
 - Cannot be specified for vRX series
 - Bridge interface name
 - [Initial value]: -
- *switch*
 - [Setting value]:

Setting value	Description
on	Automatically add an implicit route when an IP address is obtained by DHCP
off	Do not automatically add an implicit route when an IP address is obtained by DHCP

- [Initial value]: on

Description

Whether to automatically add an implicit network route of the interface that has obtained the address when using the specified interface and obtaining the IP address by DHCP is set.

If the setting of this command is changed for an interface that has already obtained an IP address by DHCP, then The new setting is reflected from the time the IP address is obtained by DHCP.

[Notes]

Bridge interface cannot be specified in vRX Amazon EC2 version.

RTX1210 can be used after Rev. 14.01.28.

RTX830 can be used after Rev. 15.02.03.

[Applicable model]

vRX series, RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.10 Setting the filter of IP packets

[Format]

ip filter filter_num pass_reject src_addr[/mask] [dest_addr[/mask] [protocol [src_port_list [dest_port_list]]]]

no ip filter filter_num [pass_reject]

[Setting value and initial value]

- *filter_num*
 - [Setting value]: Static filter number (1..21474836)
 - [Initial value]: -
- *pass_reject*
 - [Setting value]:

Setting value	Description
pass	Pass if they match (Do not log)
pass-log	Pass if they match (Do not log)
Pass-nolog	Pass if they match (Do not log)
reject	Destroy if they match (Do not log)
reject-log	Destroy if they match (Do not log)
reject-nolog	Destroy if they match (Do not log)
restrict	Pass if the line is connected, destroy if it is disconnected (Do not log only if it is destroyed)
restrict-log	Pass if the line is connected, destroy if it is disconnected (Do not log)
restrict-nolog	Pass if the line is connected, destroy if it is disconnected (Do not log)

- [Initial value]: -
- *src_addr* : Start address of IP packet
 - [Setting value]:
 - IP address
 - A.B.C.D (A to D: 0 to 255 or *)
 - If A to D are * in the above notation, all values correspond to the corresponding 8 bits
 - Two top items with - in between, top items with - in front, top items with - in back, these specify ranges
 - Multiple can be set as a separator.
 - FQDN
 - Any character string (Up to 255 single-byte characters. /: cannot be used. , cannot be used because it is used as a separator)
 - FQDNs starting with * judge strings after * as backward matching conditions, for example *.example.co.jp matches www.example.co.jp, mail.example.co.jp, etc.
 - Multiple can be set as a separator.
 - map-e
 - Keywords representing global IPv4 addresses generated by the MAP-E map rule
 - hb46pp
 - Keywords representing IP addresses obtained by the domestic standard provisioning method of IPv6 migration technology
 - Mnemonic representing application name
 - Any character string starting with "@" (Up to 32 single-byte characters. Only A-Z a-z 0-9 _ - can be used)
 - Multiple can be set as a separator.
 - * (All IP addresses supported)
 - [Initial value]: -
- *dest_addr* : End address of IP packet
 - [Setting value]:
 - Same format as *src_addr*
 - Same as one * if omitted
 - [Initial value]: -
- *mask*: Bitmask of the IP address (can be specified only if *src_addr* and *dest_addr* are network addresses)

- [Setting value]:
 - A.B.C.D (A to D: 0 to 255)
 - Hexadecimal numbers following 0x
 - Number of mask bits
 - Same as 0xffffffff if omitted
- [Initial value]: -
- *protocol*: Packet type to filter
- [Setting value]:
 - Decimal number representing protocol (0..255)
 - Mnemonic representing protocol

Mnemonic	Decimal number	Description
icmp	1	ICMP packets
tcp	6	TCP packets
udp	17	UDP packets
ipv6	41	IPv6 packets
gre	47	GRE packets
esp	50	ESP packets
ah	51	AH packets
icmp6	58	ICMP6 packets

- Comma-separated rows in the above item
- Special designation

icmp-error	ICMP packets whose TYPE is one of 3, 4, 5, 11, 12, 31, or 32
icmp-info	ICMP packets whose TYPE is one of 0, 8 to 10, 13 to 18, 30, or 33 to 36
tcpsyn	tcp packets flagged with SYN
tcpfin	tcp packets flagged with FIN
tcpfin	tcp packets flagged with RST
established	A function that allows connections from within a tcp packet flagged with ACK but rejects connections from outside within
tcpflag= <i>value/mask</i>	The AND of the value of the TCP flag and the value of TCP packets that match or do not match <i>value</i> <i>value</i> and <i>mask</i> are hexadecimal numbers from 0x to 0xffff
tcpflag!= <i>value/mask</i>	
*	All protocols

- Same as * when omitted.
- Initial value: -
- *src_port_list*: If the *protocol* contains either TCP (tcp/tcpsyn/tcpfin/tcprst/established/tcpflag) or UDP (udp), TCP/UDP source port number. ICMP type if *protocol* is ICMP icmp) alone.
- [Setting value]:
 - Port number, decimal number for type
 - Mnemonic for port number (partial)

Mnemonic	Port number
ftp	20,21
ftpdata	20

Mnemonic	Port number
telnet	23
smtp	25
domain	53
gopher	70
finger	79
www	80
pop3	110
sunrpc	111
Ident	113
ntp	123
nntp	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540
submission	587

- Two top items with - in between, top items with - in front, top items with - in back, these specify ranges.
- Comma-separated rows of the top item (up to 10)
- * (all ports, types)
- Same as * if omitted.
- [Initial value]: -
- *dest_port_list*
 - [Setting value]: If *protocol* includes either TCP(tcp/tcpsyn/tcpfin/tcprst/established/tcpflag) or UDP(udp), TCP/UDP destination port number. If *protocol* is ICMP(icmp) alone, the ICMP code
 - [Initial value]: -

[Explanation]

Set IP packet filters. Filters set by this command are used in **ip filter directed-broadcast**, **ip filter dynamic**, **ip filter set**, **ip forward filter**, **ip fragment remove df-bit**, **ip interface rip filter**, **ip interface secure filter**, and the **ip route** command.

[Notes]

Filters using restrict-log and restrict-nolog are sufficient to pass only when the line is connected, and are therefore useful for packets that do not even need to be sent to the line. For example, an NTP packet to set a clock corresponds to this. If you want to check the ICMP type and ICMP code with a filter for an ICMP packet, specify only 'icmp' in the protocol alone. Only if the protocol is 'icmp' alone, the *src_port_list* is regarded as an ICMP type and the *dest_port_list* as an ICMP code. If the protocol specifies 'icmp' and other protocols, the specification of *src_port_list* and *dest_port_list* is regarded as a TCP/UDP port number and is not compared with an ICMP packet. Also, if the protocol specifies 'icmp-error' or 'icmpinfo', the specification of *src_port_list* and *dst_port_list* is ignored. If the protocol specifies '*' or lists multiple protocols including TCP/UDP, the specification of *src_port_list* and *dest_port_list* is regarded as a TCP/UDP port number and the filter compares the port number only if the packet is TCP or UDP. If the packet is for other protocols (including ICMP), the specification of *src_port_list* and *dest_port_list* is compared with the filter as non-existent.

The specification of *src_addr* and *dest_addr* can also mix mnemonics representing IP addresses, FQDNs, map-e, hb46pp, and application names.

The specification of FQDNs for *src_addr* and *dest_addr* can be specified with RTX5000 Rev.14.00.26 or later, RTX3500 Rev.14.00.26 or later, RTX1210 Rev.14.01.26 or later, RTX830 Rev.15.02.03 or later, and Rev.15.04 or later.

By specifying the FQDNs for *src_addr* and *dest_addr*, filtering can be performed for servers that are not fixed IP addresses or servers that have multiple fixed IP addresses against one FQDN. When using an FQDN, the router itself operates as a DNS recursive server, and terminals under the router must specify this unit as a DNS server. When communication that matches the specified FQDN occurs, information on the IP address corresponding to the set FQDN is retained. The retained period can be specified with the **ip filter fqdn timer** command.

The specification of map-e to *src_addr* and *dest_addr* can be specified with vRX series, RTX5000 Rev.14.00.31 or earlier, and RTX3500 Rev.14.00.31 or earlier.

Previously, this is not possible with RTX1210 Rev.14.01.39 or earlier, and RTX830 Rev.15.02.19 or earlier.

The specification of hb46pp to *src_addr* and *dest_addr* is not possible with vRX series, RTX5000, RTX3510 Rev.23.01.01, RTX3500, RTX1300 Rev.23.00.11 or earlier, RTX1220 Rev.15.04.06 or earlier, RTX1210, and RTX830 Rev.15.02.30 or earlier.

The specification of mnemonics that represent application names to *src_addr* and *dest_addr* can be specified with vRX series, RTX5000,

Not possible with RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, and RTX830.

The mnemonics that represent application names are specified with the mnemonics described in the destination list. In the following states, the mnemonics that represent application names are not evaluated.

- The LBO state is not "normally operating".
- The specified mnemonics are not included in the destination list.

[Configuration Example]

- Record IPv4 ICMP ECHO/REPLY sent and received by LAN1 in pass-log.

```
# ip lan1 secure filter in 1 2 100
# ip lan1 secure filter out 1 2 100
# ip filter 1 pass-log * * icmp 8
# ip filter 2 pass-log * * icmp 0
# ip filter 100 pass * *
```

- Of IPv4 redirects sent from LAN2, only "for the Host" is not passed.

```
# ip lan2 secure filter out 1 100
# ip filter 1 reject * * icmp 5 1
# ip filter 100 pass * *
```

- Packets of Microsoft 365 and Windows Update are sent via PP1, and others are sent via TUNNEL1.

```
# ip route default gateway pp 1 filter 1 gateway tunnel 1
# ip filter 1 pass * @m365,@windows_update * *
```

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.11 Defining a filter set

[Format]

ip filter set *name direction filter_list* [*filter_list* ...]

no ip filter set *name* [*direction* ...]

[Setting value and initial value]

- *Name*
 - [Setting value]: A string that represents the name of a filter set.
 - [Initial value]: -
- *direction*
 - [Setting value]:

Setting value	Explanation
in	Filter in the output direction
out	Filter in the output direction

- [Initial value]: -
- *filter_list*

- [Setting value]: A string of filter numbers separated by spaces (up to 1001)
- [Initial value]: -

Description

A filter set is defined. A filter set defines filters for in/out, and specifies them by RADIUS or IP. It is applied to an interface by the *interface secure filter* command.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.12 Setting whether to filter out IP packets with the Source-route option

[Format]

```
ip filter source-route filter_out
no ip filter source-route [filter_out]
```

[Setting value and initial value]

- *filter_out*
- [Setting value]:

Set value	Description
on	Filter out
off	Do not filter out

- [Initial value] : on

Description

Set whether to filter out IP packets with the Source-route option.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.13 Setting whether to filter out directed broadcast packets

[Format]

```
ip filter directed-broadcast filter_out
ip filter directed-broadcast filter filter_num [filter_num ...]
no ip filter directed-broadcast
```

[Set value and initial value]

- *filter_out*
- [Set value] : on

Set value	Description
on	Filter out
off	Do not filter out

- [Initial value] : on
- *filter_num*
 - [Set value] : Static filter number (1..21474836)
 - [Initial value] : on

Description

Set whether to broadcast IP packets whose terminal IP addresses are addressed to directed broadcast addresses to a network to which a router is connected.

If set to off, all directed broadcast packets are discarded.

If set to off, all directed broadcast packets are passed.

If set to filter, the packets are checked by the filter set by the **ip filter** command, and only if they match the PASS filter, packets are passed.

[Note]

Checking of the **ip interface wol relay** command has priority over checking by this command. Only packets that could not be passed by checking by the **ip interface wol relay** command are checked by this command. Set to on to prevent so-called smurf attacks.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.14 Definition of dynamic filter

[Format]

```
ip filter dynamic dyn_filter_num srcaddr[/mask] dstaddr[/mask] protocol [option ...]
ip filter dynamic dyn_filter_num srcaddr[/mask] dstaddr[/mask] filter filter_list [in filter_list] [out filter_list] [option...]
no ip filter dynamic dyn_filter_num
```

[Set value and initial value]

- *dyn_filter_num*
 - Set value: Dynamic filter number (1..21474836)
 - [Initial value] : on
- *srcaddr*: Starting address of IP packet
 - [Set value] : on
 - Same format as *src_addr* in the **ip filter** command
 - [Initial value] : on
- *dstaddr*: End address of IP packet
 - [Set value] : on
 - Same format as *srcaddr*
 - [Initial value] : on
- *mask*: Bitmask of IP address (can be specified only if *srcaddr* and *dstaddr* are network addresses)
 - [Initial value] : on
- *protocol*: Mnemonic of protocol
 - [Set value] : on
 - tcp/udp/ftp/tftp/domain/www/smtp/pop3/telnet/netmeeting
 - echo/discard/daytime/chargen/ftp/ssh/telnet/smtp/time/whois/dns/domain/
 - tftp/gopher/finger/http/www/pop3/sunrpc/ident/nntp/http/ms-rpc/
 - netbios_ns/netbios_dgm/netbios_ssn/imap/snmp/snmptrap/bgp/imap3/ldap/
 - https/ms-ds/ike/rlogin/rwho/rsh/syslog/printer/rip/ripng/
 - ms-sql/radius/l2tp/pptp/nfs/msblast/ipsec-nat-t/sip/
 - ping/ping6/tcp/udp
 - submission

The following can be configured, but it does not act as a dynamic filter

- *dhcpc/dhcps/dhcpv6c/dhcpv6s*
 - [Initial value]: -
- *filter_list*
 - [Setting value]: List of filter numbers registered with the **ip filter** command
 - [Initial value]: -
- *option*
 - [Setting value]:
 - syslog=*switch*

Setting value	Description
on	Keep the communication history of a connection in SYSLOG
off	Do not keep the communication history of a connection in SYSLOG

- *timeout=time*

Setting value	Description
time	The number of seconds it takes to release connection information when data stops flowing

- [Initial value]: syslog=on

Description

A dynamic filter is defined. In the first format, an application name registered with a router in advance is specified. In the second format, a user describes an access control rule. After the keywords filter, in, and out, a filter number defined by the **ip filter** command is set.

When a connection (trigger) corresponding to the filter described after the filter keyword is detected, thereafter, the connection corresponding to the filter described after the in keyword and the out keyword is passed. The in keyword controls access in the reverse direction with respect to the trigger direction, and the out keyword controls access in the same direction as a dynamic filter. The IP address of the **ip filter** command is ignored. The arguments pass/reject are also ignored.

If tcp or udp is specified as a protocol, processing specific to an application is not performed. If it is necessary to handle a specific application, specify the application name.

[Notes]

src_addr and dstaddr can also mix mnemonics representing IP addresses, FQDNs, map-e, hb46pp, and application names.

Specifying an FQDN for *srcaddr* and *dstaddr* is not possible with RTX5000 / RTX3500 Rev. 14.00.25 or earlier, RTX1210 Rev. 14.01.25 or earlier, and RTX830 Rev. 15.02.02 or earlier.

Specifying map-e for *srcaddr* and *dstaddr* is not possible with vRX series, RTX5000 / RTX3500 Rev. 14.00.31 or earlier, RTX1210 Rev. 14.01.39 or earlier, and RTX830 Rev. 15.02.19 or earlier.

Specifying an hb46pp for *src_addr* and *dstaddr* is not possible with vRX series, RTX5000, RTX3510 Rev. 23.01.01, RTX3500, RTX1300 Rev. 23.00.11 or earlier, RTX1220 Rev. 15.04.06 or earlier, RTX1210, and RTX830 Rev. 15.02.30 or earlier.

Designations of mnemonics representing application names for *src_addr* and *dstaddr* are not possible with vRX series, RTX5000,

not possible with RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, and RTX830.

For the mnemonics representing application names, specify the mnemonics described in a communication destination list. In the following states, the mnemonics representing application names are not evaluated.

- When the LBO state is not "normal operation"
- When the specified mnemonics are not included in the communication destination list

[Configuration Example]

```
# ip filter 10 pass * * udp * snmp
# ip filter dynamic 1 * * filter 10
```

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.15 Setting a dynamic filter timeout

[Format]

ip filter dynamic timer *option=timeout* [*option=timeout...*]

no ip filter dynamic

timer

- *option* : Option name
- [Setting value]:

Setting value	Description
tcp-syn-timeout	If a connection is not established within the set time after receiving a SYN, disconnect the session
tcp-fin-timeout	If the set time passes after receiving a FIN, the connection is forcibly released

Setting value	Description
tcp-idle-time	Disconnects a connection if no TCP connection data flows within the set time.
udp-idle-time	Disconnects a connection if no UDP connection data flows within the set time.
dns-timeout	Disconnects a connection if no response is received within the set time after receiving a DNS request.

- [Initial value]:
 - tcp-syn-timeout=30
 - tcp-fin-timeout=5
 - tcp-idle-time=3600
 - udp-idle-time=30
 - dns-timeout=5
- *timeout*
 - [Setting value]: Waiting time (seconds)
 - [Initial value]: -

[Explanation]

Timeout of a dynamic filter is set.

[Notes]

This setting is commonly used in all inspections.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.16 Setting a cache timer used by an FQDN filter

[Format]

ip filter fqdn timer *time* [auto=*switch*]

no ip filter fqdn timer [*time*]

[Setting value and initial value]

- *time*
 - [Setting value]: Number of seconds (1..2147483647)
 - [Initial value]: 600
- *switch*
 - [Setting value]:

Setting value	Explanation
on	Use automatic setting
off	Do not use automatic setting

- [Initial value]: on

[Explanation]

Set a timer of a cache used by an FQDN filter.

When an FQDN is set for a start point address and an end point address in the **ip filter** command and the **ipv6 filter** command, a timer operates when communication matching the specified FQDN occurs. If there is no communication matching the FQDN filter for the number of seconds specified in *time*, a cache associating an FQDN with an IP address is deleted.

When auto=on, the timer is set to the following values.

- When communication using a fast path, the largest value among timers used in a fast path flow table is automatically set as the value of this timer.
- When communication does not use a fast path, the *time* value is set as a timer.

When auto=off, the *time* value is always set as a timer.

[Notes]

RTX5000 is Rev. 14.00.26 or later, RTX3500 is Rev. 14.00.26 or later, RTX1210 is Rev. 14.01.26 or later, RTX830 is Rev. 15.02.03
It can be used after that.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.17 Setting operation of intrusion detection function**[Format]**

ip interface intrusion detection direction [*type*] *switch* [*option*]
ip pp intrusion detection direction [*type*] *switch* [*option*]
ip tunnel intrusion detection direction [*type*] *switch* [*option*]
no ip interface intrusion detection direction [*type*] *switch* [*option*]
no ip pp intrusion detection direction [*type*] *switch* [*option*]
no ip tunnel intrusion detection direction [*type*] *switch* [*option*]

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *direction*: The direction of the packet connection to be observed
 - [Setting value]:

Setting value	Description
in	Interface facing outward
out	Interface facing outward

- [Initial value]: -
- *type*: The type of packet connection to be observed
 - [Setting value]:

Setting value	Description
ip	IP header
ip-option	IP option header
fragment	Fragment
icmp	ICMP
udp	UDP
TCP	TCP
ftp	FTP
winny	Winny
share	Share (Not available for vRX series)
Default	Anything not available

- [Initial value]: -
- *switch*
 - [Setting value]:

Setting value	Description
on	Doing
off	Do not do

- [Initial value]:
 - If TYPE is not available=off
 - If TYPE is available=on
- *option*

- [Setting value]:

Setting value	Description
reject=on	Discard malformed packets
reject=off	Discard malformed packets

- [Initial value]: off

Description

Anomalies are detected for the specified direction of packets and connections at the specified interface. If the *type* option is omitted, settings for the intrusion detection function as a whole are made.

Notes

For attacks with high risk, packets are always discarded regardless of the reject option setting.

Regarding Share, version 2 detection is available and previous versions are not supported.

Regarding Share, version 1.0 EX2 (ShareTCP version) detection is available and previous versions are not supported.

Applicable models

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.18 Setting the frequency of notification of intrusion detection information per second

[Format]

ip interface intrusion detection notice-interval frequency

ip pp intrusion detection notice-interval frequency

ip tunnel intrusion detection notice-interval frequency

no ip interface intrusion detection notice-interval no ip pp intrusion detection notice-interval

no ip tunnel intrusion detection notice-interval

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *frequency*
 - [Setting value]: Frequency (1...1000)
 - [Initial value]: 1

[Explanation]

Setting the frequency of notification of intrusion detection information per second

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.19 Setting notification suppression of duplicate intrusion detection information

[Format]

```
ip interface intrusion detection repeat-control time
ip pp intrusion detection repeat-control time
ip tunnel intrusion detection repeat-control
time no ip interface intrusion detection
repeat-control no ip pp intrusion detection
repeat-control
no ip tunnel intrusion detection repeat-control
```

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *time*
 - [Setting value]: Number of seconds (1...1000)
 - [Initial value]: 60

[Explanation]

Setting notification suppression to notify the same kind of attack against the same host only once per *time second*

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.20 Setting the maximum number of intrusion detection information displayed

[Format]

```
ip interface intrusion detection report num
ip pp intrusion detection report num
ip tunnel intrusion detection report
num no ip interface intrusion
detection report no ip pp intrusion
detection report
no ip tunnel intrusion detection report
```

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *num*
 - [Setting value]: Number of cases (1...1000)
 - [Initial value]: 50

[Explanation]

Setting the maximum number of intrusion **detection** information displayed by a **show ip intrusion detection** command

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.21 Setting MSS limits for TCP sessions

[Format]

```
ip interface tcp mss limit mss
ip pp tcp mss limit mss
```

ip tunnel tcp mss limit mss
no ip interface tcp mss limit [mss]
no ip pp tcp mss limit [mss]
no ip tunnel tcp mss limit [mss]

[Set value and initial value]

- *interface*
 - [Set value]:
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *mss*
 - [Set value]:

Set value	Description
536..1460	Maximum MSS length
Auto	Automatic setting
off	Not set

- [Initial value]:
 - auto (vRX series, RTX5000/RTX3500 Rev.14.00.22 or later, RTX1210 Rev.14.01.26 or later, RTX830 Rev.15.02.03 or later, Rev.15.04 or later)
 - off (other than above)

Description

Limit MSS of TCP sessions passing through the interface TCP packets passing through the interface are monitored, and if the value of the MSS option exceeds the set value, it is rewritten to the set value. When a keyword "auto" is specified, in the case of an MTU of an interface or a PP interface, if the other party's MRU value is known, it is rewritten to the calculated value from that MRU value.

[Note]

For PP interfaces for PPPoE, the **pppoe tcp mss limit** command can also limit MSS of TCP sessions. If both this command and the **pppoe tcp mss limit** command are enabled, the MSS is limited to the smaller value.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.22 Changing the TCP window scale option

Format

ip interface tcp window-scale sw
ip pp tcp window-scale sw
ip tunnel tcp window-scale sw
no ip interface tcp window-scale [...]
no ip pp tcp window-scale [...]
no ip tunnel tcp window-scale [...]

[Set value and initial value]

- *interface*
 - [Set value]:
 - WAN interface name
 - WAN interface name
 - Not available for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *SW*

- [Set value]:

Set value	Explanation
off	Do nothing
Remove	Remove the TCP window scale option

- [Initial value]: off

Description

Forcibly changing the window scale option of TCP packets passing through the interface.
If remove is specified, it is disabled and transferred if the window scale option was enabled.

[Note]

RTX5000 and RTX3500 can be used after Rev.14.00.21.
RTX1210 can be used after Rev.14.01.16.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.23 Setting the number of TCP sessions at which the router ends

[Format]

tcp session limit *limit*

no tcp session limit [*limit*]

[Setting value and initial value]

- *limit*: Limit value
- [Setting value]:

Setting value	Description
32-65535	Number of sessions
None	No limit

- [Initial value]:
 - 15000 (RTX5000 / RTX3500 Rev.14.00.12 以降、Rev.14.01 系以降)
 - 1000 (other than the above)

Description

Limit the number of TCP sessions at which the router ends.
When none is selected, no limit is set.

[Notes]

This restriction does not apply when there is no direct communication with the router.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.24 Setting whether to log when there is a change in IPv4 route information

[Format]

ip route change log *log*

no ip route change log [*log*]

[Setting value and initial value]

- *log*
- [Setting value]:

Setting value	Description
on	Logging Changes in IPv4 Routes

Setting value	Description
off	Do not log changes in IPv4 routes

- No setting: No setting: No setting: No setting: No setting: No setting

Description

Setting whether to log when there is a change in IPv4 route information Logs are recorded at the INFO level.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.25 Setting Security by Filtering

[Format]

```
ip interface secure filter direction [filter_list...] [dynamic filter_list...]
ip pp secure filter direction [filter_list...] [dynamic filter_list...]
ip tunnel secure filter direction [filter_list...] [dynamic filter_list...]
ip interface secure filter name set_name
ip pp secure filter name set_name
ip tunnel secure filter name set_name
no ip interface secure filter direction [filter_list]
no ip pp secure filter direction [filter_list]
no ip tunnel secure filter direction
[filter_list] no ip interface secure filter
name [set_name] no ip pp secure filter
name [set_name]
no ip tunnel secure filter name [set_name]
```

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Cannot be specified for vRX series
 - LOOPBACK interface name
 - NULL interface name
 - Bridge interface name
 - [Initial value]: -
- *direction*
 - [Setting value]:

Setting value	Description
in	Filtering received packets
out	Filtering packets to send

- [Initial value]: -
- *filter_list*
 - [Setting value]: Filter numbers separated by spaces (as the sum of the number of static and dynamic filters) up to 300 for vRX series, RTX5000, RTX3510, and RTX3500, and up to 129 for other models)
 - [Initial value]: -
- *set_name*
 - [Setting value]: String representing the name of a filter set
 - [Initial value]: -
- *dynamic*: Describe the dynamic filter number after the keyword
 - [Initial value]: -

[Explanation]

Packet filtering by the **ip filter** command is combined to limit the types of packets to be sent and received on the interface

In a format specifying a direction, filter columns to be applied to each direction are specified by filter numbers. Filters with the specified number are applied in order, and if a filter matching the packet is found, it is passed/discarded by the filter. Filters after that can not be examined. Packets that do not match all filters are discarded.

In a format specifying the name of a filter set, the specified filter set is applied. The order in which filters are examined follows the format specifying the direction. If a filter set name that is not defined is specified, the filter behaves as if it was not set.

[Notes]

Filter lists are scanned, and if there is a match, it is passed/discarded.

```
# ip filter 1 pass 192.168.0.0/24 *
# ip filter 2 reject 192.168.0.1
# ip lan1 secure filter in 1 2
```

In this setting, packets whose starting IP address is 192.168.0.1 are not examined by filter 2 because passing is determined by the first filter 1. Therefore, filter 2 has no meaning.

Packets that do not match any filters as a result of manipulating the filter list are discarded.

When using RADIUS for authentication with PP Anonymous, if an Access-Response sent from a RADIUS server has the attribute 'Filter-Id', the specified filter set is applied to that value, and the setting of the **ip pp secure filter** command is ignored.

However, if the attribute "Filter-Id" does not exist, the setting of the **ip pp secure filter** command is used as a filter.

Dynamic filters cannot be used with the LOOPBACK and NULL interfaces.

Direction cannot be specified as 'in' with the NULL interface.

Bridge interfaces cannot be specified for vRX Amazon EC2 version and RTX5000/RTX3500 Rev.14.00.11 or earlier.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.26 Setting whether to rewrite the DFbit of an IPpacket that matches a rule to 0

[Format]

ip fragment remove df-bit rule

no ip fragment remove df-bit [rule]

[Setting value and initial value]

- rule*

- [Setting value]:

Setting value	Explanation
filter <i>filter_num</i>	<i>filter_num</i> is the filter number registered with the ip filter command.

- [Initial value]: -

[Explanation]

Forwarding IP packets that match a *rule* rewrite the DF bit to 0.

[Notes]

The DF bit is used in a path MTU search algorithm, but if there is a firewall that filters ICMP packets in the middle of a path, the algorithm may not work properly, and communication may not be possible only with a specific communication partner. Such a phenomenon is called "Path MTU Discovery Blackhole". If this path MTU search blackhole exists, if the DF bit is rewritten to 0 for communication with such a partner with this command, the path MTU search will not work properly, but it will not become impossible to communicate.

[Applicable model]

[Version] vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.27 Setting Up the TOS Field of an IP Packet

[Format]

ip tos supersede *id tos* [precedence=*precedence*] *filter_num* [*filter_num_list*]
no ip tos supersede *id* [*tos*]

[Setting Value and Initial Value]

- *id*
 - [Setting Value]: Identification Number (1..65535)
 - [Initial Value]: -
- *tos*
 - [Setting Value]:
 - TOS Value to be Rewritten (0..15)
 - The following mnemonics are available

Mnemonic	TOS Value
normal	0
min-monetary-cost	1
max-reliability	2
max-throughput	4
min-delay	8

- [Initial Value]: -
- *Precedence*
 - [Setting Value]:
 - precedence Value (0..7)
 - If precedence is omitted, the PRECEDENCE Value is not changed
 - [Initial Value]: -
- *filter_num*
 - [Setting Value]: Static Filter Number (1..21474836)
 - [Initial Value]: -
- *filter_num_list*
 - [Setting Value]: Static Filter Number (1..21474836)
 - [Initial Value]: -

[Description]

When an IP packet is relayed, the TOS Field is rewritten to the specified value.

The list is checked in order of identification number, and filters in the *filter_num* list are successively applied. If the first matched IP filter is pass, pass-log, pass-nolog, restrict, restrict-log, or restrict-nolog, the TOS Field is rewritten.

If reject, reject-log, or reject-nolog, the process ends without rewriting.

If the conditions are the same between the **ip dscp supersede** command setting and this command setting, the **ip dscp supersede** command setting takes precedence.

[Applicable Model]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.28 Setting Surrogate ARP

[Format]

IP Interface Proxyarp

ip interface proxyarp vrrp vrid

no ip interface proxyarp [proxyarp]

[Setting Value and Initial Value]

- *interface*
 - [Setting Value]: LAN Interface Name, Bridge Interface Name
 - [Initial Value]: -
- *proxyarp*
 - [Setting Value]:

Setting Value	Explanation
on	Surrogate ARP Operation
off	Surrogate ARP Operation

- [Initial Value]: off
- *vrid*
 - [Setting value]: VRRP group ID (1..255)
 - [Initial value]: -

[Explanation]

Whether to perform proxy ARP operation is set. When on is set, proxy ARP operation is performed. The MAC address used at this time becomes the real MAC address of the LAN interface. When a bridge interface is specified, whether to perform proxy ARP operation in the real LAN interface housed in the bridge interface is set. The MAC address used at this time becomes the MAC address of the real LAN interface which received an ARP.

When the second format is set, proxy ARP operation is performed only when the state of VRRP in the specified VRID is a master. The MAC address used becomes the virtual MAC address of the specified VRID.

[Notes]

The second format cannot be used in vRX Amazon EC2 version and vRX Sakura cloud version.

The bridge interface cannot be specified in vRX Amazon EC2 version and RTX5000 / RTX3500 Rev.14.00.11 or earlier.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.29 Setting the lifetime of an ARP entry

[Format]

ip arp timer *timer* [retry]
no ip arp timer [*timer* [retry]]

[Setting value and initial value]

- *timer*
 - [Setting value]: Number of seconds of lifetime of an ARP entry (30..32767)
 - [Initial value]: 1200
- *retry*
 - [Setting value]: Number of times an ARP request is retransmitted (4..100)
 - [Initial value]: 4

[Explanation]

Setting the lifetime of an ARP entry A pair of IP address and MAC address obtained by the ARP procedure is stored as an ARP entry, but after the time set by this command elapses, the ARP procedure is executed again, and if there is no response to the ARP, the entry is deleted.

The *retry* parameter can be used to set the number of times an ARP request is retransmitted. The retransmission interval of an ARP request is initially two seconds, and then one second.

The *retry* parameter does not normally need to be changed from the initial value.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.30 Setting a static ARP entry

[Format]

ip interface arp static ip_address mac_address [mtu=mtu]

no ip interface arp static ip_address [...]

[Setting value and initial value]

- *interface*
 - [Setting value]: Name of the LAN interface
 - [Initial value]: -
- *ip_address*
 - [Setting value]: IP address
 - [Initial value]: -
- *mac_address*
 - [Setting value]: Name of the MAC address
 - [Initial value]: -
- *mtu*
 - [Setting value]:

Setting value	Description
interface	Using the MTU value of the interface
discovery	Using the MTU search function to set a value
64..9578 (LAN interface of RTX5000, RTX3500) Su)	MTU value
64..10218 (LAN interface of RTX5000, RTX1300) Su)	
64..1500 (other than above)	

- [Initial value]: -

[Description]

The ARP entry is set statically. The ARP entry configured with this command is not deleted when the **show arp** command executes the MTU search function.

'permanent' is displayed, and it is always enabled. Also, the entry does not disappear even if the **clear arp** command is executed.

When discovery is set to the *mtu* option, the MTU search function by ARP operates.

When the *mtu* option is omitted, the MTU of the interface is used fixedly.

[Notes]

The *mtu* option can be specified for RTX5000, RTX3510, RTX3500, and RTX1300.

When discovery is set to the *mtu* option, it is necessary to be in a state where communication with the target host is possible at the time of searching. Therefore, when communication is not possible at that time because the target host is not connected, the MTU search fails and the default value of 1500 bytes is used as the MTU.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

6.1.31 Controls the number of packets to be withheld before ARP is resolved

[Format]

ip interface arp queue length len

no ip interface arp queue length [len]

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -

- *Len*
 - [Setting value]: Queue length (0..10000)
 - [Initial value]:
 - 200 (models compatible with 1000BASE-T interface)
 - 40 (models compatible with fast pass function)
 - 200 (models not compatible with fast pass function)

[Description]

When an attempt is made to send a packet to a host whose ARP is not resolved, the MTU search function sets the maximum number of packets that can be withheld for transmission per interface until the ARP is resolved or it is determined that the ARP cannot be resolved due to a timeout.

0 When discovery is set, packets will not be withheld, so that if you ping an opponent whose ARP is not resolved, for example, the first
1 packets will fail.

[Notes]

In previous versions of this command, the maximum number of withheld packets was not set and could be withheld as much as possible.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840 and RTX830

6.1.32 Setting whether to log changes in ARP entries

[Format]

```
ip interface arp log switch
no ip interface arp log [switch]
```

[Setting value and initial value]

- *switch*
 - [Setting value]:

Setting value	Description
on	Record
off	Record not

- [Initial value]: off

[Description]

Setting whether to log changes in ARP entries

[Notes]

By executing `show log | grep ARP:`, you can check the history of past ARP entries.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840 and RTX830

6.1.33 Setting the priority of implicit routes

[Format]

```
ip implicit-route preference preference
no ip implicit-route preference [preference]
```

[Setting value and initial value]

- *preference*
 - [Setting value]: Priority of implicit routes (1..2147483647)
 - [Initial value]: 10000

[Explanation]

Setting the priority of implicit routes

The priority is indicated by an integer of 1 or more, and the higher the number, the higher the priority.

If an implicit route is different from a route obtained by the dynamic route control protocol or a static route set by the **ip route** command, the one with the higher priority is adopted. If the priority is the same as that of the static route, the static route is prioritized.

If the priority is the same as that of the route obtained by the dynamic route control protocol, the route adopted earlier in time becomes effective. Note that even if the priority of an implicit route is changed by the **ip implicit-route preference** command, the priority of an implicit route already registered in a routing table at that time is not changed.

[Notes]

An implicit route is a route through an interface for which an IP address has been set, which is implicitly registered when the interface becomes valid. For example, when a LAN interface for which an IP address has been set is in a link-up state, a network address determined from a combination of the set IP address and a netmask is registered as an implicit route through the LAN interface.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.34Set the lifetime of each entry in a flow table

[Format]

ip flow timer *protocol time*
no ip flow timer *protocol [time]*

[Setting value and initial value]

- protocol* : Protocol for specifying the lifetime
 - [Setting value]

Setting value	Explanation
tcp	TCP packet
udp	UDP packet
icmp	ICMP packet
slow	TCP packet set by the FIN/RST bit

- [Initial value]
 - tcp = 900
 - udp = 30
 - icmp = 30
 - slow =
 - 5 (other than the following)
 - 30 (vRX Amazon EC2 版、vRX VMware ESXi 版、RTX5000、RTX3500、RTX1300 Rev.23.00.04 以前、RTX1220, RTX1210, and RTX830 Rev. 15.02.26 or earlier)
- time*
 - Setting value: Number of seconds (1-21474836)
 - [Initial value] -

[Description]

Set the lifetime of each entry in a flow table for each protocol.

'slow' is applied to entries passed by FIN/RST.

If NAT or dynamic filters are used, the lifetime of those entries is applied.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.35 Setting the number of entries in a flow table

[Format]

ip flow limit *limit*

no ip flow limit [*limit*]

[Setting value and initial value]

- limit* : Limit of the number of entries

- [Setting value]:

Setting value	Explanation
10..1000000	vRX can be configured in normal mode for Amazon EC2, vRX can be configured in normal mode for VMware ESXi, vRX can be configured in cloud version for Sakura, and RTX3510
10..500000	Can be configured with RTX1300
10..300000	Can be configured with RTX840
10..131072	Can be configured with models other than the above

- [Initial value]:

- 1000000 (vRX can be configured in normal mode for Amazon EC2, vRX can be configured in normal mode for VMware ESXi, and RTX3510)
- 500000 (RTX1300)
- 300000 (RTX840)
- 131072 (other than the above)

Description

Sets the number of flow table entries that can be used for IPv4 fastpass or IPv6 fastpass respectively. Even when using the fastpass function, flows exceeding this limit value are processed by normal pass.

Notes

Not available for RTX5000 / RTX3500 Rev. 14.00.11 or earlier.

Applicable Model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.36 Set the time to be retained for reconfiguring fragment packets.

Format

ip reassembly hold-time *time*

no ip reassembly hold-time [*time*]

Set value and initial value

- time*

- Set value:

Set value	Description
Seconds (1 .. 255)	Time to be retained for reconfiguring fragment packets

- Initial value: 15 seconds

Description

Time to be retained for reconfiguring fragment packets of IPv4.

When reconfiguration is not possible even after the set time has elapsed, the packets that have been retained are discarded. Packets that have already been retained at command execution are not changed.

Notes

RTX5000 and RTX3500 can be used in Rev. 14.02.10 or later.

RTX1210 can be used in Rev. 14.02.10 or later.
RTX830 can be used in Rev. 15.02.10 or later.

Applicable Model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.1.37 Setting Up Rewriting of DSFields in IP Packets

Format

```
ip dscp supersede id dscp filter_num [filter_num_list]
no ip dscp supersede id [dscp]
```

Setup Values and Initial Values

- *id*
 - setup value: Identification number (1..65535)
 - initial value: -
- *dscp*
 - setup value:
 - DSCP value to be rewritten (0..63)
 - The following mnemonics are available

mnemonic	DSCP value
default	0
cs3	8
cs4	16
cs5	24
cs4	32
cs5	40
cs6	48
cs7	56
af11	10
af12	12
af 13	14
af 21	18
af 22	20
af 23	22
af 31	26
af 32	28
af 33	30
af 41	34
af 42	36
af 43	38
ef	46

- [Initial value]: -
- *filter_num*
 - set value: static filter number (1..21474836)
 - [Initial value]: -
- *filter_num_list*
 - set value: static filter number (1..21474836)

- [Initial value]: -

description

DS field is rewritten to a specified value when an IP packet is relayed.

The list is checked in order of identification numbers, and filters in the *filter_num* list are successively applied. If the first matched IP filter is pass, pass-log, pass-nolog, restrict, restrict-log or restrict-nolog, the DS field is rewritten.

If reject, reject-log or reject-nolog, processing ends without rewriting.

If conditions are the same between the setting of **ip tos supersede** and the setting of this command, the setting of this command takes precedence.

[Notes]

RTX5000 / RTX3500 Rev.14.00.33 or earlier, RTX1300 Rev.23.00.04 or earlier, RTX1220 Rev.15.04.04 or earlier, RTX1210 Rev.14.01.41

Not available before and RTX830 Rev.15.02.26 or earlier

[Applicable model]

vRX Sakura Cloud Edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840 and RTX830

6.2 PP side setting

6.2.1 PP side IP address setting

[Format]

ip pp remote address *ip_address*

ip pp remote address dhcp [*interface*]

no ip pp remote address [*ip_address*]

[Setting value and initial value]

- *ip_address*
- [Setting value]

Setting value	Explanation
IP address	xxx.xxx.xxx.xxx (where xxx is a decimal number)
dhcp	Keywords indicating use of a DHCP client

- Initial value: -
- dhcp : Keywords indicating use of a DHCP client
- Initial value: -
- *interface*
- [Setting value]
 - LAN interface name operating as a DHCP client
 - If omitted, use lan1
- Initial value: -

[Description]

Set the IP address of the selected party's PP side.

If you set dhcp, you must be operating as a DHCP server. Assign an IP address from the DHCP scope that you manage.

You can set up to the number of ISDN Bchs that can be used with the attached BRI/PRI interface.

If you set dhcp, the LAN interface specified on the *interface* acquires an IP address as a DHCP client and assigns it to the PP side. If it cannot be acquired, assign 0.0.0.0.

[Configuration Example]

Router A:

```
no ip pp remote address
ppp ipcp ipaddress on
```

and the router B side to be connected

```
ip pp remote address yyy.yyy.yyy.yyy
```

If you set dhcp, the actual IP address of router A on the PP side is "yyy.yyy.yyy".

[Applicable model]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.2.2 Remote IP Address Pool Configuration

[Format]

```
ip pp remote address pool ip_address [ip_address...]
```

```
ip pp remote address pool ip_address-ip_address
```

```
ip pp remote address pool dhcp
```

```
ip pp remote address pool dhcp [interface]
```

```
no ip pp remote address pool
```

[Setting value and initial value]

- *ip_address*
 - Setting value: An IP address to pool for anonymous.
 - [Initial value]: -
- *ip_address-ip_address*
 - Setting value: An IP address range.
 - [Initial value]: -
- dhcp: A keyword indicating that you are using your own DHCP server function.
 - [Initial value]: -
- dhcp: A keyword indicating that you are using a DHCP client.
 - [Initial value]: -
- *interface*
 - [Setting value]:
 - LAN interface name operating as a DHCP client.
 - If omitted, use lan1.
 - [Initial value]: -

[Description]

Set an IP address pool for anonymously assigning to the other party. It is valid only if anonymous is selected as the PP.

If you set dhcp, you must be operating as a DHCP server. Assign an IP address from the DHCP scope that you manage.

If you set dhcp, the LAN interface specified in *interface* acquires only IP address information as a DHCP client and assigns that address. If it cannot be acquired, assign 0.0.0.0.

[Note]

The number that can be set as an *ip_address* is as follows.

Model	Revisions	Maximum number that can be set
vRX Series	All revisions	1040
RTX5000	All revisions	3104
RTX3500	All revisions	1104
RTX3500	All revisions	1104
RTX1300	All revisions	101
RTX1220	All revisions	101

Models	Revisions	Maximum number that can be set
RTX1210	All revisions	103
RTX840	All revisions	32
RTX830	All revisions	32

[Supports extended licenses]

Importing an [extended license](#) expands the maximum number of IP addresses (*ip_addresses*) that can be pooled.

- *ip_address*

Licensed name	Maximum number after expansion (Value for each number of licenses)				
	1	2	3	4	5
YSL-VPN-EX1	101	-	-	-	-
YSL-VPN-EX2	301	501	701	901	1101
YSL-VPN-EX3	1541	2041	2541	3041	-

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.2.3 Time interval setting for keepalive over PP**[Format]**

pp keepalive interval *interval* [*retry-interval=retry-interval*] [*count=count*] [*time=time*]

no pp keepalive interval [*interval*] [*count*]

[Setting value and initial value]

- *Interval*
 - Time interval after which keepalive packets are sent (1..65535)
 - Default: 30
- *retry-interval*
 - Default:
 - Time interval after which keepalive packets are confirmed and failed once (1..65535)
 - If keepalive packets are confirmed, the transmission interval returns to *interval* again
 - Default: 1
- *count*
 - Default: If there is no response for this number of consecutive times, the router on the other side is judged to be down (3..100).
 - Default: 6
- *time*
 - Default:
 - Time interval after which keepalive packets are confirmed and failed until the router is judged to be disconnected ((*interval* + 1)..65535)
 - Cannot be specified at the same time as the *count* parameter.
 - [Initial value]: -

[Explanation]

Set the transmission interval of keepalive packets in the PP interface, and the number and time of retransmissions until it is determined that a line is disconnected.

Keepalive packets are transmitted at intervals specified by *interval* while a reply is received for the transmitted keepalive packets. When a reply cannot be confirmed once, the transmission interval is changed to the value of the *retry-interval* parameter. When a reply cannot be confirmed continuously for the number of times shown in the *count* parameter, it is determined that a line is disconnected.

When the time until line disconnection determination is specified by the *time* parameter, it is determined that a line is disconnected when a reply of the keepalive packet cannot be confirmed continuously for at least the specified time.

[Notes]

When the *time* parameter is specified, the value is recalculated according to the keepalive interval and the number of times of retransmission, so that a value different from the set value may be displayed in **show config**.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.2.4 Setting whether to use keepalive via PP**[Format]**

pp keepalive use lcp-echo

pp keepalive use icmp-echo dest_ip [option=value...] [dest_ip [option=value...]...]

pp keepalive use lcp-echo icmp-echo dest_ip [option=value...] [dest_ip [option=value...]...]

pp keepalive use off

no pp keepalive

use [Set value and**initial value]**

- lcp-echo: Use LCP Echo Request/Reply
 - [Initial value]: -
- lcp-echo: Use ICMP Echo/Reply
 - [Initial value]: -
- dest_ip
 - no pp keepalive check destination IP address
- [Initial value]: -
- option=value column
 - [Set value]:

option	value	Explanation
upwait	millisecond	Allowable response time for down detection (1..10000)
downwait	millisecond	Allowable response time for down detection (1..10000)
disconnect	second	no response disconnect time (1..21474836)
length	Byte	length of ICMP Echo packet (64-1500)

- [Initial value]: -

[Initial Setting]

pp keepalive use off

[Explanation]

Keepalive operation of connection to selected destination is set.

LCP Echo Request/Reply is used with lcp-echo specification, and ICMP Echo/Reply is also used at the same time if icmp-echo is also specified. When using icmp-echo, it is necessary to set an IP address.

[Notes]

Even if this command is not set, keepalive by LCP Echo is executed if it is set to on with the **pp always-on** command.

The route to the IP address to be checked with icmp-echo must be set so that the configured PP interface is sent.

When response time is limited with the downwait parameter, if the set value of the **pp keepalive interval** command is smaller, the set value of the **pp keepalive interval** command takes precedence. When only one of downwait and upwait parameters is set, the other operates as if the same value was set.

The disconnect parameter is used when reconnection at PPPoE level is required when using with PPPoE. When the disconnect parameter is set, if there is no response from icmp-echo within the set time, disconnect operation is performed once at the PPPoE level, so that reconnection can be performed in combination with the **pp always-on** command.

When other parameters are default values, if the disconnect parameter is set to about 70 seconds, disconnect operation after down detection is surely performed.

The length parameter specifies the length of the ICMP data portion, not the length of the entire IP packet.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.2.5 Setting whether to log keepalives via PP

[Format]

pp keepalive log *log*

no pp keepalive log [*log*]

[Setting value and initial value]

- *log*
- [Setting value]:

Setting value	Description
on	Logging
off	Logging

- [Initial value]: off

[Explanation]

Whether to log keepalives via PP is set.

[Notes]

This setting is commonly used for all PPs.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3 Setting RIP

6.3.1 Setting whether to use RIP

[Format]

Rip use *use*

no rip use

[Setting value and initial value]

- *Use*
- [Setting value]:

Setting value	Description
on	Using RIP
off	Do not use RIP

- [Initial value]: off

[Explanation]

Whether to use RIP is set. When this function is turned off, RIP packets are not sent to all interfaces and received RIP packets are ignored.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.2 Setting up trusted gateways for RIP

[Format]

ip interface rip trust gateway [*except*] *gateway* [*gateway*...]

ip pp rip trust gateway [*except*] *gateway* [*gateway*...]

ip tunnel rip trust gateway [*except*] *gateway* [*gateway*...]

no ip interface rip trust gateway [[except] *gateway* [*gateway*...]]

no ip pp rip trust gateway [[except] *gateway* [*gateway*...]]

no ip tunnel rip trust gateway [[except] *gateway* [*gateway*...]]

[Setting value and initial value]

- *interface*
 - Setting value: IP address
 - [Initial value]: -
- *gateway*
 - Setting value: IP address
 - [Initial value]: -

[Explanation]

Setting up trusted or unreliable gateways for RIP

If the except keyword is not specified, the listed gateways are considered trustworthy and only RIPs from them are received.

If the except keyword is specified, the listed gateways are regarded as unreliable and only RIPs from other gateways excluding them are received.

Up to 10 *gateways* can be specified.

[Notebook]

Trusted or unreliable gateways are not set up and only RIPs from all hosts are treated as trustworthy.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.3 Setting the priority of a route by RIP

[Settings]

rip preference preference [invalid-route-reactivate=*switch*]

no rip preference [*preference* [invalid-route-reactivate=*switch*]]

[Settings and initial values]

- *preference*
 - [Settings]: 1 or more
 - [Settings]: 1000
- *switch*
 - [Settings]:

Settings	Description
on	Invalid routes derived from RIP are not deleted.
off	Invalid routes derived from RIP are deleted.

- [Settings]: off

[Explanation]

Priority of a route obtained by RIP is set. The priority of a route is expressed by a numerical value of 1 or more, and the higher the number, the higher the priority. When routes obtained by static and multiple protocols such as RIP are different, the route with the higher priority is adopted. When the priority is the same, a route adopted earlier in terms of time becomes effective.

When a route is received from another router by RIP and the same route is received by a routing protocol set with higher priority than RIP such as static or OSPF, the route received by RIP is usually invalidated and deleted, but when invalid-route-reactivate option is specified as *on*, a route derived from RIP that was invalidated when a route with high priority disappears is reactivated.

[Notes]

The priority of a static route is fixed at 10000.

When the invalid-route-reactivate option is specified as *on*, the originator of RIP does not advertise the reactivated route.

It is desirable to set the `invalid-route-reactivate` option to *off* because the route may continue to remain on the routing table.

The routes remaining in the routing table can be deleted by stopping use of RIP.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.4 Configuration for sending RIP packets

[Settings]

ip interface rip send send [version version [broadcast]]

ip pp rip send send [version version [broadcast]]

ip tunnel rip send send [version version [broadcast]]

no ip interface rip send [send...]

no ip pp rip send [send...]

no ip tunnel rip send [send...]

[Settings and initial values]

- interface*

- [Settings]: LAN interface name
- [Initial values]: -

- send*

- [Settings]:

Settings	Description
on	Sending RIP packets
off	Do not send RIP packets

- [Initial values]:

- off (for tunnel interfaces)
- on (for other interfaces)

- version*

- settings: Version of RIP to send (1,2)
- [Initial values]:
 - vRX Sakura Cloud Edition
 - 2 (LAN interfaces)
 - 1 (other interfaces)
 - Other models
 - 1

- broadcast*

- settings: Broadcast IP address specified by the **ip interface address** command
- [Initial values]: -

[Description]

Sets whether or not to send a RIP packet to a specified interface.

"version version" specifies the version of the RIP to be sent.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.5 Settings for receiving RIP packets

[Format]

ip interface rip receive receive [version version [version]]

ip pp rip receive receive [version version [version]]

ip tunnel rip receive receive [version version [version]]

no ip interface rip receive [receive...]

no ip pp rip receive [*receive...*]
no ip tunnel rip receive [*receive...*]

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
 - *receive*
 - [Setting value]:
- | Setting value | Description |
|---------------|----------------------------|
| on | Receive RIP packets |
| off | Do not receive RIP packets |
- [Initial value]:
 - off (for tunnel interface)
 - on (for other interfaces)
 - *version*
 - [Setting value]: Version of the RIP to be received (1,2)
 - [Setting value]: 1 2 (for other interfaces than tunnel interface)

[Description]

Set whether or not to receive a RIP packet for the specified interface.
 "version *version*" specifies the version of the RIP to be received. If not specified, both RIP1 and RIP2 are received.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.6 Setting RIP filtering

[Format]

ip interface rip filter direction *filter_list*
ip pp rip filter *direction filter_list*
ip tunnel rip filter *direction filter_list*
no ip interface rip filter direction [*filter_list*]
no ip pp rip filter *direction filter_list*
no ip tunnel rip filter *direction filter_list*

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
 - *direction*
 - [Setting value]:
- | Setting value | Description |
|---------------|------------------------------|
| in | Filtering of received RIPs |
| out | Filtering of RIPs to be sent |
- [Initial value]: -
 - *filter_list*
 - Setting value: A sequence of static filter numbers separated by spaces (up to 100)
 - [Initial value]: -

[Description]

Set filtering of RIPs to be sent and received in the interface.

If the starting IP address of the filter set by the **ip filter command** matches the route information of the RIPs to be sent and received, if the filter is pass, it is processed, and if it is reject, only the route information is discarded.

[Applicable model]

[Settings] vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.7 Setting the number of hops to be added by RIP

[Settings]

```
ip interface rip hop direction hop
ip pp rip hop direction hop
ip tunnel rip hop direction hop
no ip interface rip hop direction hop
no ip pp rip hop direction hop
no ip tunnel rip hop direction hop
```

[Settings and initial values]

- *interface*
 - [Settings]: LAN interface name
 - [Initial values]: -
- *direction*
 - [Settings]:

Settings	Description
in	Add to the received RIP
out	Add to the RIP to be sent

- [Initial values]: -
- *hop*
 - Settings: Value to be added (0..15)
 - [Initial values]: 0

[Explanation]

Set the number of hops to be added to the RIP to be sent and received by the interface.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.8 Setting up authentication in RIP2

[Settings]

```
ip interface rip auth type type
ip pp rip auth type type
ip tunnel rip auth type type
no ip interface rip auth type [type]
no ip pp rip auth type [type]
no ip tunnel rip auth type [type]
```

[Settings and initial values]

- *interface*
 - [Settings]: LAN interface name
 - [Initial values]: -
- *type*
 - [Settings]:

Settings	Description
text	Perform text-type authentication

- [Initial values]: -

[Explanation]

Set authentication in the interface when using RIP2. Perform text-type authentication in the case of text.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.9Setting up authentication keys in RIP2

[Settings]

```
ip interface rip auth key hex_key
ip pp rip auth key hex_key
ip tunnel rip auth key hex_key
ip interface rip auth key text text_key
ip pp rip auth key text text_key
ip tunnel rip auth key text text_key
no ip interface rip auth
key no ip pp rip auth key
no ip tunnel rip auth key
no ip interface rip auth key
text no ip pp rip auth key
text
no ip tunnel rip auth key text
```

[Setting value and initial value]

- interface
 - [Setting value]: LAN interface name
 - [Initial value]: -
- hex_key
 - [Setting value]: Authentication key expressed as a column of hexadecimal numbers
 - [Initial value]: -
- text_key
 - [Setting value]: Authentication key expressed as a string
 - [Initial value]: -

[Explanation]

When using RIP2, an authentication key of an interface is set.

[Configuration Example]

```
# ip lan1 rip auth key text testing123
# ip pp rip auth key text "hello world"
# IPLAN2RIPAUTHKEY0102FF358E49A83A5E9D
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.10Setting the advertising operation mode in RIP2

[Format]

```
rip advertise mode mode
no rip advertise mode [mode]
```

[Setting value and initial value]

- Mode
 - [Setting value]:

Setting value	Explanation
1	If the network address to which the transmission interface of RIP belongs matches the destination network address of an advertisement route and the subnet mask is different, the advertisement route is not set.

Setting value	Explanation
2	If the network address to which the transmission interface of RIP belongs matches the destination network address of an advertisement route and the subnet mask is different, the advertisement route is set.

- [Initial value]:
 - 2 (RTX3510, RTX1300, RTX840)
 - 1 (other than above)

[Explanation]

If the network address to which the transmission interface of RIP belongs matches the destination network address of an advertisement route and the subnet mask is different in RIP2, the advertisement operation of the route is changed according to the setting value of *mode*.

Revisions that do not support this command operate when the setting value of *mode* is 1.
The operation of RIP1 is not affected.

[Notes]

RTX5000 can be used with Rev.14.00.32
or later RTX3500 can be used with
Rev.14.00.32 or later RTX1210 can be
used with Rev.14.01.36 or later RTX830
can be used with Rev.15.02.15 or later

[Applicable model]

vRX VMware ESXi Edition, vRX Sakura Cloud Edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.11 Setting of route retention when the line is disconnected**[Format]**

```
ip pp rip hold routing rip_hold
no ip pp rip hold routing [rip_hold]
```

[Setting value and initial value]

- *rip_hold*
- [Setting value]:

Setting value	Explanation
on	Continue to maintain the route by RIP when the line is disconnected
off	If the line is disconnected, the route by RIP is discarded.

- [Initial value]: off

Explanation

Whether to continue to maintain the route obtained by RIP from the PP interface when the line is disconnected is set.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.12 Setting of RP operation on PPside when the line is connected**[Format]**

```
ip pp rip connect send rip_action
no ip pp rip connect send [rip_action]
```

[Setting value and initial value]

- *rip_action*
- [Setting value]:

Setting value	Description
Interval	ip pp rip connect interval Sends a RIP at the time interval set by the command.
Update	Sends a RIP only when the route information changes.
None	Do not send a RIP

- [Initial value]: update

[Explanation]

Set conditions for sending a RIP at the time of line connection for a selected party.

[Configuration Example]

```
# ip pp rip connect interval 60
# ip pp rip connect send interval
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.13 Set the time interval for sending a RP on the PPside at the time of line connection

[Format]

ip pp rip connect interval *time*
no ip pp rip connect interval [*time*]

[Setting value and initial value]

- *time*
 - [Setting value]: Number of seconds (30..21474836)
 - [Initial value]: 30

[Explanation]

Set the time interval for sending a RIP at the time of line connection for a selected party.

The commands **ip pp rip send** and **ip pp rip receive** are valid when on, and the command **ip pp rip connect send** is valid when interval.

[Configuration Example]

```
# ip pp rip connect interval 60
# ip pp rip connect send interval
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.14 Set the behavior of RP on the PPside at the time of line disconnection

[Format]

ip pp rip disconnect send *rip_action*
no ip pp rip disconnect send [*rip_action*]

[Setting value and initial value]

- *rip_action*
 - [Setting value]:

Setting value	Description
None	Do not send a RIP at the time of line disconnection
Interval	Send a RIP at the time interval set by the command ip pp rip disconnect interval
Update	Send a RIP only when the route information changes

- [Initial value]: none

[Explanation]

Set the condition for sending a RIP at the time of line disconnection for a selected party.

[Configuration Example]

```
# ip pp rip disconnect interval 1800
# ip pp rip disconnect send interval
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.15 Set the time interval for sending a RP on the PPside at the time of line disconnection

[Format]

ip pp rip disconnect interval *time*

no ip pp rip disconnect interval [*time*]

[Setting value and initial value]

- *time*
 - [Setting value]: Number of seconds (30..21474836)
 - [Initial value]: 3600

[Explanation]

Set a time interval for sending RIP when a line is disconnected for a selected party.

It is valid when the **ip pp rip send** and **ip pp rip receive** commands are on, and the **ip pp rip disconnect send** command is interval.

[Configuration Example]

```
# ip pp rip disconnect interval 1800
# ip pp rip disconnect send interval
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.16 Setting of source interface switching of RP during backup

[Format]

ip pp rip backup interface *switch*

no ip pp rip backup interface

[Setting value and initial value]

- *switch*
 - [Setting value]:

Setting value	Explanation
on	Switch
off	Do not switch

- [Initial value]: off

[Explanation]

Whether to switch the source interface of RIP during backup is set. The source interface of RIP is the backup source interface when it is off, and becomes the backup destination interface when it is on.

[Notes]

The difference between them appears as a difference in the IP address of the source. The address of the backup source interface is selected when it is off, and the address of the backup destination interface is selected when it is on. In either case, RIP is transmitted through the backup line.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.17 Advertising routes forcibly with RIP

[Format]

```
ip interface rip force-to-advertise ip-address/netmask [metric metric]
ip pp rip force-to-advertise ip-address/netmask [metric metric]
ip tunnel rip force-to-advertise ip-address/netmask [metric metric]
no ip interface rip force-to-advertise ip-address/netmask [metric metric]
no ip pp rip force-to-advertise ip-address/netmask [metric metric]
no ip tunnel rip force-to-advertise ip-address/netmask [metric metric]
```

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *ip-address/netmask*
 - [Setting value]: Network address and netmask length of routes forcibly advertised, or 'default'
 - [Initial value]: -
- *metric*
 - [Setting value]: Metric value for advertising (1-15)
 - [Initial value]: -

[Description]

Even if the set route does not exist in the route table, the route is forcibly advertised with RIP to the specified interface. If 'default' is specified as the route, the default route is advertised.

[Configuration Example]

Only some hosts of LAN2 are advertised on the LAN1 side.

```
ip lan1 address 192.168.0.1/24 ip lan2
address 192.168.1.1/24
```

```
rip use on
rip filter rule with-netmask ip lan1 rip
send on version 2
ip lan1 rip receive on version 2
```

```
ip filter 1 reject 192.168.1.0/24 ip filter 100
pass *
ip lan1 rip filter out 1 100
```

```
ip lan1 rip force-to-advertise 192.168.1.28/30 ip lan1 rip force-to-
advertise 192.168.1.100/32 ip lan1 rip force-to-advertise
192.168.1.101/32
```

[Applicable model]

[Model No.] vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.18 How to Compare Filters in RIP2

[Format]

```
rip filter rule rule
no rip filter rule [rule]
```

[Setting value and initial value]

- *rule*
 - [Setting value]:

Setting value	Description
address-only	Only network addresses are compared

Setting value	Description
with-netmask	In the case of RIP2, network addresses and netmasks are compared

- [初期値] : address-only

[Explanation]

In the RIP filter, a comparison method between the set filter and the contents of an RIP entry is set.

The rip filter rule command	Protocol	Comparison method
address-only	RIP1	A netmask type filter is interpreted as a range specification, and whether or not the address part of an RIP entry is within that range is compared.
	RIP2	
with-netmask	RIP1	Whether or not the address of a netmask type filter matches the netmask, the address of an RIP entry, and the netmask is compared.
	RIP2	

[Applicable model]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.3.19 Adjusting the RIP timer

[Format]

rip timer update [*invalid* [*holddown*]]

no rip timer [*update*]

[Setting value and initial value]

- *update*
 - [Setting value]: Time between regular advertisement transmissions (10 to 60 seconds)
 - [Initial value]: 30 seconds
- *invalid*
 - [Setting value]: Time between when an advertisement is no longer accepted and when a route is deleted (20 to 360 seconds)
 - [Initial value]: update x 6 (180 seconds)
- *holddown*
 - [Setting value]: Time to advertise a route with metric 16 when a route is deleted (20 to 240 seconds)
 - [Initial value]: update x 6 (180 seconds)

[Explanation]

Set the timer value of RIP.

The following inequality must exist between the values of *update*, *invalid*, and *holddown*.

$$\begin{aligned} \text{update} \times 3 &\leq \text{invalid} \leq \text{update} \times 6 \\ \text{update} \times 2 &\leq \text{holddown} \leq \text{update} \times 4 \end{aligned}$$

[Notes]

When the **ip pp rip connect/disconnect interval** command is set for a PP interface, the setting value of that command takes precedence over the **rip timer** command. However, the **ip pp rip connect/disconnect interval** command affects the values of the *update* timer and *invalid* timer, but does not affect the value of the *holddown* timer. When the setting value of the **ip pp rip connect/disconnect interval** command is T, each timer is as follows.

<i>update</i>	T
<i>invalid</i>	T x 6
<i>holddown</i>	rip timer command setting value (default 120 seconds)

Since there is no corresponding command except for the PP interface, the setting value of the **rip timer** command is always valid.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.4Setting up VRRP

6.4.1Setting up VRRP for each interface

[Format]

```
ip interface vrrp vrid ip_address [priority=priority] [preempt=preempt] [auth=auth] [advertise-interval=time1] [down-interval=time2]
no ip interface vrrp vrid [vrid...]
```

[Setting value and initial value]

- interface
 - [Setting value]: LAN interface name
 - [Setting value]: -
- vrid
 - [Setting value]: VRRP group ID (1..255)
 - [Setting value]: -
- ip_address
 - [Setting value]: IP address of virtual router
 - [Setting value]: -
- priority
 - [Setting value]: Priority (1..254)
 - [Setting value]: 100
- preempt: Preempt mode
 - [Setting value]:

Setting value	Description
on	Use
off	Not used

- [Setting value]: on
- auth
 - [Setting value]: Text authentication string (up to 8 characters)
 - [Setting value]: -
- time1
 - [Setting value]: Interval between sending VRRP ads (1..60 seconds)
 - [Setting value]: 1
- time2
 - [Setting value]: Time until the master determines that it is down (3..180 seconds)
 - [Setting value]: 3

[Explanation]

Setting up to use a specified VRRP group
Routers belonging to the same VRRP group must match the IP address of VRID and virtual router. The behavior when these are different can not be predicted.
If the *auth* parameter is not specified, it behaves as no authentication.

The *time1* and *time2* parameters set the interval between sending VRRP ads by the master and the time until the backup monitors it and determines that it is down. In a network with a lot of traffic, setting these values longer than the initial value may stabilize the operation. These values must match all VRRP routers.

[Notes]

The *priority* and *preempt* parameters must be set to match the IP address of the virtual router to its own LAN interface.

If the given address is specified, it is ignored. In this case, the priority is the highest 255 and it always operates in preempt mode.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.4.2 Shutdown trigger setting

[Format]

```
ip interface vrrp shutdown trigger vrid interface
ip interface vrrp shutdown trigger vrid pp peer_num [dlci=dlci]
ip interface vrrp shutdown trigger vrid tunnel tunnel_num
ip interface vrrp shutdown trigger vrid route network [nexthop]
no ip interface vrrp shutdown trigger vrid interface
no ip interface vrrp shutdown trigger vrid pp peer_num
[...] no ip interface vrrp shutdown trigger vrid tunnel
tunnel_num no ip interface vrrp shutdown trigger vrid
route network
```

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *vrid*
 - [Setting value]: VRRP group ID (1..255)
 - [Initial value]: -
- *Peer_num*
 - [Setting value]: Destination information number
 - [Initial value]: -
- *dlci*
 - [Setting value]: DLCI number
 - [Setting value]: -
- *tunnel_num*
 - [Setting value]: Tunnel interface number
 - [Initial value]: -
- *network*
 - [Setting value]:
 - Network address
 - IP address/mask length
 - [Setting value]: -
 - [Initial value]: -
- *nexthop*
 - [Setting value]:
 - Interface name
 - IP address
 - [Setting value]: -

[Explanation]

When operating as a master router in a set VRRP group, it is configured to shut down according to the specified conditions.

Format	Description
LAN interface format	When the specified LAN interface links down or when down is detected by lan keepalive , it shuts down.

Format	Description
pp format	When communication becomes impossible on a line corresponding to the specified destination information number, it shuts down. When communication becomes impossible, it is determined that the layer 1 drops due to cable disconnection or the like, and in the following cases. • When the line is an ISDN line, if no call is connected • When the line is a leased line, if it is determined that the communication partner has fallen due to LCP keepalive • When the line is a frame relay and "dlci=<i>dlci</i>" is specified, if it is determined that the DLCI number specified by the PVC status check procedure cannot communicate • When down is detected by pp keepalive use setting
tunnel format	When the specified tunnel interface is down due to the following conditions, it shuts down. • When down is detected by pptp keepalive use setting in an IPsec tunnel • When down is detected by pptp keepalive use setting in any of the tunnels of L2TP/IPsec, L2TPv3, and L2TPv3/IPsec • When down is detected by pptp keepalive use setting in an IPsec tunnel • When down is detected by pptp keepalive use setting in an IPsec tunnel
Route format	When the specified route does not exist in a route table or is not suitable for an interface specified by <i>nexthop</i> or a gateway specified by an IP address, it shuts down. When <i>nexthop</i> is omitted, it does not shut down as long as the route faces any destination.

[Notebook]

Formats 3 and 7 are RTX5000/RTX3500 Rev.14.00.31 or earlier, RTX1210 Rev.14.01.27 or earlier, and RTX830 Rev.15.02.02

Previously unusable

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.5 Backup configuration

6.5.1 When provider connection is down, specify the connection destination to be PPbacked up

[Format]

```
pp backup none
pp backup pp peer_num [ipsec-fast-recovery=action]
pp backup interface
ip_address pp backup tunnel
tunnel_num no pp backup
```

[Setting value and initial value]

- none: Backup does not work
 - [Initial value]: none
- peer_num
- [Setting value]: Destination information number when using PP as a backup destination
 - [Initial value]: -
 - action: Whether to rebuild SA immediately after returning from backup
 - [Setting value]:

Setting value	Description
on	Rebuild
off	Not rebuild

- Initial value: off
- *interface*
 - Set value: IP address used as backup destination
 - Initial value: -
- *ip_address*
 - Set value: IP address of gateway
 - Initial value: -
- *tunnel_num*
 - Set value: Tunnel interface number
 - Initial value: -

Description

Specifies the interface to be backed up when the PP interface is disconnected.

If the interface to be backed up is a PP interface, the ipsec-fast-recovery option can be set. When this option is set to on, immediately after recovering from backup, the SA of IPsec is immediately rebuilt, so that the time until IPsec communication becomes possible can be shortened.

[Notes]

This command can be set for each PP interface.

The **pp always-on** command must be set to on to detect disconnection of the PP interface. In the case of a leased line **Use the pp keepalive use lcp-echo command** instead of the **pp always-on** command.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.5.2 Setting the recovery wait time from backup

Format

pp backup recovery time *time*
no pp backup recovery time [*time*]

Set value and initial value

- *time*
 - Set value:

Set value	Description
1..21474836	Number of seconds
off	Immediately returning

- Initial value: off

Description

When recovering from backup, it is set whether to immediately recover or wait for a set time before recovering.

[Notes]

This setting is commonly used for all PPs. This setting is commonly used for both leased line backup and FR backup.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.5.3 Specifying the destination of backup when provider connection via LAN goes down

Format

```
lan backup interface none
lan backup interface pp peer_num
lan backup interface backup_interface ip_address
lan backup interface tunnel tunnel_num
no lan backup interface
```

Set value and initial value

- none: Backup does not work
 - none: none
- interface
 - Set value: Name of the LAN interface to be backed up
 - Initial value: -
- peer_num
 - Set value: Destination information number when using pp as a backup
 - Initial value: -
- backup_interface
 - [Setting value]: LAN interface used as backup
 - [Initial value]: -
- ip_address
 - [Setting value]: Tunnel interface number
 - [Initial value]: -
- tunnel_num
 - [Setting value]: Tunnel interface number
 - [Initial value]: -

[Explanation]

For a specified LAN interface, interface information to be backed up when a provider connection via a LAN goes down is set.

[Notes]

For backup operation, setting with the **lan keepalive use** command is also necessary in order to detect the connection going down via the LAN.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.5.4 Setting the waiting time from backup

[Form]

```
lan backup recovery time interface time
no lan backup recovery time interface [time]
```

[Setting value and initial value]

- interface
 - [Setting value]: Name of the LAN interface to be backed up
 - [Initial value]: -
- time
 - [Setting value]:
 - Number of seconds (1..21474836)
 - off
 - [Initial value]: off

[Explanation]

Setting whether to immediately restore or wait for a set time before restoring to the specified LAN interface when restoring from backup.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.5.5 Setting whether to use keepalive via the LAN**[Form]**

lan keepalive use interface icmp-echo dest_ip [*option=value...*] [dest_ip [*option=value...*]...]

lan keepalive use interface arp dest_ip [dest_ip...]

lan keepalive use interface icmp-echo dest_ip [*option=value...*] [dest_ip [*option=value...*]...] arp dest_ip [dest_ip...]

lan keepalive use interface off

no lan keepalive use interface [...]

[Setting value and initial value]

- *interface*
 - [Setting value]: Name of the LAN interface to be backed up
 - [Initial value]: -
- *dest_ip*
 - [Setting value]: IP address to be checked for keepalive
 - [Initial value]: -
- *option = value column*
 - [Setting value]:

<i>option</i>	<i>value</i>	Explanation
upwait	Millisecond	Allowable response time for up detection (1..10000)
downwait	Millisecond	Allowable response time for down detection (1..10000)
length	Bytes	ICMP Echo packet length (64-1500)

- [Initial value]: -

[Explanation]

Set whether or not to perform keepalive operation for the specified LAN interface. I can specify icmp-echo. ICMP Echo/Reply is used, and if arp is specified, ARP Request/Reply is used. Combined use is also possible by writing together.

[Notes]

The route for the IP address confirmed by icmp-echo must be directed to the backup LAN interface.

Even when the response time is limited by the downwait parameter, if the set value of the **lan keepalive interval** command is smaller, the set value of the **lan keepalive interval** command takes precedence. If only one of downwait and upwait parameters is set, the other operates as if the same value was set.

The length parameter specifies the length of the ICMP data portion, not the length of the entire IP packet.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.5.6 Setting the time interval for keepalive over the LAN**[Format]**

lan keepalive interval interface interval [count]

no lan keepalive interval interface

[Setting value and initial value]

- *interface*

- [Setting value]: The name of the LAN interface to be backed up.
- [Initial value]: -
- *Interval*
 - [Setting value]: The time interval for sending keepalive packets (1..65535).
 - [Initial value]: 30
- *count*
 - [Setting value]: The number of times for determining down detection (3..100).
 - [Initial value]: 6

[Explanation]

For the specified LAN interface, the time interval for sending keepalive packets and the number of times for determining down detection are set. When a response packet cannot be detected continuously as many times as set in *count*, it is determined to be down.

If it is detected that no response is returned once, the time interval for sending the subsequent keepalive packets is reduced to one second. The time interval for detecting down detection is about
Therefore, even in the case of the default setting value, the time required for detecting down detection is about 35 seconds.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.5.7 Setting whether to log keepalive over the LAN

[Format]

lan keepalive log *interface log*

no lan keepalive log *interface*

[Setting value and initial value]

- *interface*
 - [Setting value]: The name of the LAN interface to be backed up.
 - [Initial value]: -
- *log*
 - [Setting value]:

Setting value	Explanation
on	Log
off	Log not taken

- [Initial value]: off

[Explanation]

Whether to log keepalive packets is set.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.5.8 Setting network monitoring function

[Format]

ip keepalive *num kind interval count gateway [gateway ...] [option=value ...]*

no ip keepalive *num*

[Setting value and initial value]

- *num* : Identification number of monitoring setting
- [Setting value]:

Setting value	Explanation
1.6000	vRX Amazon EC2 Standard Mode, vRX VMware ESXi Standard Mode, vRX Cloud Edition
1...3000	Can be set with RTX5000 and RTX3510
1...1000	Can be set with vRX Amazon EC2 Compact Mode, vRX VMware ESXi Compact Mode, RTX3500

Set value	Description
1..100	Can be set with models other than the above

- [Initial value]: -
- *kind* : Monitoring method
- [Set value]:

Set value	Description
icmp-echo	Using ICMP Echo

- [Initial value]: -
- *Interval*
 - Set value: Number of seconds between keep alive transmissions (1..65535)
 - [Initial value]: -
- *count*
 - Set value: Number of times to transmit before determining that there is no reachability (3..100)
 - [Initial value]: -
- *gateway*: Multiple specifications (up to 10)
 - [Set value]:
 - IP address
 - xxx.xxx.xxx.xxx (where xxx is a decimal number)
 - dhcp *interface*
 - RTX5000 and RTX3500 can be specified with Rev.14.00.29 or later

Set value	Description
interface	LAN interface name or WAN interface name operating as a DHCP client when using the default gateway given by DHCP

- [Initial value]: -
- *option=value column*
 - [Set value]:

option	value	Description
log	on	Outputting SYSLOG
	off	Do not output SYSLOG
upwait	Seconds	Waiting time before determining that there is reachability (1..1000000)
downwait	Seconds	Waiting time before determining that there is no reachability (1..1000000)
length	Bytes	Length of an ICMP Echo packet (64-1500)
local-address	IP address	Starting IP address
ipsec-refresh	Security gateway identifier (<i>gateway_id</i>)	DOWN→UP or UP→DOWN Force update of SA belonging to the specified security gateway when the state changes to (separate with commas if multiple are specified)
ipsec-refresh-up	Security gateway identifier (<i>gateway_id</i>)	Forcibly update the SA belonging to the specified security gateway only when the state changes from DOWN to UP (separate by commas when specifying multiple gateways).

option	value	Description
ipsec-refresh-down	Identifier of the security gateway (<i>gateway_id</i>)	Force update of the SA belonging to the specified security gateway only when the state changes from UP to DOWN (separate by commas when specifying multiple gateways).
gateway-selection-rule	head	When sending an ICMP Echo packet, even if multiple gateways are specified for the corresponding route, always send it to the first specified gateway.
	normal	When sending an ICMP Echo packet, if multiple gateways are specified for the corresponding route, select the sending gateway according to the usual rule.

- Initial value:
 - log=off
 - upwait=5
 - downwait=5
 - length=64
 - gateway-selection-rule=head

Description

Sends an ICMP Echo to the specified gateway and determines whether or not a reply can be received.

Notes

The length parameter specifies the length of the ICMP data portion, not the length of the entire IP packet.

The ipsec-refresh, ipsec-refresh-up, and ipsec-refresh-down parameters are effective in shortening the recovery time of IPsec communication when switching a main line/subordinate line of a network backup function.

The WAN interface cannot be specified for the vRX series, RTX5000, and RTX3500.

[Configuration Example]

When restoring from the subordinate line pp11 to the main line pp10 by the network backup function, the SA belonging to identifier 3 of the security gateway used for IPsec connection is forcibly updated.

```
# ip route 172.16.0.0/24 gateway pp 10 keepalive 1 gateway pp 11 weight 0
# ip keepalive 1 icmp-echo 5 5 172.16.0.1 ipsec-refresh-up=3
```

Use the network backup function to trigger the down of IP keepalive 1 to activate the route.

Activate 172.16.224.0/24.

```
# ip route 172.16.112.0/24 gateway null keepalive 1 gateway 172.16.0.1 weight 0
# ip route 172.16.224.0/24 gateway 172.16.112.1 keepalive 2
# ip keepalive 1 icmp-echo 5 5 192.168.100.101
# ip keepalive 2 icmp-echo 5 5 172.16.112.1 gateway-selection-rule=normal
```

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.6 Packet forwarding filter settings

6.6.1 Packet forwarding filter settings

Format

ip forward filter *id order gateway gateway filter filter_id ... [keepalive keepalive_id]*

no ip forward filter *id order [gateway gateway [filter filter_id ...] [keepalive keepalive_id]]*

Setting values and initial values

- id*

- Setting values: Packet forwarding filter identifiers (1..255)
- Initial values: -
- *order*
 - Setting values: Order of evaluation (1..255)
 - Initial values: -
- *gateway*
 - Setting values:

Setting values	Description
IP addresses	IP addresses of gateways to which packets are forwarded
Wan1	WAN interfaces (Not available for the vRX series, RTX5000, and RTX3500)
<i>pp peer_num</i>	PP interfaces
tunnel <i>tunnel_num</i>	TUNNEL interfaces

- Initial values: -
- *filter_id*
 - Setting values: **IP filter** command identifiers
 - Initial values: -
- *keepalive_id*
 - [Setting value]: Identifier of **ip keepalive** command
 - [Initial value]: -

[Description]

Packet forwarding filters are defined.

The *id* parameter is an identifier for grouping a plurality of packet forwarding filters.

When multiple packet forwarding filters are configured for the same interface, the same number must be specified for all of them.

The *order* parameter indicates the order of evaluation, and it is preferentially adopted as it has a younger number.

Up to 16 identifiers of an **ip filter** command can be specified as the *filter_id* parameter.

When multiple identifiers are specified, the preceding one is preferentially evaluated.

The corresponding **ip filter** command is examined in order from the beginning, and if it matches the contents of a packet, the setting of the **ip filter** command is adopted.

If the operation of the **ip filter** command is reject, it discards a packet without forwarding it; otherwise, it forwards a packet to a gateway specified by the *gateway* parameter.

The identifier of the **ip keepalive** command is specified in *keepalive_id*.

If the result of IP keepalive specified here is down, this gateway is not used. That is, even if there is an corresponding **ip filter** command, it is treated as not applicable.

In addition, it is necessary to set the **ip interface forward filter** command in order to actually operate.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.6.2 Application of packet forwarding filters to the interface

[Format]

ip interface forward filter *id*

ip pp forward filter *id*

ip tunnel forward filter *id*

ip local forward filter *id*

no ip interface forward filter [*id*]

no ip pp forward filter [*id*]

no ip tunnel forward filter [*id*]

no ip local forward filter [*id*]

[Setting value and initial value]

- interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- id*
 - [Setting value]: Identifier of the packet forwarding filter specified by the **ip forward filter** command (1..255)
 - [Initial value]: -

[Description]

Packet forwarding filters are applied to the interface.
Packets received at the specified interface are compared with the settings of the specified packet forwarding filter, and a gateway to be forwarded is determined.
The ip local forward filter command is specified when targeting packets sent by itself.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

6.7 LAN pass-through function setting

6.7.1 Setting of Ethertype to be relayed by LAN pass-through function

[Format]

lan pass-through ethertype *id ethertype [ethertype ...]*
no lan pass-through ethertype *id [...]*

[Setting value and initial value]

- id*
 - [Setting value]: Identifier of LAN pass-through function (1..8)
 - [Initial value]: -
- Ethertype*
 - [Setting value]:
 - Decimal representing Ethertype (1536..65535)
 - Hexadecimal representing Ethertype (0x0600..0xffff)
 - Mnemonic representing Ethertype

Mnemonic	Decimal	Hexadecimal	Description
IPV4	2048	0x0800	IPv4 packets
arp	2054	0x0806	ARP packets
ipv6	34525	0x86dd	IPv6 packets

- [Initial value]: -

[Explanation]

Set the Ethertype of a packet to be relayed by the LAN pass-through function. If this setting is not present, the packet is not relayed.

[Notes]

Even when relaying a packet with an IEEE802.1Q tag, it is not necessary to consider the IEEE802.1Q tag. IEEE802.1Q Set the Ethertype encapsulated by the tag.
RTX1300 can be used after Rev. 23.00.16.

[Applicable model]
RTX1300

6.7.2 Interface settings used by the LAN pass-through function

[Format]

lan pass-through member *id interface interface*
no lan pass-through member *id [...]*

[Setting value and initial value]

- *id*
 - Setting value: Identifier of the LAN pass-through function (1..8)
 - [Initial value]: -
- *interface*
 - Setting value: Name of the LAN interface
 - [Initial value]: -

[Explanation]

Interfaces used by the LAN pass-through function are set.

Between the configured interfaces, Ethertype packets configured by the **lan pass-through ethertype** command are relayed. If this setting is not present, packets are not relayed.

In the LAN interface name, interfaces used by the physical LAN interface and the LAN division function can be set.

[Notes]

The configured LAN interface operates in promiscuous mode.
RTX1300 can be used after Rev. 23.00.16.

[Applicable model]
RTX1300

CHAPTER 7

Setting Up an Ethernet Filter

7.1 Setting Up an Ethernet Filter

Format

ethernet filter *num kind src_mac* [*dst_mac* [*offset byte_list*]]

ethernet filter *num kind type* [*scope*] [*offset byte_list*]

no ethernet filter *num* [*kind ...*]

Setting Value and Initial Value

- Number*

- Setting Value:

Setting Value	Description
1..512 (RTX1210 Rev.14.01.16 or later and Rev.15.02 After the above	Number of a static filter
1..100 (other than above)	

- Initial Value: -

- kind*

- Setting Value:

Setting Value	Description
pass-log	Pass if they match (log)
Pass-Nolog	Pass if they match (do not log)
reject-log	Discard if they match (do not log)
reject-nolog	Discard if they match (do not log)

- Initial Value: -

- src_mac*

- Setting Value:

- Starting MAC address
- xx:xx:xx:xx:xx:xx (where xx is a hexadecimal number or *)
- *(corresponds to all MAC addresses)

- Initial Value: -

- DST_MAC*

- Setting Value:

- Endpoint MAC address
- Same format as starting MAC address *src_mac*
- When omitted, it is the same as one *

- Initial Value: -

- type*

- Setting Value:

Setting Value	Description
dhcp-bind	Target a host that is reserved in the specified DHCP scope
dhcp-not-bind	Target a host that is not reserved in the specified DHCP scope

- Initial Value: -

- scope*

- Setting Value:
 - DHCP Scope
 - An integer of 1..65535
 - IP addresses included in the lease scope of the DHCP scope
- Initial Value: -
- *offset*
 - Setting Value: Decimal number representing offset (set immediately after the starting MAC address of the Ethernet frame to 0)
 - Initial Value: -
- *byte_list*
 - Setting Value:
 - Byte String
 - A sequence of xx (two-digit hexadecimal number) or * (optional bytes) separated by commas (up to 16)
 - [Initial value]: -

[Description]

The filter of an Ethernet frame is set. The filter set in this command is used by the **ethernet lan filter** command.

In a normal filter, the filter is applied to an Ethernet frame which is transmitted and received by a start point MAC address, an end point MAC address, etc.

In a filter of type dhcp-bind, the filter is applied to the following Ethernet frames. Untargeted Ethernet frames are treated as if they do not match the filter.

- In the case of an IPv4 packet that corresponds to any of the following:
 - Ethernet type is IPv4 (0x0800)
 - In a PPPoE environment, Ethernet type is PPPoE data frame (0x8864), and protocol ID is IPv4 (0x0800).
 - In an 802.1Q tag VLAN environment, TPID is 802.1Q tag (0x8100), and Ethernet type is IPv4 (0x0800).

If a pair of the start point MAC address and the start point IP address of an Ethernet frame is reserved in the target DHCP scope, it is considered to match the filter.

- In the case of Ethernet type is any of the following:
 - ARP (0x0806)
 - RARP (0x8035)
 - PPPoE control packet (0x8863)
 - MAC layer control packet (0x8808)

If the start point MAC address of an Ethernet frame is reserved in the target DHCP scope, it is considered to match the filter.

In a filter of type dhcp-not-bind, the filter is applied to the following Ethernet frames. Untargeted Ethernet frames are treated as if they do not match the filter.

- In the case of Ethernet type is IPv4 (0x0800)

If the start point IP address of an Ethernet frame is included in the lease scope of the target DHCP scope and the start point MAC address is not reserved in the target DHCP scope in a filter of type dhcp-not-bind, it is considered to match the filter.

In a filter of type dhcp-bind or dhcp-not-bind, the target DHCP scope is specified by the *scope* parameter.

The *scope* parameter can specify a DHCP scope number or an IP address included in the subnet where the DHCP scope is defined. In the case of specifying a DHCP scope in an IP address, when multiple DHCP scopes are applicable, the DHCP scope with the longest netmask length among them is selected.

If the *scope* parameter is omitted, all DHCP scopes used in the interface to which the filter is applied are covered.

When a filter of type dhcp-bind or dhcp-not-bind is configured in a router operating as a DHCP relay agent, the DHCP scope and reservation information of the client in that DHCP scope are obtained from the DHCP server and referred to when the filter is applied. Acquisition of the DHCP scope and reservation information from a DHCP server is performed by writing reservation information to an option part of a DHCP message and notifying it when relaying a DHCP message.

[Notes]

In the case of using the LAN division function, since the value of 0x8100 to 0x810f is used as the Ethernet type in the router, if those Ethernet frames are filtered and cannot be transmitted or received, it is necessary to be careful because communication cannot be performed on a port using the LAN division function.

In a filter of type dhcp-bind or dhcp-not-bind, since the filter is determined by using the start point MAC address or the start point IP address of an Ethernet frame, the **ethernet lan filter** command is usually used only in the in direction. In the case of the out direction, the start point MAC address is the router's own MAC address, so it cannot match the reservation information of DHCP or the leased address.

Since a filter of type dhcp-bind uses a value that allows only clients whose reservations or addresses are leased to pass through, it is usually used in combination with pass etc. On the other hand, since a filter of type dhcp-not-bind uses a value that discards clients whose reservations or addresses are not leased, it is usually used in combination with reject etc.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

7.2 Setting up application to interface

[Format]

```
ethernet interface filter dir list
no ethernet interface filter dir [list]
```

[Setting value and initial value]

- *interface*
 - [Setting value]
 - Name of physical LAN interface
 - Name of interface used in the LAN division function
 - Cannot be specified in the vRX series
 - Name of tunnel interface
 - [Initial value] -
- *dir*
 - [Setting value]

Setting value	Description
in	Filtering incoming packets from the LAN side
out	Packets coming from the LAN side

- [Initial value] -
- *list*
 - [Setting value]

Setting value	Explanation
Static filter number sequence separated by spaces	Up to 512 (Rev.14.01.16 or later and Rev.15.02 or later)
	Up to 100 (other than the above)

- [Initial value]: -

[Description]

For packets passing through a LAN and a tunnel interface, filtering of packets by an **ethernet filter** command is combined to limit the types of packets passing.

[Notes]

When specifying a tunnel interface in the *interface* parameter, the filter is applied only when the interface is housed in a bridge interface.

Specifying a tunnel interface to the *interface* parameter is not possible in vRX Amazon EC2 version.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

7.3 Display of Ethernet filter status

[Format]

show status ethernet *filter type* [*scope*]

[Setting value and initial value]

- *type*
- [Setting value]:

Setting value	Description
dhcp-bind	Hosts reserved in the specified DHCP scope
dhcp-scope	Hosts whose addresses are leased in the specified DHCP scope

- [Initial value]: -
- *scope*
 - [Setting value]: Scope number (1-65535)
 - [Initial value]: -

[Description]

Information of an Ethernet filter is displayed.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 8

URL filter setting

8.1 Setting up a filter definition

[Format]

`url filter id kind keyword [src_addr[/mask]]`

`no url filter id`

[Setting value and initial value]

• *id*

- [Setting value]:

Setting value	Description
1..21474836	Filter number

- [Initial value]: -

• *kind*

- [Setting value]:

Setting value	Description
pass, pass-nolog	Pass if they match (Do not log)
pass-log	Pass if they match (Do not log)
reject, reject-log	Pass if they match (Do not log)
reject-nolog	Pass if they match (Do not log)

- [Initial value]: -

• *keyword*

- [Setting value]:

Setting value	Description
Any string	All or part of the URL to be filtered (Up to 255 characters)
*	Supports all URLs

- [Initial value]: -

• *src_addr* : Start IP address of an IP packet

- [Setting value]:

Setting value	Description
Any IPv4 address	One IPv4 address
Range specification	Two IP addresses with a hyphen in between, followed by a minus sign, or preceded by a minus sign (range specification)
*	Supports all IP addresses
Omitted	Same as * if omitted

- [Initial value]: -

• *mask*

- [Setting value]: Netmask length (can be specified only when *src_addr* is a network address)

- [Initial value]: -

[Explanation]

Set a filter by URL. The filter set by this command is used by the **URL interface filter** command. If the specified keyword contains uppercase alphabets, convert them to lowercase letters and save them.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

8.2 Applying URL filter to interface

[Format]

url interface filter *dir list*

url pp filter *dir list*

url tunnel filter *dir list*

no url interface filter

dir no url pp filter dir

no url tunnel filter *dir*

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name, WAN interface name
 - [Initial value]: -
- *dir*
 - [Setting value]:

Setting value	Description
in	Filtering HTTP connections in the input direction
out	Filtering HTTP connections in the output direction

- [Initial value]: -
- *list*
 - Setting value: Sort of URL filter numbers separated by spaces (within 512...RTX5000/RTX3500, within 128...other models)
 - [Initial value]: -

[Explanation]

Combining the filters set by the **URL filter** command, restricting them by the URL of HTTP packets sent and received in the interface.

The number of filters that can be set is within 512 for RTX5000 and RTX3500, within 128 for other models, or within the range that can be entered by command line string length (4095 characters).

Packets that do not match all specified filters are discarded.

[Notebook]

WAN interface can be specified by firmware after Rev.14.01 series.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

8.3 Setting the HTTP port number to be checked by URL filter

[Format]

url filter port *list*

no url filter port

[Setting value and initial value]

- *list*

- Setting value: Sort of port numbers separated by spaces (within 4)
- [Initial value]: 80

[Explanation]

Setting the HTTP port number to be checked by URL filter

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

8.4 Setting whether to use URL filters

[Format]

`url filter use switch`

`no url filter use`

[Setting value and initial value]

- *switch*
 - [Setting value]:

Setting value	Description
on	Using URL filters
off	Do not use URL filters

- [Initial value]: on

[Explanation]

Whether to use URL filters or not is set.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

8.5 Setting an action to return an HTTP response to the sender of packets discarded by URL filters

[Format]

`url filter reject redirect url`

`filter reject redirect url url`

`filter reject off`

`no url filter reject [action]`

[Setting value and initial value]

- *redirect*: Returns an HTTP response of HTTP redirect and forwards it to a block screen
 - *redirect* (for other than RTX5000, RTX3510, RTX3500)
- *off*: Ends a TCP session by TCP RST without returning an HTTP response
 - [Initial value]: off (for RTX5000, RTX3510, RTX3500)
- *url*
 - Setting value: URL to redirect (a string starting with http:// or https:// and no more than 255 single-byte characters)
 - [Initial value]: -
- *action*
- [Setting value]:
 - *redirect*
 - *off*
 - [Initial value]: -

[Explanation]

Set an action to return an HTTP response to the sender of packets discarded by URL filters. Matched keywords or reasons for blocking access are displayed on the block screen.

If *URL* is specified, when redirecting, a "?" is followed by a query with the following contents.

- Blocked access URL
- Keywords set for matched filters

URL cannot be set to anything other than `http://` or a string starting with `https://`.

[Notes]

In models that support HTTP server functions, **httpd service** on must be set when **redirect** is set and a block screen is displayed in a Web browser.

[Applicable models]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

8.6 Setting whether to output a log when a filter is matched

[Format]

`url filter log switch`
`no url filter log`

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Explanation
on	Output a log when a filter is matched
off	Output a log when a filter is matched

- [Initial value]: on

[Explanation]

Whether to output a log when a filter is matched or not is set.

[Notes]

Even if on is set, logs are not output if a **filter with** `pass`, `pass-nolog`, or `reject-nolog` specified as *kind* in the **URL filter** command is matched.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 9

PPP configuration

9.1 Setting the other party's name and password

[Format]

```
pp auth username username password [myname myname mypass] [isdn1] [clid [isdn2...]] [mscbcp] [ip_address]
[ip6_prefix]
pp auth username username password [myname myname mypass] [ip_address] [ip6_prefix]
no pp auth username username [password...]
```

[Setting value and initial value]

- *username*
 - [Setting value]: Name (up to 64 characters)
 - [Initial value]: -
- *password*
 - [Setting value]: Password (up to 64 characters)
 - [Initial value]: -
- *myname*: Keyword for entering settings on your side
 - [Initial value]: -
- *myname*
 - [Setting value]: User name on your side
 - [Initial value]: -
- *mypass*
 - [Setting value]: Password on your side
 - [Initial value]: -
- *isdn1*
 - [Setting value]: Other party's ISDN address
 - [Initial value]: -
- *clid*: Keyword indicating that MS callback authentication is used
 - [Initial value]: -
- *isdn2*
 - [Setting value]: ISDN address used for authentication
 - [Initial value]: -
- *mscbcp*: Keyword indicating that MS callback is allowed
 - [Initial value]: -
- *ip_address*
 - [Setting value]: IP address to assign to the other party
 - [Initial value]: -
- *IP6_prefix*
 - [Setting value]: Prefix to assign to a user
 - [Initial value]: -

[Description]

Set the other party's name and password Multiple settings are possible. Optionally, you can also enter settings on your side.

For models without BRI interface, use the second format.

In the case of bidirectional authentication, a process to authenticate oneself to the other party starts after the other party's user name is determined. If these parameters are not set, the setting of the **pp auth myname** command is referenced.

Optionally, an ISDN number can be configured to allow routing tied to a name or calling to a remote IP address. Set to *isdn1* is an ISDN address for transmission. If *isdn1* is omitted, the other party does not make a call.

If '*' is given to the name, it is treated as a wildcard, and the setting is used for the other party whose name does not match.

The *clid* keyword indicates that MS callback authentication is used. If this keyword is not set, the authentication of the number will not be performed. For authentication of the number, if *isdn2* is set, use *isdn2*, or if *isdn2* is not set, use *isdn1*, and if they match, the authentication will be considered successful.

Multiple *isdn2* can be set. When multiple is set, authentication will be performed at the first ISDN address, and if authentication fails, the next ISDN address will be used.

The *mscbcp* keyword indicates that MS callback is allowed. For incoming calls from this user, if it is set to **isdn callback permit** on at the same time, the MS callback will be performed.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.2 Setting the authentication type to be accepted

Format

pp auth accept *accept* [*accept*]

no pp auth accept [*accept*]

[Setting value and initial value]

- *accept*
- [Setting value]:

Setting value	Description
Pap	Accept authentication by PAP
Chap	Accept authentication by CHAP
MSCHAP	Accept authentication by MSCHAP
MSCHAP-V2	Accept authentication by MSCHAP Version 2

- [Default value]: Do not accept authentication

Description

Set whether to accept a PPP authentication request from the other party. It is always applied at the time of transmission. In the case of an incoming call that is not anonymous, it is applied after PP is selected by the outgoing number. In the case of an incoming call with anonymous, it is applied when the selection of PP by the outgoing number fails.

Even if it is configured to accept authentication by this command, it will reject authentication if its name and password are not set by the **pp auth myname** command.

It is a command for each PP.

[Notes]

Specifying *mschap* and *mschap-v2* to the *auth* parameter is not possible with RTX5000 / RTX3500 Rev.14.00.11 or earlier.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.3 Setting the authentication type required

Format

pp auth request *auth* [*arrive-only*]

no pp auth request [*auth*[*arrive-only*]]

Setting value and initial value

- *auth*

- Setting value:

Setting value	Description
Pap	Require authentication by CHAP
Chap	Require authentication by CHAP
MSCHAP	Require authentication by MSCHAP
MSCHAP-V2	Require authentication by MSCHAP Version2
Chap-pap	Require authentication by CHAP or PAP

- Initial value: -

Description

Set whether to require authentication by PAP and CHAP for the selected party. It is always applied at the time of transmission. In the case of an incoming call that is not anonymous, it is applied after PP is selected by the outgoing number. In the case of an incoming call with anonymous, it is applied when the selection of PP by the outgoing number fails.

In the case of a chap-pap keyword, CHAP is requested first, and if it is rejected by the other party, it operates to request PAP again. This allows for easy connection even when the other party supports only one of PAP or CHAP. When arrive-only keyword is specified, authentication by PPP is requested only at the time of incoming call, and not at the time of transmission.

Notebook

Specifying mschap and mschap-v2 for the *auth* parameter is not possible with RTX5000 / RTX3500 Rev.14.00.11 or earlier.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.4 Setting your name and password

Format

```
pp auth myname myname password
no pp auth myname [myname password]
```

Setting value and initial value

- *my name*
 - [Setting value]: Name (up to 64 characters)
 - [Initial value]: -
- *password*
 - [Setting value]: Password (up to 64 characters)
 - [Setting value]: -

[Explanation]

Set your name and password to be sent to the other party by PAP or CHAP. This is a command for each PP.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.5 Setting whether to prohibit double connection from the other party with the same username

[Format]

```
pp auth multi connect prohibit prohibit
no pp auth multi connect prohibit [prohibit]
```

[Setting value and initial value]

- *prohibit*

- [Setting value]:

Setting value	Explanation
on	Prohibit
off	Do not prohibit

- [Initial value]: off

[Explanation]

Sets whether to prohibit double connection from the other party with the same *username* registered by the **pp auth username** command.

[Notes]

It is convenient for operating a flat-rate system provider. When user management is performed by RADIUS, prohibition of double connection must be dealt with by the RADIUS server.

It is valid only when anonymous is selected.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.6 LCP-related settings

9.6.1 Setting up the use of the Address and Control Field Compression option

[Format]

ppp lcp acfc acfc

no ppp lcp acfc [acfc]

[Setting value and initial value]

- *acfc*

- [Setting value]:

Setting value	Explanation
on	Use
off	Do not use

- [Initial value]: off

[Explanation]

Set whether to use the Address and Control Field Compression option of [PPP, LCP] for the selected party.

[Notes]

Even if on is set, it is not used when the other party refuses.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.6.2 Setting up the use of the Magic Number option

[Format]

ppp lcp magicnumber magicnumber

no ppp lcp magicnumber [magicnumber]

[Setting value and initial value]

- *magicnumber*

- [Setting value]:

Setting value	Explanation
on	To use
off	Not used

- [Initial value]: on

[Explanation]

Sets whether or not to use the Magic Number option of [PPP, LCP] for the selected opponent.

[Notes]

Even if set to on, it is not used when the opponent refuses.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.6.3 Setting up the Maximum Receive Unit option

[Format]

`ppp lcp mru mru [length]`
`no ppp lcp mru [mru[length]]`

[Setting value and initial value]

- *mru*
- [Setting value]:

Setting value	Explanation
on	Not used
off	Not used

- [Initial value]: on
- *length*: Value of MRU
- [Setting value]:
 - 1280..1792
- [Initial value]: 1792

[Explanation]

Set whether or not to use the Maximum Receive Unit option of [PPP, LCP] for the selected opponent and the value of MRU.

[Notes]

Even if set to on, it is not used when the opponent refuses. Generally, it is allowed to be on, but it is turned off when connecting to a router that cannot connect with this option.
In the case of setting using data compression, the setting of the *length* parameter always operates as 1792.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.6.4 Setting up the use of the Protocol Field Compression option

[Format]

`ppp lcp pfc pfc`
`no ppp lcp pfc [pfc]`

[Setting value and initial value]

- *pfc*
- [Setting value]:

Setting value	Explanation
on	Not used
off	Not used

- [Initial value]: off

[Explanation]

Sets whether or not to use the Protocol Field Compression option of [PPP, LCP] for the selected opponent.

[Notes]

Even if set to on, it is not used when the opponent refuses.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.6.5 Setting up the lcp-restart parameter

[Format]

ppp lcp restart *time*
no ppp lcp restart [*time*]

[Setting value and initial value]

- *time*
 - Setting value: milliseconds (20..10000)
 - [Initial value]: 3000

[Description]

Set the retransmission time of configure-request and terminate-request of [PPP, LCP] for the selected party.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.6.6 Setting the lcp-max-configure parameter

[Format]

ppp lcp maxterminate *count*
no ppp lcp maxterminate [*count*]

[Setting value and initial value]

- *count*
 - [Setting value]: Number of times (1..10)
 - [Initial value]: 2

[Explanation]

Set the transmission frequency of terminate-request of [PPP, LCP] for the selected party.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.6.7 Setting the lcp-max-configure parameter

[Format]

ppp lcp maxconfigure *count*
no ppp lcp maxconfigure [*count*]

[Setting value and initial value]

- *count*
 - [Setting value]: Number of times (1..10)
 - [Initial value]: 10

[Explanation]

Set the transmission frequency of configure-request of [PPP, LCP] for the selected party.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.6.8 Setting the lcp-max-failure parameter

[Format]

ppp lcp maxfailure *count*
no ppp lcp maxfailure [*count*]

[Setting value and initial value]

- *count*
 - [Setting value]: Number of times (1..10)
 - [Initial value]: 10

[Explanation]

Set the transmission frequency of configure-nak of [PPP, LCP] for the selected party.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.6.9 Setting whether to send Configure-Request immediately or not

[Format]

ppp lcp silent *switch*
no ppp lcp silent [*switch*]

[Setting value and initial value]

- *switch*
 - [Setting value]:

Setting value	Explanation
on	PPP/LCP delays the transmission of Configure-Request immediately after line connection until it receives Configure-Request from the other party.
off	PPP/LCP sends Configure-Request immediately after line connection

- [Initial value]: off

[Explanation]

PPP/LCP sets whether to send Configure-Request immediately after line connection or to delay until it receives Configure-Request from the other party. Normally, it is acceptable to send Configure-Request immediately after line connection, but depending on the connection partner, it is better to delay this.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.7

AP-related settings

P

9.7.1 Setting the pap-restart parameter

[Format]

ppp pap restart *time*
no ppp pap restart [*time*]

[Setting value and initial value]

- *time*
 - [Setting value]: milliseconds (20..10000)
 - [Initial value]: 3000

[Explanation]

Set the retransmission time of [PPP, PAP]authenticate-request for the selected party.

[Applicable model]

[Settings]: vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.7.2 Setting the pap-max-authreq parameter

[Format]

ppp pap maxauthreq *count*
no ppp pap maxauthreq [*count*]

[Setting value and initial value]

- *count*
 - [Setting value]: Number of times (1..10)
 - [Initial value]: 10

[Explanation]

Set the retransmission times of [PPP, PAP]authenticate-request for the selected party.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.8

HAP-related settings

C

9.8.1

Setting the chap-restart parameter

[Format]

ppp chap restart *time*
no ppp chap restart [*time*]

[Setting value and initial value]

- *time*
 - [Setting value]: milliseconds (20..10000)
 - [Initial value]: 3000

[Explanation]

Set the retransmission time of [PPP, CHAP]challenge for the selected party.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.8.2

Setting the chap-max-challenge parameter

[Format]

ppp chap maxchallenge *count*
no ppp chap maxchallenge [*count*]

[Setting value and initial value]

- *count*
 - [Setting value]: Number of times (1..10)
 - [Initial value]: 10

[Explanation]

Set the transmission times of [PPP, CHAP]challenge for the selected party.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.9

PCP-related settings

!

9.9.1

Setting the use of Van Jacobson Compressed TCP/IP

[Format]

ppp ipcp vjc compression
no ppp ipcp vjc [*compression*]

[Setting value and initial value]

- *compression*
 - [Setting value]:

Setting value	Explanation
on	Use

Setting value	Explanation
off	Do not use

- [Initial value]: off

[Explanation]

Set whether to use [PPP, IPCP]Van Jacobson Compressed TCP/IP for the selected party.

[Notes]

Even if it is set to on, it is not used when the other party refuses.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.9.2 Setting up negotiation of PP side IP address

[Format]

ppp ipcp ipaddress negotiation
no ppp ipcp ipaddress [*negotiation*]

[Setting value and initial value]

- *negotiation*
- [Setting value]:

Setting value	Description
on	Negotiate
off	Negotiate

- [Initial value]: off

[Explanation]

Sets whether to negotiate the PP side IP address for the selected party.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.9.3 Setting up ipcp-restart parameter

[Format]

ppp ipcp restart time
no ppp ipcp restart [*time*]

[Setting value and initial value]

- *time*
- [Setting value]: Millisecond (20..10000)
- [Initial value]: 3000

[Explanation]

Set the retransmission times of configure-request and terminate-request of [PPP, IPCP] for the selected party.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.9.4 Setting up ipcp-max-terminate parameter

[Format]

ppp ipcp maxterminate count
no ppp ipcp maxterminate [*count*]

[Setting value and initial value]

- *count*
- [Setting value]: Number of times (1..10)
- [Initial value]: 2

[Explanation]

Set the number of times to send terminate-request of [PPP, IPCP] for the selected party.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.9.5 Setting up ipcp-max-configure parameter

[Format]

ppp ipcp maxconfigure count

no *ppp ipcp maxconfigure [count]*

[Setting value and initial value]

- *count*
 - [Setting value]: Number of times (1..10)
 - [Initial value]: 10

[Explanation]

Set the number of times to send terminate-request of [PPP, IPCP] for the selected party.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.9.6 Setting up ipcp-max-failure parameter

[Format]

ppp ipcp maxfailure count

no *ppp ipcp maxfailure [count]*

[Setting value and initial value]

- *count*
 - [Setting value]: Number of times (1..10)
 - [Initial value]: 10

[Explanation]

Sets the number of transmissions of configure-nak of [PPP, IPCP] for the selected party.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.9.7 Setting the IP address of the WINS server

[Format]

wins server server1 [server2]

no *wins server [server1 [server2]]*

[Setting value and initial value]

- *server1*, *server2*
 - [Setting value]: IP address (xxx.xxx.xxx.xxx (xxx is a decimal number))
 - [Initial value]: -

[Explanation]

Setting the IP address of the WINS (Windows Internet Name Service) server

[Notes]

Setting the MS extension option of IPCP and the IP address of the WINS server for passing to the client via DHCP. The router does not act as a WINS client on this server at all.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.9.8Setting whether to use the MSeXTension option of IPCP

[Format]

```
ppp ipcp msexT msexT
no ppp ipcp msexT [msexT]
```

[Setting value and initial value]

- msexT
- [Setting value]:

Setting value	Explanation
on	Use
off	Do not use

- [Initial value]: off

[Explanation]

Set whether to use the MS extension option of [PPP, IPCP] for the selected party.
Setting up using the Microsoft extension option of IPCP allows you to pass the IP address of the DNS server and the IP address of the WINS (Windows Internet Name Service) server to the Windows machine that you connect to. The IP addresses of the DNS server and the WINS server for passing are set by the **dns server** command and **wins server** command, respectively.
If off, they do not receive the addresses of the DNS server and the WINS server.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.9.9Setting whether to accept the IPaddress of the other party where the host route exists

[Format]

```
ppp ipcp remote address check sw
no ppp ipcp remote address check [sw]
```

[Setting value and initial value]

- SW
- [Setting value]:

Setting value	Explanation
on	Deny the PP-sideIP address of the notified party
off	Reject the PP-sideIP address of the notified party

- [Initial value]: on

[Explanation]

Setting whether to accept the IP address when an IP address where the host route via another PP already exists is notified as the other party's IP address at the time of PP connection.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.10SCBCP-related settings

9.10.1Setting the mscbcP-restart parameter

[Format]

```
ppp mscbcP restart time
no ppp mscbcP restart [time]
```

[Setting value and initial value]

- time
- [Setting value]: Millisecond (20..10000)

- [Initial value]: 1000

[Explanation]

Set the retransmission time of request/response of [PPP, MSCBCP] for the selected party.

[Applicable model]

[Setting value]: Setting value set to [Setting value]: Setting value set to [Setting value]: Setting value set to [Setting value]: Setting value set to [Setting value].

9.10.2 Setting the mscbcpx-maxretry parameter

[Format]

```
ppp mscbcpx maxretry count
no ppp mscbcpx maxretry [count]
```

[Setting value and initial value]

- *count*
 - [Setting value]: Number of times (1..30)
 - [Setting value]: 30

[Explanation]

Set the retransmission times of request/response of [PPP, MSCBCP] for the selected party.

[Applicable model]

[Setting value]: Setting value set to [Setting value]: Setting value set to [Setting value].

9.11

C

CP-related settings

9.11.1 Setting the compression type of all packets

[Format]

```
ppp ccp type type
no ppp ccp type [type]
```

[Setting value and initial value]

- *type*
 - [Setting value]: Setting value set to [Setting

Setting value	Explanation
stac0	Compress with Stac LZS
stac	Compress with Stac LZS
cstac	Compress with Stac LZS (for Cisco routers)
MPPE-40	Encrypt with 40bit MPPE
MPPE-128	Encrypt with 128bit MPPE
mppe-any	Encrypt with either 40bit or 128bit MPPE
None	Do not compress

- [Setting value]: stac

[Explanation]

Select the [PPP, CCP] compression method for the selected party.

[Notes]

Combined use with Van Jacobson Compressed TCP/IP is also possible.

When stac is specified for *type*, communication may not be performed normally if the line condition is bad or packet loss occurs frequently due to high load. In such a case, it automatically becomes "no compression". After that, it remains "no compression" until restart. When such a situation cannot be improved, stac0 may be specified. However, the connection destination must also correspond to stac0. The compression efficiency of stac0 is lower than that of stac.

Communication may not be possible if stac is applied when the connection destination is a Cisco router. In such a case, set the setting to cstac in such a case that communication may become possible.

Keys are exchanged for each packet in the case of mppe-40, mppe-128, and mppe-any. MPPE is an abbreviation of Microsoft Point-To-Point Encryption (Protocol), which is an extension of CCP, adopts RC4 as a cryptographic algorithm, and uses a key length of 40bit or 128bit. Set together with MS-CHAP or MS-CHAPv2 of the authentication protocol for encryption key generation.

In the vRX series, RTX5000, RTX3510, and RTX3500, stac0,stac,cstac,none can be specified.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.11.2 Setting the ccp-restart parameter

[Format]

ppp ccp restart *time*

no ppp ccp restart [*time*]

[Setting value and initial value]

- *time*
 - [Setting value]: Milliseconds (20..10000)
 - [Initial value]: 3000

[Explanation]

Set the retransmission times of configure-request and terminate-request of [PPP, CCP] for the selected party.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.11.3 Setting the ccp-max-terminate parameter

[Format]

ppp ccp maxterminate *count*

no ppp ccp maxterminate [*count*]

[Setting value and initial value]

- *count*
 - [Setting value]: Number of times (1..10)
 - [Initial value]: 2

[Explanation]

Set the number of times of transmission of terminate-request of [PPP, CCP] for the selected party.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.11.4 Setting the ccp-max-configure parameter

[Format]

ppp ccp maxconfigure *count*

no ppp ccp maxconfigure [*count*]

[Setting value and initial value]

- *count*
 - [Setting value]: Number of times (1..10)
 - [Initial value]: 10

[Explanation]

Set the number of times of transmission of terminate-request of [PPP, CCP] for the selected party.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.11.5 Setting the ccp-max-failure parameter

[Format]

ppp ccp maxfailure *count*
no ppp ccp maxfailure [*count*]

[Setting value and initial value]

- *count*
 - [Setting value]: Number of times (1..10)
 - [Initial value]: 10

[Explanation]

Set the number of times of transmission of configure-nak of [PPP, CCP] for the selected party.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.12

Setting related to IPV6CP

S

9.12.1 Setting whether to use IPV6CP

[Format]

ppp ipv6cp use *use*
no ppp ipv6cp use [*use*]

[Setting value and initial value]

- *Use*
 - [Setting value]:

Setting value	Explanation
on	Use
off	Do not use

- [Initial value]: on

[Description]

Selects whether or not to use IPV6CP for the selected party.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.13

PPoE-related settings

P

9.13.1 Specifying the LAN interface to be used with PPPoE

[Format]

pppoe use *interface*
no pppoe use

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - LAN interface name
 - VLAN interface name
 - Cannot be specified for vRX series and RTX1300
 - Tags LAN interface name
 - Cannot be specified for vRX series and RTX840, RTX830
 - [Initial value]: -

[Explanation]

Specify the interface to be used with PPPoE for the selected party. PPPoE is not used if there is no setting.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.13.2 Access concentrator name setting

[Format]

pppoe access concentrator *name*
no pppoe access concentrator

[Setting value and initial value]

- name*
 - [Setting value]: String representing the name of an access concentrator (7bit US-ASCII)
 - [Initial value]: -

[Explanation]

Set the name of an access concentrator to be connected with PPPoE for the selected party. It is used to specify which access concentrator to be connected to when there are multiple access concentrators that can be connected.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.13.3 Session auto-connect configuration

[Format]

pppoe auto connect *switch*
no pppoe auto connect

[Setting value and initial value]

- switch*
 - [Setting value]:

Setting value	Explanation
on	Auto-connect
off	Auto-connect

- [Initial value]: on

[Explanation]

Set whether to automatically connect a session of PPPoE to the selected party.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.13.4 Session auto-disconnect configuration

[Format]

pppoe auto disconnect *switch*
no pppoe auto disconnect

[Setting value and initial value]

- switch*
 - [Setting value]:

Setting value	Explanation
on	Automatically disconnect
off	Do not automatically disconnect

- [Initial value] : on

[Explanation]

Sets whether or not to automatically disconnect a PPPoE session for a selected party.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.13.5 Setting the maximum number of times to retransmit a PADI packet

[Format]

`pppoe padi maxretry times`
`no pppoe padi maxretry`

[Setting value and initial value]

- *times*
 - [Setting value] : Number of times (1..10)
 - [Initial value] : 5

[Explanation]

Setting the maximum number of times to retransmit a PADI packet in the PPPoE protocol

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.13.6 Setting the retransmission time of a PADI packet

[Format]

`pppoe padi restart time`
`no pppoe padi restart`

[Setting value and initial value]

- *time*
 - [Setting value] : Milliseconds (20..10000)
 - [Initial value] : 3000

[Explanation]

Setting the retransmission time of a PADI packet in the PPPoE protocol

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.13.7 Setting the maximum number of times to retransmit a PADR packet

[Format]

`pppoe padr maxretry times`
`no pppoe padr maxretry`

[Setting value and initial value]

- *times*
 - [Setting value] : Number of times (1..10)
 - [Initial value] : 5

[Explanation]

Setting the maximum number of times to retransmit a PADR packet in the PPPoE protocol

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.13.8 Setting the retransmission time of a PADR packet

[Format]

`pppoe padr restart time`
`no pppoe padr restart`

[Setting value and initial value]

- *time*
 - [Setting value] : Milliseconds (20..10000)
 - [Initial value] : 3000

[Explanation]

Setting the retransmission time of a PADR packet in the PPPoE protocol

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.13.9 Setting the disconnection timer of a PPPoE session

[Format]

pppoe disconnect time *time*
no pppoe disconnect time

[Setting value and initial value]

- *time*
 - [Setting value] :

Setting value	Description
1..21474836	Number of seconds
off	Do not set a timer

- [Initial value]: off

Description

Sets the time for automatically disconnecting a PPPoE session by timeout to the selected party.

Notes

LCP andNCP packets are not monitored.

[Applied model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.13.10 Specifying a Service Name

Format

pppoe service-name *name*
no pppoe service-name

[Setting Value and Initial Value]

- *Name*
 - [Setting Value]: A character string representing a service name (7bit US-ASCII, 255 characters or less)
 - [Initial value]: -

Description

Set the service name requested by PPPoE for the selected party.
It is used to select and connect an access concentrator capable of providing a requested service when there are a plurality of access concentrators that can be connected.

[Applied model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.13.11 MSSLimitation and Size Specification for TCP Packets

Format

pppoe tcp mss *limit length*
no pppoe tcp mss limit

[Setting Value and Initial Value]

- *length*
- [Setting Value]:

Setting Value	Description
1240..1452	Data Length
Auto	MSS Limiting According to MTU Value
off	MSS Not Limiting

- [Initial Value]: auto

Description

Sets whether to limit the MSS (Maximum Segment Size) of a TCP packet on a PPPoE session.

Notes

If both this command and the **ip interface tcp mss limit** command are enabled, the MSS is limited to the smaller value.

[Applied Model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.13.12 Set whether to forcibly disconnect PPPoE sessions that do not exist on the router side**Format**

pppoe invalid-session forced close sw
no pppoe invalid-session forced close

[Setting Value and Initial Value]

- *SW*
- [Setting Value]:

Setting Value	Description
on	Do not forcibly disconnect PPPoE sessions that do not exist on the router side
off	Do not forcibly disconnect PPPoE sessions that do not exist on the router side

- [Initial Value]: on

Description

Set whether to forcibly disconnect PPPoE sessions that do not exist on the router side.

[Applied Model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

9.13.13 Specifying an Interface to Relay PPPoE Frames**[Format]**

pppoe pass-through member interface interface [interface...]
no pppoe pass-through member [...]

[Setting Value and Initial Value]

- *interface*
- [Setting Value]: LAN interface name
- [Initial Value]: -

[Description]

Specify an interface that uses the PPPoE pass-through function.

A PPPoE frame is relayed between the specified interfaces.

The LAN interface name can specify a physical LAN interface and an interface used in a LAN division function.

[Notes]

The specified LAN interface operates in promiscuous mode.
RTX830 can be used with Rev.15.02.03 or later.
RTX1210 can be used with Rev.14.01.26 or later.
RTX5000 and RTX3500 can be used with Rev.14.00.26 or later.

The number of *interfaces* that can be set is as follows.

Model	Maximum number that can be set	
RTX5000	10	
RTX3510	10	
RTX3500	10	
RTX1300	8	
RTX1220	10	
RTX1210	10	
RTX840	5	
RTX830	5	

[Applicable Model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 10

DHCP Settings

This unit implements the DHCP server function, the DHCP relay agent function, and the DHCP client function as the DHCP(*1) function.

The basic network environment can be set automatically by using the DHCP function.

The DHCP client function is implemented in OSs such as Windows, and by combining these functions with the DHCP server function and the DHCP relay agent function of this unit, the basic network environment of the DHCP client can be set automatically.

The router can be set to function as a DHCP server or a DHCP relay agent, or not to function either way, by using the **dhcp service** command. The current settings can be found by using the **show status dhcp** command.

The DHCP server function receives a configuration request from a DHCP client and assigns an IP address. (lease), netmask, DNS server information, etc. are provided.

The range of the IP address to be assigned and the lease period are set by the **dhcp scope** command.

Multiple ranges of IP addresses can be set, and each range is managed by the DHCP scope number. When a configuration request is received from a DHCP client, the DHCP server automatically notifies you of unallocated IP addresses in the DHCP scope. Note that if you lease a specific IP address to a specific DHCP client, you can reserve it by using the scope number defined by the dhcp scope command. To cancel reservation, use the **no dhcp scope bind command**. The lease period of the IP address can be both timed and indefinite, which is specified by the parameters of the expire and maxexpire keywords of the **dhcp scope** command.

The lease status can be found by using the **show status dhcp** command. The IP address information of the DNS server to notify the DHCP client is set by the **dns server** command.

The DHCP relay agent function forwards requests from a local segment DHCP client to a DHCP server in a preconfigured remote network segment. The remote segment DHCP server can be configured by using the **dhcp relay server** command. If there are multiple DHCP servers, you can specify the selection method by using the **dhcp relay select** command.

Also, the DHCP client function can receive IP address and default routing information of an interface from an external DHCP server. Whether or not to make a router function as a DHCP client is determined by setting values of each command of the **ip interface address**, the **ip interface secondary address**, the **ip pp remote address**, and the **ip pp remote address pool**. The setting can be found by using the **show status dhcpc** command.

(*1)Dynamic Host Configuration Protocol; RFC1541 , RFC2131

10.1 The DHCP server relay agent function

10.1.1 Setting the Behavior of DHCP

[Settings]

dhcp service type
no dhcp service [type]

[Settings and Initial Values]

- *type*
- [Settings]:

Settings	Description
server	Function as a DHCP server.
relay	Function as a DHCP relay agent.

- [Initial Values]: -

[Explanation]

Set functions related to DHCP.

When using the DHCP relay agent function, the NAT function cannot be used.

[Notes]

For the setting values of this command in the factory default state and after executing the **cold start** command, refer to "1.7 Setting Values in Factory default State or Initial State after Deployment".

[Applicable Models]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.1.2 Setting the Behavior to Compatible with RFC2131**[Settings]**

dhcp server rfc2131 compliant *comp*

dhcp server rfc2131 compliant [*except*] *function* [*function..*]

no dhcp server rfc2131 compliant

[Settings and Initial Values]

- *Comp*

- [Settings]:

Settings	Description
on	RFC2131 準拠
off	RFC1541 Compliant

- [Initial Values]: on
- *except* : Keywords that are compatible with RFC2131 except for the specified functions
- [Initial Values]: -
- *Function*

- [Settings]:

Settings	Description
broadcast-nak	Broadcast DHCPNAK
none-domain-null	Do not add a null character to the end of a domain name
remain-silent	from clients who do not have lease information Ignore DHCPREQUEST
reply-ack	DHCPACK storing tolerance values instead of DHCPNAK Returns
use-clientid	Prefer Client-Identifier option for client identification

- [Initial Values]: -

[Explanation]

Specifies the behavior of the DHCP server. RFC2131 Compliant when on RFC2131 Compliant Operation When off
Also, specify the following parameters when only individual functions described in RFC2131 are supported based on RFC1541. Multiple parameters can be specified separated by spaces. When the *except* keyword is specified, functions other than the specified parameters become compatible with RFC2131.

broadcast-nak	DHCPNAK broadcasts to clients on the same subnet. For a DHCPREQUEST sent by a client in the INIT-REBOOT state, set a Bbit if it is addressed to giaddr.

none-domain-null	Do not add a NULL character to the end of this domain name. RFC1541 did not specify whether to add a NULL character to the end of a domain name, but RFC2131 prohibited it. On the other hand, Windows NT/2000's DHCP server adds a NULL character. Therefore, there is a clause that expects that a DHCP client on a Windows-based OS has a NULL character, and if there is no NULL character, problems such as display disorder in winipcfg.exe may occur.
remain-silent	When a DHCPREQUEST is received from a client, DHCPNAK is not sent if the client does not have lease information.
reply-ack	Even if an option value (excluding the request IP address) that is unacceptable due to the lease period, etc. is requested by the client, DHCPNAK is not returned, but a DHCPACK containing an allowable value is returned.
use-clientid	The Client-Identifier option is preferred over the chaddr field for client identification.

[Notes]

For the setting values of this command in the factory default state and after executing the **cold start** command, refer to "1.7 Setting values in the factory default state or in the initial state after deployment".

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.1.3 Setting whether to check for duplicate leased IP addresses

[Format]

dhcp duplicate *check check1 check2*

no dhcp duplicate

check

- *check1*: Waiting time for checking checks outside the LAN
- [Setting value]

Setting value	Description
1..1000	Millisecond
off	Do not check inside the LAN

- [Initial value]: 100
- *check2*: Waiting time for checking checks outside the LAN (via a DHCP relay agent)
- [Setting value]

Setting value	Description
1..3000	Millisecond
off	Do not check outside the LAN (via a DHCP relay agent)

- [Initial value]: 500

Description

When acting as a DHCP server, it sets whether to check that there are no other hosts using an IP address just before leasing it to a DHCP client.

[Notes]

Use ARP for scopes outside the LAN and PING for scopes outside the DHCP relay agent.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.1.4Defining DHCP scope

[Format]

dhcp scope *scope_num ip_address-ip_address/netmask* [except *ex_ip ...*] [*gateway gw_ip*] [*expire time*] [*maxexpire time*] **no dhcp scope** *scope_num [ip_address-ip_address/netmask* [except *ex_ip...*] [*gateway gw_ip*] [*expire time*] [*maxexpire time*]]

[Setting value and initial value]

- *scope_num*
 - Setting value: Scope number (1..65535)
 - [Initial value]: -
- *ip_address-ip_address*
 - Setting value: Scope of IP addresses to be allocated to the target subnet
 - [Initial value]: -
- *netmask*
 - Setting value:
 - xxx.xxx.xxx.xxx (where xxx is a decimal number)
 - Hexadecimal numbers following 0x
 - Number of mask bits
 - [Initial value]: -
- *ex_ip*
 - Setting value: IP addresses to be excluded from the IP addressing range (multiple addresses can be specified separated by spaces, ranges can also be specified using '-')
 - [Initial value]: -
- *gw_ip*
 - [Setting value]: IP address of the gateway of the target network
 - [Initial value]: -
- *time*: Time
 - [Setting value]:
 - expire time: Lease term when there is no lease term request from the DHCP client
 - maxexpire time: Maximum allowable lease term when there is a lease term request from the DHCP client

Setting value	Description
1..2147483647	[Setting value]: IP address (IP address) : IP address of the gateway (IP address) : IP address of the gateway (IP address) : IP address of the gateway (IP address) : IP address of the gateway (IP address) : IP address of the gateway (Rev. 14.01.31 or earlier and RTX830 Rev. 15.02.07 or earlier)
1..21474836	Minute (other than the above)
xx: xx	Time: Minute
infinity	Indefinite lease

- [Initial value]:
 - expire time=72:00
 - maxexpire time=72:00

Description

Set the scope of the IP address to be allocated as a DHCP server.

Multiple excluded IP addresses can be specified. Indefinite lease term can be specified, and maximum allowable lease term can be specified when there is a request from the DHCP client.

[Notes]

Multiple DHCP scopes of the same network can be set (excluding RTX5000 / RTX3500 Rev. 14.00.25 or earlier, RTX1210 Rev. 14.01.27 or earlier and RTX830 Rev. 15.02.02 or earlier).

The same IP address cannot be included in multiple DHCP scopes. When the IP address range includes a network address and a broadcast address, it is excluded from the assignable address.

For the vRX series, the *netmask* setting value must be within the range of /16 (255.255.0.0) to /32 (255.255.255.255).

If the configuration parameter by gateway keyword is omitted for a DHCP client that does not go through a DHCP relay agent, the router's own IP address is notified.

The expire setting value must be less than or equal to the maxexpire setting value.

For the setting values of this command in the factory default state and after executing the **cold start** command, refer to "1.7 Setting values in the factory default state or initial state after deployment".

In Rev. 14.00.21 or earlier of RTX5000 / RTX3500 and Rev. 14.01.20 or earlier of RTX1210, the following commands with the same **scope** ID are deleted when the **dhcp scope** command is executed.

- **dhcp scope bind**
- **dhcp scope option**

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.1.5 Setting DHCP reserved addresses

[Format]

```
dhcp scope bind scope_num ip_address [type]
id dhcp scope bind scope_num ip_address
mac_address dhcp scope bind scope_num
ip_address ipcp
dhcp scope bind scope_num ip_address-ip_address mac_address
no dhcp scope bind scope_num ip_address
no dhcp scope bind scope_num ip_address-ip_address
```

[Set value and initial value]

- *scope_num*
 - Setting value: Scope number (1..65535)
 - Initial value: -
- *ip_address*
 - [Set value]

Setting value	Description
xxx.xxx.xxx.xxx	(xxx is a decimal number) Reserved IP address
*	Do not specify the IP address to allocate

- Initial value: -
- *type* : Client-Identifier Determine optional *type* field
 - [Set value]

Setting value	Description
text	0x00
ethernet	0x01

- [Setting value]: -
- [Setting value]:
- [Setting value]:

Setting value	Description
If <i>type</i> is ethernet	MAC address
If <i>type</i> is text	String
If <i>type</i> is omitted	A two-digit hexadecimal sequence, beginning with the <i>type</i> field

- [Setting value]: -
- *mac_address*
- [Setting value]:
 - xx:xx:xx:xx:xx:xx (where xx is a hexadecimal number) Reserved DHCP client's MAC address
 - Only OUI (vendor ID) is specified by setting the lower three octets to an asterisk (*) as in xx:xx:xx:*

- [Setting value]: -
- `ipcp`: Keyword indicating that IPCP gives it to the remote side
- [Setting value]: -

[Explanation]

A DHCP client to which an IP address is assigned is fixedly set.

Only the client can be specified without fixing the IP address. When deleting this format, the client identifier cannot be omitted.

[Notes]

The IP address must be within the DHCP scope range specified by the `scope_num` parameter. Within one DHCP scope, multiple IP addresses cannot be set for one MAC address. When another DHCP client is reserved for an IP address under lease, the IP address is allocated after the lease ends.

The specification of `ipcp` is limited to the number of B channels that can be connected simultaneously. Also, the address given by IPCP is selected from the scope on the LAN side.

When using the first format of a command, it must be configured to use the functions of **dhcp server rfc2131 compliant** on or `use-clientid` in advance. When the functions of **dhcp server rfc2131 compliant** off or `use-clientid` are not used, reservations other than those in the second format of the command are deleted.

The client identifier in the first format of a command sets the value that the client optionally sends. When the `type` parameter is omitted, the value of the `type` field is also entered. When specifying a keyword in the `type` parameter, only the value of the Client-Identifier field is entered because the `type` field value is uniquely determined.

Reservation in the second format of a command at a MAC address uses the `chaddr` field of a DHCP packet to identify the client. This form of reservation function will only work if the RT configuration is configured to not use the functions of **dhcp server rfc2131 compliant** on or `use-clientid`, or if the DHCP client does not attach the Client-Identifier option in a DHCP packet.

When a client uses the Client-Identifier option, reservation in the second format of a command is invalid when the functions of **dhcp server rfc2131 compliant** on or `use-clientid` parameter is specified, so it must be reserved again with the value sent by the Client-Identifier option.

Multiple OUIs (vendor IDs) can be set in the second format of a command. When both OUI (vendor ID) and MAC address settings are present, the MAC address setting takes precedence.

The OUI (vendor ID) setting cannot be specified for the following models and revisions. RTX5000 / RTX3500 Rev.14.00.25 or earlier
RTX1210 Rev.14.01.27 以前
RTX830 Rev.15.02.02 or earlier

When the **dhcp scope** command is executed, the settings of the following commands with the same scope ID are deleted when the RTX5000 / RTX3500 Rev.14.00.21 or earlier and the RTX1210 Rev.14.01.20 or earlier are executed.

- **dhcp scope bind**
- **dhcp scope**

option

```
A. # dhcp scope bind 1 192.168.100.2 ethernet 00:a0:de:01:23:45
B. # dhcp scope bind 1 192.168.100.2 text client01
C. # dhcp scope bind 1 192.168.100.2 01 00 a0 de 01 23 45 01 01 01
D. # dhcp scope bind 1 192.168.100.2 00:a0:de:01:23:45
E. # dhcp scope bind 1 192.168.100.2-192.168.100.19 00:a0:de:*
```

1. If the functions of **dhcp server rfc2131 compliant** on or `use-clientid` are used

- A. B. The C format uses the Client-Identifier option to identify the client.
- The D format uses the `chaddr` field of a DHCP packet. However, if the Client-Identifier option is present, this setting is ignored.

The DHCP server uses the Client-Identifier option value in preference to the `chaddr` field value.

It is also possible to determine whether or not the client uses the Client-Identifier option by executing the **show status dhcp** command to check the client's identifier.

- If a MAC address is displayed as a leased client, the Client-Identifier option is not used
 - If a hexadecimal character string or character string is displayed as a leased client, the Client-Identifier option is used.
2. If the **dhcp server rfc2131 compliant** off or use-clientid function is not used
- A. B. It cannot be specified in the C format. The Client-Identifier option is ignored.
 - The D format uses the chaddr field of a DHCP packet.

There are the following points to be noted regarding mutual operation with the client.

- Since using individual functions alone may cause unexpected behavior on the client side, it is recommended to use it with **dhcp server rfc2131 compliant** on or **dhcp server rfc2131 compliant** off.
- If the lease information is deleted by restarting the router or reconfiguring the scope, the IP address used by the client may change when an address extension request is made or when the client is restarted within the lease period.

To prevent this, there is a setting to **dhcp server rfc2131 compliant** on (or enable the remain-silent feature). With this setting, Yamaha routers do not return DHCPNAK for DHCPREQUEST from clients that do not have lease information, and ignore it.

As a result, if the DHCPDISCOVER issued by the client at the expiration of the lease period includes the Requested IP Address option, it is possible to continue to lease the same IP address to that client.

In the format of E., only OUI (vendor ID) is specified, and IP addresses can be assigned only to devices with that OUI (vendor ID).

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.1.6 Setting DHCP address assignment behavior

[Format]

dhcp scope lease type scope_num type [fallback=fallback_scope_num]

no dhcp scope lease type scope_num [type ...]

[Setting value and initial value]

- *scope_num, fallback_scope_num*
 - [Setting value]: Scope number (1-65535)
 - [Initial value]: -
- *type*: Assignment behavior
 - [Setting value]:

Setting value	Description
bind-priority	Prioritize the assignment of reservation information
bind-only	Limit and assign reservation information only

- [初期値]: bind-priority

[Explanation]

Controls how addresses are allocated in the DHCP scope specified by *scope_num*.

If bind-priority is specified for *type*, clients reserved by the **dhcp scope bind** command are allocated the IP address as reserved, and non-reserved clients are allocated a free address that is not reserved for other clients as long as it is within the scope.

If bind-priority is specified for *type*, the fallback option cannot be specified.

If bind-only is specified for *type*, the behavior changes depending on whether the fallback scope is specified in the fallback option.

If the fallback option is not specified, an IP address is allocated only to clients reserved by the **dhcp scope bind** command, and no IP address is allocated to non-reserved clients even if there is a free address in the scope.

If bind-only is specified for *type* and fallback scope is specified at the same time with the fallback option, the behavior is as follows.

1. When a client has an IP address reserved in scope, it allocates the IP address as reserved.
2. When a client has no IP address reserved in scope but is reserved in fallback scope, it allocates the IP address as reserved in fallback scope.
3. When a client has no IP address reserved in either scope or fallback scope, the behavior changes depending on the setting of the **dhcp scope lease type command** for fallback scope.
 - a. When the **dhcp scope lease type** command for fallback scope is set to bind-priority, the client allocates it as long as there is a free address in fallback scope.
 - b. When the **dhcp scope lease type command** for fallback scope is set to bind-only, no IP address is allocated to the client.

In either case, the lease term follows the definition of each DHCP scope. The lease term follows the definition of each DHCP scope.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.1.7 Generation of reservation settings based on DHCP allocation information

[Format]

dhcp convert lease to bind scope_n [except] [idx [...]]

[Setting value and initial value]

- *scope_n*
 - [Setting value]: Scope number (1-65535)
 - [Initial value]: -
- *idx*
 - [Setting value]:

Setting value	Description
Number	Index numbers displayed by the show status dhcp summary command, up to 100
all	Target all information under allocation
Omitted	All if omitted

- [Initial value]: -

[Explanation]

Create reservation settings based on current allocation information. When an except keyword is indicated, information other than the specified number is reflected in reservation settings.

[Notes]

The following conversion rules convert IP address allocation information into reservation settings.

Client identification type of IP address allocation information (name displayed by show status dhcp)	Client identification information example	Example of reservation setting information
Client Ethernet address	00:a0:de:01:02:03	ethernet 00:a0:de:01:02:03 *1
		00:a0:de:01:02:03 *2
Client ID	(01) 00 a0 de 01 02 03	ethernet 00:a0:de:01:02:03
	(01) 00 a0 de 01 02 03 04	(01) 00 a0 de 01 02 03 04
	(01) 31 32 33	00 31 32 33

*1: If rfc2131 is set to "compliant on" or "use-clientid", the display of such IP address assignment information is likely to be the result of an ARP check, and since the client ID option is used for normal assignment, reservation settings are made in this format. However, if there are hosts using a client ID different from the MAC address, reservation by this automatic conversion does not work effectively, and reservation settings for such hosts must be made separately.

*2: If rfc2131 is set to "compliant off" or "use-clientid", the chaddr field is used.

Reservation settings are created based on assignment information at the time of command execution. If a time elapses between the summary display and the execution of this conversion command, it should be confirmed in **show config** that the reservation for the intended pair has been created after executing this command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.1.8 Setting DHCP Options

Format

dhcp scope option *scope_num* option=*value* [option=*value*...]

no dhcp scope option *scope_num* [...]

Setting Values and Initial Values

- *scope_num*
 - Setting Values: Scope Number (1..65535)
 - Initial Values: -
- *option*

- Setting Values:
 - Option Numbers
 - 1..49, 62..254
 - The Mnemonic
 - Major Mnemonics

router	3
dns	6
Hostname	12
domain	15
wins_server	44

- Initial Values: -
- *value* : Optional Values
 - Setting Values:
 - There are the following types of values, which can be used are determined by the option number. Parables For example, 'router', 'dns' and 'wins_server' are arrays of IP addresses, and 'hostname' and 'domain' are strings.

One Octet Integer	0.255
Two Octet Integer	0.65535
Two Octet Integer Array	Two Octet Integers with Commas (,)
Four Octet Integer	0..2147483647
IP Addresses	IP Addresses
Arrays of IP Addresses	IP Addresses with Commas (,)
Strings	Strings
Switch	"on","off","1","0" のいずれか
Binary	Two-digit hexadecimal numbers arranged with commas (,).

- [Initial value]: -

[Explanation]

Set the DHCP option to be sent to the scope. The **dns server** command and the **wins server** command also implicitly sent the DHCP option, but it can be specified explicitly. Also, implicit DHCP options do not allow scopes to change the value of the option, but this command allows it.

[Notes]

In Rev. 14.00.21 or earlier for RTX5000/RTX3500 and Rev. 14.01.20 or earlier for RTX1210, when the **dhcp scope** command is executed, the settings of the following commands with the same scope ID are deleted.

- **dhcp scope bind**
- **dhcp scope option**

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.1.9 Manually adding DHCP lease information

[Format]

dhcp manual lease *ip_address* [*type*] **id**

dhcp manual lease *ip_address*

mac_address **dhcp manual lease**

ip_address **ipcp**

[Setting value and initial value]

- *ip_address*
 - [Setting value]: IP address to lease
 - [Initial value]: -
- *type* : Client-Identifier Determines the optional type field
 - [Setting value]:

Setting value	Explanation
text	0x00
ethernet	0x01

- [Initial value]: -
- *Id*
 - [Setting value]:

Setting value	Explanation
If <i>type</i> is text	String
If <i>type</i> is ethernet	MAC address
If <i>type</i> is omitted	A two-digit hexadecimal sequence, headed by the <i>type</i> field

- [Initial value]: -
- *mac_address*
 - [Setting value]: XX:XX:XX:XX:XX (XX is hexadecimal) DHCP client MAC address
 - [Initial value]: -
- *ipcp* : Keywords given to the remote side by IPCP
 - [Initial value]: -

[Explanation]

Manually add lease information for a specific IP address

[Notes]

This command affects automatic DHCP address distribution and should not be used unless you intend to add lease information for a specific IP address.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.1.10 Manually delete DHCP lease information

[Format]

dhcp manual release *ip_address*

[Setting value and initial value]

- *ip_address*
 - [Setting value]: IP address to release
 - [Initial value]: -

[Description]

Manually delete lease information for a specific IP address

[Notes]

This command affects automatic DHCP address distribution and should not be used unless you intend to delete lease information for a specific IP address.

[Applicable model]

[Settings] vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.1.11 Configuring Specified DHCP Servers

[Settings]

dhcp relay server *host1* [*host2* [*host3* [*host4*]]]

no dhcp relay server

[Settings and initial values]

- *host1..host4*
 - [Settings]: IP address of the DHCP server
 - [Initial values]: -

[Explanation]

Up to four servers are configured to relay DHCPBOOTREQUEST packets.

If more than one server is specified, a BOOTREQUEST packet is copied and relayed to all servers, or

The setting of the **dhcp relay select** command determines whether only one server is selected and relayed.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.1.12 Setting the starting port number used in the DHCP relay agent function

[Formats]

dhcp relay srcport *port*

no dhcp relay srcport [*port*]

[Settings and initial values]

- *port*
 - [Settings]: Port number (1..65535)
 - [Initial values]: 68

[Explanation]

Setting the starting port number used in the DHCP relay agent function

[Notes]

RTX5000 and RTX3500 can be used with Rev.14.00.29 or later, RTX1210 Rev.14.01.36 or later, and RTX830 Rev.15.02.15 or later.

[Applicable models]

vRX VMware ESXi version, vRX Sakura Cloud Edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.1.13 Setting the DHCP server selection method

[Formats]

dhcp relay select *type*

no dhcp relay select [*type*]

[Settings and initial values]

- *type*
 - [Settings]:

Settings	Explanation
hash	Use the Hash function to select only one server

Settings	Explanation
all	Select all servers

- [Initial values]: hash

[Explanation]

Set the handling of multiple servers set by the **dhcp relay server** command.

If hash is specified, only one server is selected using the Hash function and the packet is relayed. Since this Hash function uses the chaddr field of a DHCP message as an argument, the same server should always be selected for the same DHCP client. If all is specified, the packet is duplicated and relayed to all servers.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.1.14 Setting relay criteria for DHCP BOOTREQUEST packets

[Formats]

dhcp relay threshold *time*

no dhcp relay threshold [*time*]

[Settings and initial values]

- *time*
 - [Settings]: Number of seconds (0.65535)
 - [Initial values]: 0

[Explanation]

Comparing the secs field of a DHCP BOOTREQUEST packet with the number of seconds by this command, a DHCP BOOTREQUEST packet with a smaller secs field than the setting value should not be relayed to the server.

This makes it possible to avoid relaying packets to a remote DHCP server even if there is another DHCP server on the same LAN.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.1.15 Setting DHCP operation for each interface

[Format]

ip interface dhcp service type [*host1* [*host2* [*host3* [*host4*]]]]

no ip interface dhcp service

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name, bridge interface name
 - [Initial value]: -
- *type*
 - [Setting value]:

Setting value	Description
off	It does not function as a DHCP server or a DHCP relay agent
server	It functions as a DHCP server
relay	It functions as a DHCP relay agent

- [Initial value]: -
- *host1..host4*
 - [Setting value]: IP address of the DHCP server
 - [Initial value]: -

[Description]

The operation of DHCP is set for each interface.

When a DHCP server is set, one IP address is allocated from a DHCP scope that matches the network address.

When a DHCP relay agent is set, it is necessary to set a HOST, and forwards a DHCP DISCOVER packet and a DHCP REQUEST packet to this HOST.

When it is set to off, it does not operate as a DHCP server or a DHCP relay agent. The DHCP packet is discarded.

When this setting is not available, it follows the setting of the dhcp service command. When both the setting of the dhcp service command and this setting exist, this setting takes precedence.

[Notebook]

The bridge interface cannot be specified in vRX Amazon EC2 version.

RTX5000, RTX3500 can be used with Rev.14.01.18 or later.

RTX1210 can be used with Rev.14.01.09 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.2 DHCP client function

10.2.1 DHCP client host name setting

[Format]

```
dhcp client hostname interface primary
host dhcp client hostname interface
secondary host dhcp client hostname pp
peer_num host
dhcp client hostname pool pool_num host
no dhcp client hostname interface primary
[host] no dhcp client hostname interface
secondary [host] no dhcp client hostname pp
peer_num [host]
no dhcp client hostname pool pool_num [host]
```

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - LAN interface name
 - WAN interface name
 - Not specified in vRX series, RTX5000, and RTX3500
 - Bridge interface name
 - [Initial value]: -
- *peer_num*
 - [Setting value]:
 - Counterparty information number
 - anonymous
 - [Initial value]: -
- *pool_num*
 - **ip pp remote address pool** IP address number obtained by the **dhcpc** command. For example, in a model that can obtain two IP addresses with the **ip pp remote address pool dhcpc** command, it is possible to assign an arbitrary ID to each client ID option by setting *pool_num* to "1" or "2". (**1..ip pp remote address pool** Maximum number of IP addresses obtained by the **dhcpc** command)
 - [Initial value]: -
- *host*
 - [Setting value]: Host name of the DHCP client
 - [Initial value]: -

[Description]

Set the host name of the DHCP client.

[Notes]

The bridge interface cannot be specified for vRX Amazon EC2 version and RTX5000 / RTX3500 Rev.14.00.11 or earlier.

Secondary cannot be specified when the WAN interface is set.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.2.2 Setting the IP address lease period to request

[Format]

ip *interface* **dhcp lease time** *time*

no ip *interface* **dhcp lease time** [*time*]

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - LAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - Bridge interface name
 - [Initial value]: -
- *time*
 - [Setting value]: Fraction (1..21474836)
 - [Initial value]: -

[Description]

Set the lease period of the IP address requested by the DHCP client.

[Notes]

If the request for the lease period is not accepted, use the lease period from the DHCP server if it is not requested. Bridge interface cannot be specified for vRX Amazon EC2 version and RTX5000 / RTX3500 Rev.14.00.11 or earlier.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.2.3 Setting the number of times and interval for retransmitting an IP address acquisition request

[Format]

ip *interface* **dhcp retry** *retry interval*

no ip *interface* **dhcp retry** [*retry interval*]

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - LAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - WAN interface name
 - [Initial value]: -
- *retry*
 - [Setting value]:

Setting value	Explanation
1..100	Number of times
infinity	Unlimited

- [Initial value]: infinity
- *Interval*
 - Setting value: Number of seconds (1..100)
 - [Initial value]: 5

[Description]

Set the number of times and interval for retrying when the acquisition of the IP address fails.

[Notes]

Bridge interface cannot be specified for vRX Amazon EC2 version and RTX5000 / RTX3500 Rev.14.00.11 or earlier

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.2.4 Setting the DHCP client IDoption

[Format]

```
dhcp client client-identifier interface primary [type type]
id dhcp client client-identifier interface secondary [type
type] id dhcp client client-identifier pp peer_num [type
type] id
dhcp client client-identifier pool pool_num [type type] id
no dhcp client client-identifier interface
primary no dhcp client client-identifier
interface secondary no dhcp client client-
identifier pp peer_num
no dhcp client client-identifier pool pool_num
```

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - Bridge interface name
 - [Initial value]: -
- *type*: ID The keyword indicating that the value of the optional type field is set.
 - [Initial value]: -
- *type*
 - [Setting value]: The value of the optional type field.
 - [Initial value]: 1
- *id*
 - [Setting value]:
 - ID expressed as an ASCII string
 - ID expressed as a two-digit hexadecimal number sequence
 - [Initial value]: -
- *peer_num*
 - [Setting value]:
 - Counterparty information number
 - anonymous
 - [Initial value]: -
- *pool_num*

- [Setting value]: IP address number obtained by the **ip pp remote address pool dhcpc** command. For example, in a model where two IP addresses can be obtained by the **ip pp remote address pool dhcpc** command, an arbitrary ID can be given to each client ID option by setting *pool_num* to "1" or "2". (1..**ip pp remote address pool dhcpc** The maximum number of IP addresses that can be obtained by the **pool dhcpc** command)
- [Initial value]: -

[Explanation]

Set the optional type field and ID of the DHCP client ID.

[Notes]

Bridge interface cannot be specified for vRX Amazon EC2 version and RTX5000 / RTX3500 Rev.14.00.11 or earlier. Secondary cannot be specified when the WAN interface is configured.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.2.5 Setting optional storage in messages sent by a DHCP client to a DHCP server

[Format]

```
dhcpc client option interface primary
option=value dhcpc client option interface
secondary option=value dhcpc client option pp
peer_num option=value
dhcpc client option pool pool_num option=value
no dhcpc client option interface primary
[option=value] no dhcpc client option interface
secondary [option=value] no dhcpc client option pp
peer_num [option=value]
no dhcpc client option pool pool_num [option=value]
```

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Cannot be specified for vRX series, RTX5000, and RTX3500
 - Bridge interface name
 - [Initial value]: -
- *option*
 - [Setting value]: Option number (decimal)
 - [Initial value]: -
- *value*
 - [Setting value]: Option value to be stored (can be specified in hexadecimal, separated by "") Option length information does not need to be entered.
 - [Initial value]: -
- *peer_num*
 - [Setting value]:
 - Counterparty information number
 - anonymous
 - [Initial value]: -
- *pool_num*
 - [Setting value]: IP address number obtained by the **ip pp remote address pool dhcpc** command. For example, in a model where two IP addresses can be obtained by the **ip pp remote address pool dhcpc** command, any ID can be assigned to each client ID option by setting *pool_num* to "1" or "2". (1..**ip pp remote address pool dhcpc** Maximum number of IP addresses that can be obtained with the **dhcpc** command)
 - [Initial value]: -

[Explanation]

Sets an option to be stored in a message sent by a DHCP client to a DHCP server.

[Notes]

This command is set only when it is necessary for interconnection with a server. The obtained option value is not used internally.

Bridge interface cannot be specified in vRX Amazon EC2 version and RTX5000 / RTX3500 Rev.14.00.11 or earlier.
Secondary cannot be specified when the WAN interface is set.

[Configuration Example]

Request a specific address (192.168.0.128) when obtaining a LAN2 primary address from a DHCP server.

```
# dhcp client option lan2 primary 50=c0,a8,00,80
# ip lan2 address dhcp
(Note: However, even in this case, it is up to the server whether or not the request address is given)
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

10.2.6 Setting whether or not to release information when the link is down**[Format]**

dhcp client release linkdown switch [*time*]

no dhcp client release linkdown [*switch* [*time*]]

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Description
on	When the link of the interface continues for <i>time</i> seconds, the acquired information is released.
off	Information is retained when the interface links down

- [Initial value]: off
- *time*
 - Setting value: Number of seconds (0..259200)
 - [Initial value]: 3

[Explanation]

When the interface that obtains an IP address from the DHCP server as a DHCP client links down

Set whether or not to release information obtained from the DHCP server.

A timer works when the link is down, and when the link state continues for *time* seconds, the information is released. When *time* is not set, *time* is 3 seconds.

When the information is released, an attempt is made to obtain the information when the link is next up.

[Notes]

Setting a longer value of a timer avoids the effects of unstable link conditions. The setting of this command becomes effective after the link down occurs after executing the command.

When the link is up before the timer expires, the timer is cleared and the information is not released.

When the lease period of the information expires before the timer expires, the timer is cleared and the information is released. The running timer is cleared when the following command is executed.

ip interface address, ip pp remote address, ip pp remote address pool, dhcp client release linkdown

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 11

ICMP configuration

11.1 IPv4 configuration

11.1.1 Setting whether or not to send an ICMP Echo Reply

[Format]

```
ip icmp echo-reply send send
no ip icmp echo-reply send [send]
```

[Setting value and initial value]

- send*
- [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: on

[Description]

Sets whether or not to return an ICMP Echo Reply when an ICMP Echo is received.

[Applicable models]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.1.2 Setting whether or not to send an ICMP Echo Reply when a link is down

[Format]

```
ip icmp echo-reply send-only-linkup send
no ip icmp echo-reply send-only-linkup [send]
```

[Setting value and initial value]

- send*
- [Setting value]:

Setting value	Description
on	Returns an ICMP Echo Reply only when the link is up
off	Returns an ICMP Echo Reply regardless of the link status.

- [Initial value]: off

[Explanation]

When an ICMP Echo is received with the IP address given to the link-down interface as the end IP address, whether or not to return an ICMP Echo Reply is set. When set to on, it returns an ICMP Echo only when the link is up, so that the link status can be checked by ping. When set to off, it returns an ICMP Echo regardless of the link status.

[Applicable models]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.1.3 Setting whether or not to send an ICMP Mask Reply

[Format]

```
ip icmp mask-reply send send
no ip icmp mask-reply send [send]
```

[Setting value and initial value]

- *send*
- [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: on

[Description]

When an ICMP Mask Request is received, whether or not to return an ICMP Mask Reply is set.

[Applicable models]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.1.4 Setting whether or not to send an ICMP Parameter Problem

[Format]

ip icmp parameter-problem *send send*

no ip icmp parameter-problem *send [send]*

[Setting value and initial value]

- *send*
- [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: off

[Description]

Whether or not to send an ICMP Parameter Problem is set when an error is detected in the IP option of a received IP packet.

[Applicable models]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.1.5 Setting whether or not to send an ICMP Redirect

[Format]

ip icmp redirect *send send*

no ip icmp redirect *send [send]*

[Setting value and initial value]

- *send*
- [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: on

[Explanation]

When receiving an IP packet addressed to another gateway and forwarding the packet to an appropriate gateway, it is set whether or not to send an ICMP Redirect to the transmission source of the packet at the same time.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.1.6 Setting processing when receiving ICMP Redirect

[Format]

ip icmp redirect receive action

no ip icmp redirect receive [*action*]

[Setting value and initial value]

- *action*
- [Setting value]:

Setting value	Description
on	Processing
off	Ignoring

- [Initial value]: off

[Explanation]

When receiving an ICMP Redirect, it is set whether to process it and reflect it in its route table or ignore it.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.1.7 Setting whether or not to send ICMP Time Exceeded

[Format]

ip icmp time-exceeded send send [rebound=*sw*]

no ip icmp time-exceeded send [*send* rebound=*sw*]

[Setting value and initial value]

- *send*
- [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: on
- *SW*

- [Setting value]:

Setting value	Description
on	Send from a receiving interface
off	Send according to a route

- [Initial value]: off

[Explanation]

Since the TTL of a received IP packet has become zero, if the packet is discarded, it is set whether or not to send ICMP Time Exceeded to the transmission source of the packet at the same time.

When the rebound option is set to on, the original packet is sent from the receiving interface regardless of the route.

[Notes]

The rebound option cannot be specified before RTX5000 / RTX3500 Rev.14.00.11.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.1.8 Setting whether or not to send ICMP Timestamp Reply

[Format]

ip icmp timestamp-reply send *send*
no ip icmp timestamp-reply send [*send*]

[Setting value and initial value]

- *send*
- [Setting value]:

Setting value	Description
on	Sending
off	Do not send

- [Initial value]: on

[Explanation]

Set whether to return an ICMP Timestamp Reply when receiving an ICMP Timestamp.

[Applicable model]

Set whether to send ICMP Destination Unreachable or Not when receiving ICMP Destination Unreachable; Set whether to send ICMP Destination Unreachable; Set whether to send ICMP Destination Unreachable; Set whether to send ICMP Destination Unreachable; Set whether to send ICMP Destination Unreachable; Set whether to send ICMP Destination Unreachable; Set whether to send ICMP Destination Unreachable; Set whether to send ICMP Destination Un

11.1.9 Set whether to send ICMP Destination Unreachable or not.

[Format]

ip icmp unreachable send *send* [rebound=sw]
no ip icmp unreachable send [*send* rebound=sw]

[Setting value and initial value]

- *send*
- [Setting value]: set whether to send ICMP Destination Un

Setting value	Description
on	Sending
off	Do not send

- [Initial value]: on
- SW
- [Setting value]: set whether to send ICMP Destination Un

Setting value	Description
on	Sending from a receiving interface
off	Sending according to a route

- [Initial value]: on

[Explanation]

Set whether to send ICMP Destination Unreachable to a packet sender at the same time when no destination is found in a route table or when an IP packet cannot be resolved.

When the rebound option is set to on, the original packet is sent from a receiving interface regardless of a route.

[Notes]

The rebound option cannot be specified before RTX5000/RTX3500 Rev. 14.00.11.

[Applicable model]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.1.10 Set whether to send ICMP Destination Unreachable or not for packets decrypted by IPsec.

Format

```
ip icmp error-decrypted-ipsec send switch
no ip icmp error-decrypted-ipsec send [switch]
```

[Setting value and initial value]

- *switch*
- [Setting value]: set whether to send ICMP Destination Un

Setting value	Description
on	Send ICMP Error for packets decrypted by IPsec
off	Do not send ICMP Error for packets decrypted by IPsec

- [Initial value]: on

[Explanation]

Set whether to send ICMP Error for packets decrypted by IPsec.

[Notes]

Since the ICMP Error includes the head part of a decrypted packet, if the ICMP Error is not processed by IPsec even when it is returned to a sender, there is a possibility that communication to be protected by IPsec may flow to a network without being protected. In particular, care must be taken when switching whether to process by IPsec according to a protocol in filtered routing.

Setting not to send an ICMP error causes a phenomenon such as no response to traceroute.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.1.11 Setting whether to log received ICMP

[Format]

```
ip icmp log log
no ip icmp log [log]
```

[Setting value and initial value]

- *log*
- [Setting value]:

Setting value	Description
on	Record
off	Do not record

- [Initial value]: off

[Explanation]

Sets whether to log received ICMP errors in a DEBUG level log. Echo Request and Echo Reply logs are not recorded.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.1.12 Stealth function setting

[Format]

```
ip stealth all
ip stealth interface [interface...]
no ip stealth [...]
```

[Setting value and initial value]

- *all*: Stealth operation is performed on packets received at all logical interfaces

- [Initial value]: -
- *interface*
 - all: Stealth operation is performed on packets received at the specified logical interface
 - [Initial value]: -

[Explanation]

Setting this command prevents ICMP and TCP resets caused by packets coming to the router from the specified interface.

Normally, ICMP unreachable or TCP reset is returned when packets are received from the specified interface for protocols not supported by the router, IPv6 headers, or open TCP/UDP ports. However, setting this command can prevent it and hide the presence of the router when attacked by a port scanner or the like.

Notebook

Note that PING received at the interface specified by this command will not be answered.

ICMP caused by packets not destined for the router cannot be controlled by this command. To prevent them from being sent, it is necessary to use the `ip icmp *` command set.

The bridge interface can be specified with the firmware of RTX5000 / RTX3500 Rev.14.00.12 or later and all firmware of Rev.14.01 or later.

The WAN interface can be specified with the firmware of Rev.14.01 or later.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.1.13 Setting whether to perform MTU search by ARP**[Format]**

no IP interface arp mtu discovery *sw* [minimum=*min_mtu*]

no IP interface arp mtu discovery *sw* [minimum=*min_mtu*]

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *sw*
 - [Setting value]:

Setting value	Explanation
on	MTU search by ARP
off	No MTU search by ARP

- [Initial value]: on
- *min_mtu*
 - [Setting value]: Minimum MTU of search range
 - [Initial value]: 4000

[Explanation]

Sets whether to perform MTU search by ARP.

If this command is set to on when jumbo frames are available by the **lan type** command and the **ip mtu** command at the specified interface, it searches for the opponent's MTU by repeatedly sending a large-sized ARP to the opponent who can resolve the ARP.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300

11.1.14 Set whether to send ICMP Destination Unreachable for truncated packets**[Format]**

ip icmp unreachable-for-truncated *send send*

no ip icmp unreachable-for-truncated send [*send*]

[Setting value and initial value]

- *send*
- [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: on

[Explanation]

Sets whether to send ICMP Destination unreachable (Fragmentation needed) for packets received at the LAN interface but truncated because the length exceeded the MTU of that interface.

[Notes]

In a LAN using jumbo frames, the maximum value of jumbo frames differs depending on the host and switching hub. Therefore, communication becomes impossible unless jumbo frame sizes of all devices existing on the LAN are aligned.

If a misconfiguration causes a host to be configured to send packets larger than the router's frame size, the router normally discards packets that exceed the MTU of its own interface if it receives them, but if this command is set to on, it returns an ICMP error for such packets. This makes route MTU search effective, and it is expected that the host can quickly truncate the frame size to a small size.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300

11.2 IPv6 configuration

11.2.1 Set whether to send ICMP Echo Reply

[Format]

ipv6 icmp echo-reply send *send*

no ipv6 icmp echo-reply send [*send*]

[Setting value and initial value]

- *send*
- [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: on

[Explanation]

Set whether to send ICMP Echo Reply.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.2.2 Set whether to send ICMP Echo Reply when link is down

[Format]

ipv6 icmp echo-reply send-only-linkup *send*

no ipv6 icmp echo-reply send-only-linkup [*send*]

[Setting value and initial value]

- *send*
- [Setting value]:

Setting value	Description
on	Returns ICMP Echo Reply only when link is up
off	Returns ICMP Echo Reply regardless of link status

- [Initial value]: off

[Explanation]

Set whether to return ICMP Echo Reply when receiving an ICMP Echo with the IP address given to the interface being linked down as the end IP address. When set to on, ICMP Echo is returned only when the link is up, so that the state of the link can be checked by ping. When set to off, ICMP Echo is returned regardless of the state of the link.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.2.3 Setting whether or not to send ICMP Parameter Problem

[Format]

ipv6 icmp parameter-problem send send

no ipv6 icmp parameter-problem send [send]

[Setting value and initial value]

- *send*
- [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: off

[Explanation]

Setting whether or not to send ICMP Parameter Problem

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.2.4 Setting whether or not to send ICMP Redirect

[Format]

ipv6 icmp redirect send send

no ipv6 icmp redirect send [send]

[Setting value and initial value]

- *send*
- [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: on

[Explanation]

Setting whether or not to send ICMP Redirect

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.2.5 Setting of processing when receiving ICMP Redirect

[Format]

ipv6 icmp redirect receive *action*

no ipv6 icmp redirect receive [*action*]

[Setting value and initial value]

- *action*
- [Setting value]:

Setting value	Description
on	Processing
off	Ignoring

- [Initial value]: off

[Explanation]

Setting whether to process or ignore when receiving ICMP Redirect

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.2.6 Setting whether or not to send ICMP Time Exceeded

[Format]

ipv6 icmp time-exceeded send *send* [*rebound=sw*]

no ipv6 icmp time-exceeded send [*send rebound=sw*]

[Setting value and initial value]

- *send*
- [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: on
- *SW*
- [Setting value]: on

Setting value	Description
on	Send from a receiving interface
off	Send according to a route

- [Initial value]: off

Description

Set whether to send ICMP Time Exceeded.

When the rebound option is set to on, the original packet is sent from the received interface regardless of the route.

Notes

The rebound option cannot be specified in RTX5000 / RTX3500 Rev.14.00.11 or earlier.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.2.7 Set whether to send ICMP Destination Unreachable

[Format]

ipv6 icmp unreachable send *send* [*rebound=sw*]

no ipv6 icmp unreachable send [*send rebound=sw*]

[Configuration Example and Initial Value]

- *send*
- [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: on
- *SW*
- [Setting value]:

Setting value	Description
on	Send from a receiving interface
off	Send according to a route

- [Initial value]: off

Explanation

Set whether to send ICMP Destination Unreachable.

When the rebound option is set to on, the original packet is sent from the received interface regardless of the route.

Notes

The rebound option cannot be specified in RTX5000 / RTX3500 Rev.14.00.11 or earlier.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.2.8 Set whether to log received ICMP

[Format]

ipv6 icmp log log

no ipv6 icmp log [*log*]

Setting value and initial value

- *log*
- [Setting value]:

Setting value	Description
on	Record
off	Do not record

- [Initial value]: off

[Explanation]

Set whether or not to record received ICMP in a DEBUG type log.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.2.9 Setting whether or not to send ICMP Packet-Too-Big

[Format]

ipv6 icmp packet-too-big send send

no ipv6 icmp packet-too-big send [*send*]

[Setting value and initial value]

- *send*

- [Setting value]:

Setting value	Explanation
on	Send
off	Do not send

- [Initial value]: on

[Explanation]

Set whether or not to send ICMP Packet-Too-Big

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.2.10 Setting whether or not to send ICMP error for packets decrypted by IPsec

[Format]

ipv6 icmp error-decrypted-ipsec send *switch*

no ipv6 icmp error-decrypted-ipsec send [*switch*]

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Explanation
on	Send ICMP error for packets decrypted by IPsec
off	Send ICMP error for packets decrypted by IPsec

- [Initial value]: on

[Explanation]

Set whether or not to send ICMP error for packets decrypted by IPsec.

[Notebook]

Since the ICMP error includes the head part of a decrypted packet, if the ICMP error is not processed by IPsec even when it is sent back to the sender, there is a possibility that communications that are originally protected by IPsec will flow to the network without being protected. Especially, care must be taken when switching whether or not to process by IPsec according to a protocol in filtered routing.

If you set not to send ICMP error, it causes a phenomenon such as no response for traceroute.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.2.11 Setting stealth function

[Format]

ipv6 stealth all

ipv6 stealth interface [*interface...*]

no ipv6 stealth [...]

[Setting value and initial value]

- all: stealth operation for packets from all logical interfaces
 - [Initial value]: -
- *interface*
 - all: stealth operation for packets from all logical interfaces
 - [Initial value]: -

[Explanation]

Setting this command causes ICMP and TCP resets caused by packets coming to you from a specified interface. TCP reset is not returned.

Normally, when packets are received from a specified interface for a protocol or IPv6 header that you do not support, or a TCP/UDP port that is not open, ICMP unreachable or TCP reset is returned. However, if this command is set, it can be prohibited, and the existence of a router can be hidden when attacked by a port scanner.

[Note]

Note that it will not respond to PING from the specified interface.

ICMP caused by packets that are not addressed to you cannot be controlled by this command. To prevent them from being sent, it is necessary to use the `ipv6 icmp*` command set.

The bridge interface can be specified with the firmware of RTX5000 / RTX3500 Rev.14.00.12 or later, and all firmware of Rev.14.01 or later.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

11.2.12 Setting whether to send ICMP error (Packet Too Big) for frames truncated by size error

[Format]

`ipv6 icmp packet-too-big-for-truncated send send`

`no ipv6 icmp packet-too-big-for-truncated send [send]`

[Setting value and initial value]

- `send`
- [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: on

[Explanation]

Setting whether to send ICMP Packet Too Big for frames truncated because they were received by a LAN interface but were longer than the MTU of the interface.

[Notes]

In a LAN that uses jumbo frames, the maximum value of jumbo frames differs depending on the host and switching hub. Therefore, communication cannot be performed unless jumbo frame sizes of all devices existing on the LAN are aligned.

If a misconfiguration causes a host to be configured to send frames larger than the router's frame size, the router will normally discard frames that exceed the MTU of its interface if it receives them, but setting this command to on will return an ICMP error for such frames as well. This makes route MTU search effective, and it is expected that the host will quickly truncate the frame size to a smaller size.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300

CHAPTER 12

Tunneling

12.1 Setting tunnel interface permissions

Format

```
tunnel enable tunnel_num [tunnel_num ...]
no tunnel enable tunnel_num
```

Setting values and initial values

- tunnel_num
 - Setting values:

Setting values	Description
Numbers	Tunnel interface numbers
Number 1-Number 2	Tunnel interface numbers from number 1 to number 2
Number 1-	All tunnel interface numbers from number 1 onwards
Number 1	Tunnel interface numbers from number 1 onwards
all	All tunnel interfaces

- Initial values: -

Description

Making the tunnel interface usable.
When shipped from the factory, all tunnel interfaces are disabled, and this command must be used to enable them.
If more than one is specified, all of them can be used.

Multiple designations are not possible with RTX5000/RTX3500 Rev. 14.00.25 or earlier, RTX1210 Rev. 14.01.25 or earlier, and RTX830 Rev. 15.02.02 or earlier

Applicable models

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

12.2Setting tunnel interface permission disallowance

Format

```
tunnel disable tunnel_num
```

Setting values and initial values

- tunnel_num
 - Setting values:

Setting values	Description
Numbers	Tunnel interface numbers
Number 1-Number 2	Tunnel interface numbers from number 1 to number 2
Number 1-	All tunnel interface numbers from number 1 onwards
Number 1	All tunnel interface numbers from number 1 onwards

Setting values	Description
all	All tunnel interfaces

- Initial values: -

Description

Making the tunnel interface unusable.

Setting of a tunnel destination is preferably done in a disabled state.

If more than one is specified, all of them cannot be used.

Notes

Multiple designation of tunnel interfaces is not possible with RTX5000/RTX3500 Rev. 14.00.25 or earlier, RTX1210 Rev. 14.01.25 or earlier, and RTX830 Rev. 15.02.02 or earlier

Applicable models

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

12.3 Setting tunnel interface connection type

Format

tunnel type type [*role*]

no tunnel type [*type* [*role*]]

Setting values and initial values

- type*
 - [Setting value]:

Setting value	Description
point-to-point	Point-to-point tunnel
multipoint	Point-to-multipoint tunnel

- [初期値] : point-to-point
- role*

- [Setting value]:

Setting value	Description
server	Assigning a role for a client
client	Assigning a role for a client

- [Initial value]: client

Description

A connection type of a tunnel interface is set to a point-to-point tunnel having only one connection destination or a point-to-multipoint tunnel (multipoint tunnel) having multiple connection destinations.

The *role* option is an option that can be set only when the *type* is set to multipoint, and in the multipoint tunnel, it is necessary to specify one or more servers and one or more clients from among multiple routers connected to the same tunnel.

[Notes]

The basic configuration of a multipoint tunnel is a hub-and-spoke type configuration, and normally, server is specified only in the *role* option of a hub router. Server cannot be specified in RTX840 and RTX830 Rev. 15.02.22 or earlier.

RTX1210 can be used with Rev. 14.01.20 or later.

RTX5000 / RTX3500 can be used with Rev. 14.01.26 or later.

Extended license support

RTX830 can specify server in the *role* option when an [extended license \(YSL-VPN-EX1\)](#) is imported.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

12.4 Setting of tunnel interface type

Format

tunnel encapsulation *type*

no tunnel encapsulation

[Setting value and initial value]

- *type*
 - [Setting value]:

Setting value	Description
ipsec	IPsec tunnel
ipip	IPv6 over IPv4 tunnel, IPv4 over IPv6 tunnel, IPv4 over IPv4 tunnel or IPv6 over IPv6 tunnel
pptp	PPTP tunnel
l2tp	L2TP/IPsec tunnel
l2tpv3-raw	L2TPv3 tunnel
l2tpv3	L2TPv3/IPsec tunnel
ipudp	IPUDP tunnel
map-e	MAP-E tunnel
hb46pp	IPv4 over IPv6 tunnel using national standard provisioning method of IPv6 migration technology

- [初期値] : ipsec

Description

Setting of tunnel interface type

Notes

When tunneling and NAT are used together, it is desirable to set the starting IP address by **tunnel endpoint address** command.

pptp keyword cannot be used for models that do not implement L2TP/IPsec functionality.

For models that do not implement L2TP/IPsec functionality, the l2tp keyword cannot be used.

For models that do not implement L2TPv3 functionality, the l2tpv3-raw and l2tpv3 keywords cannot be used.

IPUDP tunnels cannot be used except for data-connect connections.

For models that do not implement the data-connect connection function, the map-e keyword cannot be used.

For models that do not implement the corresponding function of IPv6 IPoE + IPv4 over IPv6 connection service using the MAP-E method, the map-e keyword cannot be used.

For models that do not implement the domestic standard provisioning method for IPv6 migration technology, the hb46pp keyword cannot be used.

[Applied models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

12.5 Setting the IPv4 address of the tunnel interface

[Format]

ip tunnel address *ip_address*[/*mask*]

no ip tunnel address [*ip_address*[/*mask*]]

[Setting value and initial value]

- *ip_address*
 - [Setting value]: IPv4 address
 - [Initial value]: -
- *mask*
 - [Setting value]:

- xxx.xxx.xxx.xxx (where xxx is a decimal number)
- Hexadecimal numbers following 0x
- Number of mask bits
- [Initial value]: -

[Explanation]

Set the IPv4 address and netmask of the tunnel interface.

By setting this command, it is possible to establish a BGP connection via the tunnel interface.

[Applied models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

12.6 Setting the IPv4 address of the other side of the tunnel interface

[Format]

```
ip tunnel remote address ip_address
no ip tunnel remote address [ip_address]
```

[Setting value and initial value]

- *ip_address*
 - [Setting value]: IPv4 address
 - [Initial value]: -

[Explanation]

Setting the IPv4 address of the other side of the tunnel interface

By setting this command, it is possible to establish a BGP connection via the tunnel interface.

[Applied models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

12.7 Setting the IP address of the other side tunnel interface endpoint

[Format]

```
tunnel endpoint remote address remote
no tunnel endpoint remote address [remote]
```

[Setting value and initial value]

- *remote*
 - [Setting value]: IP address or host name of the other side tunnel interface endpoint (within 64 single-byte characters)
 - [Initial value]: -

[Explanation]

Set the IP address or host name of the other side tunnel interface endpoint. Any IPv4/IPv6 address can be set as the IP address. IPv4 over IPv4 tunnel and IPv6 over IPv4 tunnel can be used when an IPv4 address is set as the tunnel interface endpoint, and IPv4 over IPv6 tunnel and IPv6 over IPv6 tunnel can be used when an IPv6 address is set.

When the **tunnel endpoint local address** command is not set, or when the types of IPv4/IPv6 are different between *local* and *remote*, the IP address of an appropriate interface is used as the local endpoint address. Also, when a host name is set by this command and an IP address is set by the **tunnel endpoint local address** command, name resolution of the host name is performed according to the IPv4/IPv6 type of the **tunnel endpoint local address** command.

[Notes]

The IP address and host name set by this command are used when the setting value of the **tunnel encapsulation** command is ipip. When this command is set, the settings of the **tunnel endpoint address** command and **tunnel endpoint name** command are not used.

RTX5000 / RTX3500 can be used after Rev.14.01.20.

RTX1210 can be used after Rev.14.01.20.

[Applied models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

12.8 Setting the endpoint IP address of your own tunnel interface

[Format]

tunnel endpoint local address *local*

no tunnel endpoint local address [*local*]

[Setting value and initial value]

- *[Settings]: Local*

- [Setting value]: IP address or host name of the tunnel interface endpoint on your side (up to 64 single-byte characters).
- [Initial value]: -

[Explanation]

Set the IP address or host name of the tunnel interface endpoint on your side. Any IPv4/IPv6 address can be set as the IP address. IPv4 over IPv4 tunnel and IPv6 over IPv4 tunnel can be used when an IPv4 address is set as the tunnel interface endpoint, and IPv4 over IPv6 tunnel and IPv6 over IPv6 tunnel can be used when an IPv6 address is set.

If the **tunnel endpoint remote address** command is not set, or if the IPv4/IPv6 types are different between *local* and *remote*, the setting of this command is not reflected. When the host name is set by this command and the IP address is set by the **tunnel endpoint remote address** command, name resolution of the host name is performed according to the IPv4/IPv6 type of the **tunnel endpoint remote address** command.

[Notes]

The IP address and host name set by this command are used because the **tunnel encapsulation** command setting is This is the case with ipip.

Not available for RTX5000/RTX3500 Rev. 14.00.21 or earlier, and RTX1210 Rev. 14.01.19 or earlier.

Dynamic addresses of IPv6 are not available for RTX5000/RTX3500 Rev. 14.00.25 or earlier, RTX1210 Rev. 14.01.32 or earlier, and RTX830 Rev. 15.02.07 or earlier.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

12.9 Set the tunnel interface endpoint IP address

[Format]

tunnel endpoint address [*local*] *remote*

no tunnel endpoint address [[*local*] *remote*]

[Setting value and initial value]

- *Local*

- [Setting value]: IP address of the tunnel interface endpoint on your side
- [Initial value]: -

- *remote*

- [Setting value]: IP address of the tunnel interface endpoint on the other side
- [Initial value]: -

[Description]

Set the tunnel interface endpoint IP address. The IP address can be any IPv4/IPv6 address, but *local* and *remote* must have the same IPv4/IPv6 type. IPv4 over IPv4 tunnel and IPv6 over IPv4 tunnel can be used when an IPv4 address is set as the tunnel interface endpoint, and IPv4 over IPv6 tunnel and IPv6 over IPv6 tunnel can be used when an IPv6 address is set.

If *local* is omitted, the IP address of the appropriate interface is used.

[Notes]

The IP address set by this command is used when the **tunnel encapsulation** command setting is pptp, l2tp, l2tpv3-raw, l2tpv3, or ipip. In an IPsec tunnel, the tunnel endpoints are set by using the **ipsec ike local address** and the **ipsec ike**

set by the **remote address** command.

When receiving with Anonymous of a PPTP server or L2TP/IPsec server, it is not necessary to set it.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

12.10 Setting the name of the tunnel endpoint

[Format]

tunnel endpoint name [*local_name*] *remote_name* [*type*]

no tunnel endpoint name [*local_name* *remote_name* *type*]

[Setting value and initial value]

- *local_name*
 - [Setting value]: Your side endpoint
 - [Initial value]: -
- *remote_name*
 - [Setting value]: Mating side endpoint
 - [Initial value]: -
- *type*: Type of name
 - [Setting value]:

Setting value	Description
fqdn	FQDN
tel	NGN network telephone number

- [Initial value]: fqdn

[Description]

Specify the name of the tunnel endpoint.

[Notebook]

If the **tunnel endpoint address** command is set, it has priority.

This command is used when the **tunnel encapsulation** command setting is pptp, l2tpv3-raw, l2tpv3, ipip, or ipudp.

For pptp, l2tpv3-raw, l2tpv3, and ipip tunnels, specify the domain name (FQDN) in the name.

For ipudp tunnels, specify the NGN network telephone number in the name. It is described without hyphens. The *type* parameter cannot be used for models that do not implement a data-connect connection function.

Specifying the name of an ipip tunnel is not possible for RTX5000/RTX3500 Rev. 14.00.21 or earlier and RTX1210 Rev. 14.01.19 or earlier.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

12.11 Setting up a server for a multipoint tunnel

[Format]

tunnel multipoint server id *ip_address*

no tunnel multipoint server id [*ip_address*]

[Setting value and initial value]

- *id*
 - [Setting value]: Server identifier (1..3)
 - [Initial value]: -
- *ip_address*
 - [Setting value]: IPv4/IPv6 address or host name
 - [Initial value]: -

[Description]

In a multipoint tunnel, an address of a router to which a server role is assigned is set. This command is enabled for a **tunnel** interface (a **tunnel** interface on the client side of a multipoint tunnel) for which the connection type is set to multipoint and the *role* option is set to client in the tunnel type command.

When multiple sets of this command are made and multiple servers are specified, a tunnel is connected to all connectable servers. Up to three servers can be specified.

[Notes]

A multipoint tunnel has a hub-and-spoke configuration as a basic configuration, and a hub router is usually used as a server.

RTX1210 is available for Rev. 14.01.20 or later.

RTX5000/RTX3500 is available for Rev. 14.01.26 or later.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

12.12 Setting your name to be used in a multipoint tunnel

[Format]

tunnel multipoint local name *name*

no tunnel multipoint local name [*name*]

[Setting value and initial value]

- *name*
 - [Setting value]: Name (up to 64 single-byte characters, 32 double-byte characters)
 - [Initial value]: -

[Description]

Setting your name to be used in a multipoint tunnel

The name set by this command is notified to the connection partner after the tunnel connection, and the connection partner also uses it as tunnel identification information.

It is used in SYSLOG, etc.

[Notes]

RTX1210 is available for Rev. 14.01.20 or later.

RTX5000/RTX3500 is available for Rev. 14.01.26 or later.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

12.13 Setting the maximum number of connection partners in a multipoint tunnel

[Format]

tunnel multipoint limit *limit*

no tunnel multipoint limit [*limit*]

[Setting value and initial value]

- *limit*
 - [Setting value]:
 - Maximum number (1 .. 100)(vRX series, RTX5000, RTX3500, RTX1210, RTX1220, RTX1300)
 - Maximum number (1 .. 1000)(RTX3510)
 - [Initial value]:
 - 100 (vRX series, RTX5000, RTX3500, RTX1210, RTX1220, RTX1300)
 - 1000 (RTX3510)

[Description]

The maximum number of connection partners that can be connected in a selected tunnel interface is set. This command is enabled in a tunnel interface (a **tunnel** interface on the server side of a multipoint tunnel) for which the connection type of the tunnel type command is set to multipoint and the *role* option is set to server.

The upper limit of the total number of connection partners of all tunnel interfaces is the maximum number of tunnels to ground determined for each model. Therefore, when using multiple tunnel interfaces, not only the maximum number set by this command but also the maximum number of tunnels to ground for each model are limited. Even if the number of connection partners is lower than the maximum number set by this command, if the total number of all tunnel interfaces reaches the maximum number of tunnels to ground for each model, a new connection cannot be made.

[Notes]

RTX1210 can be used after Rev. 14.01.20.

RTX5000 / RTX3500 can be used after Rev. 14.02.26.

RTX830 can be used after Rev. 15.02.22. However, it cannot be used when an extended license is not imported.

[Supports extended licenses]

RTX830 can use this command when an [extended license \(YSL-VPN-EX1\)](#) is imported.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX830

12.14 Setting the MAP-E type of the tunnel interface

[Format]

tunnel map-e type *type*

no tunnel map-e type [*type*]

[Setting value and initial value]

- *type*
 - [Setting value]:

Setting value	Description
v6plus	v6 plus
ocn	OCN Virtual Connect Service
ipv6option	BIGLOBE IPv6 option

- [Initial value]: v6plus

[Description]

Setting the MAP-E type of the tunnel interface.

Setting which MAP-E service to use when the **tunnel encapsulation** command is set to *map-e*.

[Notes]

RTX1210 can be used after Rev. 14.02.10.

RTX830 can be used after Rev. 15.02.10.

The *ipv6option* keyword of the *type parameter* is used for RTX5000 / RTX3500 Rev. 14.00.33 or earlier, RTX1300 Rev. 23.00.04 or earlier,

RTX1220 Rev. 15.04.04 or earlier, RTX1210 Rev. 14.01.41 or earlier, and RTX830 Rev. 15.02.28 or earlier cannot be used.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

12.15 Setting the conversion type of the tunnel interface

[Format]

tunnel translation type

no tunnel translation [*type*]

[Setting value and initial value]

- *type*
 - [Setting value]:

Setting value	Explanation
nat46	NAT46 Tunnel

- [Initial value]: -

[Description]

Setting the conversion type of the tunnel interface.

[Notes]

Cannot be used together with the **tunnel encapsulation** command, and the command entered later becomes effective.

RTX830 Rev. 15.02.20 or later can be used.

RTX1220 Rev.15.04.04 or later。

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX840, RTX830

12.16 Setting your name and password to be sent to the provisioning server using the domestic standard provisioning method of IPv6 migration technology.

[Format]

tunnel hb46pp auth *myname myname password*

no tunnel hb46pp auth myname [*myname password*]

[Setting value and initial value]

- *Myname*
 - Setting value: Name (32 characters or less)
 - [Initial value]: -
- *password*
 - [Setting value]: Password (up to 32 characters)
 - [Initial value]: -

[Explanation]

In the domestic standard provisioning method of IPv6 migration technology, a name and a password to be transmitted to a provisioning server are set.

The characters that can be used for the name and password are single-byte alphanumeric characters, hyphens (-), and underscores (_).

[Notes]

RTX1300 is available in Rev.23.01.02 or later. RTX1220 is available in Rev.23.01.02 or later. RTX1220 is available in Rev.15.04.07 or later. RTX830 is available in Rev.15.02.31 or later.

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX840, RTX830

12.17 Setting the provisioning server name used in the domestic standard provisioning method of IPv6 migration technology

[Format]

tunnel hb46pp server *server*

no tunnel hb46pp server [*server*]

[Setting value and initial value]

- *server*
 - [Setting value]: Server name (up to 255 characters)
 - [Initial value]: -

[Explanation]

In the domestic standard provisioning method of IPv6 migration technology, the server name to be transmitted to the provisioning server is set by single-byte alphanumeric characters, hyphens (-), and periods (.).

[Notes]

RTX830 is available in Rev.15.02 or later.

RTX830 is available in Rev.15.02 or later.

RTX830 is available in Rev.15.02.31 or later. RTX830 is available in Rev.15.02.31 or later.

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX840, RTX830

CHAPTER 13

IPsec configuration

IPsec functionality is implemented to ensure security for IP communications by encryption. IPsec uses the key exchange protocol IKE (Internet Key Exchange). The required key is automatically generated by IKE, but the pre-shared key that becomes the key seed must be registered in advance with the `ipsec ike pre-shared-key` command. This key can be configured for each security gateway, and whether to respond to a key exchange request is configured with the `ipsec ike remote address` command. Management information that registers keys, key life, encryption and authentication algorithms, etc. is managed by SA (Security Association). An ID that distinguishes SA is automatically assigned. The ID and status of SA can be checked with the `show ipsec sa` command. SA has a life time that matches the life of the key. A parameter that can be specified by the user among attributes of SA is called a policy. The number is called a policy ID, defined with the `ipsec sa policy` command, and the life time is set with the `ipsec ike duration ipsec-sa`, `ipsec ike duration isakmp-sa` commands.

SA is deleted with the **`ipsec sa delete`** command, and SA is initialized with the **`ipsec refresh sa`** command. It is also possible to update SA automatically with the **`ipsec auto refresh`** command.

There are two main types of communication by IPsec: tunnel mode and transport mode.

Tunnel mode is a mode for using VPN (Virtual Private Network) by IPsec. A router acts as a security gateway, encrypts IP packet data flowing on the LAN, and communicates with the opposing security gateway. No special configuration is required for the host that starts or ends on the LAN because the router does all the processing required for IPsec.

When using tunnel mode, define a virtual interface called a tunnel interface, and set a route so that IP packets to be processed flow to the tunnel interface. Each tunnel interface is managed by a tunnel interface number. Tunnel **`select`** command is used to switch the tunnel number for configuration. Tunnel **`enable`** and **`tunnel disable`** commands are used to use or not use the tunnel interface, respectively.

Setting by destination information number		Setting by tunnel interface number
<code>pp enable</code> <code>pp disable</code> <code>pp select</code>	<==>	<code>tunnel enable</code> <code>tunnel disable</code> <code>tunnel select</code>

Transport mode is a special mode that guarantees security against communications that start or end at the router itself. It can be used for special cases such as entering a remote router via TELNET from the router (vRX series is not supported). To use transport mode, define it with the **`ipsec transport`** command, and to stop using it, delete it with the **`no ipsec transport`** command.

The identifier and tunnel interface number of the security gateway differs by model, as shown in the table below.

Model	Identifier of security gateway	Tunnel interface number
vRX Series	1-6000 (*1)	1-6000 (*1)
RTX5000	1-3000	1-3000
RTX3510	1-1000	1-1000
RTX3500	1-1000	1-1000
RTX1300	1-100	1-100
RTX1220	1-100	1-100
RTX1210	1-100	1-100
RTX840	1-20	1-20
RTX830	1-20	1-20

*1 When operating in compact mode of vRX Amazon EC2 version and vRX VMware ESXi version, it becomes 1-1000.

This unit supports main mode and aggressive mode. When both routers composing a VPN have a fixed global address, use main mode, and when only one router has a fixed global address, use aggressive mode.

To use main mode, you need to set the IP address of the opposite router with the **ipsec ike remote address** command. When using aggressive mode, the setting depends on whether or not it has a fixed global address. For routers with a fixed global address, set the **ipsec ike local name** command and set any with the **ipsec ike remote address command**. For routers without a fixed global address, set the **ipsec ike local name** command and set the IP address with the **ipsec ike remote address command**.

In main mode, you cannot set both the **ipsec ike local name** and the **ipsec ike remote name** commands. Also, in aggressive mode, you cannot set both the **ipsec ike local name** and the **ipsec ike remote name** commands at the same time. If you set this, it may not work properly.

13.1 Setting IPsec Operation

Format

ipsec use *use*

no ipsec use [*use*]

Setting Value and Initial Value

- *Use*
 - Setting Value

Setting Value	Description
on	Operating
off	Not Operating

- Setting Initial Value: on

Setting Value

Setting whether or not to operate IPsec.

Setting Value

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.2 Setting Up the IKE Version

Format

ipsec ike version *gateway_id* *version*

no ipsec ike version *gateway_id* [*version*]

Setting Value and Initial Value

- *gateway_id*
 - [Setting value]: Identifier of the security gateway
 - [Initial value]: -
- *version*
 - [Setting value]: Version of IKE to use
 - [Setting value]:

Setting value	Description
1	IKE version 1
2	IKE version 2

- [Initial value]: 1

[Explanation]

Set the version of IKE to be used by the security gateway.

[Notes]

Connections other than the version specified by *version* are not accepted.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.3Setting the authentication method for IKE

[Format]

```
ipsec ike auth method gateway_id method
no ipsec ike auth method gateway_id [method]
```

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of the security gateway
 - [Initial value]: -
- *method*
 - [Setting value]:

Setting value	Description
Auto	Automatically select the authentication method
pre-shared-key	Pre-shared key
certificate	Digital signature
eap-md5	EAP-MD5

- [Initial value]:
 - auto

[Explanation]

Setting the authentication method for IKE

When auto is set in METHOD, the authentication method is determined according to the following conditions.

- Pre-shared key method
 - If the **ipsec ike pre-shared-key** command is set.
- Digital signature method

If all of the following conditions are met:

 - **The** certificate is stored in the location specified by the **ipsec ike pki file** command.
 - **The ipsec ike eap request** command and the **ipsec ike eap myname** command are not set.
- EAP-MD5 method

If all of the following conditions are met:

 - **The** certificate is stored in the location specified by the **ipsec ike pki file** command.
 - **The ipsec ike eap request** command and the **ipsec ike eap myname** command are not set.

When a plurality of conditions are met among the above-mentioned conditions for determining the authentication method, the authentication method is prioritized in the following order.

1. Pre-shared key method
2. Digital signature method
3. EAP-MD5 method

When a condition other than auto is specified in *method*, authentication is performed by the method specified in *method* regardless of the above-mentioned conditions for determining the authentication method.

[Notes]

This command is valid only for IKEv2 and does not affect the operation of IKEv1.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.4 Setting whether to automatically add a route based on the ID received by IKE

[Format]

```
ipsec ike auto received-id-route-add gateway_id switch
no ipsec ike auto received-id-route-add gateway_id [switch]
```

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *switch*
 - [Setting value]:

Setting value	Description
on	Automatically adding routes
off	Do not automatically add routes

- [Initial value]: off

[Notes]

When operating as a Responder of a security gateway, whether to automatically add routes based on IDs (IPv4 addresses or IPv4 network addresses) received from an Initiator of the security gateway in phase 2 of IKEv1 is set.

This command is valid only when the tunnel is operating in tunnel mode of IPsec, and when IKEv1 is used for key exchange and negotiation of IKE is performed in aggressive mode.

Addition/deletion of routes are linked to UP/DOWN of an IPsec tunnel, and routes are added when an IPsec SA for transmission is established, and routes are also deleted when the IPsec SA for transmission is deleted.

[Notes]

Routes are not added when IDs are not exchanged in phase 2 of IKEv1. Routes are not added when the IDs exchanged in phase 2 of IKEv1 are IPv6. Changing the setting of this command deletes SA and initializes the state of IKE. This command is valid only in IKEv1 and does not affect the operation of IKEv2. This command is valid in tunnel mode and aggressive mode and does not affect the operation of transport mode and the operation of main mode.

Routers used as Initiators of a security gateway must set local IDs and remote IDs in one of the following ways to send IDs in phase 2 of IKEv1. In a multipoint tunnel, it is necessary to set them in method 1.

1. Set with the **local-id** and **remote-id** parameters of the **ipsec sa policy** command
2. Set with the *local-id* parameter and the *remote-id* parameter of the **ipsec sa policy** command

If both the *local-id/remote-id parameter* of the **ipsec sa policy** command and the **local-id/remote-id** parameter of the **remote-id** command are set, the ID set in the *local-id/remote-id* parameter of the **ipsec sa policy** command is sent in phase 2 of IKEv1.

Cannot be used with RTX1300 Rev.23.00.08 or earlier.

[Applicable models]

vRX Sakura Cloud Edition, RTX3510, RTX1300

13.5 Pre-shared key registration

[Format]

```
ipsec ike pre-shared-key gateway_id
key ipsec ike pre-shared-key gateway_id
text text no ipsec ike pre-shared-key
gateway_id [...]
```

[Setting value and initial value]

- *gateway_id*
 - Setting value: Security gateway identifier
 - [Initial value]: -
- *key*
 - Setting value: Key hexadecimal sequence starting with 0x (up to 128 bytes)

- [Initial value]: -
- *text*
 - Setting value: Key represented by an ASCII string (up to 128 characters)
 - [Initial value]: -

[Description]

Pre-shared keys necessary for key exchange are registered. If not set, key exchange is not performed. The same pre-shared key must be set in the other party router for key exchange.

[Configuration Example]

```
ipsec ike pre-shared-key 1 text himitsu
ipsec ike pre-shared-key 8 0xCDEEEDC0CEDDCD
```

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.6 PKI file configuration for IKEv2 authentication

[Format]

```
ipsec ike pki file gateway_id certificate=cert_id [crl=crl_id]
no ipsec ike pki file gateway_id [...]
```

[Setting value and initial value]

- *gateway_id*
 - Setting value: Security gateway identifier
 - [Initial value]: -
- *cert_id*
 - Setting value:

Setting value	Description
1..8	Identifier of a certificate file

- [Initial value]: -
- *crl_id*
 - [Setting value]:

Setting value	Description
1..8	Identifier of a CRL file

- [Initial value]: -

[Explanation]

Set the PKI file used for authentication of IKEv2.

When performing authentication of a digital certificate method, the identifier of the file in which the certificate used for *cert_id* is stored is specified.

When performing EAP-MD5 authentication, the initiator specifies the identifier of the file in which his/her certificate is stored in *cert_id* to verify the other party's certificate.

[Notes]

This command is valid only for IKEv2 and does not affect the operation of IKEv1.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.7 Setting up your name and password for EAP-MD5 authentication

[Format]

```
ipsec ike eap myname gateway_id name password
no ipsec ike eap myname gateway_id [...]
```

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of a security gateway
 - [Initial value]: -
- *name*
 - [Setting value]: Name (within 256 single-byte characters)
 - [Initial value]: -
- *password*
 - [Setting value]: Password (within 64 single-byte characters)
 - [Initial value]: -

[Explanation]

Setting up the name and password to be used when EAP-MD5 authentication is requested.

[Notes]

This command is valid only for IKEv2 and does not affect the operation of IKEv1.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.8 Setting up user authentication with EAP-MD5

[Format]

```
ipsec ike eap request gateway_id sw group_id
no ipsec ike eap request gateway_id [...]
```

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of a security gateway
 - [Initial value]: -
- *SW*
 - [Setting value]:

Setting value	Explanation
on	Request
off	Do not request

- [Initial value]: off
- *group_id*
 - [Setting value]: Identification number of a user group used for authentication
 - [Initial value]: -

[Explanation]

Sets whether to request EAP-MD5 authentication from a client in IKEv2. When *group_id* is specified, the user included in the corresponding user group is authenticated.

The setting by this command is valid only when the router operates as a response side, and performs user authentication with EAP-MD5 when an AUTH payload is not included in an IKE AUTH exchange sent from the security gateway on the initiator side.

[Notes]

This command is valid only for IKEv2 and does not affect the behavior of IKEv1.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.9 Setting whether to send a certificate request payload with EAP-MD5 authentication

[Format]

```
ipsec ike eap send certreq gateway_id switch
no ipsec ike eap send certreq gateway_id [switch]
```

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Security gateway identifier
 - [Initial value]: -
- *switch*
 - [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: off

[Explanation]

For the EAP-MD5 authentication method, a certificate request is sent to the IKE_AUTH exchange sent from the initiator security gateway.

(CERTREQ) Set whether to include the payload.

[Notes]

This command is valid only for IKEv2 and does not affect the behavior of IKEv1.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.10 Setting whether to initiate an IKE key exchange

[Format]

```
ipsec auto refresh [gateway_id] switch
no ipsec auto refresh [gateway_id]
```

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Security gateway identifier
 - [Initial value]: -
- *switch*
 - [Setting value]:

Setting value	Description
on	Initiate a key exchange
off	Do not initiate a key exchange

- [Initial value]:
 - off (overall behavior)
 - on (*gateway_id*毎)

[Explanation]

Whether to initiate an IKE key exchange It always accepts a key exchange initiated by another router regardless of this command.

A format that does not specify the *gateway_id* parameter determines the overall behavior of the router. When this setting is off, the router does not initiate a key exchange.

A format that specifies the *gateway_id* parameter is provided to suppress initiation of a key exchange for a specified security gateway.

For example, in the following setting, only the first security gateway does not initiate a key exchange.

```
ipsec auto refresh on
ipsec auto refresh 1 off
```

[Notebook]

In the setting of **ipsec auto refresh off**, a format that specifies the *gateway_id* parameter has no effect. For example, in the following setting:

The first security gateway does not initiate a key exchange.

```
ipsec auto refresh off (default setting) ipsec
auto refresh 1 on
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.11 Setting whether to reject a key exchange when the setting is different

[Format]

```
ipsec ike negotiate-strictly gateway_id switch
no ipsec ike negotiate-strictly gateway_id
```

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *switch*
 - [Setting value]:

Setting value	Description
on	Refuse key exchange
off	Accept key exchange

- [Initial value]: off

[Explanation]

When operating as IKEv1, it is set whether to refuse key exchange when the setting is different. When this command setting is off, it operates in the same way as the previous revision. That is, even if the parameter proposed by the other party is different from his/her own setting, if the parameter is supported, it is accepted. When this command setting is on, it rejects the other party's suggestion in the same situation. Parameters to which this command applies and corresponding commands are as follows.

Parameters	Corresponding commands
Cryptographic algorithm	ipsec ike encryption
Group	ipsec ike group
Hashing algorithm	ipsec ike hash
PFS	ipsec ike pfs
Mode of phase 1	IPSEC IKE local name etc.

[Notes]

This command does not affect the operation as IKEv2.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.12 Setting whether to continue key exchange without stopping when IKE key exchange fails

Format

```
ipsec ike always-on gateway_id switch
no ipsec ike always-on
```

[Setting value and initial value]

- *gateway_id*

- [Setting value]: Identifier of security gateway
- [Initial value]: -
- *switch*
- [Setting value]:

Setting value	Description
on	Continue key exchange
off	Pause key exchange

- [Initial value]: off

Description

When IKE key exchange fails, key exchange can be continued without stopping. When using IKE keepalive, it always continues key exchange without setting this command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.13 Setting of retransmission frequency and interval of key exchange

Format

```
ipsec ike retry count interval [max_session]
no ipsec ike retry [count interval [max_session]]
```

[Setting value and initial value]

- *count*
 - [Setting value]: Number of retransmissions (1..50)
 - [Initial value]: 10
- *Interval*
 - [Setting value]: Number of seconds between retransmissions (1..100)
 - [Initial value]: 5
- *max_session*
 - [Setting value]: Maximum number of phases 1 operating simultaneously (1..5)
 - [Initial value]: 3

[Explanation]

Set the number and interval of retransmissions to be executed when a packet for key exchange does not reach the other party.

The *max_session* parameter specifies the maximum number of phases 1 operating simultaneously in IKEv1. When a router is in a state where phase 1 is not established and retransmissions continue, it starts a new phase 1 for the purpose of rushing key generation.

This parameter limits the number of phases 1 operating simultaneously in such a situation. Note that this parameter is limited only to phase 1 on the start side and has no effect on phase 1 on the response side.

[Notes]

The *max_session* parameter has no effect when operating as IKEv2. A key exchange session initiated for the same other party security gateway is always at most one session.

If the load on the other party security gateway is very high, it may be possible to succeed in key exchange by adjusting the setting value of this command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.14 Setting the name of the other party security gateway

[Format]

```
ipsec ike remote name gateway name [type]
no ipsec ike remote name gateway [name]
```

[Setting value and initial value]

- *gateway*

- [Setting value]: Identifier of the other party security gateway
- [Initial value]: -
- *name*
 - [Setting value]: Name (256 characters or less)
- [Initial value]: -
- *type*: Type of id
 - [Setting value]:

Setting value	Explanation
ipv4-addr	ID_IPV4_ADDR
fqdn	ID_FQDN
user-fqdn (or rfc822-addr)	ID_USER_FQDN(ID_RFC822_ADDR)
ipv6-addr	ID_IPV6_ADDR
key-id	ID_KEY_ID
tel	NGN network phone number (ID_IPV6_ADDR) (Cannot be specified for vRX Amazon EC2 version and vRX Sakura cloud version)
tel-key	NGN network phone number (ID_KEY_ID) (Cannot be specified for vRX Amazon EC2 version and vRX Sakura cloud version)

- [Initial value]: -

[Explanation]

Set the name and type of the other party security gateway.

The following describes the effects of this command and points to note depending on the version of IKE that works.

- IKEv1

This command setting is used in phase 1 aggressive mode, not in main mode, and the *type* parameter is not considered when determining the other party security gateway.

- IKEv2

When determining the other party security gateway, the settings of the *name* and *type* parameters must match. If the *type* parameter is 'tel', the other party IPv6 address (ID_IPV6_ADDR) is used to determine the other party security gateway.

If the *type* parameter is 'tel-key', the setting value is used to determine the other party security gateway as ID_KEY_ID.

If the *type* parameter is other than 'key-id', an attempt is made to determine the IP address of the other party security gateway from *name*, and if it can be determined, a key exchange is initiated for that host. In this case, it is not necessary to set the **ipsec ike remote address** command.

However, if the **ipsec ike remote address** command is set, the destination host at startup is determined according to that setting.

[Notes]

The 'tel' and 'tel-key' are used in the Data Connect inter-location connection function.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.15 Setting the IP address of the other party's security gateway

[Format]

ipsec ike remote address gateway_id ip_address

no ipsec ike remote address gateway_id [ip_address]

[Setting value and initial value]

- *gateway_id*
 - Setting value: Identifier of the security gateway
 - [Initial value]: -
- *ip_address*
 - [Setting value]:

Setting value	Description
IP address or host name	IP address or host name of the other party's security gateway (up to 255 single-byte characters)
Any	Automatic selection

- [Initial value]: -

[Explanation]

Setting the IP address or host name of the other party's security gateway If set by host name, IP address is searched by DNS from the host name when key exchange is started.

In addition, the effects and precautions of this command, which differ depending on the IKE version in which it works, are as follows.

- IKEv1

If it is the responding side, the host specified by this command is used to determine the other party's security gateway. If 'any' is set, it accepts key exchange from any host as the other party's security gateway. Instead, it cannot initiate key exchange from itself. For example, if it has a fixed global address in aggressive mode, it is used.

- IKEv2

The host set by this command is used only as the destination for initiating key exchange. 'any' explicitly indicates that it does not initiate key exchange from its own side.

If it is the responding side, the other party's security gateway is determined by setting this command to **ipsec ike remote name**.

This is done by setting commands, etc.

[Notes]

If you specify a host name, be sure to set a DNS server using the **dns server** command. In IPsec main mode connection, the IP address and host name of the other party's security gateway are not set duplicately. Operation is not guaranteed when the IP address and host name of the other party's security gateway are set duplicately.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.16 Setting the other party's ID

[Format]

```
ipsec ike remote id gateway_id ip_address[/mask]
no ipsec ike remote id gateway_id [ip_address[/mask]]
```

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of the security gateway
 - [Initial value]: -
- *ip_address*
 - [Setting value]: IP address
 - [Initial value]: -
- *mask*
 - [Setting value]: Netmask
 - [Initial value]: -

[Explanation]

Set the other party's ID used in phase 2 of IKEv1.

If this command is not set, the ID is not transmitted in phase 2.

If the *mask* parameter is omitted, the ID of type 1 is transmitted. Also, if the *mask* parameter is specified, the ID of type 4 is transmitted.

[Notes]

This command does not affect the operation of IKEv2.

[Applicable model]

[Version]: vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840

13.17 Set the name of your own security gateway

[Format]

ipsec ike local name *gateway_id name* [*type*]

no ipsec ike local name *gateway_id* [*name*]

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of the security gateway
 - [Initial value]: -
- *name*
 - [Setting value]: Name (up to 256 characters)
- [Initial value]: -
- *type*: Type of id
 - [Setting value]:

Setting value	Description
ipv4-addr	ID_IPV6_ADDR
fqdn	ID_FQDN
user-fqdn (or rfc822-addr)	ID_USER_FQDN (ID_RFC822_ADDR)
ipv6-addr	ID_IPV6_ADDR
key-id	ID_KEY_ID
tel	NGN network phone number (ID_KEY_ID) (Not available for vRX Amazon EC2 version and vRX Sakura cloud version)
tel-key	NGN network phone number (ID_KEY_ID) (Not available for vRX Amazon EC2 version and vRX Sakura cloud version)

- [Initial value]: -

[Explanation]

Set the name and ID type of your own security gateway.

Note that if the *type* parameter is set to 'ipv4-addr', 'ipv6-addr', 'tel' or 'tel-key' when operating as IKEv1, the operation is equivalent to setting 'key-id'. If IKEv2 and the *type* parameter is 'tel', your own IPv6 address (ID_IPV6_ADDR) is used for key exchange. If IKEv2 and the *type* parameter is 'tel-key', the setting value is used for key exchange as ID_KEY_ID.

[Notes]

The 'tel' and 'tel-key' are used by the Data Connect inter-location connection function.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.18 Set the IP address of your own security gateway

[Format]

```
ipsec ike local address gateway_id ip_address
ipsec ike local address gateway_id vrrp interface vrid
ipsec ike local address gateway_id ipv6 prefix prefix on interface
ipsec ike local address gateway_id ipcp pp peer_num
no ipsec ike local address gateway_id [ip_address]
```

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of your own security gateway
 - [Initial value]: -
- *ip_address*
 - [Setting value]: IP address of your own security gateway
 - [Initial value]: -
- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *vrid*
 - [Setting value]: VRRP group ID (1..255)
 - [Initial value]: -
- *Prefix*
 - [Setting value]: Prefix
 - [Initial value]: -
- *peer_num*
 - [Setting value]: PP interface number
 - [Initial value]: -

[Description]

Set the IP address of your own security gateway.

In the second format specifying the vrrp keyword, only when operating as a VRRP master, a virtual IP address of the specified LAN interface/VRRP group ID is used as your own security gateway address.

Key exchange is not performed if you are not a VRRP master.

In the third format specifying the ipv6 keyword, an IPv6 dynamic address is specified.

In the fourth format specifying the ipcp keyword, a PP interface for acquiring an IPCP address is specified.

[Notes]

If this command is not set, IKE is started using the IP address of the interface close to the other party's security gateway.

The second format cannot be used with vRX Amazon EC2 version and vRX Sakura cloud version.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.19 Setting your own ID

[Format]

```
ipsec ike local id gateway_id ip_address[/mask]
no ipsec ike local id gateway_id [ip_address[/mask]]
```

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Security gateway identifier
 - [Initial value]: -

- *ip_address*
 - [Setting value]: IP address
 - [Initial value]: -
- *mask*
 - [Setting value]: Netmask
 - [Initial value]: -

[Description]

Set your own ID used in phase 2 of IKEv1.

If this command is not set, do not send an ID in phase 2.

If the *mask* parameter is omitted, an ID of type 1 is sent.

If the *mask* parameter is specified, an ID of type 4 is sent.

[Notes]

This command does not affect the operation as IKEv2.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.20 Setting the IKE keepalive function

[Format]

ipsec ike keepalive use gateway_id switch [down=disconnect] [send-only-new-sa=send]

ipsec ike keepalive use gateway_id switch heartbeat [interval count [upwait]] [down=disconnect] [send-only-new-sa=send] **ipsec ike keepalive use gateway_id switch icmp-echo ip_address** [length=length] [interval count [upwait]] [down=disconnect]

ipsec ike keepalive use gateway_id switch dpd [interval count [upwait]] **ipsec ike keepalive use gateway_id switch rfc4306** [interval count [upwait]] **no ipsec ike keepalive use gateway_id** [switch]

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Security gateway identifier
 - [Initial value]: -
- *switch*: Keepalive operation
 - [Setting value]:

Setting value	Explanation
on	Using keepalives
off	Do not use keepalives
auto	Send only when the opposing router sends keepalives (valid only for heartbeat and rfc4306)

- [Initial value]: auto
- *ip_address*
 - [Setting value]: IP address of the destination to send a ping (IPv4/IPv6)
 - [Initial value]: -
- *length*
 - [Setting value]: Length of the data part of ICMP echo (64..1500)
 - [Initial value]: 64
- *Interval*
 - [Setting value]: Number of seconds between keep-alive packet transmissions (1..600)
 - [Initial value]: 10
- *count*
 - [Setting value]: Number of attempts until it is considered a failure when no keep-alive packet is received (1..50)
 - [Initial value]: 6

- *upwait*
 - [Setting value]: Time from when an IPsec SA is generated until the tunnel interface is actually enabled (0..1000000)
 - [Initial value]: 0
- *send*
 - [Setting value]:

Setting value	Description
on	When old and new SAs are mixed, keep-alive packets are sent only to new SAs
off	When old and new SAs are mixed, keep-alive packets are sent to both old and new SAs
auto	When old and new SAs are mixed, keep-alive packets are sent to both old and new SAs only when keep-alive packets for old SAs from the other side are received, otherwise keep-alive packets are sent only to new SAs

- [Initial value]:
 - auto (vRX Sakura Cloud Edition, RTX1300, RTX3510, RTX840)
 - off (other than above)

Description

Set the operation of IKE keep-alive.

The operation of this command differs depending on the version of IKE to be operated as follows.

• IKEv1

As a method of keep-alive, three types can be selected: heartbeat, ICMP Echo, and DPD (RFC3706). The first format is automatically a heartbeat format.

First and second formats are used to use the heartbeat format. When the *switch* parameter is set to auto in the heartbeat method, heartbeat packets are sent only when a heartbeat packet is received from the other side. Therefore, IKE keep-alive does not work when both settings are set to auto.

When using ICMP Echo, the third format is used to set the IP address of the destination. Optionally, the length of the data part of an ICMP Echo can be specified. In this method, even if the *switch* parameter is set to auto, it works as if it is set to on.

When using DPD, the fourth format is used. In this method, even if the *switch* parameter is set to auto, it works as if it is set to on.

In addition, when a method (format) not supported by IKEv1 is set, heartbeat is used as an alternative method. At this time, the setting contents are reflected in the *switch*, *count*, *interval*, and *upwait* parameters.

• IKEv2

As a keep-alive method, two types can be selected: RFC4306 (IKEv2 standard) and ICMP Echo. The first format is automatically the RFC4306 method.

When the *switch* parameter is set to auto, a response packet is sent only when a keep-alive packet of the RFC4306 method is received. Note that in IKEv2, keep-alive packets of this method must always be answered, so it works as if the *switch* parameter is set to auto or off.

When using ICMP Echo, the third format is used to set the IP address of the destination. Optionally, the length of the data part of an ICMP Echo can be specified. In this method, it works as if the *switch* parameter is set to auto or on.

In addition, when a method (format) not supported by IKEv2 is set, it works as an alternative method using RFC4306. At this time, the setting contents are reflected in the *switch*, *count*, *interval*, and *upwait* parameters.

[Notes]

When the destination is beyond the PP interface, the down option can be specified. When the down option is specified, it is possible to disconnect the PP interface when a keep-alive down is detected and when the number of IKE retransmissions expires. It can be used when an improvement of a tunnel establishment state can be expected by reconnecting the PP interface in a state on the network side.

When using heartbeat as a keep-alive method, the send-only-new-sa option can be specified. When the send-only-new-sa option is set to on, keep-alive packets are sent only to new SAs when old and new SAs after key exchange are mixed, and the load during key exchange can be reduced. When the send-only-new-sa option is set to on, keep-alive packets are sent to old SAs only when keep-alive packets to old SAs from the other side are received, otherwise it works as if the send-only-new-sa option is set to on.

When building a tunnel with a Yamaha router that does not support the send-only-new-sa option, if the send-only-new-sa option is set to on, the tunnel will go down, so it must be set to auto or off.

The *length* parameter specifies the length of the ICMP data part, not the length of the entire IP packet.

It is not possible to use multiple methods together for the same other side.

The send-only-new-sa option is not available for RTX5000 / RTX3500 Rev.14.00.28 or earlier, and the auto specification is not available for vRX Amazon EC2, vRX VMware ESXi, RTX5000, RTX3500, RTX1220, RTX1210, and RTX830.

[Applicable models]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.21 Setting whether to output SYSLOG related to IKE keep-alive

Format

ipsec ike keepalive log gateway_id log

no ipsec ike keepalive log gateway_id [log]

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *log*
 - [Setting value]:

Setting value	Description
on	Output
off	Do not output

- [Initial value]: on

[Explanation]

Set whether to output SYSLOG related to IKE keepalive. This SYSLOG is an output of DEBUG level.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.22 Configuration of cryptographic algorithm used by IKE

[Format]

ipsec ike encryption gateway_id algorithm

no ipsec ike encryption gateway_id [algorithm]

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *algorithm*
 - [Setting value]:

Setting value	Description
3des-cbc	DES-CBC
des-cbc	DES-CBC

Setting value	Description
aes-cbc	AES-CBC
aes256-cbc	AES256-CBC

- [Initial value]: 3des-cbc

Description

Configuration of cryptographic algorithm used by IKE

An algorithm set by this command is proposed when working as an initiator. When working as a responder, any algorithm supported can be used regardless of the setting of this command.

However, when the **ipsec ike negotiate-strictly** command is set to on in IKEv1, all algorithms supported by the responder can be used.

Notebook

In IKEv2, when the **ipsec ike proposal-limitation** command is set to on, an algorithm set by this command is proposed. When the **ipsec ike proposal-limitation** command is set to off, or when a model does not support the **ipsec ike proposal-limitation** command, all algorithms supported are simultaneously proposed and selected by the other security gateway regardless of the setting of this command. Also, when working as a responder, safer algorithms are selected from those proposed.

The cryptographic algorithms supported by IKEv2 and the priority of selection in response are as follows.

- AES256-CBC > AES192-CBC > AES128-CBC > 3DES-CBC > DES-CBC

*Supports AES192-CBC only in IKEv2. However, AES192-CBC cannot be selected by the command.

[Configuration Example]

```
# ipsec ike encryption 1 aes-cbc
```

Applicable model

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.23 Queue length setting for accumulating received IKE packets

Format

ipsec ike queue length *length*

no ipsec ike queue length [*length*]

[Setting value and initial value]

- *length*: Queue length
- [Setting value]:

Setting value	Model
6000...24000	vRX Amazon EC2 version (operating in normal mode), vRX VMware ESXi version (operating in normal mode), vRX Sakura cloud version
3000...12000	RTX3510, RTX5000
1100...4400	RTX1300 Rev.23.00.09 or later
1000...4000	vRX Amazon EC2 version (operating in compact mode), vRX VMware ESXi version (operating in compact mode), RTX3500
100...200	RTX1300 Rev.23.00.05 or later, RTX1220, RTX1210, RTX830 Rev.15.02.22 or later
20.40	RTX830 Rev.15.02.20 or later

- [Initial value]:
 - 12000 (vRX Amazon EC2 version (operating in normal mode), vRX VMware ESXi version (operating in normal mode), vRX Sakura cloud version)
 - 6000 (RTX3510, RTX5000)
 - 2200 (RTX1300 Rev.23.00.09 or later)

- 2000 (vRX Amazon EC2 version(operating in compact mode), vRX VMware ESXi version(operating in compact mode), RTX3500)
- 200 (RTX1300 Rev.23.00.05 以前、RTX1220、RTX1210、RTX830 Rev.15.02.22 以降)
- 40 (RTX840, RTX830 Rev.15.02.20 or earlier)

[Description]

Set the length of the queue for accumulating received IKE packets. This setting determines the behavior of a router when it receives concentrated IKE packets in a short period of time. The larger the set value, the more packets can be processed without being missed when IKE packets are concentrated, but conversely, the longer time that IKE packets stay in a router causes a delay in keep-alive response, increasing the possibility of erroneously detecting a tunnel failure. In normal operation, this setting does not need to be changed, but if there is a situation where many tunnels are constituted and many SAs are erased at the same time, the value should be set larger.

[Notebook]

The length of the queue can increase the number of IKE packets that can be received and processed at one time. However, if it is made too large, processing of IKE packets accumulated in the router will be delayed, increasing the possibility of being detected as a timeout by the opposite router. Therefore, it is necessary to be careful when changing the setting of this command.

In normal operation, this setting does not need to be changed.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.24 Configuration of groups used by IKE

[Format]

```
ipsec ike group gateway_id group [group]
no ipsec ike group gateway_id [group [group]]
```

[Setting value and initial value]

- *gateway_id* : identifier of the security gateway
 - [Initial value]: -
- *group* : identifier of the group
 - [Setting value]:
 - modp1536
 - modp1024
 - modp1536
 - modp2048
 - [Initial value]:
 - modp1024

[Explanation]

Configuration of groups used by IKE

If it acts as an initiator, it proposes a group set by this command. If it acts as a responder, it can use any supported group regardless of the configuration of this command.

In addition, the effects and cautions of this command depending on the version of IKE that works are as follows.

• IKEv1

When two types of groups are set, the first is proposed in phase 1 and the second is proposed in phase 2. Group 1
When only the type is set, the set groups are proposed in both phases 1 and 2.

Also, if the **ipsec ike negotiate-strictly** command is set to on, only the set groups can be used even if it acts as a responder.

• IKEv2

Only the group set first is always used. The second group set is ignored.

Also, if a group proposed as an initiator is rejected by the other party and another group is requested, it proposes again in that group (if the requested group can be supported). After that, the group re-proposed is used preferentially for the same other party's security gateway until the IPsec setting is changed or restarted.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.25 Configuration of hash algorithm used by IKE

[Format]

```
ipsec ike hash gateway_id algorithm
no ipsec ike hash gateway_id [algorithm]
```

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *algorithm*
 - [Setting value]:

Setting value	Description
MD5	MD5
sha	SHA-1
sha256	SHA-256
sha384	SHA-384
sha512	SHA-512

- [Initial value]: sha

[Explanation]

Configuration of hash algorithm used by IKE

An algorithm set by this command is proposed when it works as a start-up. Any supported algorithm can be used when it works as a responder regardless of the configuration of this command.

However, when the **ipsec ike negotiate-strictly** command is set to on in IKEv1, even a responder can use only the configured algorithm.

[Notebook]

In IKEv2, negotiation parameters corresponding to hash algorithm of IKEv1 are authentication algorithm (Integrity Algorithm) and PRF (Pseudo-Random Function). When the ipsec ike proposal-limitation command is set to on in IKEv2, an algorithm set by this command is proposed. When the ipsec ike proposal-limitation command is set to off or when a model does not support the ipsec ike proposal-limitation command, all supported algorithms are simultaneously proposed and selected by the other party's security gateway regardless of the setting of this command. Also, when it works as a responder, safer algorithms are selected from those proposed.

Authentication algorithms that can be supported by IKEv2 and priority of selection when responding are as follows.

- HMAC-SHA2-512-256 > HMAC-SHA2-384-192 > HMAC-SHA2-256-128 > HMAC-SHA-1-96 > HMAC-MD5-96

*HMAC-SHA2-512-256 and HMAC-SHA2-384-192 are supported by vRX Amazon EC2 version, vRX VMware ESXi version, RTX5000,

RTX3500, RTX1220, RTX1210, RTX840, and RTX830 cannot be used. PRFs

that can be supported by IKEv2 and priority of response selection are as follows.

- HMAC-SHA2-512 > HMAC-SHA2-384 > HMAC-SHA2-256 > HMAC-SHA-1 > HMAC-MD5

*HMAC-SHA2-512 and HMAC-SHA2-384 are supported by vRX Amazon EC2 version, vRX VMware ESXi version, RTX5000, RTX3500,

RTX1220, RTX1210, RTX840, and RTX830 cannot be used.

The sha384 and sha512 keywords in the *algorithm* parameter are supported by vRX Amazon EC2 version, vRX VMware ESXi version, RTX5000, RTX3500, RTX1220, RTX1210, RTX840, and RTX830 cannot be used.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

13.26 Setting whether to output to the log when the SPI value of the received packet is invalid

[Format]

```
ipsec log illegal-spi switch
no ipsec log illegal-spi
```

[Setting value and initial value]

- *switch*

- [Setting value]:

Setting value	Explanation
on	Log output
off	Not output to the log

- [Initial value]: off

[Explanation]

IPsec sets whether to output to the log when the SPI value of the received packet is invalid. The SPI value and the other party's IP address are output to the log.

To reduce the possibility of DoS due to sending a large number of packets containing invalid SPI values, the log records only a maximum of 10 types of packets per second. It is not possible to know the number of packets actually received.

[Notes]

At the time of key exchange, even if one starts using a new key due to a difference in the generation speed of the key, this log may be temporarily output because the other cannot use the key yet.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.27 Setting the type of IKE payload

[Format]

ipsec ike payload type gateway_id type1 [type2]

no ipsec ike payload type gateway_id [type1 ...]

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *type1*: Format of message for IKEv1
 - [Setting value]:

Setting value	Description
1	Maintaining compatibility with release 2 of Yamaha router
2	Maintaining compatibility with release 3 of Yamaha router
3	Adjusting the way of generating initial vectors (IV) to some implementations

- [Initial value]: 2
- *type2*: Format of message for IKEv2
 - [Setting value]:

Setting value	Description
1	Maintaining compatibility with release 1 of Yamaha router's IKEv2
2	Adjusting key exchange and key usage to some implementations

- [Initial value]: 2

Description

Adjust the type of payload for IKEv1 and IKEv2

When connecting to an older revision of Yamaha router with IKEv1, the *type2* parameter must be set to 1.

When connecting to the following revision of Yamaha router with IKEv2, the *type2* parameter must be set to 1.

Model	Revision
FWX120	Rev.11.03.02

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.28 Setting of IKEv1 key exchange type

[Format]

ipsec ike backward-compatibility gateway_id type

no ipsec ike backward-compatibility gateway_id [type]

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *type* : Type of key exchange used in IKEv1
 - [Setting value]:

Setting value	Description
1	Maintaining compatibility with release 1 (past release) of Yamaha router
2	Maintaining compatibility with release 2 (new release) of Yamaha router

- [Initial value]: 1

Description

Set the type of key exchange used in IKEv1.

When connecting to an older revision of Yamaha router with IKEv1, the *type* parameter must be set to 1.

[Notes]

RTX5000 can be used in Rev.14.00.12 or later.

RTX3500 can be used in Rev.14.00.12 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.29 Setting whether or not to send an information payload for IKE

[Format]

ipsec ike send info gateway_id info

no ipsec ike send info gateway_id [info]

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *info*
 - [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: on

[Explanation]

Whether or not to send an information payload is set during IKEv1 operation. For reception, all information payloads are interpreted regardless of this setting.

[Notes]

This command is used for special purposes such as verifying connectivity. It is necessary to set it to on in steady operation.

This command does not affect the operation as IKEv2. In IKEv2, information payloads are always sent and received as needed.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.30 Setting whether or not to use PFS

[Format]

ipsec ike pfs gateway_id pfs

no ipsec ike pfs gateway_id [pfs]

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *PFS*
 - [Setting value]:

Setting value	Description
on	Use
off	Do not use

- [Initial value]: off

[Explanation]

Whether or not to use PFS (Perfect Forward Secrecy) is set when working as an initiator of IKE. When working as a responder, it works according to whether or not the other security gateway uses PFS regardless of the setting of this command.

However, if it works as IKEv1 and the **ipsec negotiate-strictly** command is on, the setting of this command must match whether or not the other security gateway uses PFS.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.31 Setting XAUTH

[Format]

ipsec ike xauth myname gateway_id name password

no ipsec ike xauth myname gateway_id

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *name*
 - [Setting value]: Name notified by XAUTH (up to 32 characters)
 - [Initial value]: -
- *password*
 - [Setting value]: Password notified by XAUTH (up to 32 characters)
 - [Initial value]: -

[Explanation]

Set the name and password to be notified when XAUTH authentication is requested.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.32 Setting the user ID used for XAUTH authentication and EAP-MD5 authentication**[Format]****auth user** *userid username password***no auth user** *userid [username ...]***[Setting value and initial value]**

- *User ID*
 - [Setting value]:
 - User identification number

Setting value	Model
1..6000	vRX Amazon EC2 version (only when operating in normal mode) vRX VMware ESXi version (only when operating in normal mode) vRX Sakura cloud version
1..3000	RTX5000
1..1000	Others

- [Initial value]: -
- *username*
 - [Setting value]:
 - User name (up to 256 characters, at least 3 characters)
 - [Initial value]: -
- *password*
 - [Setting value]:
 - Password (up to 64 characters, at least 3 characters)
 - [Initial value]: -

[Explanation]

Setting the user ID used for XAUTH authentication of IKEv1 or EAP-MD5 authentication of IKEv2

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.33 Setting the attribute of the user ID used for XAUTH authentication and EAP-MD5 authentication**[Format]****auth user attribute** *userid attribute=value [attribute=value ...]***no auth user attribute** *userid [attribute=value ...]***[Setting value and initial value]**

- *userid*
 - [Setting value]:
 - user identification number

Setting value	Model
1..6000	vRX Amazon EC2 version (only when operating in normal mode) vRX VMware ESXi version (only when operating in normal mode) vRX Sakura cloud version
1..3000	RTX5000
1..1000	Others

- [Initial value]: -
- *attribute=value*
 - [Setting value]: User attribute

- [Initial value]: xauth=off

[Explanation]

Setting the attribute of the user ID used for XAUTH authentication of IKEv1 or EAP-MD5 authentication of IKEv2. The attributes that can be set are as follows.

attribute	Value	Description
xauth	on	Use this ID for IPsec XAUTH authentication
	off	Do not use this ID for IPsec XAUTH authentication
xauth-address	IP address [/netmask] (IPv6 address possible)	Notify this address as an internal IP address when connecting to IPsec
xauth-dns	IP address (IPv6 address possible)	Notify this address as a DNS server address when connecting to IPsec
xauth-wins	IP address (IPv6 address possible)	Notify this address as a WINS server address when connecting to IPsec
xauth-filter	String representing the name of a filter set	Apply this filter when connecting to IPsec
eap-md5	on	Use this ID for IKEv2 EAP-MD5 authentication
	off	Do not use this ID for IKEv2 EAP-MD5 authentication

If the same attribute is specified in duplicate, a command error occurs.

[Notes]

The attribute value explicitly set in this command is applied in priority to the attribute value set by the **auth user group attribute** command for the user group to which the corresponding user ID belongs.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.34 User group settings used for XAUTH authentication and EAP-MD5 authentication

[Format]

auth user group *groupid userid* [*userid ...*]

no auth user group *groupid*

[Setting value and initial value]

- *groupid*
 - [Setting value]:
 - User group identification number

Setting value	Model
1.6000	vRX Amazon EC2 version(only), vRX VMware ESXi version(only when operating in normal mode), vRX Sakura cloud version
1..3000	RTX5000
1..1000	Others

- [Initial value]: -
- *userid*
 - [Setting value]: User identification number or range of user identification numbers (multiple can be specified)

- [Initial value]: -

[Description]

User group to be used for XAUTH authentication of IKEv1 or EAP-MD5 authentication of IKEv2 is set.

[Configuration Example]

```
# auth user group 1 100 101 102
# auth user group 1 200-300
# auth user group 1 100 103 105 107-110 113
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.35 User group attribute settings used for XAUTH authentication and EAP-MD5 authentication**[Format]**

auth user group attribute *groupid* attribute=*value* [attribute=*value* ...]

no auth user group attribute *groupid* [attribute=*value* ...]

[Setting value and initial value]

- *groupid*
 - [Setting value]:
 - User group identification number

Setting value	Model
1..6000	vRX Amazon EC2 version (when operating in normal mode) vRX VMware ESXi version (only when operating in normal mode), vRX Sakura cloud version
1..3000	RTX5000, RTX3510
1..1000	Others

- [Initial value]: -
- *attribute=value*
 - [Setting value]: User group attribute
 - [Initial value]: xauth=off

[Explanation]

Set the attributes of the user group used for IPsec XAUTH authentication of IKEv1 or IPsec EAP-MD5 authentication of IKEv2. The attributes that can be set are as follows.

Attribute	value	Description
xauth	on	Use the user ID included in this group for IPsec XAUTH authentication
	off	Do not use the user ID included in this group for IPsec XAUTH authentication
xauth-address-pool	IP address range (IPv6 address possible)	When IPsec is connected, select an address from this address pool and notify it as an internal IP address
xauth-dns	IP address (IPv6 address possible)	When IPsec is connected, notify this address as a DNS server address
xauth-wins	IP address (IPv6 address possible)	When IPsec is connected, notify this address as a WINS server address
xauth-filter	String representing the name of the filter set	When IPsec is connected, apply this filter

attribute	value	Description
eap-md5	on	Do not use this ID for IKEv2 EAP-MD5 authentication
	off	Do not use this ID for IKEv2 EAP-MD5 authentication

The IP address range that is the attribute value of xauth-address-pool is described in one of the following formats.

- IP address[/netmask]
- IP address-IP address[/netmask]

If the same attribute is specified in duplicate, a command error occurs.

Notebook

The attribute value set by this command is valid for all users included in the corresponding user group.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.36 Setting up user authentication with XAUTH

Format

ipsec ike xauth request gateway_id auth [group_id]

no ipsec ike xauth request gateway_id [auth ...]

Setting value and initial value

- *gateway_id*
 - Setting value: Identifier of security gateway
 - Initial value: -
- *group_id*
 - Setting value: Identifier of user group used for authentication
 - [Initial value]: -
- *auth*
 - [Setting value]:

Setting value	Description
on	Request
off	Do not request

- [Initial value]: off

[Explanation]

When performing IPsec authentication, it is set whether to request user authentication by XAUTH from a client after Phase 1 is completed.

When *group_id* is specified, users included in the corresponding user group are authenticated.

When *group_id* is not specified or authentication cannot be performed with user information included in the specified user group, authentication using a RADIUS server is additionally attempted if there is a RADIUS server setting.

[Notes]

The setting by this command is valid only when the router operates as a passive side, and when XAUTHInitPreShared (65001) is included as an authentication method in the proposal of isakmp SA parameter sent from the security gateway on the initiator side, this proposal is accepted and user authentication by XAUTH is performed.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.37 Setting internal IP address pool

[Format]

ipsec ike mode-cfg address pool pool_id ip_address[/mask]

ipsec ike mode-cfg address pool pool_id ip_address-ip_address[/mask]

no ipsec ike mode-cfg address pool pool_id [ip_address ...]

[Setting value and initial value]

- *pool_id*
 - setting value: Address pool ID (1..65535)
 - [Initial value]: -
- *ip_address*
 - setting value: IP address (IPv6 address is acceptable)
 - [Initial value]: -
- *ip_address-ip_address*
 - setting value: IP address range (IPv6 address is acceptable)
 - [Initial value]: -
- *mask*
 - setting value: Netmask (prefix length for IPv6 addresses)
 - [Initial value]: -

[Explanation]

Set the address pool of internal IP addresses to be allocated to IPsec clients.
The address pool set by this command is used by the **ipsec ike mode-cfg address gateway_id ...** command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.38 Setting the IKE XAUTH Mode-Cfg method

[Format]

ipsec ike mode-cfg method gateway_id method [option]
no ipsec ike mode-cfg method gateway_id [method...]

[Setting value and initial value]

- *gateway_id*
 - setting value: Identifier of the security gateway
 - [Initial value]: -
- *method*
 - setting value:

setting value	explanation
set	SET method

- [Initial value]: set
- *option*
 - setting value:

setting value	explanation
openswan	Openswan compatible mode

- [Initial value]: -

explanation

Set the address assignment method in Mode-Cfg of IKE XAUTH. Only the SET method can be specified.
If 'openswan' is specified in *option*, it becomes Openswan compatible mode and can connect to Openswan.

[Notes]

When using a Yamaha router on the calling side of a dial-up VPN, XAUTH cannot connect if *option* is specified.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.39 Setting up an internal IP address pool to be assigned to an IPsec client

[Format]

```
ipsec ike mode-cfg address gateway_id pool_id
no ipsec ike mode-cfg address gateway_id [pool_id]
```

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of a security gateway
 - [Initial value]: -
- *pool_id*
 - [Setting value]: Address pool ID
 - [Initial value]: -

[Explanation]

Setting up an internal IP address pool to be referred to when assigning an internal IP address to an IPsec client. Since notification of the internal IP address to the IPsec client is performed in Config-Mode used for XAUTH authentication, notification is not performed when XAUTH authentication is not performed.

When an internal IP address to be assigned to each authenticated user is set by any of the following methods, an individually set address is notified, not from the address pool.

- When it is registered with a RADIUS server
- When it is configured using the following command
 - **auth user** *attribute* *userid* *xauth-address=address[/mask]*
 - **auth user group** *attribute* *groupid* *xauth-address-pool=address-address[/mask]*

When the addresses registered in the address pool are exhausted, no address assignment is performed.

[Notes]

When using YMS-VPN1 as a VPN client, it must be configured to notify the internal IP address in order to perform XAUTH authentication.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.40 Registering a concurrent connection restriction license for a VPN client

[Format]

```
ipsec ike license-key license_id key
no ipsec ike license-key license_id [...]
```

[Setting value and initial value]

- *license_id*
 - [Setting value]: Identification number of a router key (1..500)
 - [Initial value]: -
- *key*
 - [Setting value]: Router key (up to 64 characters)
 - [Initial value]: -

[Description]

Setting up a router key (license key) to accept a VPN connection from the VPN client software (concurrent connection version).

Each router key is assigned a unique number of concurrent connections, and by registering a plurality of different router keys, the maximum number of concurrent connections for the total of each router key can be secured. At this time, the VPN client software may use any client key corresponding to the router key registered in this command. Regardless of the client key used by the VPN client software, connection restrictions are applied based on the maximum number of concurrent connections for each registered router key.

[Notes]

RTX830 can be used after Rev.15.02.15.

[Configuration Example]

```
[For YMS-VPN1-CP/YMS-VPN7-CP]
# tunnel select 1
# tunnel template 2-20
# ipsec tunnel 1
# ipsec sa policy 1 1 esp aes-cbc sha-hmac
# ipsec ike log 1 payload-info
# ipsec ike remote address 1 any
# ipsec ike xauth request 1 on 11
# ipsec ike mode-cfg address 1 1
# ipsec ike license-key use 1 on #
tunnel enable 1
# ipsec ike license-key 1 abcdefg-10-hijklmno
# ipsec ike license-key 2 pqrstuv-10-wxyz0123
# ipsec ike mode-cfg address pool 1 172.16.0.1-172.16.0.20/32
# auth user 1 user1 pass1
# auth user 2 user2 pass2
    [Description]
# auth user 20 user20 pass20
# auth user group 11 1-20
# auth user group attribute 11 xauth=on xauth-dns=10.10.10.1
```

```
[For YMS-VPN8-CP]
# pp select anonymous
# pp bind tunnel1-tunnel20
# pp auth request mschap-v2
# pp auth username user1 pass1
# pp auth username user2 pass2
#
# pp auth username user20 pass20
# ppp ipcp ipaddress on
# ppp ipcp msexp
# ip pp remote address pool 172.16.0.1-172.16.0.20
# ip pp mtu 1258
# pp enable anonymous
# tunnel select 1
# tunnel encapsulation l2tp
# ipsec tunnel 1
# ipsec sa policy 1 1 esp 3des-cbc sha-hmac
# ipsec ike keepalive use 1 off
# ipsec ike local address 1 172.16.0.254
# ipsec ike remote address 1 any
# ipsec ike license-key use 1 on
# l2tp tunnel disconnect time off
# ip tunnel tcp mss limit auto
# tunnel enable 1
#
# ipsec ike license-key 1 abcdefg-10-hijklmno
# ipsec ike license-key 2 pqrstuv-10-wxyz0123
# ipsec transport 1 1 udp 1701
# ipsec auto refresh on
# l2tp service on
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.41 Applying a license to restrict simultaneous connections for VPN clients

[Format]

```
ipsec ike license-key use gateway_id sw
no ipsec ike license-key use gateway_id [...]
```

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *SW*
 - [Setting value]:

Setting value	Description
on	Allow application of router key
off	Do not allow application of router key

- [Initial value]: off

[Explanation]

Whether to allow application of a router key (license key) for accepting VPN connection from VPN client software (simultaneous connection version) is set.

A gateway that is allowed to apply a router key can connect to VPN client software having a corresponding client key.

[Notes]

RTX830 can be used after Rev.15.02.15

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.42 Setting the log type of IKE

[Format]

ipsec ike log *[gateway_id]* *type* [*type*]

no ipsec ike log *[gateway_id]* [*type*]

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *type*
 - [Setting value]:

Setting value	Description
message-info	Contents of an IKE message
payload-info	Contents of payload processing
key-info	Contents of key calculation processing

- [Initial value]: -

[Explanation]

Set the log type to be output. All logs are output in SYSLOG at the debug level.

For models that support IKEv2, the *gateway_id* parameter can be omitted. A setting in which the *gateway_id* parameter is omitted is applied to communications at a point in time when a security gateway cannot be specified when acting as a responder.

[Notes]

If this command is not set, only minimal logs are output. A plurality of *type* parameters can also be set.

[Applied models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.43 Setting whether or not to encapsulate ESP with UDP to send and receive

[Format]

ipsec ike esp-encapsulation *gateway_id* *encap*

no ipsec ike esp-encapsulation *gateway_id*

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Security gateway identifier

- [Initial value]: -
- *encap*
- [Setting value]:

Setting value	Description
on	Encapsulating ESP with UDP to send
off	Encapsulating ESP without UDP to send

- [Initial value]: off

Description

Encapsulating ESP with UDP to send and receive in order to establish IPsec communications in an environment where ESP cannot pass due to NAT or the like. The setting of this command must be matched on both routers.

[Notes]

Cannot be used with the **ipsec ike nat-traversal** command.

This command does not affect IPsec communications with SA established by IKEv2.

[Applied models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.44 Setting whether to limit negotiation parameters

[Format]

ipsec ike proposal-limitation gateway_id switch

no ipsec ike proposal-limitation gateway_id [switch]

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Security gateway identifier
 - [Initial value]: -
- *switch*
 - [Setting value]:

Setting value	Description
on	Setting negotiation parameters not set
off	Setting negotiation parameters not set

- [Initial value]: off

Explanation

Setting whether to limit each negotiation parameter for constructing SA to a specific setting value when starting key exchange with IKEv2. When this command setting is set to off, all available negotiation parameters are proposed. The parameters to which this command is applied and the corresponding commands are as follows.

Parameters	Commands
Cryptographic algorithms	ipsec ike encryption
Groups	ipsec ike group
Hashing algorithms	ipsec ike hash
Cryptographic and authentication algorithms	IPSEC sa policy *When CHILD SA was created

[Notes]

This command is valid only for IKEv2 and does not affect the operation of IKEv1.

RTX1210 can be used after Rev.14.01.09.
 RTX5000 and RTX3500 can be used after Rev.14.00.18.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.45 Configuring Message ID Management for IKE

[Format]

```
ipsec ike message-id-control gateway_id switch
no ipsec ike message-id-control gateway_id [switch]
```

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *switch*
 - [Setting value]:

Setting value	Description
on	Manage sending request messages by message ID
off	Do not manage sending request messages by message ID

- [Initial value]: off

[Description]

Set the message ID management method when sending IKEv2 request messages from own machine.
 When set to on, if all response messages for sent IKE messages using the same IKE SA have not been received, no new IKE messages will be sent.

[Notes]

This command is valid only for IKEv2 and does not affect the operation of IKEv1.
 RTX1210 can be used after Rev.14.01.09.
 RTX5000 and RTX3500 can be used after Rev.14.00.18.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.46 Setting the CHILD SA Creation Method

[Format]

```
ipsec ike child-exchange type gateway_id type
no ipsec ike child-exchange type gateway_id [type]
```

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *type*: Type of CHILD SA creation method for IKEv2
 - [Setting value]:

Setting value	Description
1	Maintains compatibility with the conventional operation of IKEv2 on Yamaha routers - When there is no valid Child SA due to a key update failure, etc., a new Child SA is created by exchanging IKE_SA. - Key update of IKE SA is performed by exchanging CREATE_CHILD_SA. However, when the key update by exchanging CREATE_CHILD_SA is performed for a specified number of times, an IKE SA is created by exchanging IKE_SA_INIT at the timing of the next key update. The number of times is specified by the <i>count</i> parameter of the ipsec ike retry command.
2	CREATE_CHILD_SA Exchange Matching Some Implementations - When there is no valid Child SA due to a key update failure, etc., a new Child SA is created by exchanging CREATE_CHILD_SA. - Always use the CREATE_CHILD_SA exchange to create a Child SA. Key update of

- [Initial value]: 1

[Explanation]

Set the CHILD SA creation method for IKEv2.

When connecting models corresponding to this command, it is necessary to connect with the same setting of *type*.

[Notes]

This command is valid only for IKEv2 and does not affect the operation of IKEv1.

RTX1210 can be used with Rev. 14.00.18 or later.

RTX5000 and RTX3500 can be used with Rev. 14.00.18 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.47 Setting whether to receive a start packet for key exchange

[Format]

ipsec ike negotiation receive gateway_id switch

no ipsec ike negotiation receive gateway_id [switch]

[Setting value and initial value]

- gateway_id*
 - [Setting value]: Security gateway identifier
 - [Initial value]: -
- switch*
 - [Setting value]:

Setting value	Description
on	Receiving a start packet for key exchange
off	Does not receive a start packet for key exchange

- [Setting value]: on

[Explanation]

Set whether to receive a start packet for key exchange in IKEv2.

When it is set not to receive, as a result, it does not operate as a passive side but always operates as a start side.

[Notes]

This command is valid only in IKEv2 and does not affect the operation of IKEv1.

When it is set to off, it is necessary to set the ipsec ike remote address or the ipsec ike remote name with an IP address.

RTX5000 Rev.14.00.26 以降、RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降で使

It can be used.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.48 SA-related settings

Note that all SAs are cleared when restarted.

13.48.1 SA lifetime setting**[Format]**

ipsec ike duration sa gateway_id second [kbytes] [rekey rekey] [forced-reduction=del_time]

no ipsec ike duration sa gateway_id [second [kbytes] [rekey rekey] [forced-reduction=del_time]]

[Setting value and initial value]

- **sa**

- [Setting value]:

Setting value	Description
ipsec-sa (or ike-sa)	IPsec SA (CHILD SA)
isakmp-sa (or ike-sa)	ISAKMP SA (IKE SA)

- [Initial value]: -

- **gateway_id**

- [Setting value]: Security gateway identifier

- [Initial value]: -

- **second**

- [Setting value]: Number of seconds (300..691200)

- [Initial value]: 28800 seconds

- **kbytes**

- [Setting value]:

Setting value	Description
100..100,000	Number of bytes in kilos (RTX5000 / RTX3500 Rev.14.00.33 or earlier, RTX1220 Rev.15.04.04 or earlier, RTX1210 Rev.14.01.41 or earlier, RTX830 Rev.15.02.26 or earlier) (previous)
100..2147483647	Number of bytes in kilos (models and revisions other than the above)
off	Do not set byte lifetime (RTX5000 / RTX3500 Rev.14.00.33 or earlier, RTX1220 Rev.15.04.04 or earlier, RTX1210 Rev.14.01.41 or earlier, and RTX830 Cannot be specified before Rev.15.02.26)

- [Initial value]:

- (RTX5000 / RTX3500 Rev.14.00.33 or earlier, RTX1220 Rev.15.04.04 or earlier, RTX1210 Rev.14.01.41 or earlier, RTX830 Rev.15.02.26 or earlier)

- 2,000,000 (models and revisions other than the above)

- **rekey** : Timing to update SA

- Set value:

Set value	Description
70% - 90%	Percentage

Set value	Description
off	

- [Initial value]: 75%
- del_time
 - [Setting value]: Time to forcibly shorten the lifetime of an old SA (1..691200)
 - [Initial value]: -

[Explanation]

Sets the lifetime of each SA.

If the kbytes parameter is specified, the SA will expire either when the time specified by the second parameter has elapsed or after processing the specified number of bytes of data.

The kbytes parameter is valid only when ipsec-sa (child-sa) is specified as the sa parameter.

The SA is updated when 75% of the number of bytes specified in the kbytes parameter has been processed.

When an IPsec SA (CHILD SA) is updated, if the remaining lifetime of the existing (old) IPsec SA (CHILD SA) is 30 seconds or more, its lifetime will be shortened to 30 seconds.

The rekey parameter determines the timing for updating the SA.

For example, if 20000 is specified for the second parameter and 75% is specified for the rekey parameter, a new SA will be generated 15000 seconds after the SA was created.

The rekey parameter represents a ratio relative to the second parameter and is unrelated to the value of the kbytes parameter.

When isakmp-sa (ike-sa) is specified as the sa parameter, the rekey parameter can be set to "off".

In this case, unless it is necessary to create an IPsec SA (CHILD SA), renewal of the ISAKMP SA (IKE SA) will be deferred, thereby minimizing the number of ISAKMP SA (IKE SA) establishments.

Notes Depending on IKE Version

· IKEv1

When operating as the initiator, the lifetime value configured by this command is proposed.

When operating as the responder, the device conforms to the lifetime value proposed by the peer, regardless of this command's configuration.

If the rekey parameter for the ISAKMP SA is set to off, the following two points must be observed to achieve the intended effect:

Set the ISAKMP SA lifetime shorter than the IPsec SA lifetime.

Allow dangling SAs; in other words, set the ipsec ike restrict-dangling-sa command to off.

When connecting to the following models/revisions:

RTX5000 / RTX3500 Rev.14.00.33 or earlier , RTX1220 Rev.15.04.04 or earlier ,
 RTX1210 Rev.14.01.41 or earlier , RTX830 Rev.15.02.26 or earlier , NVR700W Rev.15.00.23 or earlier
 the kbytes parameter must be set to 2 GB or less.
 These models/revisions cannot correctly recognize byte lifetime values exceeding 2 GB.

· IKEv2

In IKEv2, SA lifetime values are not negotiated; each security gateway independently manages them.

Therefore, the lifetime configured by this command is always applied to the established SA.
 However, if the peer security gateway updates the SA earlier, the SA will be updated accordingly.

If a time is specified for the forced-reduction option, when an SA is updated, the lifetime of the old SA can be forcibly changed to the configured value, thereby shortening the time until it expires.

However, if a byte lifetime value is specified for the kbytes parameter of an IPsec SA (CHILD SA), even if del_time is set to 31 seconds or more, the shortened value will be 30 seconds.

In IKEv1, if the remaining lifetime is already shorter than the configured value, it will not be changed.

If the lifetime of the ISAKMP SA (IKE SA) expires before the IPsec SA (CHILD SA), the ISAKMP SA (IKE SA) lifetime will be adjusted to match the IPsec SA (CHILD SA) lifetime.

Note that even if this command is configured, the lifetime of already existing SAs will not change. The new lifetime value applies only to newly created SAs.

[Note]

The forced-reduction option cannot be specified on:

vRX Amazon EC2 edition , vRX VMware ESXi edition, RTX5000 / RTX3500 Rev.14.00.33 or earlier, RTX1300 Rev.23.00.04 or earlier, RTX1220 Rev.15.04.04 or earlier, RTX1210 Rev.14.01.41 or earlier, RTX830 Rev.15.02.26 or earlier

[Applicable Models]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.48.2 SA Policy definition

[Format]

ipsec sa policy *policy_id* gateway_id ah [*ah_algorithm*] [*local-id=local-id*] [*remote-id=remote-id*] [*anti-replay-check=check*]

ipsec sa policy *policy_id* gateway_id esp [*esp_algorithm*] [*ah_algorithm*] [*anti-replay-check=check*]

no ipsec sa policy *policy_id* [*gateway_id*]

[Configuration Value and Initial Value]

- *policy_id*
 - [Setting value]: Policy ID (1..2147483647)
 - [Initial value]: -
- *gateway_id*
 - [Setting value]: Identifier of the security gateway
 - [Initial value]: -
- *ah*: Keyword indicating the Authentication Header (AH) protocol
 - [Initial value]: -
- *esp*: Keyword indicating the Encapsulating Security Payload (ESP) protocol
 - [Initial value]: -
- *ah_algorithm*: Authentication algorithm
 - [Setting value]: -

Setting value	Description
md5-hmac	HMAC-MD5
sha-hmac	HMAC-SHA-1
sha256-hmac	HMAC-SHA2-256
sha384-hmac	HMAC-SHA2-384
sha512-hmac	HMAC-SHA2-512

- [Initial value]:
 - sha-hmac (for AH protocol)
 - - (for ESP protocol)
- *esp_algorithm* : Cryptographic algorithm
 - [Setting value]:

Setting value	Description
3des-cbc	DES-CBC
des-cbc	DES-CBC
aes-cbc	AES128-CBC
aes256-cbc	AES256-CBC

- [Initial value]: aes-cbc
- *local-id*
 - [Setting value]: Private network on your side
 - [Initial value]: -
- *remote-id*
 - [Setting value]: Private network on the other side

- [Initial value]: -
- *check*
- [Setting value]:

Setting value	Description
on	Check sequence number
off	Do not check sequence number

- [Initial value]:
 - off (RTX3510、RTX1300)
 - on (other than the above)

Description

Define SA policy. This definition is necessary for setting tunnel mode and transport mode. This definition can be used in multiple tunnel mode and transport mode.

Local-id and *remote-id* describe the range of start/end point addresses of packets to be encapsulated in network address. Thereby, multiple IPsec SAs can be generated for one security gateway, and SAs can be used properly according to the contents of IP packets.

In the case of *check=on*, duplicate sequence numbers and numerical order checks are performed for each received packet, and packets that cause errors are discarded. When discarding, check the debug level

```
[IPSEC] sequence difference
[IPSEC] sequence number is wrong
```

and logs are recorded.

If the other side performs priority/bandwidth control at tunnel interface, packets may be received with sequence number order switched. In such a case, the above log may be displayed and packets may be discarded even if there is no actual error, so it is better to turn off the setting.

In IKEv2, when the **ipsec ike proposal-limitation** command is set to on, algorithms set by *ah_algorithm* and *esp_algorithm parameters* of this command are proposed. When the **ipsec ike proposal-limitation** command is set to off, or in a model that does not support the **ipsec ike proposal-limitation** command, all supported algorithms are proposed at the same time regardless of the setting of this command, and the other side security gateway is selected. When acting as a responder, algorithms are selected in the following order of priority from received proposals.

- Authentication algorithm
HMAC-SHA2-512 > HMAC-SHA2-384 > HMAC-SHA2-256 > HMAC-SHA-1 > HMAC-MD5
※HMAC-SHA2-512 and HMAC-SHA2-384 are vRX Amazon EC2 version, vRX VMware ESXi version, RTX5000, RTX3500,
Not available for RTX1220, RTX1210, RTX840, and RTX830.
- Cryptographic algorithm
AES256-CBC > AES192-CBC > AES128-CBC > 3DES-CBC > DES-CBC
※Only IKEv2 supports AES192-CBC. However, it is not possible to select AES192-CBC by command. In addition, *local-id* and *remote-id* parameters are not effective in IKEv2.

[Notes]

Local-id and *remote-id* set in both must match.

The sha384-hmac and sha512-hmac keywords of *ah_algorithm parameter* are vRX Amazon EC2 version, vRX VMware ESXi edition, RTX5000, RTX3500, RTX1220, RTX1210, RTX840, and RTX830.

[Configuration Example]

```
# ipsec sa policy 101 1 esp aes-cbc sha-hmac
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.48.3 Manual update of SA

[Format]

IPSEC refresh sa

Manually update SA.

[Notes]

Delete all managed SA and initialize the state of IKE.

Since this command does not notify the other party to delete SA, the **ipsec sa delete all** command is preferable in normal operation.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.48.4 Setting the behavior of dangling SA**[Format]**

ipsec ike restrict-dangling-sa gateway_id action

no ipsec ike restrict-dangling-sa gateway_id [action]

[Setting value and initial value]

- *gateway_id*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *action*
 - [Setting value]:

Setting value	Explanation
auto	Synchronize IKE SA and IPsec SA only on the start side of aggressive mode
off	Do not synchronize IKE SA and IPsec SA.

- [Initial value]: auto

[Description]

This command sets a limit on the behavior of dangling SA of IKEv1.

Dangling SA refers to the state when the corresponding IPsec SA is left without deleting when deleting IKE SA. Basically, RT series implements it with the policy of allowing dangling SA and deletes IKE SA and IPsec SA independently.

When set to off, the start side of aggressive mode eliminates dangling SA and deletes IKE SA and IPsec SA in synchronization. This behavior is necessary for IKE keepalive to operate normally.

When set to off, the behavior always permits dangling SA and deletes IKE SA and IPsec SA independently.

If it is not the client side of dial-up VPN, IKE SA and IPsec SA are always set regardless of this command setting. are managed independently and the timing of deletion is not always synchronized.

[Notes]

Even if a dangling SA is forcibly deleted, communication will not be disturbed because a new IPsec SA based on the new IKE SA usually exists.

On the client side of dial-up VPN, this command can change the behavior; otherwise, a dangling SA does nothing and continues to communicate.

The reason why a dangling SA is not allowed on the client side of dial-up VPN is that it is necessary for IKE keepalive to function properly.

In IKE keepalive, keepalive is performed based on IKE SA. When a dangling SA occurs, there is no IKE SA for keepalive for that SA and the keepalive operation cannot be performed. Therefore, in order to make the IKE keepalive work properly, if a dangling SA occurs, it must be forcibly deleted and communication must be performed on the IPsec SA where the corresponding IKESA exists.

This command does not affect the behavior of IKEv2. The specification of IKEv2 prohibits the existence of dangling SA.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.48.5 Settings for using IPsec NAT traversal

[Format]

ipsec ike nat-traversal *gateway switch* [*keepalive=interval*] [*force=force_switch*] [*type=type*]

no ipsec ike nat-traversal *gateway* [*switch ...*]

[Setting value and initial value]

- *gateway*
 - [Setting value]: Identifier of security gateway
 - [Initial value]: -
- *switch*: Operation
 - [Setting value]:

Setting value	Description
on	Enable NAT traversal operation
off	Disable NAT traversal operation

- [Setting value]: off
- *interval*: NAT keep alive transmission interval
 - [Setting value]:

Setting value	Description
off	Do not transmit
30-100000	Time [seconds]

- [Setting value]: 300
- *force_switch*
 - [Setting value]:

Setting value	Description
on	Use NAT traversal even if there is no NAT on the communication path
off	Do not use NAT traversal if there is no NAT on the communication path

- [Setting value]: off
- *type*
 - [Setting value]:

Setting value	Description
1	Maintains compatibility with conventional operation of Yamaha routers
2	Match payload exchanged when NAT traversal is used to some implementations

- [Setting value]: 1

Description

Set NAT traversal operation Negotiate NAT traversal in IKE when this setting exists.

When the other party does not support NAT traversal or there is no NAT processing on the communication path, NAT traversal is not used and communication is performed using ESP packets.

Opposing routers and terminals also need to set NAT traversal. When only one of them is set, NAT traversal is not used and communication is performed using ESP packets.

When connecting between models corresponding to *type*, it is necessary to connect with the same setting of *type*. Also, when 2 is specified for *type*, connection with a model not corresponding to *type* is not possible.

In IKEv2, the *force_switch* parameter affects only when operating as an initiator. This option is used in communications

It is used when connecting to an opposing device that requires NAT traversal operation even if there is no NAT processing on the road. Note that it is usually 'off' is desirable.

[Notes]

It cannot be used in conjunction with the **ipsec ike esp-encapsulation** command.

It cannot be used in tunnel interfaces where IPComp is set.

In IKEv1, it can be used only in main mode and ESP tunnels in aggressive mode. It cannot be used in AH, nor in transport mode.

However, it can be used in IKEv1 which is used in L2VPN using L2TP/IPsec and L2TPv3, even in main mode and ESP tunnels in transport mode.

In IKEv2, it can be used only when establishing an ESP tunnel. It cannot be used in AH, nor in transport mode.

NAT traversal in IKEv1 main mode is available for RTX5000 / RTX3500 Rev.14.00.21 and earlier and RTX1210 Rev.14.01.19.

It cannot be used before.

The *type* option is not available for RTX5000 / RTX3500 Rev. 14.00.21 or earlier and RTX1210 Rev. 14.01.19 or earlier.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.48.6 SA deletion

[Format]

ipsec sa delete *id*

[Setting value and initial value]

- *ID*
- [Setting value]:

Setting value	Description
Number	SAID
all	All SA

- [Initial value]: -

[Explanation]

Delete the specified SA.

The SA ID is automatically assigned and can be confirmed with the **show ipsec sa** command.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.49 Tunnel interface related settings

13.49.1 Configuring fragments for IPv4 packets outside the IPsec tunnel

[Format]

ipsec tunnel fastpath-fragment-function follow df-bit *switch*

no ipsec tunnel fastpath-fragment-function follow df-bit [*switch*]

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Description
on	When an ESP packet needs to be fragmented, it is determined whether to fragment according to the DF bit of the ESP packet.

Setting value	Description
off	When an ESP packet needs to be fragmented, it is fragmented regardless of the DF bit of the ESP packet.

- [Initial value]: off

[Explanation]

When an ESP packet needs to be fragmented, it is set whether to fragment according to the DF bit. Even if an ESP packet has the DF bit set by the ipsec tunnel outer df-bit command, it will be fragmented if off is set by this command. This command is configured for the tunnel interface and targets only ESP packets processed by the fast path.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.49.2 Configuring control of the DFbit for IPv4 packets outside the IPsec tunnel

[Format]

ipsec tunnel outer df-bit *mode*

no ipsec tunnel outer df-bit [*mode*]

[Setting value and initial value]

- *Mode*
- [Setting value]:

Setting value	Description
copy	Copy the DF bit of the inner IPv4 packet to the outer packet
Set	Always 1
clear	Always 0

- [Initial value]: copy

[Explanation]

Controls how the DF bit is set for IPv4 packets outside the IPsec tunnel.

In the case of copy, the DF bit of the inner IPv4 packet is copied to the outer packet as it is.

In the case of set or clear, the DF bit of the outer IPv4 packet is set to 1 or 0, respectively, regardless of the DF bit of the inner IPv4 packet.

It is a command for each tunnel interface.

[Notes]

When IPsec packets must be fragmented due to the magnitude relationship between the MTU value of the tunnel interface and that of the real interface, the DF bit is set to 0 regardless of the setting of this command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.49.3 Setting the SA Policy to use

[Format]

ipsec tunnel policy_id

no ipsec tunnel [*policy_id*]

[Setting value and initial value]

- *policy_id*
- [Setting value]: Integer (1..2147483647)
- [Initial value]: -

[Explanation]

Setting the policy of the SA to be used for the selected tunnel interface.

[Applicable model]**13.49.4 Configuring Data Compression Using IPComp**

[Format]

```
ipsec ipcomp type type
no ipsec ipcomp type [type]
```

[Parameters and Default Values]

Value	Description
deflate	Compresses data using the deflate algorithm
none	Does not perform data compression

[Initial value]: none

[Explanation]

Configures whether to perform data compression using IPComp.

The only supported compression algorithm is deflate.

No special configuration is required to decompress received IPComp packets.

That is, if an IPComp packet compressed using a supported algorithm is received, it will be decompressed regardless of the current configuration.

It is not always necessary to configure this command on both security gateways.

If it is configured on only one side, only IP packets transmitted from that security gateway will be compressed.

IPComp cannot be used when only transport mode is employed..

[Notes]

Data compression methods also include CCP (used in PPP) and FRF.9 (used in Frame Relay).

There is no fundamental difference between the deflate algorithm used by IPComp and the Stac-LZS algorithm used by CCP/FRF.9.

However, in CCP/FRF.9, data compression is performed after encryption by IPsec.

As a result, the compression is applied to data that has already been randomized by encryption, which provides almost no effect.

In contrast, IPComp performs data compression before encryption by IPsec, allowing a certain degree of compression efficiency.

Additionally, unlike CCP/FRF.9, compressed data remains compressed across the entire path to the peer security gateway.

Therefore, compression benefits can be expected even if this device's output interface is a LAN interface.

[Supported Models]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.49.5 Tunnel Backup Configuration

```
tunnel backup none
```

```
tunnel backup interface ip_address
```

```
tunnel backup pp peer_num [switch-router=switch1]
```

```
tunnel backup tunnel tunnel_num [switch-interface=switch2]
```

- None : not use tunnel backup
 - [Initial value]: -none
- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *ip_address*
 - [Setting value]: Gateway IP Address for the backup destination
 - [Initial value]: -

- **Peer_num**
 - [Initial value]: Destination information number of the backup destination
 - [Setting value]: -
- **tunnel_num**
 - [Initial value]: Tunnel interface number
 - [Setting value]: -
- **switch1**: Whether or not to split the router receiving the backup into two
 - [Setting value]:

Setting value	Description
on	Divide
off	Do not divide

- [Setting value]: off
- **switch2**: Whether or not to re-create the tunnel according to the backup of the LAN/PP interface
 - [Setting value]:

Setting value	Description
on	Re-create
off	Do not re-create

- [Setting value]: on

[Setting value]

An interface to be used as a backup when a failure occurs in the tunnel interface is specified.

The switch-router option is set to on when the following two conditions are satisfied.

- There are two routers on the receiving side of the backup, and one of them is connected to the backup source line, and the other is connected to the backup destination line.
- Firmware or image of a Yamaha router connected to the backup source line is older than this revision.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.49.6 Tunnel template setting

[Format]

tunnel template *tunnel_num* [*tunnel_num* ...]

no tunnel template

[Setting value and initial value]

- **tunnel_num**
 - [Setting value]: Tunnel interface number or tunnel interface number range specified by inserting a hyphen (-) in between
 - [Setting value]: -

[Setting value]

A tunnel interface to be the deployment destination of a command set in the interface is set, with the tunnel interface selected by the **tunnel select** command as the deployment source.

Commands that are also applied to the destination tunnel interface by setting it to the tunnel interface of the deployment source are as follows. For commands with *1 added at the end, refer to [Notes].

- **ipsec tunnel**
- **IPsec sa policy**
- Commands starting with **ipsec ike whose** parameters take the identifier of the security gateway
- **ipsec auto refresh** (if specifying the identifier of the security gateway in the argument)
- **tunnel encapsulation**
- **tunnel ngn arrive permit**
- **tunnel ngn bandwidth**
- **tunnel ngn disconnect time**
- **tunnel ngn radius auth**
- Commands starting with **I2tp** (*1)
- **Tunnel enable**

The following commands among the commands are deployed only when a value of a specific parameter matches the tunnel interface number of the deployment source. In that case, the value of the parameter is replaced with the tunnel

interface number of the deployment destination.

Commands	Parameters
ipsec tunnel	Policy ID
IPsec sa policy	Policy ID
Commands starting with ipsec ike	Identifier of the security gateway
ipsec auto refresh	Identifier of the security gateway
Tunnel enable	Tunnel interface number

In the **ipsec sa policy** command, the identifier of the security gateway is replaced with the tunnel interface number of the deployment destination.

In the **ipsec ike remote name** command, the tunnel interface number of the deployment destination is added to the end of the name of the other party's security gateway.

When a command identical to that set in the deployment source tunnel interface is already set in the deployment destination tunnel interface, the command set in the deployment destination tunnel interface has priority.

The settings referred to when the router operates after command expansion can be confirmed by specifying the expand keyword in the **show config tunnel** command.

[Notes]

It can be used only when the tunnel interface is selected.

Commands with (*1) added at the end among the commands to be expanded are not supported in RTX5000 / RTX3500 Rev.14.00.11 or earlier.

[Configuration Example]

As the deployment destination tunnel interface, specification of the number and specification of the range can be described simultaneously.

```
tunnel select 1
  tunnel template 8 10-20
tunnel select 2
  tunnel template 100 200-300 400
```

The following two settings show the same content.

```
tunnel select 1
  tunnel template 2
    ipsec tunnel 1
    ipsec sa policy 1 1 esp aes-cbc sha-hmac
    ipsec ike encryption 1 aes-cbc
    ipsec ike group 1 modp1024
    ipsec ike local address 1 192.168.0.1
    ipsec ike pre-shared-key 1 text himitsu1
    ipsec ike remote address 1 any
    ipsec ike remote name 1 pc
  tunnel enable 1
tunnel select 2
  ipsec ike pre-shared-key 2 text himitsu2
```

```
tunnel select 1
  ipsec tunnel 1
  ipsec sa policy 1 1 esp aes-cbc sha-hmac
  ipsec ike encryption 1 aes-cbc
  ipsec ike group 1 modp1024
  ipsec ike local address 1 192.168.0.1
  ipsec ike pre-shared-key 1 text himitsu1
  ipsec ike remote address 1 any
  ipsec ike remote name 1 pc
  tunnel enable 1
tunnel select 2
  ipsec tunnel 2
  IPSEC SA POLICY 2 2 ESPH AES-BCBC SHAH-MAC
```

```

ipsec ike encryption 2 aes-cbc
ipsec ike group 2 modp1024
ipsec ike local address 2 192.168.0.1
ipsec ike pre-shared-key 2 text himitsu2
ipsec ike remote address 2 any
ipsec ike remote name 2 pc2
tunnel enable 2

```

[Applicable model]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.50 Transport mode related settings

13.50.1 Transport mode related settings

[Format]

ipsec transport id *policy_id* [*proto* [*src_port_list* [*dst_port_list*]]]

no ipsec transport id [*policy_id* [*proto* [*src_port_list* [*dst_port_list*]]]]

[Setting value and initial value]

- *id*
 - Setting value: Transport ID (1..2147483647)
 - Initial value: -
- *policy_id*
 - Setting value: Policy ID (1..2147483647)
 - Initial value: -
- *proto*
 - Setting value: Protocol
 - Initial value: -
- *src_port_list*: Source port number string for UDP and TCP
 - Setting value:
 - Decimal number representing the port number
 - Mnemonic representing the port number
 - *(All ports)
 - Initial value: -
- *dst_port_list*: Destination port number string for UDP and TCP
 - Setting value:
 - Decimal number representing the port number
 - Mnemonic representing port number
 - *(All ports)
 - [Initial value]: -

[Explanation]

Transport mode is defined.

After definition, communication in transport mode is started for IP packets that match *proto*, *src_port_list*, and *dst_port_list* parameters.

[Notes]

TCP protocol cannot be specified in the vRX series.

[Configuration Example]

- TELNET data is communicated in transport mode.

```

# ipsec sa policy 101 1 esp aes-cbc sha-hmac
# ipsec transport 1 101 tcp * telnet

```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

13.50.2 Transport mode template settings

[Format]

ipsec transport template *id1 id2* [*id2* ...]

no ipsec transport template *id1* [*id2* ...]

[Setting value and initial value]

- *id1*
 - [Setting value]: Transport ID of deployment source
 - [Initial value]: -
- *id2*
 - [Setting value]: Transport ID of deployment destination or transport ID range specified by inserting a hyphen (-) between them.
 - [Initial value]: -

[Explanation]

Transport ID to be deployed setting of specified **ipsec transport** command is set. Policy ID of deployment destination is set to the same value as transport ID of deployment destination.

If a setting already exists for transport ID of deployment destination, the deployment destination

setting takes precedence. By this command, the **ipsec transport** command setting can be

deployed up to the number of VPN destinations.

It cannot be deployed beyond the number of VPN destinations.

[Notes]

RTX3500 can be used after Rev.14.00.12.

RTX3500 can be used after Rev.14.00.12.

[Configuration Example]

Transport ID and transport ID ranges can be described simultaneously as the destination setting.

```
ipsec transport 1 1 udp 1701 *
ipsec transport template 1 10 20-30
```

The following two settings show the same content.

```
ipsec transport 1 1 udp 1701 *
ipsec transport template 1 2 10-12
```

```
ipsec transport 1 1 udp 1701 *
ipsec transport 2 2 udp 1701 *
ipsec transport 10 10 udp 1701 *
ipsec transport 11 11 udp 1701 *
ipsec transport 12 12 udp 1701 *
```

[Supports extended license]

When an [extended license](#) is imported, the maximum number of transport IDs (*id*) to deploy setting of **ipsec transport** command is expanded.

- *id*

License name	Maximum number after expansion (Value per license)				
	1	2	3	4	5
YSL-VPN-EX1	100	-	-	-	-
YSL-VPN-EX2	300	500			
YSL-VPN-EX3				3000	

[Applicable model]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.51 PKI Related Configuration

13.51.1 Configuring Certificate Files

[Format]**pki certificate file** *cert_id file type [password]***no pki certificate file** *cert_id [file ...]***[Parameters and Default Values]**

- *cert_id*
 - Value

Value	Description
1..8	Identifier of the certificate file

- [Initial value]: -
- *file*
 - [Setting value]: Absolute or relative path to the certificate file
 - [Initial value]: -
- *type* : File format
 - Value

Value	Description
pkcs12	PKCS#12 format file
x509-pem	X.509 PEM format file

- [Initial value]: -
- *password*
 - [Setting value]: Password to decrypt the file (up to 64 single-byte characters)
 - [Initial value]: -

[Description]

Configures a certificate file.

If a relative path is specified for *file*, it is interpreted relative to the directory specified by the environment variable *pwd* set by the *set* command.

If *pkcs12* is specified for *type*, a password must be specified to decrypt the file.

[Supported Models]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

13.51.2 Configuring CRL Files

[Format]**pki crl file** *crl_id file***no pki crl file** *crl_id [file]***[Parameters and Default Value]**

- *crl_id*
 - Value

Value	Description
1..8	Identifier of the CRL file

- [Initial value]: -
- *file*
 - [Setting value]: Absolute or relative path to the CRL file
 - [Initial value]: -

[Explanation]

Configures a CRL file.

If a relative path is specified for file, it is interpreted relative to the directory specified by the environment variable pwd set by the set command.

[Applicable model]

[vRX Series] RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX83000, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 14

L2TP Function Configuration

L2TP/IPsec Function

L2TP (Layer Two Tunneling Protocol) is a tunneling protocol that realizes VPN (Virtual Private Network) connection between networks. L2TP itself does not have an encryption mechanism, but there is L2TP/IPsec that realizes VPN connection that secures data confidentiality and integrity by using IPsec together. Yamaha router operates as a server of remote access VPN using L2TP/IPsec. It enables secure communication with terminals in private networks under Yamaha routers over the Internet from L2TP clients installed in smartphones, etc.

L2TP/IPsec supported by Yamaha routers has the following restrictions.

- L2TP alone does not provide functions. Only L2TP/IPsec is supported.
- It operates as a server of remote access VPN. It does not operate as a client.
- It does not support LAN-to-LAN connection VPN.
- Port number 1701 of UDP is used for the first wait of an L2TP packet. It cannot be changed.
- It supports only IKEv1 and cannot use IKEv2.

L2TPv3 Function

L2TPv3 (Layer Two Tunneling Protocol version 3) is a tunneling protocol that realizes VPN connection (L2VPN) at the data link layer (L2). By encapsulating L2 frames as IP packets, it is possible to transfer L2 frames between routers, and it is possible to build a network of the same segment at multiple bases. L2TPv3 itself does not have an encryption mechanism, but there is L2TPv3/IPsec that realizes a VPN connection that secures data confidentiality and integrity by using it together with IPsec. In Yamaha routers, you can build L2VPN using L2TPv3 and L2VPN using L2TPv3/IPsec.

The following restrictions are applied to L2TPv3 supported by Yamaha routers.

- As an encapsulation method of L2 frames, it supports only the method of encapsulating as UDP packets (L2TPv3 over UDP). It does not support the method of encapsulating as IP packets (L2TPv3 over IP) using IP protocol number 115.
- Port number 1701 of UDP is used to receive L2TPv3 packets. It cannot be changed.
- The only L2 frames that can be tunneled by L2TPv3 are Etherframes.
- Only transport mode of IKEv1 is supported by L2TPv3/IPsec.

14.1 Setting whether to operate L2TP

Format

```
l2tp service service [version [version]]
no l2tp service [service [version [version]]]
```

Setting value and initial value

- *service*
 - Setting value

Setting value	Explanation
on	Enabling L2TP
off	Disabling L2TP

- Initial value: off
- *version*
 - Setting value

Setting value	Explanation
l2tp	Enabling L2TP/IPsec
l2tpv3	Enabling L2TPv3, L2TPv3/IPsec

- Initial value: -

Confi

Setting whether to operate L2TP

Version can specify the version of L2TP that operates. When version is not specified, both L2TPv2 and L2TPv3 operate.

When L2TP is enabled, open port number 1701 of UDP and wait for the connection of an L2TP connection.

When L2TP is disabled, close port number 1701 of UDP and disconnect all connected L2TP connections.

Notebook

Version option cannot be specified in vRX Amazon EC2 version.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

14.2 Configuration for L2TP tunnel authentication**Format**

l2tp tunnel auth *switch* [*password*]

no l2tp tunnel auth [*switch* ...]

[Setting value and initial value]

- *switch*
 - [Setting value]:

Setting value	Description
on	Perform L2TP tunnel authentication
off	Do not perform L2TP tunnel authentication

- [Initial value]: off
- *password*
 - [Setting value]: Password used for L2TP tunnel authentication (up to 32 characters)
 - [Initial value]: -

Description

Whether to perform L2TP tunnel authentication is set.

If password is omitted, the model name ("vRX" in the case of the vRX series) is used as a password.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

14.3 Setting cutting timer for L2TP tunnel**[Format]**

l2tp tunnel disconnect *time time*

no l2tp tunnel disconnect time [*time*]

[Setting value and initial value]

- *time*
 - [Setting value]:

Setting value	Description
1..21474836	Number of seconds
off	Do not set timer

- [Initial value]: 60

Description

Setting cutting timer for L2TP tunnel

For selected L2TP tunnel, the time for cutting L2TP tunnel by timeout is set when data packet is not inputted or not transmitted.

Since all data packets except for L2TP control message are used, cutting of L2TP tunnel by cutting timer may not be performed when PPP keepalive is used.

It can only be configured for tunnel interface.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

14.4 Setting L2TP keepalive

[Format]

l2tp keepalive *use switch* [*interval* [*count*]]

no l2tp keepalive *use* [*switch* ...]

[Setting value and initial value]

- *switch*

- [Setting value]:

Setting value	Description
on	Using L2TP keepalive
off	Do not use L2TP keepalive

- [Initial value]: on

- *Interval*

- [Setting value]: Time interval for sending keepalive packets [seconds] (1.600)

- [Initial value]: 10

- *count*

- [Setting value]: Number of times to judge down detection (1.50)

- [Initial value]: 6

Description

Select whether to use L2TP keepalive or not.

When keepalive is performed, keepalive by Hello message of L2TP operates according to setting values of *interval* and *count*.

It can only be configured for tunnel interface.

[Applicable model]

[Model] vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

14.5 L2TP keepalive log settings

[Format]

l2tp keepalive *log* *log*

no l2tp keepalive *log* [*log*]

[Setting value and initial value]

- *log*

- [Setting value]:

Setting value	Description
on	L2TP keepalive is output to log
off	Do not output L2TP keepalive to log

- [Initial value]: off

Confi

Set whether to output L2TP keepalive log. All logs are output to SYSLOG at the debug level. It can be set only for tunnel interface.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

14.6 Setting whether to output L2TP connection control syslog

[Format]

l2tp syslog syslog

no l2tp syslog [*syslog*]

[Setting value and initial value]

- *syslog*
- [Setting value]:

Setting value	Description
on	Logs related to L2TP connection control are output to SYSLOG. Do not output to
off	Logs related to L2TP connection control are output to SYSLOG. Do not output to

- [Initial value]: off

Description

Set whether to output logs related to L2TP connection control to SYSLOG. Logs related to L2TP keepalive are not output. All logs are output to SYSLOG at the debug level. Can be set only for tunnel interface.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

14.7 Setting up L2TPv3 constant connection

[Setting value]

L2TP always-on sw

no l2tp always-on [*sw*]

[Setting value and initial value]

- *SW*
- [Setting value]:

Setting value	Description
on	Always connect
off	Always not connect

- [Initial value]: on

Description

Set whether to always connect L2TPv3 connections. Can be set only for tunnel interface.

[Notebook]

RTX3500 is available after Rev. 14.00.12.

RTX3500 is available after Rev. 14.00.12.

[Applicable model]

[VRX] VMware ESXi version, vRX Sakura Cloud Edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

14.8 Setting the host name of an L2TP tunnel

[Format]

l2tp hostname *hostname*

no l2tp hostname [*name*]

[Setting value and initial value]

- *Name*
 - [Setting value]: Host name (up to 32 characters)
 - [Initial value]: Model name

[Explanation]

Set the host name to be notified to the connection partner.

It is displayed in the L2TP tunnel information output by the show status l2tp command. If this command is not set, the model name is used as the host name. Only the tunnel interface can be set.

[Notes]

RTX5000 can be used with Rev.14.00.12 or later.

RTX3500 can be used with Rev.14.00.12 or later.

[Applicable model]

vRX VMware ESXi version, vRX Sakura Cloud Edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

14.9 Setting the Local Router ID of L2TPv3

[Format]

l2tp local router-id *ipv4_address*

no l2tp local router-id [*ipv4_address*]

[Setting value and initial value]

- *ipv4_address*
 - [Setting value]: IPv4 address
 - [Initial value]: 0.0.0.0

[Explanation]

Set the Router ID to be notified to the connection partner of L2TPv3.

Set the same IPv4 address as the Remote Router ID of the connection partner. It is not necessary to use the IPv4 address set in the router. It can only be set for the tunnel interface.

[Notes]

RTX5000 can be used with Rev.14.00.12 or later.

RTX3500 can be used with Rev.14.00.12 or later.

[Applicable model]

vRX VMware ESXi version, vRX Sakura Cloud Edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

14.10 Setting the Remote Router ID of L2TPv3

[Format]

l2tp remote router-id *ipv4_address*

no l2tp remote router-id [*ipv4_address*]

[Setting value and initial value]

- *ipv4_address*
 - [Setting value]: IPv4 address
 - [Initial value]: 0.0.0.0

[Explanation]

Set the Router ID of the connection partner of L2TPv3.

Set the same IPv4 address as the Local Router ID of the connection partner.

It is not necessary to use the IPv4 address set in the router. It can only be set for the tunnel interface.

[Notes]

RTX5000 can be used with Rev.14.00.12 or later.

RTX3500 can be used with Rev.14.00.12 or later.

[Applicable model]

vRX VMware ESXi version, vRX Sakura Cloud Edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

14.11 Setting the Remote End ID of L2TPv3

[Format]

l2tp remote end-id *end-id*

no l2tp remote end-id [*end-id*]

[Setting value and initial value]

- *end-id*
 - [Setting value]: Arbitrary character string (up to 32 characters)
 - [Initial value]: None

[Description]

Set the Remote End ID of L2TPv3.

Set the same character string as the Remote End ID of the connection partner. It can be set only for the tunnel interface.

[Notes]

RTX5000 can be used in Rev.14.00.12 or later.

RTX3500 can be used in Rev.14.00.12 or later.

[Applicable model]

vRX VMware ESXi version, vRX Sakura Cloud Edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 15

IPIP Tunneling Configuration

IPIP Tunneling Capability

IPIP Tunneling (IP over IP) is a tunneling protocol that enables VPN (Virtual Private Network) connections between networks by encapsulating IP packets with additional IP headers. Since IPIP Tunneling does not have any authentication or encryption mechanism, it is used in environments where secure communication such as closed network services is provided.

Yamaha Routers can use proprietary IPIP Keepalives. Using IPIP Keepalives offers the following benefits:

- By confirming the response of the opposing router and establishing a tunnel, packets can be reliably sent to the opposing router.
- When a tunnel end point is specified by a host name, even if the IP address corresponding to the host name changes, it can be automatically restored by performing name resolution again after disconnection detection.

15.1 IPIP Keepalives

[Format]

ipip keepalive use switch [*interval* [*count*]]

no ipip keepalive use [*switch* ...]

[Setting value and initial value]

- *switch*
 - [Setting value]:

Setting value	Description
on	Using IPIP Keepalives
off	Do not use IPIP Keepalives

- [Initial value]: off
- *Interval*
 - Setting value: Time interval for sending keepalives packets (1.600)
 - [Initial value]: 10
- *count*
 - Setting value: Number of keepalives packets sent before it is considered to be down (1.50)
 - [Initial value]: 6

Description

Whether to use IPIP Keepalives is selected.

When keepalives are performed, proprietary IPIP Keepalives operate according to the setting values of *interval* and *count*. Can be set only for tunnel interfaces.

When keepalives are enabled, if no keepalives response can be confirmed *count* consecutively, it is considered that there is no connectivity and the tunnel is down.

Also, when a tunnel end point is specified by a name, if there is no response even if keepalives are sent *count* times, name resolution is executed again.

[Notebook]

RTX5000 / RTX3500 can be used after Rev.14.01.20.

RTX1210 can be used after Rev.14.01.20.

Applicable models

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

15.2IPIP Keepalives Log Settings

Format

```
ipip keepalive log log
no ipip keepalive log [log]
```

Setting values and initial values

- log
 - Setting values:

Setting values	Description
on	Do not output IPIP Keepalives to logs
off	Do not output IPIP Keepalives to logs

- Initial values: off

Description

Sets whether to output IPIP keepalive logs. All logs are output to a SYSLOG at the debug level. It can be set only at the tunnel interface.

[Notes]

RTX5000 / RTX3500 can be used with Rev.14.01.22 or later.
RTX1210 can be used with Rev.14.01.20 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 16

SIP configuration

16.1 Common setting

16.1.1 Setting whether or not to use SIP

[Format]

sip use *use*
no sip use

[Setting value and initial value]

- Use*
- [Setting value]:

Setting value	Description
off	Not used
on	Not used

- [Initial value]: off

[Explanation]

Whether or not to use the SIP protocol is set.

[Notes]

Changing the setting from on to off becomes effective after restart.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

16.1.2 Setting the timer value of the session-timer function of SIP

[Format]

sip session timer *time* [update=*update*] [refresher=*refresher*]
no sip session timer

[Setting value and initial value]

- time*
- [Setting value]:

Setting value	Description
Number of seconds (60..540)	
0	Do not use the session-timer function

- [Initial value]: off

- update*

- [Setting value]:

Setting value	Description
on	Using the UPDATE method
off	Do not use the UPDATE method

- [Initial value]: off

- refresher*

- [Setting value]:

Setting value	Description
None	Do not set the refresher parameter
uac	Set uac to the refresher parameter
uas	Set uas to the refresher parameter

- [Initial value]: uac

[Description]

Set the timer value of the session-timer function of SIP.

The timer automatically disconnects a call when the other party suddenly drops due to power failure or the like during a call of SIP.

If *update* is set to on, the UPDATE method can be used in the session-timer function at the time of calling.

When *refresher* is set to none, no refresher parameter is set, and when uac/uas is set, calls are made with respective parameter values.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

16.1.3 Selecting the IP protocol to use when calling by SIP

[Format]

sip ip protocol *protocol*

no sip ip protocol

[Setting value and initial value]

- *protocol*
- [Setting value]:

Setting value	Description
udp	Use UDP
tcp	Use TCP

- [Initial value]: udp

[Description]

Select the IP protocol to be used for call control at the time of calling by SIP.

[Notebook]

When an incoming call is received, transmission is performed by the received protocol regardless of this setting.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

16.1.4 Setting whether to support 100rel when calling by SIP

[Format]

sip 100rel *switch*

no sip 100rel

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Description
on	Support 100rel
off	Does not support 100rel

- [Initial value]: off

[Description]

Whether to support 100rel (RFC3262) when calling by SIP is set.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

16.1.5 Setting to add User-Agent header to outgoing SP packets

[Format]

sip user agent sw [*user-agent*]

no sip user agent

[Setting value and initial value]

- *SW*
- [Setting value]:

Setting value	Description
on	Adding
off	Do not add

- [Initial value]: off
- *user-agent*
 - Setting value: String to be written in header
 - [Initial value]: -

[Description]

User-Agent header can be added to outgoing SIP packets.

The character string to be added can be set with the *user-agent* parameter, but only ASCII characters can be set within 64 characters.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

16.1.6 Setting when INVITE at incoming call by SIP does not specify refresher

[Format]

sip arrive session timer refresher *refresher*

no sip arrive session timer refresher

[Setting value and initial value]

- *refresher*
- [Setting value]:

Setting value	Description
uac	specify refresher=uac
uas	specify refresher=uac

- [Initial value]: uac

[Explanation]

UAC/UAS can be specified when INVITE at incoming call by SIP does not specify refresher.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

16.1.7 Setting whether to support PN-UAType header at incoming call by SIP

[Format]

sip arrive ringing p-n-uatype *switch*

no sip arrive ringing p-n-uatype

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Explanation
on	Append P-N-UAType header
off	Do not add P-N-UAType header

- [Initial value]: off

[Explanation]

Whether to add P-N-UAType header to Ringing response sent at incoming call by SIP or not is set.

[Notebook]

The setting applies to all incoming calls.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

16.1.8 Set request for session timer at incoming call by SIP**[Format]**

sip arrive session timer method *method*

no sip arrive session timer method [*method*]

[Setting value and initial value]

- *method*
- [Setting value]:

Setting value	Explanation
Auto	Automatically judge
invite	Only use INVITE

- [Initial value]: auto

[Explanation]

Set request to be used in session timer function at incoming call by SIP.

When set to auto, both UPDATE and INVITE can be used, and if UPDATE is supported by the sender or server Update can be used.

When set to invite, it works without using UPDATE even if UPDATE is supported by the sender or server.

It cannot be set to use UPDATE only.

Also, since it cannot be set for each server, this setting is valid for all incoming calls.

For outgoing call, it can be set by *update* option of **sip server session timer** or **sip session timer**.

[Applicable model]

vRX VMware ESXi Edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

16.1.9 Setting whether or not to verify the username on incoming SIP calls**[Format]**

sip arrive address check *switch*

no sip arrive address check

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Description
on	Verify the username

Setting value	Description
off	Do not verify the username

- [Initial Value] : on

[Description]

When a SIP server is configured, this setting determines whether to verify that the Request-URI of an incoming call matches the contents of the Contact header sent in the REGISTER request.

In VoIP functionality using SIP, if both SIP server-based configuration and Peer-to-Peer configuration are used together, this setting should be set to off.

It should also be set to off when using RTV01 as the SIP server.

[Note]

This verification is enabled only when a sip server configuration is present.

[Supported Models]

vRX VMware ESXi edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

16.1.10 Configuring the SIP Response Code Returned When No Incoming Port Is Available**[Format]**

sip response code *busy code*

no sip response code busy

[Configuration Value and InitialValue]

- Code : Response code

Value	Description
486	Returns 486
503	Returns 503

- [Initial value]: 486
- [Description]
Configures the response code returned when an incoming SIP call cannot be accepted because all ports are busy.
- [Supported Models]
vRX VMware ESXi edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

16.1.11 Configuring the IP Address Used for SIP**[Format]**

sip outer address *ipaddress*

no sip outer address

[Parameters and Default Values]

- *ipaddress*
- Value

Value	Description
auto	Automatically set
IP address	Specifies an IP address

- [Initial value]: auto

[Description]

Configures the IP address used for SIP. This value is also used for RTP/RTCP.

[Note]

It is recommended to use the default setting.

[Supported Models]

vRX VMware ESXi edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

16.1.12 Setting whether to log SIP messages

[Format]

sip log *switch*
no sip log

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Description
on	Logging SIP messages
off	Do not log SIP messages

- [Initial value]: off

[Explanation]

Set whether to log SIP messages to DEBUG level logs.

[Applicable models]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 17

SNMP Settings

By setting SNMP (Simple Network Management Protocol), you can monitor and change network management information for SNMP management software. At this time, Yamaha Router becomes an SNMP agent.

Yamaha Router supports communication by SNMPv1, SNMPv2c, and SNMPv3. It also supports RFC1213 (MIB-II) and private MIB as MIB (Management Information Base). Private MIB can be found from the following URL.

- YAMAHA private MIB: <https://www.rtpro.yamaha.co.jp/RT/docs/mib/>

SNMPv1 and SNMPv2c notify the other party of the name of a group called a community, and only communicate between hosts belonging to the same community. In this case, you can set a separate community name for two access modes: read-only and read-write.

As you can see, community names function as a kind of password, but on the other hand, they are always plaintext and flow over the network, which makes them vulnerable in terms of security. If more secure communication is required, SNMPv3 is recommended.

SNMPv3 supports authentication and encryption of communication contents. SNMPv3 eliminates the concept of community and uses a new security model called USM (User-based Security Model) to ensure a higher level of security.

SNMP messages that notify the status of Yamaha Router are called traps. In addition to SNMP standard traps, Yamaha Router may send its own traps to notify specific events with some functions. Note that these unique traps are defined as private MIBs.

Multiple hosts can be set for each SNMP version for the destination host of the trap.

Both read-only and send trap community names used by SNMPv1 and SNMPv2c have default values of "public". Since "public" is often a community name on the SNMP management software side, please change it to an appropriate community name when security is considered in the communication of this version. However, as mentioned above, since community names flow over the network in plaintext, please be careful not to use login passwords or administrative passwords for community names.

In the factory default state, access is not possible at all in each SNMP version. Also, the destination host of the trap is not set and traps are not sent anywhere.

17.1 Setting up hosts that are allowed to access by SNMPv1

[Format]

```
snmp host host [ro_community [rw_community]]
no snmp host [host]
```

[Setting value and initial value]

- host: Hosts that are allowed to access by SNMPv1
- [Setting value]:

Setting value	Description
ip_address	One IP address or a hyphen in between IP address (range specification)
lanN	LAN interface name
bridgeN	Bridge interface name
Any	Allow access from all hosts
None	Prohibit access from all hosts

- [Initial value]: none
- ro_community
 - Setting value: Read-only community name (up to 16 characters)
- [Initial value]: -
- rw_community

- Setting value: Readable community name (up to 16 characters)
- [Initial value]: -

[Description]

Setting up hosts that are allowed to access by SNMPv1

Allow access by SNMPv1 from any host when 'any' is set.

If a host is specified by IP address, lanN, or bridgeN, the community name can be set at the same time. Access mode readable/writable is prohibited when the *rw_community* parameter is omitted. Setting values of **snmp community read-only** command and **snmp community read-write** command are used when the *ro_community parameter* is also omitted.

Notebook

Specifying the IP address range and specifying the LAN interface name in the *host* parameter is not possible with RTX5000/RTX3500 Rev.14.00.17 or earlier. Specifying bridge interface is not possible with vRX Amazon EC2 version and RTX5000/RTX3500 Rev.14.00.17 or earlier.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.2 Setting up a community name for SNMPv1 read only

[Format]

snmp community read-only *name*

no snmp community read-only

[Setting value and initial value]

- *name*
 - [Setting value]: Community name (up to 16 characters)
 - [Initial value]: Public

[Explanation]

Set the community name whose access mode by SNMPv1 is read-only.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.3 Setting the read/write community name for SNMPv1

[Format]

snmp community read-write *name*

no snmp community read-write

[Setting value and initial value]

- *Name*
 - [Setting value]: Community name (up to 16 characters)
 - [Initial value]: -

[Explanation]

Set the community name whose access mode by SNMPv1 can be read/write.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.4 Setting the destination of SNMPv1 traps

[Format]

snmp trap host *host* [*community*]

no snmp trap host *host*

[Setting value and initial value]

- *host*
 - [Setting value]: IP address of the host to which SNMPv1 traps are sent (IPv4/IPv6)

- [Initial value]: -
- *community*
 - [Setting value]: Community name (up to 16 characters)
 - [Initial value]: -

[Explanation]

Specify the host to which SNMPv1 traps are sent. Multiple hosts can be specified at the same time by setting multiple commands. The community parameter of this command is used for the *community* name when sending traps, but if it is omitted, the setting value of **snmp trap community** command is used.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.5Setting the community name for SNMPv1 traps

[Format]

snmp trap community *name*
no snmp trap community

[Setting value and initial value]

- *Name*
 - [Setting value]: Community name (up to 16 characters)
 - [Initial value]: public

[Explanation]

Setting the community name for sending SNMPv1 traps

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.6Setting the host to which SNMPv2c access is allowed

[Format]

snmpv2c *host* *host* [*ro_community* [*rw_community*]]
no snmpv2c *host* [*host*]

[Setting value and initial value]

- *host*: Host to which SNMPv2c access is allowed
 - [Setting value]:

Setting value	Description
<i>ip_address</i>	One IP address or a hyphen (-) in between IP address (range specification)
<i>lanN</i>	LAN interface name
<i>bridgeN</i>	Bridge interface name
Any	Allow access from all hosts
None	Prohibit access from all hosts

- None.
- *ro_community*
 - Setting value: Read-only community name (up to 16 characters)
 - Initial value: -
- *rw_community*
 - Setting value: Readable/writable community name (up to 16 characters)
 - Initial value: -

Description

Allow access by SNMPv2c.
Allow access by SNMPv2c from any host when 'any' is set.

If a host is specified by IP address, lanN, or bridgeN, the community name can be set at the same time. When the *rw_community* parameter is omitted, access in which the access mode is read/write is prohibited. When the *ro_community* parameter is also omitted, setting values of **snmpv2c community read-only** command and **snmpv2c community read-write** command are used.

Notes

Specifying the range of IP addresses and specifying the LAN interface name in the *host* parameter is not possible with RTX5000 / RTX3500 Rev.14.00.17 or earlier. Specifying a bridge interface is not possible with vRX Amazon EC2 version and RTX5000 / RTX3500 Rev.14.00.17 or earlier.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.7 Setting community name for SNMPv2c read only

Format

snmpv2c community read-only *name*
no snmpv2c community read-only

Setting value and initial value

- *name*
 - Setting value: community name (up to 16 characters)
 - Initial value: public

Description

Setting community name for which the access mode by SNMPv2c is read only.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.8 Setting community name for SNMPv2c read write

Format

snmpv2c community read-write *name*
no snmpv2c community read-write

Setting value and initial value

- *name*
 - Setting value: community name (up to 16 characters)
 - Initial value: -

Description

Setting community name for which the access mode by SNMPv2c is read write

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.9 Setting destination of SNMPv2c trap

Format

snmpv2c trap *host* *host* [*type* [*community*]]
no snmpv2c trap *host* *host*

Setting value and initial value

- *host*
 - Setting value: IP address of destination host of SNMPv2c trap (IPv4/IPv6)
 - Initial value: -
- *type*: Message type
 - Setting value:

Setting value	Description
trap	Send trap

Setting value	Description
inform	Send Inform request

- [Initial value]: trap
- *community*
 - [Setting value]: community name (up to 16 characters)
 - [Initial value]: -

[Explanation]

Specifies the host that sends an SNMPv2c trap. Multiple hosts can be specified at the same time by setting multiple commands. The *community parameter* of this command is used as the *community* name when sending a trap, but if it is omitted, the setting value of the **snmpv2c trap community** command is used.

If 'inform' is specified in the *type* parameter, it is retransmitted up to three times at intervals of 5 seconds until there is a response from the destination.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.10 Setting the community name of an SNMPv2c trap

[Format]

snmpv2c trap community name
no snmpv2c trap community

[Setting value and initial value]

- *name*
 - [Setting value]: community name (up to 16 characters)
 - [Initial value]: public

[Explanation]

Setting the community name when sending an SNMPv2c trap

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.11 Setting the SNMPv3 engine ID

[Format]

snmpv3 engine id engine_id
no snmpv3 engine id

[Setting value and initial value]

- *engine_id*
 - [Setting value]: SNMP engine ID (up to 27 characters)
 - [Initial value]: MAC address of LAN1

[Explanation]

Setting a unique ID to identify the SNMP engine. The other party is notified of the SNMP engine ID by SNMPv3 communication.

The format notified to the other party is as follows.

- When the *engine_id* is the initial value
 "8000049e03" + (MAC address of LAN1)
- When the *engine_id* is set to any value
 "8000049e04" + ASCII string of the setting value

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.12 Setting the SNMPv3 context name

[Format]

snmpv3 context name name

no snmpv3 context name**[Setting value and initial value]**

- *name*
 - [Setting value]: SNMP context name (up to 16 characters)
 - [Initial value]: -

[Explanation]

Setting the name to identify the SNMP context The other party is notified of the SNMP context name by SNMPv3 communication.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.13 Setting the user managed by SNMPv3 USM

[Format]

```
snmpv3 usm user user_id name [group group_id] [auth auth_pass [priv priv_pass]]
no snmpv3 usm user_id
```

[Setting value and initial value]

- *user_id*
 - [Setting value]: User number (1..65535)
 - [Initial value]: -
- *name*
 - [Setting value]: User name (up to 32 characters)
 - [Initial value]: -
- *group_id*
 - [Setting value]: User group number (1..65535)
 - [Initial value]: -
- *auth*: Authentication algorithm
 - [Setting value]:

Setting value	Description
MD5	HMAC-MD5-96
sha	HMAC-SHA1-96

- [Initial value]: -
- *auth_pass*
 - [Setting value]: Authentication password (8 characters or more, 32 characters or less)
 - [Initial value]: -
- *priv*: Cryptographic algorithm
 - [Setting value]:

Setting value	Description
des-cbc	DES-CBC
aes128-cfb	AES128-CFB

- [Initial value]: -
- *priv_pass*
 - [Setting value]: Encryption password (8 characters or more, 32 characters or less)
 - [Initial value]: -

[Explanation]

User information that can be accessed by SNMPv3 is set.

If a user group number is specified, it is subject to access control by VACM. If not specified, the user can access all MIB objects.

SNMPv3 enables authentication and encryption of communication contents, and this command sets an algorithm and a password together with the user name. Only encryption without authentication is not possible.

The presence or absence of authentication and encryption, the algorithm and the password must be matched with the user setting on the opposite SNMP manager side.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.14 Setting hosts to allow access by SNMPv3

[Format]

snmpv3 *host* *host* *user* *user_id* ...

snmpv3 *host* none

no snmpv3 host [*host*]

[Setting value and initial value]

- *host*: Hosts to allow access by SNMPv3

- [Setting value]:

Setting value	Description
<i>ip_address</i>	One IP address or a hyphen (-) in between IP address (range specification)
<i>lanN</i>	LAN interface name
<i>bridgeN</i>	Bridge interface name
any	Allow access from all hosts

- [Initial value]: -
- none : Prohibit access from all hosts
 - [Initial value]: none
- *user_id* : User number
 - [Setting value]:
 - One number or a number (range specification) with a - in between, and these arranged arbitrarily (up to 128 numbers)
 - [Initial value]: -

- Description

Set the hosts to allow SNMPv3 access.

If 'any' is set in the *host* parameter, SNMPv3 access from any host is allowed. Note that even if the host to which the access was made matches the *host* parameter, it cannot be accessed unless it matches the user specified in the *user_id* parameter.

[Notes]

Specifying the IP address range and specifying the LAN interface name in the *host* parameter is not possible with RTX5000 / RTX3500 Rev.14.00.17 or earlier. Bridge interface specification is not possible with vRX Amazon EC2 version and RTX5000 / RTX3500 Rev.14.00.17 or earlier.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.15 Configuring MB View Family Managed by SNMPv3 VACM

[Format]

snmpv3 vacm *view* *view_id* *type* *oid* [*type* *oid* ...]

no snmpv3 vacm *view* *view_id*

[Setting value and initial value]

- *view_id*
 - [Setting value]: View number (1..65535)
 - [Initial value]: -
- *type*
 - [Setting value]:

Setting value	Description
include	Make the specified object ID a managed object
exclude	Exclude the specified object ID from the managed object

- [Initial value]: -
- *oid*
 - [Setting value]: MIB object ID (the number of sub-IDs is two or more and 128 or less)
 - [Initial value]: -

[Explanation]

Set the MIB view family used for management by VACM. The MIB view family is a set of MIB variables specified when granting access rights.

A pair of *type* and *oid* parameters means that the MIB subtree after the specified object ID is managed or not. Also, when multiple pairs are specified, priority is given to the type parameter corresponding to the specified object ID up to a lower level if there is an inclusion relation among the specified object IDs. Up to 128 pairs can be specified.

[Configuration Example]

- The inetnet subtree (1.3.6.1) and later are managed. However, the enterprises subtree (1.3.6.1.4.1) and later are excluded from the managed object.

```
# snmpv3 vacm view 1 include 1.3.6.1 exclude 1.3.6.1.4.1
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.16 Setting Access Policy Managed by SNMPv3 VACM

[Format]

```
snmpv3 vacm access group_id read read_view write write_view
no snmpv3 vacm access group_id
```

[Setting value and initial value]

- *group_id*
 - [Setting value]: Group number (1..65535)
 - [Initial value]: -
- *read_view*
 - [Setting value]:

Setting value	Description
<i>view_id</i>	View number for setting readable access rights
None	Do not set a view that can be read

- [Initial value]: -
- *write_view*
 - [Setting value]:

Setting value	Description
<i>view_id</i>	View number for setting readable access rights
None	Do not set a view that can be read

- [Initial value]: -

[Description]

Set the MIB view family that can be accessed for user groups. Access to MIB variables that are not included in the MIB view family configured by this command is prohibited.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.17 Setting the destination of SNMPv3 traps

[Format]

snmpv3 trap *host* *host* [*type*] *user* *user_id*

no snmpv3 trap *host* *host*

[Setting value and initial value]

• *host*

- [Setting value]: IP address of the host to which SNMPv3 traps are sent (IPv4/IPv6)
- [Initial value]: -
- *type*: Message type
- [Setting value]:

Setting value	Description
trap	Send traps
inform	Submit an Inform request

- [Initial value]: trap

• *user_id*

- [Setting value]: User number
 - [Initial value]: -

[Description]

Specify the host to which SNMPv3 traps are sent. Multiple hosts can be specified at the same time by setting multiple commands. The user setting set by the **snmpv3 usm user** command is used for setting when sending traps.

If 'inform' is specified in the *type* parameter, the system retransmits up to three times at five second intervals until a response is received from the destination.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.18 Setting the start address of SNMP transmission packets

[Format]

snmp local address *ip_address*

no snmp local address

[Setting value and initial value]

• *ip_address*

- [Setting value]: IP address (IPv4/IPv6)
- [Initial value]: Automatic selection from the address set in the interface.

[Description]

Set the start IP address of SNMP transmission packets.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.19 Configuring sysContact

[Format]

snmp syscontact *name*

no snmp syscontact

[Setting value and initial value]

• *name*

- [Setting value]: Name to be registered as sysContact (up to 255 characters)
- [Initial value]: -

[Description]

Set the MIB variable sysContact. To include spaces, the entire parameter must be double-quoted (") or single-quoted (').

It must be surrounded by a round mark (').

The sysContact variable is generally used to fill in the administrator's name and contact information.

[Configuration Example]

```
# snmp syscontact "RT administrator"
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.20 Configuring sysLocation

[Format]

snmp syslocation *name*

no snmp syslocation

[Setting value and initial value]

- *name*
 - [Setting value]: Name to be registered as sysLocation (up to 255 characters)
 - [Initial value]: -

[Explanation]

Set MIB variable sysLocation. To include spaces, enclose the entire parameter in double quotes (") or single quotes ('). Generally, sysLocation is a variable to fill in the installation location of equipment.

[設定例]

```
# snmp syslocation "RT room"
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.21 Set sysName

[Format]

snmp sysname *name*

no snmp sysname

[Setting value and initial value]

- *name*
 - [Setting value]: Name to be registered as sysName (up to 255 characters)
 - [Initial value]: -

[Explanation]

Set MIB variable sysName. Enclose the entire parameter in double quotes (") or single quotes (') to include spaces. Generally, sysName is a variable to fill in the name of equipment.

[設定例]

```
# snmp sysname "RTX5000 with BRI module"
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.22 Setting whether to send SNMP standard traps

[Format]

snmp trap enable *snmp trap* [*trap...*]

snmp trap enable snmp all

no snmp trap enable

snmp [setting value and

initial value]

- *trap*: Type of standard trap
- [Setting value]:

Setting value	Description
coldstart	When power is on
warmstart	When restarting
linkdown	Link down
linkup	linkup
authenticationfailure	Authentication failure

- [Initial value]: -
- all: Send all standard traps
- [Initial value]: -

[Initial Value]

snmp trap enable snmp all

Description

Whether to send SNMP standard traps is set.

When all is set, all standard traps are sent. When traps are individually set, only the set traps are sent.

[Notes]

Whether to send authenticationFailure traps is controlled by this command.

ColdStart traps are sent after startup by power-on/restart and after reboot by firmware revision up.

ColdStart traps are sent.

linkDown traps can be controlled for each interface by the **snmp trap send linkdown** command. For an interface, whether or not a linkDown trap is sent is only if transmission is permitted by the **snmp trap send linkdown** command and this command is also permitted.

[Applicable model]

[Model] vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.23 Setting whether or not to send SNMP traps by CPU utilization monitoring function

[Format]

snmp trap cpu threshold *switch*

no snmp trap cpu threshold

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: off

[Explanation]

Setting whether or not to send SNMP traps when exceeding the upper limit of CPU utilization threshold that issues a warning set by system cpu threshold or falling below the lower limit of the threshold

[Notes]

RTX5000 and RTX3500 can be used with Rev. 14.00.29 or later. RTX1210 can be used with Rev. 14.01.34 or later.
 RTX830
 It can be used with Rev. 15.02.10 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.24 Setting whether or not to send SNMP traps by memory utilization monitoring function

[Format]

snmp trap memory threshold *switch*
no snmp trap memory threshold

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Description
on	Send
off	Do not send

- [Initial value]: off

[Explanation]

Setting whether or not to send SNMP traps when exceeding the upper limit of memory utilization threshold that issues a warning set by system memory threshold or falling below the lower limit of the threshold

[Notes]

RTX5000 and RTX3500 can be used with Rev. 14.00.29 or later. RTX1210 can be used with Rev. 14.01.34 or later.
 RTX830
 RTX5000 can be used with Rev. 15.02.10 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.25 Setting delay time for sending SNMP traps

[Format]

snmp trap delay-timer [*wait*]
snmp trap delay-timer off
no snmp trap delay-timer [*wait*]

[Setting value and initial value]

- *wait*
- Setting value: The number of seconds of delay time before sending SNMP traps (1 .. 21474836).
- [Initial value]: -

[Explanation]

Specifies the interval from when an event to send SNMP traps occurs until when a trap is sent. When off is set, an SNMP trap is sent immediately. The delay time to be set is a minimum guaranteed value and may be delayed by more than the setting value.

[Notes]

RTX5000 can be used with Rev. 14.00.26 or later. RTX3500 can be used with Rev. 14.00.26 or later. RTX1210 can be used with Rev. 14.01.28 or later. RTX830 can be used with Rev. 15.02.03 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.26SNMP linkDown trap transmission control settings

[Format]

```
snmp trap send linkdown interface switch
snmp trap send linkdown pp peer_num switch
snmp trap send linkdown tunnel tunnel_num
switch no snmp trap send linkdown interface
no snmp trap send linkdown pp peer_num
no snmp trap send linkdown tunnel tunnel_num
```

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Cannot be specified with vRX series, RTX5000, and RTX3500
 - BRI interface name
 - Can be specified with RTX5000, RTX3500, and RTX1210
 - [Initial value]: -
- *peer_num*
 - [Setting value]: Destination information number
 - [Initial value]: -
- *tunnel_num*
 - [Setting value]: Tunnel interface number
 - [Initial value]: -
- *switch*
 - [Setting value]:

Setting value	Explanation
on	Send
off	Do not send

- [Initial value]: on

Description

Sets whether to send linkDown traps of specified interfaces.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.27Setting whether to display PP interface information in the range of MIB2

[Format]

```
snmp yrifppdisplayatmib2 switch
no snmp yrifppdisplayatmib2
```

[Setting value and initial value]

- *switch*
 - [Setting value]:

Setting value	Explanation
on	Set MIB variable yrIfPpDisplayAtMib2 to "enabled(1)"
off	Set MIB variable yrIfPpDisplayAtMib2 to "disabled(2)"

- [Initial value]: off

Description

Set the value of MIB variable `yrIfPpDisplayAtMib2`. This MIB variable determines whether to display PP interface in the range of MIB2. To display the same as Rev.4 or earlier, set MIB variable to "enabled(1)", that is, set on with this command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.28 Setting whether to display tunnel interface information in the range of MIB2**[Format]**

`snmp yriftunneldisplayatmib2 switch`

`no snmp yriftunneldisplayatmib2`

[Setting value and initial value]

- `switch`
- [Setting value]:

Setting value	Description
on	MIB variable <code>yrIfTunnelDisplayAtMib2</code> is set to "enabled(1)"
off	MIB variable <code>yrIfTunnelDisplayAtMib2</code> is set to "disabled(2)"

- Initial value: off

Description

MIB variable `yrIfTunnelDisplayAtMib2` is set to the value. This MIB variable determines whether or not a tunnel interface is displayed in the range of MIB2. To display the same information as before Rev.4, set the MIB variable to "enabled(1)", that is, set it to on with this command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.29 Setting whether or not switch interface information is displayed in the range of MIB2**[Format]**

`snmp yrifswitchdisplayatmib2 switch`

`no snmp yrifswitchdisplayatmib2`

[Setting value and initial value]

- `switch`
- [Setting value]:

Setting value	Description
on	MIB variable <code>yrIfSwitchDisplayAtMib2</code> is set to "enabled(1)"
off	MIB variable <code>yrIfSwitchDisplayAtMib2</code> is set to "disabled(2)"

- Initial value: on

Description

MIB variable `yrIfSwitchDisplayAtMib2` is set to the value. This MIB variable determines whether or not the switch interface is displayed in the range of MIB2.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.30 Setting forced display of addresses for PP interfaces**[Format]**

`snmp display ipcp force switch`

no snmp display ipcp force**Setting value and initial value**

- *switch*
- Setting value:

Setting value	Description
on	IP addresses assigned by IPCP are always displayed as addresses for PP interfaces
off	IP addresses assigned by IPCP are not necessarily displayed as addresses for PP interfaces

- Initial value: off

Description

If NAT is not used or if a fixed IP address is specified as the outer address of NAT, the IP address obtained by IPCP is used as the address for PP interfaces. In this case, SNMP can check what kind of addresses are obtained as IPCP in the procedure for checking the IP addresses of normal interfaces.

However, if 'ipcp' is specified as the outer address of NAT, the IP address obtained by IPCP is used as the outer address of NAT and is not assigned to the interface. Therefore, even if SNMP checks the IP addresses of interfaces, it is not possible to know what kind of addresses are obtained by IPCP.

If this command is set to on, even if the IP address obtained by IPCP is used as the outer address of NAT, SNMP displays that address as the address for the interface. Since the address is not actually assigned to the interface, it is not used as a starting IP address.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.31 Setting whether to send traps when the links of each port of the LAN interface are up/down

Format

snmp trap link-updown separate-l2switch-port interface switch

no snmp trap link-updown separate-l2switch-port interface

Setting value and initial value

- *interface*
 - Setting value: Name of the LAN interface with a switching hub
 - Initial value: -
- *switch*
 - Setting value:

Setting value	Description
on	Send a trap
off	Do not send a trap

- [Initial value]: off

Description

Set whether to send a trap when the link of each port is up/down.

Applied model

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.32 Setting whether to send a radio wave strength trap

Format

snmp trap mobile signal-strength switch [level]

no snmp trap mobile signal-strength [switch [level]]

[Setting value and initial value]

- *switch*

- [Setting value]:

Setting value	Description
on	Send a trap
off	Do not send a trap

- [Initial value]: off

- *level* : Threshold of the number of antennas

- [Setting value]:

Setting value	Description
0..3	Number of antennas
Omitted	Out of range if omitted

- [Initial value]: -

Description

Whether to send a radio wave strength trap of a mobile terminal is set. Trap transmission is permitted when a router acquires radio wave strength regardless of automatic/manual operation, and a trap is transmitted when the number of antennas of the radio wave strength is equal to or less than the threshold.

Notebook

Traps are sent `yrIfMobileStatusTrap`.

Applied model

RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.33 Setting of interface number to be statically assigned to a switch**Format**

snmp ifindex switch static *index index switch*

no snmp ifindex switch static *index index [switch]*

[Setting value and initial value]

- *index*
 - Setting value: Index of object ID (10000000 .. 19999999)
 - [Initial value]: -
- *switch* : A pair of MAC addresses or port numbers
 - [Initial value]: -

Description

The beginning of the index of the object ID indicating the interface of the switch is specified statically.

Notebook

Operation is not guaranteed when object IDs are duplicated.

If the beginning of the index of object ID is specified statically, the object ID indicating the interface of the switch is not assigned dynamically.

If **snmp yrswindex switch static index** command is set, only switches specified by **snmp yrswindex switch static index** command are assigned an index.

Applied model

RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.34 Setting of switch number to be statically assigned to a switch**Format**

snmp yrswindex switch static index *index switch*

no snmp yrswindex switch static index *index [switch]*

[Setting value and initial value]

- *index*
 - [Setting value]: Index of the object ID (1 .. 2147483647)
 - [Initial value]: -
- *switch*: A combination of a MAC address or a port number
 - [Initial value]: -

[Explanation]

Statically specify the index of the object ID of the switch.

[Notes]

If the index of the object ID is specified statically, the index of the object ID of the switch is not allocated dynamically.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.35Setting conditions for SNMP traps by switch state

[Format]

snmp trap enable switch *switch trap* [*trap...*]
snmp trap enable switch *switch all*
snmp trap enable switch *switch*
none no snmp trap enable switch
switch

[Setting value and initial value]

- *switch*: A combination of default, MAC address or port number
 - [Initial value]: -
- *trap*: Types of traps
 - [Setting value]:

Setting value	Description
linkdown	linkup
linkdown	linkdown
fanlock	fan abnormality
loopdetect	loop detection
poesuppply	Power supply starts
poeterminate	power supply stop
oversupply	power supply capacity over
overtemp	temperature abnormality
powerfailure	power supply abnormality

- [Initial value]: -
- *all*: Send all traps
 - [Initial value]: -
- *none*: Do not send all traps
 - [Initial value]: -

[Initial Value]

snmp trap enable switch default all

[Explanation]

Conditions for sending traps are set according to the monitoring state of the selected switch. When setting by specifying default, the operation is determined when there is no SNMP trap condition setting for each switch.

When all is set, all traps are sent. When none is set, all traps are not sent. When traps are individually set, only the set traps are sent.

Linkup/linkdown traps are traps of the standard MIB, and to send them, **snmp trap enable snmp** command must also be allowed to send traps.

To send loop detection traps, **switch control function set loopdetect-linkdown linkdown** command or **switch control function set loopdetect-linkdown linkdown-recovery** command must be set on the switch side.

When power supply start, power supply stop, power supply capacity over, temperature abnormality, and power supply abnormality traps are set, traps are not sent by switches other than SWX2200-8PoE.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

17.36 Setting SNMP trap conditions common to switches

[Format]

snmp trap enable switch common trap [trap...]

snmp trap enable switch common

all snmp trap enable switch common

none no snmp trap enable switch

common

[Setting value and initial value]

- *trap*: Types of traps
- [Setting value]:

Setting value	Description
find-switch	When the switch goes under surveillance.
detect-down	When the switch goes out of surveillance.

- [Initial value]: -
- all: Send all traps.
- [Initial value]: -
- none: Do not send all traps.
- [Initial value]: -

[Initial Value]

snmp trap enable switch common all

Description

Setting conditions for sending traps according to the monitoring state of the switch.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 18

Setting up RADIUS

Authentication and account management for ISDN connections can be performed using a RADIUS server. Authentication and account management for PPTP connections are not supported.

18.1 Setting up whether to use authentication with RADIUS

[Format]

radius auth *auth*
no radius auth [*auth*]

[Setting value and initial value]

- auth*
 - [Setting value]:

Setting value	Description
on	Use
off	Not used

- [Initial value]: off

Description

Setting up whether to ask the RADIUS server if a user name (UserID for PAP or NAME for CHAP) received from the other party is not included in the user name you own (specified by the **pp auth username** command) when some kind of authentication is required for anonymous.

Notebook

Authentication with RADIUS and account with RADIUS can be used independently.
For supported attributes, refer to the document <<https://www.rtpo.yamaha.co.jp>> on the WWW site.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

18.2Setting up whether to use an account with RADIUS

[Format]

radius account *account*
no radius account [*account*]

[Setting value and initial value]

- account*
 - [Setting value]:

Setting value	Description
on	Use
off	Not used

- [Initial value]: off

Description

Setting up whether to use an account with RADIUS.

Notebook

Authentication with RADIUS and account with RADIUS can be used independently.

For supported attributes, refer to the document <<https://www.rtpro.yamaha.co.jp>> on the WWW site.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

18.3 Specifying a RADIUS server

[Format]

radius server *ip1* [*ip2*]

no radius server [*ip1* [*ip2*]]

[Setting value and initial value]

- *IP1*
 - [Setting value]: IP address of RADIUS server (**positive**) (IPv6 address possible)
 - [Initial value]: -
- *IP2*
 - [Setting value]: IP address of RADIUS server (**secondary**) (IPv6 address possible)
 - [Initial value]: -

[Explanation]

Setting up RADIUS server. Up to two can be specified, and if the first server does not reply, query the second server.

[Notes]

RADIUS has two functions of authentication and account, and each server can be individually set by **radius auth server/radius account server** command. The setting by **radius server** command is effective when these individual settings are not performed, and is used for both authentication and account.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

18.4 Specifying RADIUS authentication server

[Format]

radius auth server *ip1* [*ip2*]

no radius auth server [*ip1* [*ip2*]]

[Setting value and initial value]

- *IP1*
 - [Setting value]: IP address of RADIUS authentication server (**positive**) (IPv6 address possible)
 - [Initial value]: -
- *IP2*
 - [Setting value]: IP address of RADIUS authentication server (**secondary**) (IPv6 address possible)
 - [Initial value]: -

[Explanation]

Setting up RADIUS authentication server. Up to two can be specified, and if the first server does not reply, query the second server.

[Notes]

If the command does not specify the IP address of RADIUS authentication **server**, specify the IP address is used as authentication server.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

18.5 Specifying RADIUS account server

[Format]

radius account server *ip1* [*ip2*]

no radius account server [*ip1* [*ip2*]]

[Setting value and initial value]

- *IP1*
 - [Setting value]: IP address of RADIUS account server (*positive*) (IPv6 address possible)
 - [Initial value]: -
- *IP2*
 - [Setting value]: IP address of RADIUS account server (*secondary*) (IPv6 address possible)
 - [Initial value]: -

[Explanation]

Setting up RADIUS account server. Up to two can be specified, and if the first server does not reply, query the second server.

[Notes]

If the command does not specify the IP address of RADIUS account server, IP address specified by **radius server** command is used as account server.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

18.6 Setting up UDP port of RADIUS authentication server

[Format]

radius auth port *port_num*

no radius auth port [*port_num*]

[Setting value and initial value]

- *port_num*
 - [Setting value]: UDP port number
 - [Initial value]: 1645

[Explanation]

Setting up UDP port number of RADIUS authentication server

[Notes]

RFC2138 uses 1812 as the port number.

[Applicable model]

[Settings]: vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840

18.7 Setting the UDP port of a RADIUS account server

[Format]

radius account port *port_num*

no radius account port [*port_num*]

[Settings and initial values]

- [*Settings*]: *port_num*
 - [Settings]: UDP port number
 - [Settings]: 1646

[Explanation]

[Settings]: UDP port number of a RADIUS account server

[Notes]

RFC 2138 specifies that 1813 is used as the port number.

[Applicable model]

[Settings]: vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

18.8[Settings]: RADIUS secret

[Format]

radius secret *secret*

no radius secret [*secret*]

[Settings and initial values]

- *secret*
 - [Settings]: Secret string (up to 16 characters)
 - [Settings]: -

[Explanation]

[Settings]: RADIUS secret

[Applicable models]

[Settings]: vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

18.9[Settings]: RADIUS retransmission parameters

[Format]

radius retry *count time*

no radius retry [*count time*]

[Settings and initial values]

- *count*
 - [Settings]: Retransmission times (1..10)
 - [Settings]: 4
- *time*
 - [Settings]: milliseconds (20..10000)
 - [Settings]: 3000

[Explanation]

[Settings]: Retransmission times of RADIUS packets and their time intervals

[Applicable models]

[Settings]: vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 19

NAT function

[Settings]: NAT function allows routers to connect IP networks with different address systems by converting the start/end IP addresses of IP packets and TCP/UDP port numbers.

[Settings]: NAT function allows data to be transferred between a private address space and a global address space, or multiple hosts to be accommodated in one global IP address.

In Yamaha routers, only the conversion of the start/end IP address is called NAT, and the one that involves the conversion of the TCP/UDP port number is called IP masquerading.

A description representing an address translation rule is called a NAT descriptor, and each NAT descriptor defines an address space to be subjected to address translation. To describe the address space, use the **nat descriptor address inner** and **nat descriptor address outer** commands. The former is a command that defines the address space inside NAT processing (INNER), and the latter is an address space outside NAT processing (OUTER). In principle, by setting these two commands in pairs, correspondence between the address before conversion and the address after conversion is defined.

NAT descriptors are applied to interfaces. The network connected to interfaces is outside NAT processing, and the network connected from interfaces via this machine is inside NAT processing.

NAT descriptors have an action type attribute. When using features such as IP masquerading and static address assignment, the corresponding action type must be selected.

19.1 Setting the Action Type of NAT Functions

[Format]

- nat descriptor backward-compatibility type**
- no nat descriptor backward-compatibility [type]**

[Setting Value and Initial Value]

- type
- [Setting Value]:

Setting Value	Description
1	Disable port-saving IP masquerade function
2.	Enable port-saving IP masquerade function for TCP packets
3.	Enable port-saving IP masquerade function for TCP and UDP packets

- [Initial value]:
 - 1 (RTX5000, RTX3500)
 - 2 (other than the above)

[Description]

The operation type of the entire NAT function is set.

Models of RTX5000/RTX3500 Rev.14.00.32 or later and Rev.14.01 series or later are compatible with the port-saving IP masquerade function, and can establish a session with a plurality of connection destinations using the same port number in IP masquerade. Also, when the type parameter is set to 3, both TCP packets and UDP packets can be subject to the port-saving IP masquerade function.

The operation of the NAT function when the *type* parameter is set to 1 in this command is equivalent to the operation of the NAT function in models and firmware not equipped with this command before Rev.14 series. If a problem occurs when the operation is performed with the *type* parameter set to 2 or 3, it is necessary to use the NAT function with the *type* parameter set to 1.

[Notes]

Restarting the router is required in order to reflect the change of setting by this command.

The type parameter 3 cannot be specified for Rev.15.04 series or earlier, vRX Amazon EC2 version Rev.19.00.08 or earlier, vRX VMware ESXi version Rev.19.01.09 or earlier, vRX Sakura cloud version Rev.19.02.10 or earlier, RTX1300 Rev.23.00.16 or earlier, RTX3510 Rev.23.01.03 or earlier, and RTX840 Rev.23.02.02 or earlier.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.2 Setting up NAT descriptor application to interface

[Format]

```
ip interface nat descriptor nat_descriptor_list [reverse nat_descriptor_list]
ip interface nat descriptor nat_descriptor_list [reverse nat_descriptor_list]
ip interface nat descriptor nat_descriptor_list [reverse nat_descriptor_list]
no ip interface nat descriptor [nat_descriptor_list [reverse nat_descriptor_list]
no ip pp nat descriptor [nat_descriptor_list [reverse nat_descriptor_list]
no ip interface nat descriptor [nat_descriptor_list [reverse nat_descriptor_list]
```

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - LAN interface name
 - WAN interface name
 - not specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *nat_descriptor_list*
 - [Setting value]: A sequence of NAT descriptor numbers (1..2147483647) separated by spaces (up to 16)
 - [Initial value]: -

[Explanation]

For packets passing through the applied interface, NAT conversions defined by the NAT descriptor are processed in order as defined in the list.

In the NAT descriptor described after reverse, NAT conversions are performed on IP addresses and port numbers opposite to normal processing IP addresses and port numbers.

[Notes]

In the case of a LAN interface, an ARP request on the same LAN is responded to for addresses outside the NAT descriptor.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.3 Setting the NAT Descriptor Operation Type

[Format]

```
nat descriptor type nat_descriptor type [hairpin=sw]
no nat descriptor type nat_descriptor [type [hairpin=sw]]
```

[Setting value and initial value]

- *nat_descriptor*
 - [Setting value]: NAT descriptor number (1..2147483647)
 - [Initial value]: -
- *type*
 - [Setting value]:

Setting value	Description
None	Do not use NAT conversion function
nat	Utilizing dynamic NAT conversion and static NAT conversion
masquerade	Static NAT conversion and IP masquerade conversion

Setting value	Description
nat-masquerade	Dynamic NAT conversion, static NAT conversion, and IP masquerade conversion

- [Initial value]: none
- SW
- [Setting value]: none

Setting value	Description
on	Hairpin NAT function is utilized
off	Hairpin NAT function is not utilized

- [Initial value]: off

Description

Operation type of NAT conversion is specified.

Notes

nat-masquerade saves packets that cannot be dynamically NAT converted by IP masquerade conversion. For example, if the outer address is 16

If one is available, 15 are NAT converted and the rest are IP masquerade converted.

Hairpin option cannot be specified for vRX Amazon EC2 version, vRX VMware ESXi version, RTX5000, RTX3500, RTX1220 Rev.15.04.03 or earlier, RTX1210, and RTX830 Rev.15.02.23 or earlier. Also, hairpin option cannot be specified when none is specified for *type*.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.4 Setting the outer IP address for NAT processing

Format

nat descriptor address outer nat_descriptor outer_ipaddress_list

no nat descriptor address outer nat_descriptor [outer_ipaddress_list]

Setting value and initial value

- *nat_descriptor*
 - Setting value: NAT descriptor number (1..2147483647)
 - [Initial value]: -
- *outer_ipaddress_list*: List of NAT target outer IP address ranges or mnemonic
 - [Setting value]:

Setting value	Description
IP address	One IP address or an IP address (range specification) with - in between, and optionally arranged
IPCP	IP address notified from the connection destination by the IP-Address option of PPP's IPCP
primary	IP address set by the <i>ip interface address</i> command
secondary	IP address set by the <i>ip interface secondary address</i> command
map-e	An IP address automatically generated by MAP-E (Not specified for vRX Amazon EC2 version and vRX VMware ESXi version)
hb46pp	IP address acquired by the domestic standard provisioning method of IPv6 migration technology (Not specified for vRX series, RTX5000, RTX3500, RTX1210, and O and not specified in the past revisions listed in the notes section)

- [Initial value]: IPCP

Description

Specify the range of outer IP addresses to be subjected to dynamic NAT processing. In an IP masquerade, a leading outer IP address is used.

[Notes]

Mnemonics cannot be listed.

Parameters that can be used differ depending on the interface applied.

Application interface	LAN	PP	Tunnel
IPCP	X	○	x
primary	x	x	x
secondary	x	x	x
IP address	x	y	z
map-e	x	x	y
hb46pp	x	x	z

The hb46pp keyword of the *outer_ipaddress_list* parameter is used for RTX3510 Rev.23.01.01 or earlier, RTX1300 Rev.23.00.11 or earlier,

RTX1220 Rev.15.04.05 or earlier and RTX830 Rev.15.02.30 or earlier cannot be specified.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.5 Setting the inner IP address of NAT processing

[Format]

nat descriptor address inner nat_descriptor inner_ipaddress_list

no nat descriptor address inner nat_descriptor [*inner_ipaddress_list*]

[Setting value and initial value]

- *nat_descriptor*
 - [Setting value]: NAT descriptor number (1..2147483647)
 - [Initial value]: -
- *inner_ipaddress_list*: List of inner IP address ranges for NAT processing or mnemonic
 - [Setting value]:

Setting value	Explanation
IP address	One IP address or - in-between IP addresses (range specification), and optionally arranged
auto	All

- [Initial value]: auto

[Description]

Specify the range of the inner IP address to be subjected to NAT/IP masquerading processing.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.6 Setting up a static NAT entry

[Format]

nat descriptor static nat_descriptor id outer_ip=inner_ip [*count*]

nat descriptor static nat_descriptor id outer_ip=inner_ip/netmask

no nat descriptor static nat_descriptor id [*outer_ip=inner_ip* [*count*]]

[Setting value and initial value]

- *nat_descriptor*
 - [Setting value]: NAT descriptor number (1..2147483647)
 - [Initial value]: -
- *id*
 - [Setting value]: Identification of a static NAT entry (1..2147483647)
 - [Initial value]: -
- *outer_ip*
 - [Setting value]: Outer IP address (1)
 - [Initial value]: -
- *inner_ip*
 - [Setting value]: Inner IP address (1)
 - [Initial value]: -
- *count*
 - [Setting value]:
 - Number of consecutive settings
 - 1 if omitted
 - [Initial value]: -
- *netmask*
 - [Setting value]:
 - xxx.xxx.xxx.xxx (where xxx is a decimal number)
 - Hexadecimal numbers following 0x
 - Mask bits (16...32)
 - [Initial value]: -

[Explanation]

Specifies a combination of IP addresses to be fixedly allocated by NAT conversion. When the number of addresses is specified simultaneously, the range is specified starting from the specified address.

[Notes]

The outer address does not need to be an address set as a NAT processing target.
When using only static NAT, care must be taken in setting the **nat descriptor address outer** and **nat descriptor address inner** commands. Since the initial values are ipcp and auto, for example, some IP addresses are set as a dummy to prevent dynamic operation.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.7Setting whether to use rlogin, rcp and ssh when using IP masquerade

[Format]

nat descriptor masquerade rlogin *nat_descriptor use*
no nat descriptor masquerade rlogin *nat_descriptor [use]*

[Setting value and initial value]

- *nat_descriptor*
 - *nat_descriptor_number* (1..2147483647)
 - [Initial value]: -
- *Use*
 - [Setting value]:

Setting value	Explanation
on	Use
off	Do not use

- [Initial value]: off

[Explanation]

Whether to allow the use of rlogin, rcp and ssh when using IP masquerade is set.

[Notes]

When set to on, port numbers are not converted for rlogin, rcp and ssh traffic. Also, when set to on, rsh cannot be used.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.8 Setting static IP masquerade entry

[Format]

nat descriptor masquerade static nat_descriptor id inner_ip protocol [outer_port=]inner_port

no nat descriptor masquerade static nat_descriptor id [inner_ip protocol [outer_port=]inner_port]

[Setting value and initial value]

- *nat_descriptor*
 - nat_descriptor_number (1..2147483647)
 - [Initial value]: -
- *id*
 - nat_settings_identification of static IP masquerade entry (number greater than or equal to 1)
 - [Initial value]: -
- *inner_ip*
 - nat_settings_inner_ip_address
 - [Initial value]: -
- *protocol*
 - [Setting value]:

Setting value	Explanation
esp	ESP
ESP	Protocol for TCP
UDP	Protocol for UDP
icmp	Protocol for ICMP
Protocol number	Protocol numbers assigned by IANA

- [Initial value]: -
- *outer_port*
 - [Setting value]: Outer port number to be fixed (mnemonic)
 - [Initial value]: -
- *inner_port*
 - [Setting value]: Outer port number to be fixed (mnemonic)
 - [Initial value]: -

[Explanation]

Ports are fixed so that port number conversion is not performed in communication by IP masquerading.

[Notes]

When *outer_port* and *inner_port* are specified, port numbers are converted from *outer_port* to *inner_port* for packets from the outside to the inside of an interface and from *inner_port* to *outer_port* for packets from the inside to the outside when IP masquerading is applied.

If *outer_port* is not specified and only *inner_port* is specified, port numbers are not converted.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.9Setting the erasure timer for NAT's IPaddress map

[Format]

```
nat descriptor timer nat_descriptor time
nat descriptor timer nat_descriptor protocol=protocol [port=port_range] time
nat descriptor timer nat_descriptor tcpfin time2
no nat descriptor timer nat_descriptor [time]
no nat descriptor timer nat_descriptor protocol=protocol [port=port_range] [time]
no nat descriptor timer nat_descriptor tcpfin [time2]
```

[Setting value and initial value]

- nat_descriptor
 - [Setting value]: NAT descriptor number (1..2147483647)
 - [Initial value]: -
- time
 - [Setting value]: Number of seconds of erasure timer (30..21474836)
 - [Initial value]: 900
- time2
 - [Setting value]: Number of seconds of erasure timer after passing TCP/FIN (1-21474836)
 - [Initial value]: 60
- protocol
 - [Setting value]: Protocol
 - [Initial value]: -
- port_range
 - [Setting value]: Port number range, valid only when protocol is TCP or UDP
 - [Initial value]: -

[Description]

A NAT timer representing a period for holding session information of NAT or IP masquerade is set. In the case of IP masquerade, a NAT timer for each protocol and port number can be set. In the case of an unspecified protocol, the value of the NAT timer set in the first format is used.

In the case of IP masquerade, a NAT timer after passing TCP/FIN can be set. Since a session passed by TCP/FIN is a session to be terminated, it is possible to reduce the amount of NAT table used by shortening this timer. In the case of DNS, regardless of the setting value in this command, session information is deleted in about 10 seconds after the response packet passes.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.10Behavior setting when there is no conversion table corresponding to a packet received from the outside

[Format]

```
nat descriptor masquerade incoming nat_descriptor action [ip_address]
no nat descriptor masquerade incoming nat_descriptor
```

[Setting value and initial value]

- nat_descriptor
 - [Setting value]: NAT descriptor number (1..2147483647)
 - [Initial value]: -
- action
 - [Setting value]:

Set value	Description	
	Packets addressed to TCP/0-1023	Other than the above
through	Destroy and return RST	Passing without conversion
reject	Destroy and return RST	Destroy and return nothing

Set value	Description	
	Packets addressed to TCP/0-1023	Other than the above
discard	Destroy and return nothing	
forward	Transfer to the specified host	

- Initial value: reject
- *ip_address*
 - Set value: IP address of the transfer destination
 - Initial value: -

Initial value

Set an operation when there is no conversion table corresponding to a packet received from the outside by IP masquerade.

If *action* is forward, *ip_address* must be set.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.11 Setting the range of ports used by IP masquerade

Format

```
nat descriptor masquerade port range nat_descriptor port_range1 [port_range2 [port_range3 [port_range4]]]
no nat descriptor masquerade port range nat_descriptor [port_range1 [port_range2 [port_range3
[port_range4]]]]
```

Set value and initial value

- *nat_descriptor*
 - Set value: NAT descriptor number (1..2147483647)
 - Initial value: -
- *port_range1, port_range2, port_range3, port_range4*
 - Set value: Range of port numbers with - in between
 - Initial value:

In the Rev. 14.00 series, it is set as follows according to the maximum number of ports used by IP masquerade

 - 4096: port_range1=60000-64095
 - 10000: port_range1=60000-64095, port_range2=54096-59999
 - 20000: port_range1=60000-64095, port_range2=49152-59999, port_range3=44096-49151
 - 40000: port_range1=60000-64095, port_range2=49152-59999, port_range3=24096-49151
 - 65534: port_range1=49152-65534, port_range2=30000-49151, port_range3=10000-29999, port_range4=1024-9999

In the Rev. 14.01 series and later, it is set as follows regardless of the maximum number of ports used by IP masquerade

 - port_range1=60000-64095, port_range2=49152-59999, port_range3=44096-49151 (default number of ports is 20000)

[Description]

A range of port numbers to be used by IP masquerade is set.

Port numbers are first used from the range of *port_range1*. When all port numbers in *port_range1* are in use, start using port numbers in the range of *port_range2*. In this way, port numbers are used in order from small numbered port ranges from the range of *port_range1* to *port_rangeN*.

In the RTX5000/RTX3500, the maximum number of concurrent sessions of NAT is 65534, but in the initial setting, only ports of 64511 excluding well-known ports can be used, so when expanding the number of concurrent sessions to 65534, it is necessary to widen the port range so that ports of 65534 can be used with this command, or set the type parameter to 2 or 3 with the nat descriptor backward-compatibility command.

In the RTX5000/RTX3500 Rev. 14.00.32 and later and Rev. 14.01 series and later, a session with multiple connection destinations can be established using the same port number, so that a session exceeding the number of ports set by this command can be established. In the RTX5000/RTX3500 Rev. 14.00.32 and later and Rev. 14.01 series and later, the maximum number of sessions is set with the nat descriptor masquerade session limit total command. However, even in the RTX5000/RTX3500 Rev. 14.00.32 and later and Rev. 14.01 series and later, if the type parameter is changed to 1 with the nat descriptor backward-compatibility command, the maximum number of sessions is equivalent to the number of ports set by this command, so when changing the maximum number of sessions, it is necessary to change the setting of this command.

[Notes]

The following table shows the maximum number of ports used and the number of available port ranges for each model.

Model	Maximum number of ports used	Number of ports
RTX1210 Rev.14.01.34 and later, RTX830 Rev.15.02.10 and later and Rev.15.04 and later	65534	64
RTX1210 Rev.14.01.26 and later, RTX830 Rev.15.02.03 and later	65534	16
RTX1210 Rev. 14.01.20 or earlier, RTX830 Rev. 15.02.01	65534	4
RTX5000,RTX3500 Rev. 14.00.32 or later	65534	64
RTX5000,RTX3500 Rev. 14.00.29 or earlier	65534	4

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.12Setting the port number recognized as FTP

[Format]

nat descriptor ftp port nat_descriptor port [port...]
no nat descriptor ftp port nat_descriptor [port...]

[Setting value and initial value]

- *nat_descriptor*
 - [Setting value]: NAT descriptor number (1..2147483647)
 - [Initial value]: -
- *port*
 - [Setting value]: Port number (1..65535)
 - [Initial value]: 21

[Explanation]

TCP regards the port number set by this command as communication of the FTP control channel and processes it.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.13Setting the range of port numbers not to be converted by IP masquerade

[Format]

nat descriptor masquerade unconvertible port nat_descriptor if-possible
nat descriptor masquerade unconvertible port nat_descriptor protocol port
no nat descriptor masquerade unconvertible port nat_descriptor protocol [port]

[Setting value and initial value]

- *nat_descriptor*
 - [Setting value]: NAT descriptor number (1..2147483647)
 - [Initial value]: -
- *protocol*
 - [Setting value]:

Setting value	Explanation
TCP	TCP
UDP	UDP

- [Initial value]: -
- *port*
 - [Setting value]: Range of port numbers

- [Initial value]: -

[Explanation]

Setting the range of port numbers not to be converted by IP masquerade

When if-possible is specified, if the port number to be processed is not used for other communication, the value is not converted and used as it is.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.14 Setting whether to log NAT address assignment

[Format]

nat descriptor log *switch*

no nat descriptor log

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Explanation
on	To record
off	Not recorded

- [Initial value]: off

[Explanation]

Whether to log NAT address assignment is set.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.15 Setting whether to rewrite the IP address included in a SIP message

[Format]

nat descriptor sip nat_descriptor sip

no nat descriptor sip nat_descriptor

[Setting value and initial value]

- *nat_descriptor*
 - [Setting value]: NAT descriptor number (1..2147483647)
 - [Initial value]: -
- *sip*
 - [Setting value]:

Setting value	Explanation
on	Convert
off	Do not convert
auto	Follow the setting value of the sip use command

- [Initial value]:
 - auto (model and revision that can be pointed out by auto)
 - on (other than above)

[Explanation]

Whether to rewrite the IP address included in a SIP message by static NAT or static IP masquerade is set.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.16Setting whether to delete the DFbit during IP masquerade conversion

[Format]

```
nat descriptor masquerade remove df-bit remove
no nat descriptor masquerade remove df-bit [remove]
```

[Setting value and initial value]

- *Remove*
- [Setting value]:

Setting value	Explanation
on	Do not delete the DF bit during IP masquerade conversion
off	Do not delete the DF bit during IP masquerade conversion

- [Initial value]: on

[Explanation]

Whether to delete the DF bit during IP masquerade conversion is set.

The DF bit is used for route MTU search, which requires that an ICMP error for too long packets be returned correctly to the originator. However, since the IP address and the like are rewritten during IP masquerade processing, an ICMP error may not be returned correctly to the originator. If that happens, packets cannot be delivered forever. In this way, a situation in which an ICMP error for route MTU search does not reach correctly is called a route MTU black hole.

If the DF bit is deleted simultaneously during IP masquerade conversion, this route MTU black hole can be avoided. Instead, the route MTU search will not be performed, which may reduce communication efficiency.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.17Setting the number of sessions per host to be converted with IP masquerade

[Format]

```
nat descriptor masquerade session limit nat_descriptor id limit
no nat descriptor masquerade session limit nat_descriptor id
```

[Setting value and initial value]

- *nat_descriptor*
 - [Setting value]: NAT descriptor number (1..2147483647)
 - [Initial value]: -
- *Id*
 - [Setting value]: Identification number for setting the number of sessions (1)
 - [Initial value]: -
- *limit*
 - [Setting value]:
 - Limit (1..500000) (RTX3510)
 - Limit (1..250000) (RTX1300)
 - Limit (1..65534)
 - Limit (1..65534) (other than the above)
 - [Initial value]:
 - 500000 (RTX3510)
 - 250000 (RTX1300)
 - 150000 (RTX840)
 - 65534 (other than the above)

[Description]

Set the maximum number of sessions to be converted by IP masquerade for each host.

The host is identified by the IP address of the packet start point, and the number of registrations in a conversion table starting from any host is limited to *limit*.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

19.18 Set the total number of sessions to be converted by IP masquerade

[Format]

nat descriptor masquerade session limit *total nat_descriptor limit*

no nat descriptor masquerade session limit *total nat_descriptor*

[Setting value and initial value]

- *nat_descriptor*
 - nat descriptor number (1..2147483647)
 - [Initial value]: -
- *limit*
 - [Setting value]:
 - Limit (1..2147483647)
 - [Initial value]:
 - 500000 (vRX series (when operating in normal mode), RTX3510)
 - 250000 (RTX1300)
 - 150000 (RTX840)
 - 65534 (other than above)

[Description]

Set the maximum number of sessions to be converted by IP masquerade in one NAT descriptor. Unlike the **nat descriptor masquerade session limit** command, the target is the total number of sessions of all hosts.

[Notebook]

The setting of this command is valid only when the *type* parameter is set to 2 or 3 in the **nat descriptor backward-compatibility** command.

RTX5000 can be used with Rev.14.00.32 or later.

RTX3500 can be used with Rev.14.00.32 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 20

DNS configuration

This machine has the following functions as DNS (Domain Name Service) functions: name resolution, recurrent server function, upper DNS server selection function, and simple DNS server function (static DNS record registration). The name resolution function specifies a name instead of an IP address parameter such as **ping**, **tracert**, **rdate**, **ntpd**, and **telnet** commands, and resolves the IP address in display functions such as SYSLOG.

The recurrent server function enters between the DNS server and the client to relay DNS packets. The DNS query packet received from the client to this machine is relayed to the DNS **server** configured by commands such as **dns server**. The response from the DNS server arrives at this machine and forwards it to the client. It has a cache of the number of times (default value = 256) set by the **dns cache max entry** command, and returns a reply for the data in the cache without querying the DNS server, which has the effect of reducing traffic by DNS. The cache is retained for the time written in the data if it is obtained from the DNS server.

In order to use the DNS function, it is necessary to set the DNS server to be contacted with a command such as **dns server**. This setting is also used for DHCP client configuration information in the DHCP server function. There are multiple commands for setting the DNS server to be contacted, but if the DNS server is set by multiple of these commands, the setting of the highest priority command available is used. The priority of each command is as follows in descending order.

1. **dns server select** command
2. **dns server** command
3. **dns server pp** command
4. **dns server** pp

Note that even if the DNS server to be contacted is not set at all by these commands, if the DNS server obtained from the DHCP server exists, it will be used automatically.

20.1 Setting whether to use DNS

[Format]

dns service *service*
no dns service [*service*]

[Setting value and initial value]

- *service*
- [Setting value]:

Setting value	Description
recursive	Operate as a DNS recursive server
off	Stop service

- [初期値] : recursive

[Explanation]

Set whether to operate as a DNS recursive server. If set to off, no DNS-like functions will be performed. Port 53/udp will also be closed.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

20.2 Set IP address of DNS server

[Format]

dns server *ip_address* [edns=sw] [nat46=*tunnel_num*] [*ip_address* [edns=sw] [nat46=*tunnel_num*]...]
no dns server [*ip_address* [edns=sw] [nat46=*tunnel_num*]...]

[Setting value and initial value]

- *ip_address*
- Setting value: IP address of DNS server (can be set up to 4 places separated by spaces)

- [Initial value]: -
- *SW*
- [Setting value]:

Setting value	Description
on	Communicate to the target DNS server with DNS
off	Communicate to the target DNS server with DNS

- [Initial value]: off
- *tunnel_num*
- [Setting value]: Tunnel interface number
- [Initial value]: -

[Explanation]

Specify the IP address of the DNS server.

This IP address is also used to notify a DHCP client when the router acts as a DHCP server, or to notify the other party with the MS extension option of IPCP.

If the DNS server is also configured for other commands, the setting of the command with the highest priority is used. Refer to the description at the beginning of this chapter for the priority of various commands that configure a DNS server.

If *edns=on* is omitted, name resolution to the target DNS server communicates with DNS.

If *edns=on* is specified, name resolution to the target DNS server communicates with DNS. If name resolution is not possible with *edns=on*, changing to *edns=off* may resolve the name. EDNS supports version 0.

Specifying the *nat46* option enables DNS46 functionality and queries A records addressed to this DNS server. Convert to AAAA record query.

Also, AAAA records included in the response from the DNS server are converted using the setting of the **nat46 ip address pool** command.

Convert to A records. The converted A records are registered in the DNS cache.

For *tunnel_num*, specify the tunnel interface number for which the **tunnel translation nat46** command is configured.

[Notes]

The *edns* option is not available for vRX Amazon EC2, RTX5000/RTX3500 Rev. 14.00.28 or earlier, RTX1210 Rev. 14.01.34 or earlier, and RTX830 Rev. 15.02.13 or earlier.

The *nat46* option is not available for vRX series, RTX5000, RTX3500, RTX1220 Rev. 15.04.03 or earlier, RTX1210, and RTX830 Rev. 15.02.19 or earlier.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

20.3 Setting DNS Domain Names

[Format]

dns domain *domain_name*

no dns domain [*domain_name*]

[Setting values and initial values]

- *domain_name*
- [Setting value]: A string representing a DNS domain.
- [Initial value]: -

[Explanation]

Set the DNS domain to which the router belongs.

If name resolution fails when using the router's host function (ping, traceroute), complement this domain name and try to resolve it again. If the router acts as a DHCP server, the configured domain name is also used to notify a DHCP client. Notify a DHCP client of a network with the router and of sub-networks it includes.

To set an empty string, enter **dns domain**.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

20.4Set a destination number to notify a DNS server.

[Format]

dns server pp peer_num [edns=sw]
no dns server pp [peer_num [edns=sw]]

[Setting value and initial value]

- peer_num
 - Setting value: Destination number to notify a DNS server.
 - [Initial value]: -
- SW
 - [Setting value]:

Setting value	Explanation
on	Communicate with the target DNS server in DNS
off	Communicate with the target DNS server in DNS

- [Initial value]: off

[Explanation]

Set the destination number to notify the DNS server. If the destination information number is set by this command, when name resolution is performed in DNS, a call is first made to this destination and a query is made to the DNS server notified by the IPCPMS extension of PPP.

If the destination cannot be connected or if it can be connected but there is no notification from the DNS server, name resolution is not performed.

If other commands also have a DNS server configured, the setting of the command with the highest priority is used. Refer to the explanation at the beginning of this chapter for the priority of various commands for setting up a DNS server.

If the edns option is omitted or edns=off is specified, name resolution to the target DNS server is performed in DNS.

If edns=on is specified, name resolution to the target DNS server is performed in DNS. If name resolution is not possible with edns=on, changing to edns=off may allow name resolution. EDNS supports version 0.

[Notes]

When using this function, it is necessary to set **ppp ipcp msex** on in the destination information specified by the **dns server pp command**.

The edns option is not available for vRX Amazon EC2 edition, RTX5000/RTX3500 Rev.14.00.28 or earlier, RTX1210 Rev.14.01.34 or earlier, and RTX830 Rev.15.02.13 or earlier.

[設定例]

```
# pp select 2
pp2# ppp ipcp msex on
pp2# dns server pp 2
```

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

20.5Interface configuration for obtaining a DNS server address

[Format]

dns server dhcp interface [edns=sw] [nat46=tunnel_num]
no dns server dhcp

[Setting value and initial value]

- interface
 - [Setting value]:
 - WAN interface name
 - WAN interface name

- Not available for vRX series, RTX5000, and RTX3500
- Bridge interface name
- [Initial value]: -
- SW
- [Setting value]:

Setting value	Description
on	EDNS performs communication to the target DNS server
off	Communication to the target DNS server is done in DNS.

- Initial value: off
- *tunnel_num*
 - Setting value: Tunnel interface number
 - Initial value: -

Description

Set the interface to get the DNS server address. If the interface name is set by this command, when name resolution is performed in DNS, a query is made to the DNS server address obtained from the DHCP server at the specified interface. If the DNS server address cannot be obtained from the DHCP server, name resolution is not performed.

If the DNS server is also set for other commands, the setting of the command with the highest priority is used. Refer to the description at the beginning of this chapter for the priority of various commands to set the DNS server.

If the edns option is omitted or edns=off is specified, name resolution to the target DNS server is performed in DNS.

If edns=on is specified, name resolution to the target DNS server is performed in EDNS. If name resolution is not possible with edns=on, changing to edns=off may result in name resolution. EDNS supports version 0.

Specifying the nat46 option enables DNS46 functionality and allows querying of A records addressed to this DNS server. Convert to AAAA record query.

Also, AAAA records included in the response from the DNS server can be set using the setting value of the **nat46 ip address pool** command.

Convert to A records. The converted A records are registered in the DNS cache.

For *tunnel_num*, specify the tunnel interface number for which the **tunnel translation nat46 command** was set.

[Notes]

This functionality requires that the specified interface operates as a DHCP client.

Bridge interfaces cannot be specified for vRX Amazon EC2 version and RTX5000/RTX3500 Rev.14.00.11 or earlier. The edns option cannot be used for vRX Amazon EC2 version, RTX5000/RTX3500 Rev.14.00.28 or earlier, RTX1210 Rev.14.01.34 or earlier, and RTX830 Rev.15.02.19 or earlier.

The nat46 option cannot be used for vRX series, RTX5000, RTX3500, RTX1220 Rev.14.01 or earlier, RTX1210, and RTX830 Rev.15.02.19 or earlier.

Applicable Models

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

20.6 Setting the Order of Notifying DNS Servers in DHCP/DHCPv6/IPCP MS Extensions

Format

dns notice order protocol server [*server*]

no dns notice order protocol [*server* [*server*]]

Setting Value and Initial Value

- *protocol*
- Setting Value

Setting Value	Description
DHCP	Notification by DHCP
dhcpv6	Notification by DHCPv6

Setting Value	Description
MSEXT	Notification by IPCP MS Extensions

- Initial Values: dhcp, dhcpv6, and msex

server

- Setting Value

Setting Value	Description
None	None
Me	The Machine
server	Servers set in the dns server command, and servers allocated by DHCPv6 when <i>protocol</i> is specified as dhcpv6

- Initial Value
 - me server (when *protocol* is dhcp or msex)
 - Me (when *protocol* is dhcpv6)

Description

The order of notifying DNS servers, which can notify multiple DNS servers in the DHCP, DHCPv6, and IPCP MS extensions, is set.

When *server* is set to none, the DNS servers are not notified regardless of other settings.

When *server* is set to "me", the machine notifies that it will use its own DNS recursive server function.

When *server* is set to "server", when *protocol* is specified as dhcp or msex, the server set in the **dns server** command is notified, and when *protocol* is specified as dhcpv6, the DNS servers notified from the IPv6 network by DHCPv6 are notified.

When dhcpv6 is specified in the *protocol*, in an environment that cannot be linked with an IPv6 network, the router is notified regardless of the setting value of the *server*.

The IPv6 DNS server address is not notified at all.

Since the number of servers that can be notified is limited to a maximum of two in the IPCP MS extension, only the first one and the machine itself are notified when me is followed, and only the first two are notified when the *server* alone is set.

[Notes]

The dhcpv6 parameter cannot be specified for vRX Amazon EC2 version, RTX5000, RTX3510, RTX1210 Rev. 14.01.34 or earlier, and RTX830 Rev. 15.02.13 or earlier.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

20.7Setting whether to process queries for private addresses

[Format]

dns private address spoof *spoof*
no dns private address spoof [*spoof*]

[Setting value and initial value]

- spoof*
- [Setting value]:

Setting value	Description
on	Processing
off	Processing not performed

- [Initial value]: off

[Explanation]

When on, the DNS recursive server function returns an error of "NXDomain", i.e., "There is no such record", to the query itself without forwarding the query to the upper server for the query for the PTR record of a private address.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

20.8 Setting whether to restrict AAAA record queries to the DNS server**[Format]**

```
dns service aaaa filter switch
no dns service aaaa filter [switch]
```

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Description
on	Restrict AAAA record queries
off	Do not restrict AAAA record queries

- [Initial value]: off

[Explanation]

Set whether to restrict AAAA record queries to the DNS server.

If a connection fails because the AAAA record is drawn even though there is no connection environment with IPv6, this command prevents an AAAA record from being answered to the AAAA record query.

Communications in which this machine is a DNS relay server and communications originating from this machine are affected.

[Notes]

RTX830 can be used with Rev.15.02.03 or later.

RTX1210 can be used with Rev.14.01.26 or later.

RTX5000 and RTX3500 can be used with Rev.14.00.26 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

20.9 Setting whether to resolve names by DNS in SYSLOG display**[Format]**

```
dns syslog resolv resolv
no dns syslog resolv [resolv]
```

[Setting value and initial value]

- *resolv*
- [Setting value]:

Setting value	Explanation
on	Solved
off	Not resolved

- [Initial value]: off

[Explanation]

Set whether to resolve the name by DNS in the SYSLOG display.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

20.10 Selecting a DNS server according to the content of a DNS query**[Format]**

```
dns server select id server [edns=sw] [nat46=tunnel_num] [server2 [edns=sw] [nat46=tunnel_num]] [type] query
[original-sender] [restrict pp connection-pp]
```

```
dns server select id pp peer_num [edns=sw] [default-server [edns=sw]] [type] query [original-sender] [restrict pp connection-pp]
dns server select id dhcp interface [edns=sw] [nat46=tunnel_num] [default-server [edns=sw] [nat46=tunnel_num]] [type]
query [original-sender] [restrict pp connection-pp]
dns server select id reject [type] query [original-sender]
no dns server select id
```

[Setting value and initial value]

- *id*
 - [Setting value]: Number in the DNS server selection table
 - [Initial value]: -
- *server*
 - [Setting value]: IP address of the primary DNS server
 - [Initial value]: -
- *server2*
 - [Setting value]: IP address of the secondary DNS server
 - [Initial value]: -
- *type*: DNS record type
 - [Setting value]:

Setting value	Description
a	IP address of the host
aaaa	IPv6 address of the host
ptr	Pointer for reverse lookup of IP addresses
mx	Mail server
ns	Name server
cname	Other names
Any	Matches all types
Omitted	Abbreviated is a

- [Initial value]: -
- *query*: Content of a DNS query
 - [Setting value]:

Setting value	Description
If <i>type</i> is a, aaaa, mx, ns, cname	<i>query</i> is a character string representing a domain name and is backward match. For example, "yamaha.co.jp" matches rtpro.yamaha.co.jp." If specified, matches all domain names.
If <i>type</i> is ptr	<i>query</i> is an IP address (<i>ip_address[/masklen]</i>) and matches only IP addresses if <i>masklen</i> is omitted, and matches all IP addresses included in a network address if <i>masklen</i> is specified. FQDNs described in the .in-addr.arpa domain included in a DNS query are compared after being converted to an IP address. Setting to match all IP addresses is not possible.
If reject keyword is specified	If <i>query</i> is exact match, "*" is used for forward match and backward match. In other words, if it is "NetVolante.*", it matches NetVolante.jp, NetVolante.rtpro.yamaha.co.jp, etc. Also, backward match matches "*yamaha.co.jp".

- [Initial value]: -
- *original-sender*

- Setting value: Range of IP addresses from which DNS queries are sent
- [Initial value]: -
- *connection-pp*
 - [Setting value]: Connection destination information number for checking the connection status when selecting a DNS server
 - [Setting value]: -
- *peer_num*
 - [Setting value]: Connection destination information number when using a DNS server notified by IPCP from the connection destination
 - [Setting value]: -
- *interface*
 - [Setting value]: LAN interface name, WAN interface name, or bridge interface name when using a DNS server obtained from a DHCP server
 - [Setting value]: -
- [Setting value]:
default-server
- [Setting value]:
 - IP address of the DNS server used when the DNS server could not be obtained from the connection destination specified by the *peer_num* parameter
 - DNS used when the DNS server could not be obtained from the interface specified by the *interface* parameter
IP address of the server
 - [Setting value]: -
- *SW*
 - [Setting value]:

Setting value	Description
on	Communication to the target DNS server is performed by DNS
off	Communication to the target DNS server is performed by DNS

- [Setting value]: off
- *tunnel_num*
 - [Setting value]: Tunnel interface number
 - [Setting value]: -

[Explanation]

As a DNS server requesting resolution of a DNS inquiry, a plurality of combinations of the connection destination information number and the DNS server for confirming the contents of the DNS inquiry and the connection state of a transmission source and a line of the DNS inquiry are registered, and an appropriate DNS server can be selected from the combinations according to the DNS inquiry. The table is searched from a lower number, and if query matches the contents of the DNS inquiry, it tries to resolve the DNS inquiry using that DNS server. If it matches once, it does not search tables after that. If all tables are searched and there is no match, it uses the DNS server specified by another command. Refer to the description at the beginning of this chapter for the priority of various commands for setting the DNS server.

In the case of a format using the reject keyword, if *query* matches, it discards its DNS inquiry packet and does not resolve the DNS inquiry.

If restrict pp clause is specified, whether the destination specified by *connection-pp* is up is added to the selection condition of the server. The server is not selected unless the destination is up. If the destination is up and other conditions also match, the specified server is selected.

If the edns option is omitted or edns=off is specified, name resolution to the target DNS server communicates with DNS. If edns=on is specified, name resolution to the target DNS server communicates with EDNS. If name resolution is not possible with edns=on, changing to edns=off may enable name resolution. EDNS supports version 0.

If the nat46 option is specified, the DNS46 feature is enabled and an A record query to this DNS server is performed. Convert to an AAAA record query.

Also, if the AAAA record included in the response from the DNS server is set using the configuration value of the **nat46 ip address pool** command,

Convert to an A record. The converted A record is registered in the DNS cache.

For *tunnel_num*, specify the tunnel interface number for which the **tunnel translation nat46** command is set.

[Notes]

The bridge interface cannot be specified for vRX Amazon EC2 version and RTX5000/RTX3500 Rev.14.00.11 or earlier.
The WAN interface cannot be specified for vRX series, RTX5000, and RTX3500.
The nat46 option cannot be specified for vRX Amazon EC2 version, RTX5000/RTX3500 Rev.14.00.28 or earlier, RTX1210 Rev.14.01.34 or earlier, and RTX830 Rev.15.02.13 or earlier.
The nat46 option cannot be specified for vRX series, RTX5000, RTX3500, RTX1220, RTX1210, and RTX830.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

20.11Registering a static DNS record

[Format]

ip host *fqdn value* [ttl=ttl]
dns static *type name value* [ttl=ttl]
no ip host *fqdn* [*value*]
no dns static *type name* [*value*]

[Setting value and initial value]

- type* : Name type
 - [Setting value]

Setting value	Description
a	IPv6 address of the host
aaaa	IPv6 address of the host
ptr	Pointer for reverse lookup of IP address
mx	Mail server
ns	Name server
cname	Another name

- [Initial value]: -
 - name, value*

- [Setting value]:

The meaning differs depending on the *type* parameter as follows

Type parameter	name	value
a	FQDN	IPv6 address
aaaa	FQDN	IPv6 address
ptr	IPv6 address	FQDN
mx	FQDN	FQDN
ns	FQDN	FQDN
cname	FQDN	FQDN

- [Initial value]: -
 - FQDN*
 - [Setting value]: Host name including domain name
 - [Initial value]: -
- ttl*
 - [Setting value]: Number of seconds (1 to 4294967295)
 - [Initial value]: -

[Description]

Define a static DNS record.

The **ip host** command is a simplified version of setting both a **andptr** in the **dns static** command.

[Notes]

The DNS record returned for query has the following characteristics.

- The setting value of the *ttl* parameter is set in the TTL field. When the *ttl* parameter is omitted, 1 is set.
- Only one DNS record is set in the Answer section, and one in the Authority/Additional section.
DNS record is not set
- The preference field of an MX record is set to zero

[Configuration Example]

```
# ip host pc1.rtpco.yamaha.co.jp 133.176.200.1
# dns static ptr 133.176.200.2 pc2.yamaha.co.jp
# dns static cname mail.yamaha.co.jp mail2.yamaha.co.jp
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

20.12 Setting the Starting Port Number of a DNS Inquiry Packet

[Format]

dns srcport *port*[-*port*]

no dns srcport [*port*[-*port*]]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number (1..65535)
 - [Initial value]: 10000-10999

[Explanation]

Set the starting port number of a DNS inquiry packet transmitted by a router.

If only one port number is set, the specified port number is used as the starting port.

If the port number is specified within a range, the port number within the range is used randomly each time a DNS inquiry packet is transmitted.

[Notes]

When a DNS inquiry packet is handled by a filter, it must be taken into account that the starting number changes randomly.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

20.13 Setting up hosts that can access a DNS server

[Format]

dns host *ip_range* [*ip_range*...]

dns host

any **dns host**

none **dns**

host *lan* **no**

dns host

[Setting value and initial value]

- *ip_range*: IP addresses or mnemonics of hosts that allow access to a DNS server
 - [Setting value]:

Setting value	Description
IP addresses (ranged) with a hyphen (-) in between, and optionally arranged	Allow access from a specified host
lanN	Allow access from a LAN interface
wan1	Allow access from a WAN interface (Cannot be specified for vRX series, RTX5000, and RTX3500)
bridge1	Allow access from a bridge interface
vlanN	Allow access from a VLAN interface (Cannot be specified for vRX series)
lanN/M	Allow access from a tag VLAN interface (Cannot be specified for vRX series)

- [Initial value]: -
- *any*
 - Setting value: Forbid access from all hosts
 - [Initial value]: any
- *None*
 - Setting value: Forbid access from all hosts
 - [Initial value]: -
- *lan*
 - Setting value: Forbid access from all LAN side networks
 - [Initial value]: -

Description

Setting up hosts that allow access to a DNS server function

[Notes]

If a LAN interface is specified in this command, access from IP addresses other than network addresses and limited broadcast addresses is allowed. Access is not allowed unless the specified LAN interface has neither a primary address nor a secondary address.

Specifying mixed IP addresses and mnemonics and specifying multiple mnemonics is not possible for RTX5000, RTX3500, and RTX1210 prior to Rev. 14.01.10

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

20.14 Setting whether to use a DNS cache

[Format]

dns cache use *switch*

no dns cache use [*switch*]

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Description
on	Using a DNS cache
off	Do not use the DNS cache.

- [Initial value]: on

[Description]

Set whether to use the DNS cache.

When *switch* is set to on, the DNS cache is used. That is, a reply from an upper DNS server to a DNS inquiry packet transmitted by a router is retained inside the router, and even when the same inquiry occurs next time, the contents of the cache are returned without querying the server.

The reply obtained from the upper DNS server contains multiple RR records, but the retention time of the DNS cache is the shortest of TTLs of those RR records. Also, if there is no RR record at all, it is 60 seconds.

The number of DNS entries retained inside the router is set with the **dns cache max entry** command.

When *switch* is set to off, the DNS cache is not used. The reply from the upper DNS server to the DNS inquiry packet transmitted by the router is not retained inside the router, and even if there is a same inquiry, an inquiry is made to the DNS server every time.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

20.15 Setting the maximum number of entries in the DNS cache

[Format]

dns cache max entry *num*

no dns cache max entry [*num*]

[Setting value and initial value]

- *num*
 - [Setting value]: Maximum number of entries (1...1024)
 - [Initial value]: 256

[Description]

Setting the maximum number of entries in the DNS cache

A set number of replies from the upper DNS server can be retained inside the router as a DNS cache. If the set number is exceeded, the oldest entries are discarded in the order in which the replies were returned.

The reply obtained from the upper DNS server contains multiple RR records, but the retention time of the DNS cache is the shortest of TTLs of those RR records. Also, if there is no RR record at all, it is 60 seconds. Entries whose retention time has elapsed since the reply was obtained are deleted from the DNS cache.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

20.16 Setting whether to unify DNS fallback behavior across routers

[Format]

dns service fallback *switch*

no dns service fallback [*switch*]

[Setting value and initial value]

- *switch*
 - [Setting value]:

Setting value	Explanation
on	Unifying DNS fallback behavior with IPv6 priority
off	DNS fallback behavior varies from function to function

- [Initial value]: off

[Description]

Setting whether to unify DNS fallback behavior across all functions of the router

If you want to convert a host name into an IP address in DNS, first query the DNS server for IPv4/IPv6 and check if the address is

DNS fallback is an operation in which the other address is queried when it cannot be resolved. When the router itself queries, whether to give priority to IPv4 or IPv6 varies from function to function. Specifically, in the following functions, IPv6 is given priority in DNS fallback behavior, but IPv4 is given priority in other functions.

- HTTP revision upgrade function
- HTTP upload function

Setting this command to on causes IPv6 to be given priority across all functions of the router.

[Notes]

As a DNS recursive server, when an inquiry about a PC or the like in a LAN is forwarded to a higher-level DNS server, the contents of the inquiry about the PC or the like are forwarded to the higher-level server as it is, so that the implementation of the PC or the like is reflected as it is and is not affected by this command setting.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 21

NAT46/DNS46 function

NAT46/DNS46 function is a function that converts IPv4 packets into IPv6 packets and forwards them.

Originally, communication is not possible between hosts in networks with different IP versions. However, when this function is used, in a configuration where the LAN is an IPv4 network and the WAN is an IPv6 network, it is possible to access a server in the WAN from a PC in the LAN.

You can use services provided by IPv6 addresses without modifying a LAN already built with IPv4 addresses.

21.1 IPv4 address pool configuration for use with NAT46 function

[Format]

```
nat46 ip address pool ipaddress_list
no nat46 ip address pool [ipaddress_list]
```

[Setting value and initial value]

- *IPaddress_list*
 - [Setting value]: IPv4 address (range) or IPv4 network address with - in between, and optionally arranged.
 - [Initial value]: -

[Description]

Set a pool of IPv4 addresses used to convert IPv4 addresses to IPv6 addresses by NAT46 function. When the DNS46 function converts an AAAA record to an A record, the IPv6 address of the AAAA record is converted to an IPv4 address within the range set by this command.

The correspondence between an IPv4 address and an IPv6 address performed by the DNS46 function is used when the NAT46 function converts an IP header in subsequent communication.

Up to eight *ipaddress_lists* can be set. However, if the total number of IPv4 addresses included in the *ipaddress_list* exceeds 254, a command error occurs.

[Notes]

It is valid only when nat46 is selected as a conversion type by the tunnel translation command.

RTX830 can be used with Rev.15.02.20 or later.

RTX1220 Rev.15.04.04 以降で使用可能。

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX840, RTX830

21.2 Setting IPv6 Prefix Used by NAT46 Function

[Format]

```
nat46 ipv6 prefix prefix_id
no nat46 ipv6 prefix [prefix_id]
```

[Setting value and initial value]

- *prefix_id*
 - [Setting value]: Prefix number (1..4294967295)
 - [Initial value]: -

[Description]

Set the prefix used to convert a source IPv4 address to a source IPv6 address by the NAT46 function.

Specify the prefix number set by the ipv6 prefix command.

[Notes]

The prefix of the ipv6 prefix command specified by this command must satisfy the following conditions.

- The prefix length must be /96.
- XXXX:XXXX:XXXX:XXXX:YYXX:XXXX:0000:0000/96: The 64th to 71st bit (YY) must be 0.

RTX830 can be used with Rev.15.02.20 or later.

RTX1220 Rev.15.04.04 以降で使用可能。

[設定例]

Set the IPv6 prefix used by the NAT46 function from the RA prefix of /64 received by LAN2.

Prefix given by RA (/64): XXXX:XXXX:XXXX:XXXX:0000:0000:0000/64

Prefix given to IPv4 addresses: XXXX:XXXX:XXXX:XXXX:0000:0000:0000/96

IPv4 addresses converted to IPv6 addresses: XXXX:XXXX:XXXX:XXXX:0000:0000:YYY.YYY.YYY.YYY

```
# ipv6 prefix 1 ra-prefix@lan2::/96
# nat46 ipv6 prefix 1
```

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX840, RTX830

21.3 Setting to statically associate destination addresses used by the NAT46 function

[Format]

nat46 static id ipv4_address ipv6_address

no nat46 static id *[[ipv4_address] ipv6_address]*

[Setting value and initial value]

- *id*
 - Setting value: Identification information (1..2147483647)
 - Initial value: -
- *ipv4_address*
 - Setting value: IPv4 address (1)
 - Initial value: -
- *ipv6_address*
 - Setting value: IPv6 address (1)
 - Initial value: -

[Description]

Statically set the IPv4 address corresponding to the IPv6 address of the destination used by the NAT46 function.

Set when accessing by specifying an IPv4 address instead of a host name as the destination (when using the NAT46 function without resolving names with the DNS46 function).

[Notebook]

It is necessary to set an address different from the IPv4 address set by the nat46 ip address pool command.

RTX830 can be used after Rev.15.02.20.

RTX1220 Rev.15.04.04 以降で使用可能。

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX840, RTX830

21.4 Display of NAT46 entries

Format

show status nat46 table *[tunnel tunnel_num] [type]*

Setting value and initial value

- *Tunnel_num*: Tunnel interface number
 - Initial value: -
- *type*
 - Setting value:

Setting value	Description
static	Display information of static entry
dynamic	Display information of dynamic entry
all	Display information of static entry and dynamic entry

- [Initial value]: all

Explanation

Display NAT46 entries Displays static entry and dynamic entry information when TYPE is omitted.

Notes

RTX830 can be used with Rev.15.02.20 or later.

RTX1220 Rev.15.04.04 or later

Applicable model

RTX3510, RTX1300, RTX1220, RTX840, RTX830

CHAPTER 22

Priority Control/Bandwidth Control

Priority Control and Bandwidth Control functions switch the order of packets input to an interface and output them to another interface. When these functions are not used, packets are processed in the order they are input.

Priority Control prioritizes classed queues, outputs packets of a higher queue first, and when the queue is empty, outputs packets of the next-ranked queue.

Bandwidth Control monitors classed queues in a round-robin manner, but provides a difference in the bandwidth available for each queue by giving a difference in the frequency of monitoring.

Classes use the **queue class filter** command to classify packets by definition similar to packet filtering.

On the RTX3510, classes are from 1 to 250, and on the vRX series, RTX5000, and RTX3500, classes are from 1 to 100.

On other models of the vRX series, classes are identified by numbers from 1 to 16. Classes available for priority control and bandwidth control are as follows.

Models	Classes Available for Priority Control	Classes Available for Bandwidth Control
RTX3510	1 to 16	1 to 250
On the vRX series, RTX5000, and RTX3500	1 to 16	1 to 100
Models Other Than the Above	1 to 4	1 to 16

Classes have higher priority as they are numbered.

The packet processing algorithm is selected from priority control, bandwidth control, and simple FIFO by the **queue interface type** command.

This can be selected for each interface.

On the RTX5000, RTX3510, and RTX3500, class structures can be layered so that priority control classes can be added to the second layer. That is, the first layer can set bandwidth control or priority control, and the second layer can set priority control.

22.1 Interface Speed Configuration

Format

speed *interface speed*

speed pp *speed*

no speed *interface [speed]*

no speed pp *[speed]*

Setting Values and Initial Values

- *interface*
 - Setting Values
 - LAN Interface Name
 - WAN Interface Names
 - Not Specified on the vRX series, RTX5000, and RTX3500
 - Initial Values: -
- *speed*
 - Setting Values: Interface Speed (bit/s)
 - Initial Values: 0 (for PP interface)

Explanation

Interface Speed is set for the specified interface.

Priority Control and Bandwidth Control Settings are Required for the **queue interface type** command.

Since CBQ is used for parameter calculation when bandwidth control is used, it is desirable to match the physical speed. In that case, if the line speed fluctuates dynamically due to MP, it should be set to the minimum speed.

Notes

Adding 'k', 'M', or 'G' after the *speed* parameter is treated as kbit/s, Mbit/s, or Gbit/s, respectively. ('G' means Not Available on the RTX5000, RTX3500, RTX1220, RTX1210, RTX840, and RTX830)

Second and fourth formats are available on the RTX5000, RTX3500, and RTX1210.

Applicable Models

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

22.2 Filter Settings for Classification**Format**

queue class filter num class1[/class2] [cos=cos] ip src_addr [dest_addr [protocol [src_port [dest_port]]]]

queue class filter num class1[/class2] [cos=cos] ipv6 src_addr [dest_addr [protocol [src_port [dest_port]]]]

Setting Filter Parameters Parameters Parameters Parameters Parameters Parameters Parameters Parameters

Parameters Parameters Parameters Parameters Parameters Parameters Parameters Parameters Parameters Parameters Parameters

Parameters Parameters Parameters Parameters Parameters Parameters Parameters Parameters Parameters Parameters Options

Options Options

Queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ipv6 src_addr [dest_addr [protocol [src_port [dest_port]]]]

queue class filter num dscp [cos=cos] ip src_addr [dest_addr [protocol [src_port [dest_port]]]] **queue class filter num dscp** [cos=cos] ipv6 src_addr [dest_addr [protocol [src_port [dest_port]]]] **queue class filter num class1 ip dpi src_addr [dest_addr [application]]**

queue class filter num class1 ipv6 dpi src_addr [dest_addr [application]]

queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ip dpi src_addr [dest_addr [application]]

queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ipv6 dpi src_addr [dest_addr [application]]

queue class filter num class1 ip dpi src_addr [dest_addr [group_num]]

queue class filter num class1 ipv6 dpi src_addr [dest_addr [group_num]]

queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ip dpi src_addr [dest_addr [group_num]]

queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ipv6 dpi src_addr [dest_addr [group_num]]

no queue class filter num [...]

[Setting value and initial value]

- [Setting value]: -
 - [Setting value]: Class filter identification number
 - [Setting value]: -
- Class 1
 - [Setting value]:

Setting value	Description
1..250 (RTX3510)	Class
1..100 (vRX series, RTX5000, RTX3500)	
1..16 (other than above)	

- [Setting value]: -
- Class 2
 - [Setting value]: Second hierarchical class (1..4)
 - [Setting value]: -
- Prec
 - Setting value: Precedence value(0..7)
 - [Setting value]: -
- Cos
 - [Setting value]:

Setting value	Description
0-7	CoS value
Precedence	Store the TOS precedence (0-7) of a packet to be transferred as a ToS-CoS conversion in the COS value

- [Setting value]: -
- *src_addr*: IP packet start address
 - [Setting value]:
 - IP addresses
 - A.B.C.D (A to D: 0 to 255 or *)
 - In the above notation, if A to D are *, all values corresponding to the corresponding 8 bits
 - IPv6 addresses
 - Two upper items with - in between, an upper item with - in front, and an upper item with - in back specify ranges.
 - Multiple values can be set as separators.
 - FQDN
 - Arbitrary character string (within 255 single-byte characters. /: cannot be used. , cannot be used because it is used as a separator)
 - FQDNs starting with * judge strings after * as backward matching conditions. For example, *.example.co.jp matches www.example.co.jp, mail.example.co.jp, etc.
 - Multiple values can be set as separators.
 - * (for all IP addresses or IPv6 addresses)
- [Setting value]: -
- *dest_addr*: IP packet end address
 - [Setting value]:
 - Same format as *src_addr*
 - Same as one * if omitted
 - [Setting value]: -
- *protocol*: packet type to filter
 - [Setting value]:
 - Decimal number representing protocol
 - mnemonic representing protocol

icmp	1
tcp	6
udp	17

- Sequence separated by commas of the above items (up to 5)
- *(All protocols)
- established
- Same as * if omitted.
- [Settings]: -
- *src_port*: Source port number for UDP and TCP
 - [Settings]:
 - Decimal number for port number
 - Mnemonic (partial) for port number

Mnemonic	Port number
ftp	20,21
ftpdata	20
telnet	23
smtp	25

Mnemonic	Port number
domain	53
gopher	70
finger	79
www	80
pop3	110
sunrpc	111
Ident	113
NTTP	123
NTTP	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540
submission	587

- Two top items with - in between, top items with - in front, top items with - in back, these specify ranges.
- Sequence separated by commas of the top item (up to 10)
- *(All ports)
- Same as * if omitted.
- [Settings]: -
- *dest_port*: Destination port number for UDP and TCP
 - Settings: Same format as *src_port*
 - [Settings]: -
- *application* : Applications or categories to be filtered
 - Settings:
 - Mnemonic representing applications
 - Mnemonics for categories starting with "@"
 - The above strings are separated by commas (up to 10, applications and categories can be mixed).
 - If omitted, they are the same as a single *.
 - [Initial value]: -
- *group_num*: Group ID
 - [Setting value]: Group ID of applications grouped by **dpi group set command**
 - [Initial value]: -

[Explanation]

Filters for classification are set.

In the case of a precedence format, classes (1-8) are divided according to the precedence (0-7) of a TOS field of a packet to be transferred, priority control or shaping, and bandwidth control by Dynamic Traffic Control or CBQ are performed. Conversion from a precedence value to a class can be specified by the mapping option. For example, in the following example, conversion of a precedence value = 1 to class 8 and conversion of a precedence value = 4 to class 3 are performed.

queue class filter 1 precedence mapping=1:8,4:3 ip *

When the entire mapping option is omitted, or when a mapping option is specified but a precedence value is not described in it, conversion as shown in the following table is performed.

Precedence value	0	1	2	3	4	5	6	7
Classes	1	2	3	4	5	6	7	8

In the case of a dscp format, classes (1-9) are divided according to PHB defined by the DSCP value of a DS field of a packet to be transferred, and priority control or bandwidth control by shaping or Dynamic Traffic Control is performed.

When cos=cos is specified, a specified CoS value is stored in the user_priority field of an IEEE802.1Q tag added to a packet matched with the filter. When precedence is specified in cos, a value corresponding to the precedence value of the IP header of the packet is stored in the user_priority field.

Packets corresponding to the packet filter are classified into the specified class. Whether or not to use a filter set by this command or in what order it is applied is set by the **queue interface class filter list** command in each interface.

When application or group_num is specified, classification is performed using the application identification result of DPI. Packets whose application identification has been completed are immediately classified into the specified class. Packets whose identification processing is in progress or whose DPI has not been identified during activation do not match the DPI filter and are classified into the class according to normal settings.

Class1 and class2 can be specified by concatenating them with a '/' (slash). Class2 can be specified by RTX5000, RTX3510, and RTX3500.

[Notes]

The cos parameter cannot be specified in the vRX series.
Specifying the FQDN for src_addr and dest_addr parameters is not possible in RTX5000/RTX3500 Rev.14.00.25 or earlier, RTX1210 Rev.14.01.25 or earlier, and RTX830 Rev.15.02.02 or earlier.
The application parameter and the group_num parameter can be specified by RTX5000, RTX3510, RTX3500, RTX1220, RTX1210, RTX830 Rev.15.02.10 or earlier cannot be used.

The fifth and sixth formats can be specified by RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, and RTX1210.

[Configuration Example]

```
# queue class filter 1 4 ip * * udp 5004-5060 *
# queue class filter 2 10/3 ip * 172.16.1.0/24 tcp telnet *
# queue class filter 5 precedence ip 172.16.5.0/24 * tcp * *
# queue class filter 6 precedence/4 ip * 172.16.6.0/24 tcp * *
# queue class filter 10 dscp ip 172.16.10.0/24 *
# queue class filter 11 dscp/4 ip * 172.16.11.0/24
# queue class filter 12 4 ip dpi * * @audio_video
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

22.3 Choosing a queuing algorithm type

[Format]

queue interface type type [shaping-level=level]
queue pp type type
no queue interface type [type]
no queue pp type [type]

[Setting value and initial value]

- interface
 - [Setting value]
 - LAN interface name
 - WAN interface name
 - Cannot be specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- type
 - [Setting value]:

Setting value	Description
fifo	Queuing in First In, First Out format
priority	Priority control queuing
cbq	Bandwidth control queuing

Setting value	Description
wfq	Queuing in Weighted Fair Queue format
shaping	Bandwidth control

- [Initial value]: fifo
- *level*: Layer for calculating bandwidth speed
- [Setting value]:

Setting value	Description
1	Layer 1
Layer 2	Layer 2

- [Initial value]: 2

[Explanation]

For a specified interface, a queuing algorithm type is selected.

Fifo is the most basic queue. In the case of fifo, packets are always sent from those arriving at a router first. Packets are not switched in order. If the number of packets accumulated in the fifo queue exceeds the value specified by the **queue interface length** command, the last packet of the queue, i.e., the last arrival, is discarded.

Priority performs priority control. Packets are classified by a **queue class filter** command and a **queue interface class filter list** command, and packets of classes with the highest priority are transmitted from packets waiting to be transmitted.

cbq controls bandwidth for BRI and PRI interfaces. Bandwidth allocated to each class is preliminarily set by a **queue interface class property** command, and packets classified by a **queue class filter** command and a **queue interface class filter list** command are transmitted so that the bandwidth is the specified bandwidth. It can be configured only for PP interfaces.

When using wfq, it is possible to reduce the drop in response time of TELNET compared to that of fifo when using simultaneously a protocol such as TELNET, which requires less bandwidth but fast response time, and a protocol such as FTP, which requires wider bandwidth than the response time. Another feature of wfq is that it does not require configuration. Since there is no place to set it, fine adjustment is not possible compared to priority control and bandwidth control, but bandwidth can be easily balanced between flows. It can be configured only for PP interfaces.

shaping performs bandwidth control for LAN interfaces. It can be configured only for LAN interfaces.

The shaping-level option can be specified only when priority and shaping are specified in the type parameter. When shaping-level is set to 1, bandwidth speed is calculated with a frame size including preamble, SFD (Start Frame Delimiter), and IFG (Inter Frame Gap).

[Notes]

RTX5000, RTX3500, RTX1210	<i>The type parameter can be fifo, priority, cbq, wfq, or shaping.</i>
Models other than the above	<i>The type parameter can be fifo, priority, or shaping.</i>

The shaping-level option cannot be specified in RTX5000 / RTX3500 Rev.14.00.17 or earlier and RTX1210 Rev.14.01.08 or earlier.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

22.4 MP Interleave Configuration

[Format]

```
ppp mp interleave [delay] switch
no ppp mp interleave [[delay] switch]
```

[Setting value and initial value]

- *delay*
 - [Setting value]: Delay (ms)

- [Setting value]: 30
- *switch*
- [Setting value]: off

Setting value	Description
on	Using MP interleave
off	Do not use MP interleave

- [Initial value]: off

[Explanation]

Sets whether to use MP interleave. In *delay*, the maximum delay allowed by the preferred protocol is set. The size of a packet to be divided is determined by the value of *delay* and the line speed.

[Notes]

The delay set in *delay* is not guaranteed.

If the same setting is not performed on the data receiving side, the effect is not demonstrated.

At the same time, compression cannot be used. Since this function is ignored when using compression, it is necessary to disable compression with the following settings.

```
ppp ccp type none
```

[Configuration Example]

```
# queue class filter 1 4 ip VOIP-GATEWAY * * * *
# queue class filter 2 3 ip * * icmp * *
# queue class filter 3 1 ip * * * * *
# pp select 1
pp1# pp bind bri2.1
pp1# queue pp type priority
pp1# queue class filter list 1 2 3
pp1# isdn remote address call 03-123-4567
pp1# ppp mp use on
pp1# ppp mp interleave on
pp1# ppp mp maxlink 1
pp1# ppp ccp type none
pp1# pp enable 1
```

[Applicable model]

RTX5000, RTX3500, RTX1210

22.5 Application of classification filter

[Format]

queue interface class filter list

filter_list queue pp class filter list

filter_list queue tunnel class filter list

filter_list

no queue interface class filter list [filter_list]

no queue pp class filter list [filter_list]

no queue tunnel class filter list [filter_list]

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - LAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *filter_list*
 - [Setting value]: Class filter array separated by spaces
 - [Initial value]: -

[Explanation]

Set the order in which filters set by the **queue class filter** command are applied to the specified LAN interface, WAN interface, or selected PP, tunnel. Packets that do not match the filter are classified into the default class specified by the **queue interface default class** command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

22.6 Queue length setting for each class

[Format]

```
queue interface length len1 [len2...lenN] [drop-threshold=dthreshold-mid[,dthreshold-high]]
queue pp length len1
[ len2...len16] no queue interface
length [len1...] no queue pp
length [len1...]
```

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - LAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *len1..lenN*
 - [Setting value]:
 - queue length (1..10000) from class 1 to class 16
 - Class 1 to Class 100 queue length (1..10000) for vRX series, RTX5000 and RTX3500
 - Class 1 to Class 250 queue length (1..10000) for RTX3510
 - Initial value:
 - 600 (RTX5000, RTX3510, RTX3500)
 - 200 (other models)
- *len1..len16*
 - Set value: Class 1 to Class 250 queue length (1..10000)
 - Initial value: 20
- *dthreshold-mid*
 - Set value: Threshold of queue size when the discard priority of AF PHB is medium (1%..100%)
 - Initial value: 75%
- *dthreshold-high*
 - Set value: Threshold of queue size when the discard priority of AF PHB is high (1%..100%)
 - Initial value: 50%

Description

Specifies the number of packets that can be queued in a specified class for an interface. For classes that are omitted, the last specified queue length applies to the rest of the class.

In the case of DiffServ-based QoS, the values specified by *dthreshold-mid* and *dthreshold-high* parameters are thresholds that can be stacked in a queue corresponding to medium and high discard priority of AF PHB. The threshold is expressed as a percentage (%) of the queue length of the class.

If *dthreshold-high* is omitted, the value is the same as *dthreshold-mid*. The threshold corresponding to low discard priority is always 100%.

Notes

The *dthreshold-mid* and *dthreshold-high* parameters cannot be specified for RTX840 and RTX830.

When the queue length of a second hierarchical class is specified by the **queue interface length secondary** command in RTX5000, RTX3510, and RTX3500, the queue length set by the **queue interface length secondary** command takes precedence.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

22.7 Default class setting

Format

```
queue interface default class
class0 queue pp default class
class1 queue tunnel default
class class0
no queue interface default class [class0]
no queue pp default class [class1]
no queue tunnel default class [class0]
```

Set value and initial value

- *interface*
 - Set value:
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - Initial value: -
- *Class 0*
 - Set value: Class (1..16; 1..100 for vRX series, RTX5000, and RTX3500; 1..250 for RTX3510)
 - Initial value: 2
- *Class 1*
 - Set value: Class (1..16)
 - Initial value: 2

Explanation

Specifies which class packets that do not match the filter are classified for the interface.

Notes

Forms 3 and 6 are for vRX Amazon EC2 version, RTX5000/RTX3500 Rev.14.00.31 or earlier, RTX1210 Rev.14.01.39 or earlier, and

Not available for RTX830 Rev.15.02.19 or earlier

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

22.8 Class attribute setting

Format

```
queue interface class property class bandwidth=bandwidth
queue interface class property class type=type
queue pp class property class bandwidth=bandwidth [parent=parent] [borrow=borrow] [maxburst=maxburst]
[minburst=minburst] [packetize=packetize]
no queue interface class property class [...]
no queue pp class property class [bandwidth=bandwidth...]
```

Set value and initial value

- *interface*
 - Set value:
 - WAN interface name
 - WAN interface name
 - Not available for vRX series, RTX5000, and RTX3500
 - Initial value: -
- *class*
 - Set value: Class (1..16; 1..100 for vRX series, RTX5000, and RTX3500; 1..250 for RTX3510)
 - Initial value: -
- *bandwidth*
 - Set value:
 - Bandwidth allocated to class (bit/s)

- Adding 'k', 'M', or 'G' after a number is treated as kbit/s, Mbit/s, or Gbit/s, respectively. Adding '%' after a number gives a percentage of the bandwidth of the entire line.
 - G' is not available for RTX5000, RTX3500, RTX1220, RTX1210, and RTX830.
- If 'ngn' is specified, it is set to the band determined when connecting data connect locations.
 - It is not available for vRX Amazon EC2 version and vRX Sakura cloud version.
- Initial value: -
- *Parent*
 - Set value: Parent class number (0..16)
 - Initial value: 0
- *Borrow*: Set whether to borrow bandwidth from the parent class when bandwidth runs out
 - Set value:

Set value	Description
on	Borrow
off	Don't borrow

- Initial value: on
- *maxburst*
 - Set value: Maximum number of bytes that can be continuously transmitted (1..10000)
 - Initial value: 20
- *minburst*
 - Set value: Maximum number of bytes that can be continuously transmitted during stable transmission (1..10000)
 - Set value: maxburst/10
- *Packetsize*
 - Set value: Average packet length of packets flowing in a class (1..10000)
 - Initial value: 512
- *type*
 - Set value:

Set value	Description
priority	Specify that it is used as a priority control class.

- Initial value: -

Description

Set the attributes of the specified class.

Notebook

The total bandwidth allocated to each class in the *bandwidth* parameter must not exceed the bandwidth of the entire line. The bandwidth of the entire line is set by a **speed** command. When performing bandwidth control by cbq, the bandwidth allocated to each class must be a value equal to or smaller than that of the parent class. When 'ngn' is specified, it is automatically set to the bandwidth determined at the time of connection in connection between data connect bases. When using multiple data connect bases, it is necessary to divide classes for each tunnel interface. Also, it is necessary to configure the LAN interface used in the tunnel ngn interface command.

When shaping is specified in the **queue interface type** command, bandwidth control by Dynamic Traffic Control can be performed. To perform Dynamic Traffic Control, specify two speeds connected by "," (comma) in the bandwidth parameter to set guaranteed bandwidth and upper limit bandwidth. Regardless of the description order, the smaller value always becomes the guaranteed bandwidth. The total guaranteed bandwidth must not exceed the bandwidth of the entire line.

The parameter *parent/borrow/maxburst/minburst/packetsize* is valid only when cbq is specified in the **queue interface type command**.

In cbq, class number 0 represents a root class. The root class is a virtual class that always has 100% bandwidth and is the parent class of the other class by default. Packets cannot be allocated directly to the root class, and its bandwidth is allocated only to lend to other classes.

When bandwidth runs out, if it is set to borrow from the parent class (borrow=on), the maximum speed of this class can be increased to the maximum speed of the parent class. Since the root class with 100% bandwidth is usually the parent class, the bandwidth of this class can be expanded to the maximum speed of the line. In this case, the *bandwidth* setting is used as a measure of how much bandwidth is divided from other classes when the line is congested.

If it is set not to borrow bandwidth (*borrow=off*), the maximum speed of this class becomes the *bandwidth* value and no more bandwidth is used. It is effective when it is desired to limit the bandwidth of specific traffic.

The *type* parameter is valid only when shaping is specified in the **queue interface type command**. Even if speed is allocated by bandwidth control in an interface, by specifying priority in the *type* parameter, the class becomes a priority control class and packets are transferred with priority over the bandwidth control class. If there are multiple classes for which priority is specified in the *type* parameter, the higher the class number, the higher the priority. The *type* parameter can be specified by vRX series, RTX5000, RTX3510, and RTX3500.

A class for which this command is not set always has 100% bandwidth allocated. Therefore, it is necessary to set bandwidth control settings.

If you want to do this, you do not need to set this command for at least two of the target class and the default class. Don't. If you forget to set the default class, 100% bandwidth is allocated to the default class, so that the target class always has a narrower bandwidth than the default class.

The **queue pp class property** command can be specified by RTX5000, RTX3500, and RTX1210.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

22.9 Dynamic Class Control settings

[Format]

queue interface class control class [except *ip_address* ...] [option=*value* ...]

no queue interface class control class [except *ip_address*...]

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Not specified by vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *class*
 - [Setting value]: Class for enabling DCC (1..16; 1..100 for vRX series, RTX5000, and RTX3500; 1..250 for RTX3510)
 - [Initial value]: -
- *ip_address*
 - [Setting value]:

Setting value	Description
IP address	Set IP addresses of hosts to be excluded from monitoring, such as servers (multiple addresses can be specified, separated by spaces, and ranges can also be specified using a hyphen "-")

- [Initial value]: -
- *option = value column*
 - [Setting value]:

option	value	Description
forwarding	reject, 1..16	Class to which traffic considered excessive transmission is forwarded
watch	source	Bandwidth monitoring per destination IP address
	destination	Bandwidth monitoring per destination IP address
threshold	Occupancy rate, seconds	Set the threshold for over-transmission by connecting bandwidth occupancy rate and occupancy time with commas (1%..100%, seconds 10..86400)

option	value	Description
time	infinity	Time to block traffic considered excessive transmission or change the class used (in seconds)
	10..604800	
mode	forced	Change the operation mode to forced control mode
	adaptive	Change the operation mode to adaptive control mode
trigger	winny	Start control triggered by Share detection
	share	Start control triggered by Share detection
	masquerade-session	Control is started using the limit on the number of IP masquerade conversion sessions as a trigger.
Notice	on	Notify that control is being performed.
	off	Not notify that control is being performed.

- [Initial value]:
 - watch=source
 - threshold=70%,30
 - time=600
 - mode=forced
 - notice=on

[Explanation].

For a specified interface, the same host monitors whether excessive transmission/reception is performed and bandwidth is not tightened. When the QoS type applied to the interface to be monitored is shaping, the occupancy rate for the class band set by the **queue interface class property** command (when a guaranteed value and an upper limit value are specified for the class band, the occupancy rate for the guaranteed value).

Rate) is monitored. When the QoS type is priority, the occupancy rate for the interface band is monitored. In monitoring, the occupancy rate is obtained every 10 seconds, and when the occupancy rate exceeds a specified number of seconds, it is determined that the threshold value is exceeded.

For example, when threshold=70% and 30 are set, it is determined that the threshold value is exceeded when 10 seconds consecutively for which the bandwidth utilization rate is 70% or more continues three times.

When excessive transmission from the same host (watch=source) or to the same host (watch=destination) is detected, the traffic is transferred to the class specified in the *forwarding* parameter, and packets are sent out according to the class setting of the forwarding destination. When reject is specified in the forwarding parameter, the traffic is blocked. Further, when *forwarding* parameter is omitted, no forwarding control is performed, but hosts exceeding threshold can be confirmed from the **show status qos** command.

The *time* parameter indicates the time when forwarding control is performed, and when infinity is specified, the target traffic is blocked or the usage class is changed indefinitely.

The mode parameter specifies the operation mode. When forced is specified, control of the flow is executed immediately after the occupancy time specified by the threshold parameter elapses. Also, control of the flow is canceled immediately after the control time specified by the time parameter elapses. When adaptive is specified, control is suspended while the usage band of the class is less than 90% of a guaranteed band even after the occupancy time specified by the threshold parameter elapses. Control cancellation is suspended while the usage band of the class is 90% or more of a guaranteed band even after the control time specified by the time parameter elapses.

Hosts pending control are not displayed by the **show status qos command**, and control is canceled at that point if the occupancy rate of threshold is divided while control is pending.

The trigger parameter specifies an event in the router that triggers the start of control. It can be written together by separating with commas ",".

The notice parameter specifies whether to notify the host that it is controlled by Dynamic Class Control. If on is specified, Web access to any http server (port number: 80) is performed for the first time after the host is controlled.

When this is done, a notification is displayed on the Web screen. The notice parameter can be used with models equipped with Web GUI functions.

[Notes]

Traffic can be forwarded in only one stage. If this command is also set for a transfer destination class, the setting of the second stage is invalid and double transfer of traffic is not performed.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 23

OSPF

OSPF is a type of interior gateway protocol and a link state type dynamic routing protocol based on graph theory.

23.1 Enable OSPF

Format

ospf configure

refresh [説明]

Enable OSPF-related settings. After changing OSPF-related settings, restart the router or use this command to be implemented.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.2 OSPF usage settings

Format

ospf use *use*

no ospf use [*use*]

Set value and initial value

- *Use*
 - Set value:

Set value	Explanation
on	Use OSPF
off	OSPF not used

- Initial value: off

Explanation

Set whether to use OSPF.

[Notes]

The following functions are not yet supported.

- NSSA (RFC1587)
- OSPF over demand circuit (RFC1793)
- OSPF MIB

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.3 Route priority setting by OSPF

[Format]

ospf preference *preference*

no ospf preference [*preference*]

[Setting value and initial value]

- *preference*
 - [Setting value]: Route priority by OSPF (a number greater than or equal to 1)
 - [Initial value]: 2000

[Explanation]

Route priority by OSPF is set. The priority is expressed by a number greater than or equal to 1, and the higher the number, the higher the priority. When routes obtained by multiple protocols such as OSPF and RIP are different, the route with the higher priority is adopted. When the priority is the same, a route adopted earlier in time becomes effective.

[Notes]

The priority of a static route is fixed at 10000.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.4 Router ID setting by OSPF

[Format]

ospf router id *router-id*

no ospf router id [*router-id*]

[Setting value and initial value]

- *router_id*
 - [Setting value]: IP address
 - [Initial value]: -

[Explanation]

Router ID of OSPF is specified.

[Notes]

When the router ID is not set by this command, one of the primary IPv4 addresses given to the following interfaces is automatically selected and used as the router ID.

- LAN interface
- LOOPBACK interface
- PP interface

If there is no interface to which a primary IPv4 address is given, the initial value is not set.

To prevent unintended IP addresses from being used as router IDs, it is desirable to specify the router ID explicitly by this command.

When OSPF and BGP-4 are used together, either this command or the `bgp router id` command are set.

In the following revisions, both this command and the `bgp router id` command can be set, but always the same router ID must be specified.

Model	Revisions
vRX series	All revisions
RTX1300	All revisions
RTX1220	All revisions
RTX1210	Rev.14.01.16
RTX5000	Rev.14.00.21
RTX3510	All revisions
RTX3500	Rev.14.00.21

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.5 Setting whether to reflect the route received by OSPF in the routing table

[Format]

ospf export from ospf [*filter filter_num...*]

no ospf export from ospf [*filter filter_num...*]

[Setting value and initial value]

- *filter_num*
 - [Setting value]: Filter number of **ospf export filter** command
 - [Initial value]: All routes are reflected in the routing table.

[Explanation]

Set whether to reflect the route received by OSPF in the routing table. Only the route that matches the specified filter is reflected in the routing table. When no command is set or when filter keywords and after are omitted, all routes are reflected in the routing table.

[Notes]

Filter numbers can be set up to 101.

This command does not affect the OSPF link state database. That is, the behavior of exchanging information with other routers in OSPF does not change regardless of how this command is set. The only change is whether the route calculated by OSPF is actually used to route packets.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.6 Route introduction by external protocol

[Format]

ospf import from protocol [filter *filter_num*...]

no ospf import from protocol [filter *filter_num*...]

[Setting value and initial value]

- *protocol*: External protocol to introduce into the OSPF routing table.
 - [Setting value]:

Setting value	Explanation
static	Static routes (not including implicit routes)
Rip	Rip
BGP	BGP

- [Initial value]: -
- *filter_num*
 - [Setting value]: Filter number
 - [Initial value]: -

[Explanation]

Set whether to introduce a route by an external protocol into the OSPF route table. The introduced route is advertised to other OSPF routers as an external route.

filter_num specifies the filter number defined by the **ospf import filter** command. The route that is to be introduced from the external protocol is inspected by the specified filter, and if it corresponds to the filter, the route is introduced into OSPF. The route that does not have the corresponding filter is not introduced. Also, if the filter keyword and after are omitted, all routes are introduced into OSPF.

The metric value, metric type, and tag that are parameters for advertising routes are those specified by the corresponding **ospf import filter** command in the filter inspection. If the filter keyword and after are omitted, the following parameters are used.

- metric=1
- type=2
- tag=1

[Notebook]

Filter numbers can be set up to 300 for vRX series, RTX5000, RTX3510, and RTX3500, and up to 101 for other models.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.7 Setting filters for handling routes received by OSPF

[Format]

ospf export filter *filter_num* [*nr*] *kind* *ip_address/mask*...

no ospf export filter *filter_num* [...]

[Setting value and initial value]

- *filter_num*
- [Setting value]: Filter number
 - [Initial value]: -
- *nr*: How to interpret the filter
 - [Setting value]:

Setting value	Description
not	Introduce a route that does not correspond to the filter
reject	Do not introduce a route that corresponds to the filter
When omitted	A route that corresponds to the filter is introduced.

- [Initial value]: -
- *kind*: Filter type
 - [Setting value]:

Setting value	Description
include	A route included in the specified network address (not including the network address itself)
Refines	A route included in the specified network address (not including the network address itself)
equal	A route that matches the specified network address

- [Initial value]: -
- *ip_address/mask*
 - [Setting value]: IP address and mask length representing the network address
- [Initial value]: -

Explanation

A filter to be applied when introducing a route received from another OSPF router by OSPF into a route table is defined. The filter defined in this command has an effect only when specified in the filter term of the **ospf export from ospf** command. In *ip_address/mask*, a network address is set. Multiple of these can be set, and inspection is performed for each network address at the time of inspection of the route.

When *nr* is omitted, a route is introduced if there is at least one filter corresponding to it.

When reject is specified, a route is introduced if it does not correspond to the filter in all inspections. When reject is specified, a route is not introduced if there is at least one filter corresponding to it.

In *kind*, an inspection method of the route is set.

include	A route that matches the network address and a route included in the network address are applicable.
Refines	A route included in the network address is applicable, but a route that matches the network address is not included.
equal	A route that matches the network address is applicable only.

[Notes]

Care must be taken when setting up more than one filter specified by the **ospf export from ospf** command. Not A network address that matches the specified filter is not determined whether or not to be introduced by that filter, so it is checked by the next filter.

It will be inspected. Therefore, for example, in the following setting, all routes are introduced, and there is no meaning of the filter.

```
ospf export from ospf filter 1 2
ospf export filter 1 not equal 192.168.1.0/24
ospf export filter 2 not equal 192.168.2.0/24
```

In filter No.1, a route other than 192.168.1.0/24 is introduced, and a route other than 192.168.2.0/24 is introduced in filter No.2. In other words, since the route 192.168.1.0/24 is introduced by filter No.2 and the route 192.168.2.0/24 is introduced by filter No.1, there is no route that is not introduced.

If you do not want to introduce the route 192.168.1.0/24 and the route 192.168.2.0/24, you need to make the following settings.

```
ospf export from ospf filter 1
ospf export filter 1 not equal 192.168.1.0/24 192.168.2.0/24
```

Or

```
ospf export from ospf filter 1 2 3
ospf export filter 1 reject equal 192.168.1.0/24
ospf export filter 2 reject equal 192.168.2.0/24
ospf export filter 3 include 0.0.0.0/0
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.8 Filter definition applied to introduction of external routes

Format

ospf import filter *filter_num* [*nr*] *kind* *ip_address/mask...* [*parameter...*].

no ospf import filter *filter_num* [[*not*] *kind* *ip_address/mask...* [*parameter...*]]

[Setting value and initial value]

- *filter_num*
 - *filter_num*
 - [Initial value]: -
- *nr* : How to interpret the filter
 - [Setting value]:

Setting value	Description
not	Advertise routes that do not fall under the filter
reject	Advertise routes that do not fall under the filter
When omitted	Advertise routes that do not fall under the filter

- [Default]: -

- *kind*
 - [Setting value]:

Setting value	Description
include	Routes included in the specified network address (including the network address itself)
Advertisement: Advertisement	Routes included in the specified network address (not including the network address itself)
equal	Routes that match the specified network address

- [Default]: -
- *IP_address/mask*
 - Setting value: IP address and mask length representing the network address
 - [Default]: -
- *parameter*: Parameters for advertising external routes
 - [Setting value]:

Setting value	Description
metric	Metric value (0..16777215)
type	Metric type (1..2)
tag	Tag value (0..4294967295)

- [Default]: -

[Explanation]

Filters to be applied when introducing external routes into the route table of OSPF are defined. Filters defined in this command have an effect only when specified in the filter term of the **ospf import from** command.

In *ip_address/mask*, a network address is set. Multiple filters can be set, and each network address is inspected at the time of inspection of the route, and if there is at least one filter corresponding to it, it is applied.

When *nr* is omitted, the route is advertised if there is at least one filter corresponding to it. When not specified, the route is advertised if there is no filter corresponding to it in all inspections. When reject is specified, the route is not advertised if there is at least one filter corresponding to it.

In *kind*, an inspection method of the route is set.

include	Routes that match the network address and routes included in the network address are applicable.
Refuges	Routes included in the network address are applicable, but routes that match the network address are not included.
equal	Only routes that match the network address are applicable.

When the keyword *not* is placed before *kind*, the judgment of whether it is applicable or not applicable is reversed. For example, in *not equal*, routes that do not match the network address are applicable.

In *parameter*, a metric value, a metric type, and a tag can be respectively specified by *metric*, *type*, and *tag* as parameters when advertising the corresponding route as an external route of OSPF. When these are omitted, the following values are adopted.

- metric=1
- type=2
- tag=1

[Notes]

Care must be taken when setting multiple filters specified by the **ospf import from** command. Since the filter does not decide whether to introduce a network address that matches the specified filter, it is inspected by the next filter. Therefore, for example, all routes will be advertised in the following settings, and there is no meaning of filters.

```
ospf import from static filter 1 2
ospf import filter 1 not equal 192.168.1.0/24
ospf import filter 2 not equal 192.168.2.0/24
```

The first filter advertises routes other than 192.168.1.0/24, and the second filter advertises routes other than 192.168.2.0/24. In other words, since the route 192.168.1.0/24 is advertised by the second filter and the route 192.168.2.0/24 is advertised by the first filter, there is no route that is not advertised.

If you do not want to advertise the route 192.168.1.0/24 and the route 192.168.2.0/24, you need to make the following settings:

```
ospf import from static filter 1
ospf import filter 1 not equal 192.168.1.0/24 192.168.2.0/24
```

Or

```
ospf import from static filter 1 2 3
ospf import filter 1 reject equal 192.168.1.0/24
ospf import filter 2 reject equal 192.168.2.0/24
ospf import filter 3 include 0.0.0.0/0
```

[Applicable model]

[Settings] vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.9 OSPF area setting**[Settings]****ospf area** *area* [auth=*auth*] [stub [cost=*cost*]]**no ospf area** *area* [auth=*auth*] [stub [cost=*cost*]]**[Settings and initial values]**• *Area*

• [Settings]:

Settings	Description
backbone	Backbone areas
Numbers equal to or greater than 1	Non-backbone areas
IP address notation (0.0.0.0 is not allowed)	Non-backbone areas

• [Settings]: -

• *auth*

• [Settings]:

Settings	Description
text	Plaintext authentication
MD5	MD5 certification

• [Settings]: No authentication

• *stub*: Specifies that it is a stub area.

• [Settings]: Not a stub area

• *cost*

• Numbers equal to or greater than 1

• [Settings]: -

[Settings]

OSPF areas are set.

Cost is a number equal to or greater than 1 and is used as the cost of a default route advertised by an area boundary router in an area. If *cost* is not specified, the advertisement of the default route is not performed.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.10 Advertising routes to areas**[Settings]****ospf area network** *area network/mask* [restrict]**no ospf area network** *area network/mask* [restrict]**[Settings and initial values]**• *Area*

• [Settings]:

Settings	Description
backbone	Backbone areas
Numbers equal to or greater than 1	Non-backbone areas
IP address notation (0.0.0.0 is not allowed)	Non-backbone areas

• [Settings]: -

• *network*

- Settings: IP addresses
- [Settings]: -
- *mask*
- Settings: Netmask length
- [Settings]: -

[Settings]

When an area boundary router advertises routes to other areas, individual routes within the network range specified by *network/mask* are summarized and advertised in *network/mask*. When restrict keywords are specified, routes within the *network/mask* range are not advertised to other areas at all, including summarized routes.

[Applicable model]

[Settings] vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.11Advertisement of stubbed connection

[Settings]

ospf area stubhost area host [cost cost]

no ospf area stubhost area host

[Settings and initial values]

- [Settings]
- [Settings]:

Settings	Description
backbone	Backing Area
Numbers equal to or greater than 1	Non-backing Area
IP address notation (0.0.0.0 is not allowed)	Non-backing Area

- [Settings]: -
- *host*
- Settings: IP address
- [Settings]: -
- *cost*
- Settings: Numbers equal to or greater than 1
- [Settings]: -

[Explanation]

Adverting that a specified host is connected stubbed at a specified cost is performed in the area.

[Applicable model]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.12Setting Virtual Link

[Settings]

ospf virtual-link router_id area [parameters...]

no ospf virtual-link router_id [area [parameters...]]

[Settings and initial values]

- *router_id*
- Settings: Router ID of the other party of the virtual link
- [Settings]: -
- *Area*
- Settings

Settings	Description
Numbers equal to or greater than 1	Non-backing Area
IP address notation (0.0.0.0 is not allowed)	Non-backing Area

- [Settings]: -
- *Parameters*
 - Settings: Column with NAME=VALUE
 - [Settings]:
 - retransmit-interval = 5 seconds
 - transmit-delay = 1 second
 - hello-interval = 10 seconds
 - dead-interval = 40 seconds
 - authkey=None
 - md5key=None
 - md5-sequence-mode=second

[Explanation]

Setting Virtual Link A virtual link is set to a router specified by *router_id* via the area specified by *area*. *Parameters* can set parameters of the virtual link. Parameters are specified in the form of NAME=VALUE and are of the following types:

NAME	VALUE	Description
retransmit-interval	Number of seconds	Sets the retransmission interval in seconds when sending LSA continuously. (1..)
transmit-delay	Number of seconds	Sets the time in seconds from when the link state changes until the LSA is sent. (1..)
hello-interval	Number of seconds	Sets the transmission interval of HELLO packets in seconds. (1..)
dead-interval	Number of seconds	Sets the time in seconds until it is determined that the other party is down when the other party cannot receive HELLO from the other party. (1..)
authkey	String	Sets a string representing an authentication key for plain text authentication. (Maximum of 8 characters)
md5key	"(ID),(KEY)"	Sets an ID representing an authentication key for MD5 authentication and a key string KEY. The ID is a decimal number from 0 to 255, and the KEY is a string of up to 16 characters. Up to two MD5 authentication keys can be set. When multiple MD5 authentication keys are set, multiple packets with the same contents are sent with authentication data based on each key added. A key whose key ID matches is a target for comparison at reception.
md5-sequence-mode	"second"	Number of seconds of transmission time
	"increment"	Monotonous increase

[Notes]

- About hello-interval/dead-interval
The values of hello-interval and dead-interval must be the same value between all neighboring routers that can communicate directly from that interface. If an OSPFHELLO packet whose values of these parameters are different from the set value is received, it is ignored.
- About MD5 authentication keys
A function allowing multiple MD5 authentication keys to be set is for smoothly changing the MD5 authentication keys. In normal operation, only one MD5 authentication key should be set. When changing the MD5 authentication key, first set two new and old MD5 authentication keys on one router, and then change the new MD5 authentication key on a neighboring router. Finally, delete the old key on a router with the two keys set.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.13 OSPF area setting for the specified interface

[Format]**ip interface ospf area** *area* [*parameters...*]**IP PP OSPF area** *area* [*parameters...*]**ip tunnel ospf area** *area* [*parameters...*]**no ip interface ospf area** [*area* [*parameters...*]]**no ip pp ospf area** [*area* [*parameters...*]]**no ip tunnel ospf area** [*area* [*parameters...*]]**[Set value and initial value]**

- *interface*
 - Set value: LAN interface name, LOOPBACK interface name
 - [Initial value]: -

- *area*

- [Set value]:

Set value	Explanation
backbone	Backbone area
Number equal to or greater than 1	Non-backbone area
IP address notation (0.0.0.0 is not acceptable)	Non-backbone area

- [Initial value]: Interface does not belong to an OSPF area
- [*Settings*]: *NAME=VALUE*
 - [Setting value]: Column of *NAME=VALUE*
 - [Initial value]:
 - type=broadcast (when setting up a LAN interface)
 - type=point-to-point (when setting up a PP, TUNNEL or LOOPBACK interface)
 - passive=An interface is not passive
 - cost=1 (when setting up a LAN interface and a LOOPBACK interface), pp depends on the line speed
 - priority=1
 - transmit-interval=5 seconds
 - transmit-delay=1 second
 - hello-interval=10 seconds (when setting up a point-to-point)
 - hello-interval=10 seconds (when setting up a point-to-point)
 - hello-interval=30 seconds (when setting up a non-broadcast)
 - hello-interval=30 seconds (when setting up a point-to-multipoint)
 - dead-interval=hello-interval times four
 - poll-interval=120 seconds
 - authkey=none
 - md5key=none
 - md5-sequence-mode=second

[Explanation]

Sets an OSPF area to which the specified interface belongs.

The type of the NAME parameter sets what type of network the interface is. In *parameters*, link parameters are set. Parameters are specified in the form of NAME=VALUE and include the following types:

NAME	VALUE	Explanation
type	broadcast	Broadcast
	point-to-point	Point Point
	point-to-multipoint	Point Multipoint
	non-broadcast	NBMA
passive		OSPF packets are not sent to the interface. Set when there is no other OSPF router on the interface.
cost	Cost	Sets the cost of the interface. The initial value is determined by the type of the interface and the line speed. For a LAN interface, it is set to 1, and for a PP interface, it is set to $S[\text{kbit/s}]$ when the line speed of the bound line is $S[\text{kbit/s}]$. For example, if it is 64 kbit/s, it is 1562, and if it is 1.536 Mbit/s, it is 65. (0..65535) COST=100000/S For a TUNNEL interface, 1562 is the default value.
priority	Priority	Sets the priority when selecting the specified router. A router with a large PRIORITY value is selected as the specified router. If it is set to 0, it will not be selected as the specified router. (0..255)
retransmit-interval	Number of seconds	Sets the retransmission interval in seconds when sending LSA continuously. (1..)
transmit-delay	Number of seconds	Sets the time, in seconds, after the link state changes before sending LSA. (1..)
hello-interval	Number of seconds	Sets the transmission interval of HELLO packets in seconds. (1..)
dead-interval	Number of seconds	Sets the time in seconds until it is determined that a neighboring router is down when it cannot receive HELLO from the neighboring router. (1..)
poll-interval	Number of seconds	This parameter is valid only for non-broadcast links, and sets the transmission interval of HELLO packets in seconds when the neighboring router is down. (1..)
authkey	String	Sets a character string representing an authentication key for plain text authentication (within 8 characters).

NAME	VALUE	Description
md5key	"(ID),(KEY)"	Sets an ID representing an authentication key for MD5 authentication and a key string KEY. The ID is a decimal number from 0 to 255, and the KEY is a character string within 16 characters. Up to two MD5 authentication keys can be set. When a plurality of MD5 authentication keys are set, multiple packets with the same contents are transmitted by adding authentication data using each key. A key whose key ID matches is a target for comparison at reception.
md5-sequence-mode	"second"	Number of seconds of transmission time
	"increment"	Monotonous increase

When setting to a LOOPBACK interface, the interface type can be specified with the *type* parameter and the cost of the interface can be specified with the *cost* parameter. Only the following two types can be specified by the type of the LOOPBACK interface.

NAME	VALUE	Types of routes advertised	Handling OSPF-like interfaces	
			Types	Status
type	Loopback	Loopback Inter Host routes with only face IP addresses	point-to-point	Loopback
	loopback-network	Loopback Inter Implicit faces Network routes	NBMA	DROther

[Notes]

- About the type of the NAME parameter

Only broadcast is allowed for a LAN interface as the type of the NAME parameter. The PP interface can be set to either point-to-point when using PPP, or point-to-multipoint or non-broadcast when using frame relay.

When using non-broadcast (NBMA) in a frame relay, a PVC is set between all of the frame relay bases, and each router connected to the FR must be in a state where it can communicate directly with other routers, that is, it must be in a full mesh. Since neighboring routers cannot be automatically recognized by non-broadcast, all neighboring routers need to be set with the **ip pp ospf neighbor** command.

When using point-to-multipoint, the PVC of the frame relay does not need to be a full mesh, and partial meshes lacking a part can be used. Since neighboring routers automatically recognize using InArp, InArp is indispensable. In RT, whether or not to use InArp can be controlled with the **fr inarp** command, but since it is configured to use InArp by default, all you have to do is give the appropriate IP address to the interface with the **ip pp address** command.

For interfaces set to point-to-multipoint, the setting of the **ip pp ospf neighbor** command is ignored.

Although point-to-multipoint has fewer network restrictions than non-broadcast and is easier to set, traffic flowing through the line is larger instead. In non-broadcast, a designated router is selected in the same way as in broadcast, and OSPF traffic such as HELLO is limited only to between each router and the designated router, but in point-to-multipoint, there is a point-to-point link between all communicable router pairs, so that OSPF traffic is also exchanged between all communicable router pairs.

About passive

Passive specifies when there are no other OSPF routers in the network to which the interface is connected. By specifying passive, the interface does not send OSPF packets, so that useless traffic can be suppressed or malfunction can be prevented on the receiver side.

For a LAN interface (an interface with type=broadcast), the route to the network to which the interface is connected is not advertised to other OSPF routers unless the **ip interface ospf area** command is set. Therefore, for a LAN interface connecting to a network that does not use OSPF, an **ip interface ospf area** with passive

By setting the command, the network can advertise routes to other OSPF routers without using OSPF.

If the **ip interface ospf area** command is not set for a PP interface, the route to the network to which the interface connects is treated as an external route. Since it is an external route, it is necessary to set up the **ospf import** command to advertise to other OSPF routers.

- About hello-interval/dead-interval

The value of hello-interval/dead-interval must be the same as that of all neighboring routers that can communicate directly from that interface. If an OSPF HELLO packet is received with these parameter values different from the set value, it is ignored.

About MD5 authentication keys

A function allowing setting of multiple MD5 authentication keys is for smoothly changing the MD5 authentication keys. In normal operation, only one MD5 authentication key is set. To change the MD5 authentication keys, first set two new and old MD5 authentication keys on one router, then change the MD5 authentication keys to new ones on neighboring routers, and finally delete the old keys on a router with two keys set.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.14 Specifying OSPF routers connected to a non-broadcast network

[Format]

```
ip interface ospf neighbor ip_address [eligible]
ip pp ospf neighbor ip_address [eligible]
ip tunnel ospf neighbor ip_address [eligible]
no ip interface ospf neighbor ip_address [eligible]
no ip pp ospf neighbor ip_address [eligible]
no ip tunnel ospf neighbor ip_address [eligible]
```

[Setting value and initial value]

- *interface*
 - Setting value: LAN interface name
 - Initial value: -
- *ip_address*
 - Setting value: IP address of neighboring routers
 - Initial value: -

[Description]

Specify OSPF routers connected to a non-broadcast network.

A router with the eligible keyword specified is qualified as a designated router.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.15 Setting network routing when s tubs are present

[Format]

```
ospf merge equal cost stub merge
no ospf merge equal cost stub
```

[Setting value and initial value]

- *merge*
 - Setting value:

Setting value	Explanation
on	Do not merge stubs that are equal cost with other routes.

Setting value	Explanation
off	Do not merge stubs that are equal cost with other routes.

- Initial value: on

[Description]

Set how to handle stubs that are equal cost to other routes.

In the case of on, routes to stubs are merged with other routes for equal cost multipath operation. This follows the description in RFC2328.

In the case of off, routes to stubs are ignored.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.16 Setting whether to log OSPF state transition and packet transmission/reception

[Format]

`no ospf log log [log...]`

`no ospf log [log...]`

Setting value and initial value

- `log`
- Setting value:

Setting value	Explanation
interface	State transition of the interface
neighbor	State transition of neighboring routers
packet	Packets sent and received

- [Initial value]: OSPF logs are not recorded.

[Explanation]

Logs of the specified type are recorded at the INFO level.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

23.17 Time interval setting to reflect the external route in OSPF when the interface state changes

[Format]

`ospf reric interval time`

`no ospf reric interval [time]`

[Setting value and initial value]

- `time`
- [Setting value]: Number of seconds (one or more)
- [Initial value]: 1

[Explanation]

Time interval to reflect the external route in OSPF when the interface state of the router changes is set.

OSPF monitors the interface state change at one second intervals, and if there is a change, reflects the latest external route to itself, but when the interface state change occurs continuously, reflection processing of multiple external routes is performed collectively at the interval of seconds specified by *time*.

[Notes]

In an environment where multiple tunnels may be uploaded simultaneously, setting the value of this command appropriately will cause OSPF and

The load on the system can be reduced by introducing the BGP external route.

The setting value of this command also affects the reflection of the external route to BGP. If the setting values of this command and **bgp reric interval** command are different, the setting value of this command takes precedence.

The setting value of this command is not related to OSPF or BGP behavior for the change of the route or the change of IP address. The setting value of this command is reflected immediately without executing the **ospf configure refresh** command.

RTX1210 can be used with Rev.14.01.16 or later.

RTX5000 and RTX3500 can be used with Rev.14.01.21 or later.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 24

BGP

24.1 Setting Up BGP

[Format]

BGP use *use*
no bgp use [*use*]

[Setting Values and Initial Values]

- *Use*
- [Setting Values]

Setting Values	Explanation
on	Starting
off	Does not start

- [Initial Values]: off

Explanation

Setting Up or Not to Start BGP

[Notes]

BGP cannot be used if a secondary address is assigned to any interface.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.2Setting Up Route Aggregation

[Format]

bgp aggregate *ip_address/mask* filter *filter_num* ...
no bgp aggregate *ip_address/mask* [*filter filter_num...*]

[Setting Values and Initial Values]

- *ip_address/mask*
 - [Setting Values]: IP address/netmask
 - [Initial Values]: -
- *filter_num*
 - [Setting value]: Filter number (1..2147483647)
 - [Initial value]: -

[Explanation]

Set an aggregation route for advertising in BGP. The number defined by the **bgp aggregate filter** command is specified for the filter number.

[Applied model]

[Setting value]: vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.3Setting a filter for aggregating routes

[Format]

bgp aggregate filter *filter_num* protocol [*reject*] kind *ip_address/mask* ...
no bgp aggregate filter *filter_num* [*protocol* [*reject*] kind *ip_address/mask* ...]

[Setting value and initial value]

- *filter_num*
 - [Setting value]: Filter number (1..2147483647)
 - [Initial value]: -

- *protocol*
- [Setting value]:

Setting value	Explanation
static	Static routes (including implicit routes)
Rip	Rip
OSPF	OSPF
BGP	BGP
all	All protocols

- [Initial value]: -
- *kind*
- [Setting value]:

Setting value	Explanation
include	Routes included in the specified network (including the network address itself)
Refine routes	Routes included in the specified network (not including the network address itself)
equal	Routes that match the specified network

- [Initial value]: -
- *ip_address/mask*
 - Setting value: IP address/netmask
- [Initial value]: -

[Explanation]

Filters for aggregating routes advertised in BGP are defined. Filters defined in this command have an effect only when specified in the filter clause of the **bgp aggregate** command.

IP_address/mask sets the network address. Multiple settings can be made, and among them, settings with a longer matching network length are adopted.

If you place the reject keyword before *kind*, the routes are not aggregated.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.4 Setting AS number

Format

bgp autonomous-system *as*

no bgp autonomous-system [*as*]

Setting value and initial value

- *as*
 - [設定値]: AS 番号(1..65535)
 - [Initial value]: -

Explanation

Set the AS number of the router.

Notebook

BGP does not work until the AS number is set.

[Applicable model]

[Model No.]: vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840

24.5 Router ID setting

[Format]

```
bgp router id ip_address
no bgp router id [ip_address]
```

[Setting value and initial value]

- *ip_address*
 - [Setting value]: IP address
 - [Initial value]: Automatically selects from the primary addresses assigned to the interface.

[Explanation]

Router ID setting

[Notes]

When the router ID is not set by this command, one of the primary IPv4 addresses assigned to the following interfaces is automatically selected and used as the router ID.

- LAN interface
- LOOPBACK interface
- PP interface

If there is no interface to which a primary IPv4 address is assigned, the initial value is not set.

To prevent unintended IP addresses from being used as the router ID, it is desirable to specify the router ID explicitly by this command.

When using OSPF and BGP-4 together, set either this command or the ospf router id command.

In the following revisions, both this command and the ospf router id command can be set, but it is necessary to specify the same router ID.

Model	Revisions
vRX series	All revisions
RTX3510	All revisions
RTX1300	All revisions
RTX1220	All revisions
RTX1210	Rev.14.01.16
RTX5000	Rev.14.00.21
RTX3500	Rev.14.00.21

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.6 Setting route priority by BGP

[Format]

```
bgp preference preference
no bgp preference [preference]
```

[Setting value and initial value]

- *preference*
 - [Setting value]: Priority (1..2147483647)
 - [Initial value]: 500

[Description]

Setting the priority of a route by BGP The priority is indicated by an integer of 1 or more, and the higher the number, the higher the priority. If a route obtained by BGP and other protocols is different, a route with high priority is adopted. When the priority is the same, a route adopted earlier becomes effective.

[Notes]

The initial value of priority given to each protocol is as follows.

Static	10000
RIP	1000
OSPF	2000
BGP	500

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.7[Settings]: [Settings]: [Settings]: [Settings]: [

[Format]

bgp export *remote* *as* *filter* *filter* *num* ...

bgp export aspath seq "aspath regexp" filter filter num ...

no bgp export *remote as* [*filter filter num ...*]

```
no bgp export aspath seq ["aspath regexp" [filter filter num ...]]
```

[Settings and initial values]

- *[Settings]: [Settings]: [*
 - [Settings]: AS number of the other party (1..65535)
 - [Settings]: -
- *seq*
 - [Settings]: Evaluation order when AS path is specified (1..65535)
 - [Settings]: -
- *aspath_regexp*
 - [Settings]: Regular expression
 - [Settings]: -
- *filter_num*
 - [Settings]: Filter number (1..2147483647)
 - [Settings]: -

[Explanation]

Set a filter for the route received by BGP. When setting a filter by specifying *remote_as*, the route corresponding to the filter for the route received from a connection destination is introduced into an actual routing table, and other protocols such as RIP and OSPF are also notified. The route that does not correspond to the filter is not applied to routing, and other protocols are not notified. For the number of the filter, specify the number defined by the **bgp export filter** command.

When setting a filter by specifying *aspath_regex*, the route corresponding to the filter is introduced for the route whose AS path matches the regular expression in the same way as when specifying *remote_as*. For *aspath_regex*, specify a search pattern that can be used with the **grep** command.

When setting multiple filters by specifying `aspath_regex`, they are evaluated in descending order of seq. When setting a filter by specifying `aspath_regex`, they are evaluated with priority over the filter by specifying `remote_as`.

[Notes]

Example of representing an AS path by regular expression

- Matches all AS paths

```
# bgp export aspath 10 ".*" filter 1
```

- Matches an AS path whose AS number starts with 1000 or 1100

```
# bgp export aspath 20 "^1[01]00 .*" filter 1
```

- Matches an AS path whose AS number matches the one whose AS path matches the one whose AS path matches the one whose AS path matches the one whose AS path

```
# bgp export aspath 30 "2000" filter 1
```

- Exact match with a path whose AS path matches the one whose AS path matches the one whose AS path matches the one whose AS path matches the one whose AS path matches

```
# bgp export aspath 40 "^3000 3100 3200$" filter 1
```

- Matches an AS path with a path that contains an AS_SET

```
# bgp export aspath 50 "{.*}" filter 1
```

Up to 101 filter numbers can be set.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.8Setting a filter to be applied to a route received by BGP

[Format]

bgp export filter *filter_num* [reject] *kind* *ip_address/mask* ... [*parameter*]

no bgp export filter *filter_num* [[reject] *kind* *ip_address/mask* ... [*parameter*]]

[Setting value and initial value]

- *filter_num*
 - filter_num_filter_num_filter_num_filter_num_filter_num_filter_num_filter_name filter_num_filter_name
 - filter_num_filter_name
 - [Initial value]: -
- *kind*
 - [Setting value]:

Setting value	Explanation
include	Routes included in the specified network (including the network address itself)
Refines	Routes included in the specified network (not including the network address itself)
equal	Routes included in the specified network

- [Initial value]: -

- *ip_address/mask*

- [Setting value]:

Setting value	Description
ip_address/mask	IP address/mask
all	All networks

- Initial value: -

- *parameter*: A pair of TYPE=VALUE

- Value setpoint:

TYPE	Value	Description
preference	0..255	Priority for selecting one when the same route is received from multiple parties

- Initial value: 0

Description

Filters to be applied to routes received by BGP are defined. Filters defined in this command are used in the **bgp export** command.

They have an effect only if they are specified in the filter clause.

In *ip_address/mask*, a network address is set. When there are multiple settings, settings that match the longest prefix are adopted.

If you put the keyword reject before *kind*, the route is rejected.

Notes

The preference setting is used to prioritize between BGP routes. The overall priority of a BGP route is set by the **bgp preference** command.

[Configuration Example]

```
# bgp export filter 1 include 10.0.0.0/16 172.16.0.0/16
# bgp export filter 2 reject equal 192.168.0.0/24
```

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.9 Applying filters to routes introduced into BGP**Format**

```
bgp import remote_as protocol [from_as] filter filter_num ...
no bgp import remote_as protocol [from_as] [filter filter_num ...]
```

Setpoint and initial value

- *remote_as*
 - Setpoint: AS number of the other party (1..65535)
 - Initial value: -
- *protocol*
 - Setpoint:

Setpoint	Description
static	Static routes (including implicit routes)
Rip	RIP
OSPF	OSPF
BGP	BGP
aggregate	Aggregation routes

- Initial value: -
- *from_as*
 - Setpoint: AS received for a route to be introduced (only when bgp is specified in *protocol*) (1..65535)
 - Initial value: -
- *filter_num*
 - Setpoint: Filter number (1..2147483647)
 - Initial value: -

Description

Set filters to be applied when introducing routes other than BGP such as RIP and OSPF. No routes corresponding to filters are introduced. Specify the number defined by the **bgp import filter** command for the filter number. When introducing a BGP route, it is necessary to specify the AS number received for that route.

Notebook

When this command is not set, no external routes are introduced. Up to 102 filter numbers can be set.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.10 Enabling BGP settings**[Format]**

```
bgp configure
```

refresh [説明]

Enable BGP settings. After changing BGP settings, you must restart the router or run this command.

(i)

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.11 Filter settings to be applied to routes introduced into BGP

[Format]

bgp import filter *filter_num* [reject] *kind ip_address/mask ... [parameter ...]*

no bgp import filter *filter_num* [[reject] *kind ip_address/mask ... [parameter ...]*]

[Setting value and initial value]

- *filter_num*

- [Setting value]: Filter number (1..2147483647)
- [Initial value]: -

- *kind*

- [Setting value]:

Setting value	Explanation
include	Routes included in the specified network (including the network address itself)
Routes included in the specified network	Routes included in the specified network (not including the network address itself)
equal	Routes included in the specified network

- [Initial value]: -

- *ip_address/mask*

- [Setting value]:

Setting value	Explanation
IP_address/mask	IP address/netmask
all	All networks

- [Initial value]: -

- *parameter* : pairs of TYPE=VALUE

- [Setting value]:

TYPE	Value	Explanation
metric	1..16777215	Metric values to be notified by MED (Multi-Exit Discriminator) (if not specified, do not send MED)
preference	0..255	Priority to be notified by Local Preference

- [Initial value]:

- preference=100

[Explanation]

Filters to be applied to routes introduced into BGP are defined. The filter defined in this command is the filter of the **bgp import** command.

It has an effect only when specified in the filter clause.

In *ip_address/mask*, a network address is set. When there are multiple settings, settings with the longest prefixes are adopted.

If you put the keyword reject before *kind*, the route is rejected.

[Configuration Example]

```
# bgp import filter 1 include 10.0.0.0/16 172.16.0.0/16
# bgp import filter 2 reject equal 192.168.0.0/24
```

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.12 Setting the connection destination with BGP

[Format]

```
bgp neighbor neighbor_id remote_as remote_address [parameter...]
no bgp neighbor neighbor_id [remote_as remote_address [parameter...]]
```

[Setting value and initial value]

- *neighbor_id*
 - [Setting value]: Number of the neighboring router (1...2147483647)
 - [Initial value]: -
- *remote_as*
 - [Setting value]: AS number of the neighboring router (1...65535)
 - [Initial value]: -
- *remote_address*
 - [Setting value]: IP address of the neighboring router
 - [Initial value]: -
- *parameter*: Pair of TYPE=VALUE
 - [Setting value]:

TYPE	VALUE	Description
hold-time	off, seconds	Time to down decision (3..28,800 seconds)
metric	1..21474836	Metrics notified with MED (Multi-Exit Discriminator)
passive	ON or OFF	Suppressing the connection of active BGP connections or not
gateway	IP address/interface	Gateway to the connection destination
local-address	IP address	Own address of the BGP connection
ignore-capability	ON or OFF	Ignore capability

- [Initial value]:
 - hold-time=180
 - metric is not sent
 - passive=off
 - gateway is not specified
 - local-address is not specified
 - ignore-capability=off

Description

Neighbor routers to which the BGP connection is connected are defined.

[Notes]

Sends a KEEPALIVE message at intervals of about one-third of the time set in the hold-time parameter. If a KEEPALIVE message cannot be received even after waiting for the hold-time parameter time, it is determined that the connection is down.

Since the metric parameter serves as the initial value of all MEDs, it takes precedence when setting MED with the **bgp import** command.

gateway specifies a gateway (next hop) to which the connection destination is connected when the connection destination is not in the same segment.

Up to 32 commands can be set.

Since the vRX series updates the neighboring router and route information by enabling keep-alive, it is necessary to set the hold-time parameter to something other than 'off'.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.13Pre-shared key configuration for TCP MD5 authentication used with BGP

[Format]

```
bgp neighbor pre-shared-key neighbor_id text text_key
no bgp neighbor pre-shared-key neighbor_id [text text_key]
```

[Setting value and initial value]

- neighbor_id
 - Setting value: Number of the neighboring router (1...2147483647)
 - [Initial value]: -
- text_key
 - [Setting value]: Key expressed as an ASCII string (up to 80 characters)
 - [Initial value]: -

[Explanation]

Set a pre-shared key for TCP MD5 authentication used by BGP. Connections of BGP are established only between peers whose pre-shared keys set match.

[Notes]

RTX1210 can be used after Rev. 14.01.11.
RTX5000 and RTX3500 can be used after Rev. 14.00.18.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.14BGP logging settings

[Format]

```
bgp log log [log]
no bgp log [log ...]
```

[Setting value and initial value]

- log
 - [Setting value]:

Setting value	Description
neighbor	State transition for neighboring routers
packet	Packets sent and received

- [Initial value]: Logs are not recorded.

[Explanation]

Logs of the specified type are recorded at the INFO level.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.15Advertising routes by forcing BGP

[Format]

```
bgp force-to-advertise remote_as ip_address/mask [parameter ...]
no bgp force-to-advertise remote_as ip_address/mask [parameter ...]
```

[Setting value and initial value]

- remote_as
 - [Setting value]: AS number of the other party
- [Initial value]: -
- ip_address/mask
 - [Setting value]: IP address/netmask
- [Initial value]: -

- *parameter*
 - [Setting value]:
 - Pairs with TYPE=VALUE

TYPE	VALUE	Description
metric	1 .. 16777215	Metric values notified by MED (Multi-Exit Discriminator)
preference	0..255	Priority for selecting one when the same route is received from multiple parties

- [Initial value]: preference=100

[Explanation]

When the route set by this command does not exist in the routing table, BGP forcibly advertises routes to routers with the specified AS number. When 'default' is specified as the route, the default route is advertised. The configured command becomes effective when bgp configure refresh command is executed.

[Notebook]

RTX5000, RTX3500 can be used after Rev.14.01.18.

RTX1210 can be used after Rev.14.01.11.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.16 Setting the time interval for reflecting external routes in BGP when the interface state changes

[Format]

bgp reric interval *time*

no bgp reric interval [*time*]

[Setting value and initial value]

- *time*
 - [Setting value]: Number of seconds (1 or more)
 - [Initial value]: 1

[Explanation]

When the state of the interface of a router changes, a time interval for reflecting an external route in BGP is set.

In BGP, the state change of the interface is monitored at one second interval, and if there is a change, the latest external route is reflected to itself, but when the state change of the interface occurs continuously, the reflection processing of multiple external routes is performed collectively at the interval of seconds specified by *time*.

[Notes]

In an environment where multiple tunnels may be uploaded at once, setting the value of this command appropriately will cause OSPF or

It is possible to reduce a load on a system by introducing an external route of BGP.

The setting value of this command also affects the reflection of the external route to OSPF. If the setting value of this command and the **ospf reric interval** command are different, the setting value of the **ospf reric interval** command takes precedence.

The setting value of this command is not related to OSPF or BGP operation for the change of the route or the change of IP address. The setting value of this command is immediately reflected without executing the **bgp configure refresh** command.

RTX1210 can be used after Rev. 14.01.16.

RTX5000 and RTX3500 can be used after Rev. 14.00.21.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.17 Default MED Value Configuration

[Format]

```
bgp default med med
no bgp default med [med]
```

[Setting value and initial value]

- no bgp default med
 - no bgp default med med (1..2147483647)
 - no bgp default 2147483647

[Explanation]

BGP's optimal route selection sets a default MED value for routes without the MED attribute added. If this command is not set, routes without the MED attribute added will have the maximum MED value (2147483647) and have the lowest priority. The setting of this command does not affect routes with the MED attribute added.

no notes

RTX5000 and RTX3500 can be used after Rev. 14.02.15.
RTX1210 can be used after Rev. 14.02.15.
RTX830 can be used after Rev. 15.02.15.

[Applicable model]

vRX VMware ESXi version, vRX Sakura Cloud Edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

24.18 BGP sets a priority rule for route selection for routes received.

[Format]

```
bgp export route selection rule rule
no bgp export route selection rule [rule]
```

[Setting value and initial value]

- rule
 - [Setting value]:

Setting value	Explanation
ebgp-only	Routes with the same destination received by EBGp are compared.
all	Routes with the same destination received by all BGP are compared.

- [Initial value]: ebgp-only

[Explanation]

When a route with the same destination is received by BGP from multiple parties, a rule for route selection according to the priority for selecting one is set.

The setting of this command changes the type of route to be compared according to the *preference* of the **bgp export filter** command.

When ebgp-only is set in *rule*, comparison by *preference* works only for routes received by all BGP. When all is set in *rule*, comparison by *preference works* for routes received by all BGP. Therefore, comparison by *preference works* for routes received by all BGP. This makes it possible to make the priority of a route received by all BGP higher than that of a route received by all BGP.

In a configuration using only IBGP, the setting of this command does not change the selected route.

When multiple routes with the same destination are received from neighboring routers with the same neighboring router number, it is not possible to make a difference in the priority of route selection by changing the rule by this command. In this case, priority of a route can be set using MED for EBGp and Local Preference for IBGP.

Revisions that do not support this command operate when *rule* is *sebgp*-only.

[Notes]

For the route selection process that can be configured with this command, refer to the following URL.

- https://www.rtpro.yamaha.co.jp/RT/docs/bgp/index.html#rt_select

If you want to control a specific route so that it is prioritized in an environment where the same destination route is received between EBGp and IBGP, this command can be set.

RTX5000 / RTX3500 Rev.14.00.33 or earlier, RTX1300 Rev.23.00.04 or earlier, RTX1220 Rev.15.04.04 or earlier, RTX1210 Rev.14.01.41

It is not available before and before RTX830 Rev.15.02.26.

[Applicable models]

vRX Sakura Cloud Edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER25

IPv6

25.1 Common settings

25.1.1 Whether to handle IPv6 packets

Format

```
ipv6 routing routing
no ipv6 routing [routing]
```

Setting value and initial value

- *routing*
 - Setting value:

Setting value	Description
on	It is treated as an object to be processed.
off	It is not treated as an object to be processed.

- [Initial value]: on

Description

Whether to route IPv6 packets is set. IPv6-related operations on the PP side do not work at all unless this switch is turned on.
Even when this switch is turned off, setting by TELNET, access by TFTP, PING, etc. are possible.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.1.2Setting the link MTU of the IPv6 interface

Format

```
ipv6 interface mtu mtu0
IPV6 PP MTUTUTU1
ipv6 tunnel mtu mtu2
no ipv6 interface mtu [mtu0]
no ipv6 pp mtu [mtu1]
no ipv6 tunnel mtu [mtu2]
```

Setting value and initial value

- *interface*
 - Setting value: LAN interface name
 - Initial value: -
- *MTU*
 - Setting value: Value of MTU (1280..1500; RTX5000,RTX3500 are 1280..9578,RTX3510,RTX1300)
TheLAN interface is 1280..10218)
 - Initial value:
 - MTU2=1280
 - mtu1=1500
 - MTU2=1280

Description

Setting the MTU value of the IPv6 interface

Notes

The `ipv6 tunnel mtu` command is available for RTX5000 / RTX3500 Rev.14.00.29 or later, RTX1210 Rev.14.01.34 or later, RTX830 Rev.15.02.10

It can be used after Rev.15.04 or later.

In the L2TP connection, the MTU setting of the tunnel interface or PP interface is ignored and encapsulated, and packets after encapsulation are fragmented according to the MTU setting of the sending physical interface.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.1.3 Setting the MSS limit of a TCP session

Format

ipv6 interface tcp mss limit mss

ipv6 pp tcp mss limit mss

ipv6 tunnel tcp mss limit mss

no ipv6 interface tcp mss limit [mss]

no ipv6 pp tcp mss limit [mss]

no ipv6 tunnel tcp mss limit [mss]

Setting value and initial value

- *interface*
 - Setting value: LAN interface name
 - Initial value: -
- *mss*
 - Setting value:

Set value	Description
536..1440	Maximum MSS length
Auto	Automatic setting
off	Not set

- [Initial value]:
 - off (RTX5000、RTX3500、RTX1210 Rev.14.01.25 以前、RTX830 Rev.15.02.02 以前)
 - auto (other than above)

Description

Limit MSS of TCP sessions passing through the interface. TCP packets passing through the interface are monitored, and if the value of the MSS option exceeds the set value, it is rewritten to the set value. When specifying the keyword `auto`, in the case of an MTU of an interface or a PP interface, if the other party's MRU value is known, it is rewritten to the value calculated from the MRU value.

[Notes]

For a PP interface for PPPoE, the `pppoe tcp mss limit` command can also limit the MSS of a TCP session. If both this command and the `pppoe tcp mss limit` command are enabled, the MSS is limited to the smaller value.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.1.4 Change the TCP window scale option

Format

ipv6 interface tcp window-scale sw

ipv6 pp tcp window-scale sw

ipv6 tunnel tcp window-scale sw

no ipv6 interface tcp window-scale [...]

no ipv6 pp tcp window-scale [...]

no ipv6 tunnel tcp window-scale [...]

Set value and initial value

- *interface*
 - Set value: LAN interface name
 - [Initial value]: -
- *SW*
 - [Set value]:

Set value	Description
off	Do nothing
Remove	Remove the TCP window scale option

- [Initial value]: off

Description

Forcibly changes the window scale option of TCP packets passing through the interface.
If remove is specified, it is disabled and transferred if the window scale option was enabled.

[Notes]

RTX5000 and RTX3500 can be used after Rev.14.00.21.
RTX1210 can be used after Rev.14.01.16.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.1.5 Setting whether to discard IPv6 packets with routing header of type 0

Format

ipv6 rh0 discard *switch*
no ipv6 rh0 discard

Set value and initial value

- *switch*
 - Set value:

Set value	Description
on	Destroy
off	Destroy not

- [Initial value]: on

Description

Selects whether to discard IPv6 packets with routing headers of type 0.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.1.6 Configure IPv6 Fastpass function

[Format]

ipv6 routing process *process*
no ipv6 routing process

[Setting value and initial value]

- *process*
 - [Setting value]:

Setting value	Description
fast	Use fastpass function
normal	Process all IPv6 packets with normal path without using fastpass function

- [Initial value]: fast

[Explanation]

Whether to process the transfer of IPv6 packets with fastpass function or normal path function is set.

[Notes]

Although there is no limitation on the functions that can be used with fastpass, some packets are not processed by fastpass but processed by normal path.

When fast is set in this command, IPv6 multicast packets are also processed by fastpass function.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.1.7 Setting the number of packets that can be withheld before address resolution is completed in ICMPv6

[Format]

```
ipv6 interface icmp-nd queue length len
no ipv6 interface icmp-nd queue length [len]
```

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *len*
 - [Setting value]: Queue length (0.10000)
 - [Initial value]: 200

[Explanation]

When an attempt is made to send a packet to a host for which address resolution of Neighbor Discovery of ICMPv6 has not been completed, the maximum number of packets that can be withheld from transmission for each interface is set until it is determined that the address resolution is completed or cannot be resolved by timeout.

[Notes]

RTX5000 is Rev. 14.00.26 or later, RTX3500 is Rev. 14.00.26 or later, RTX1210 is Rev. 14.01.33 or later, RTX830 is Rev. 15.02.09

It can be used after that.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.1.8 Setting the maximum number of entries in the neighbor cache

[Format]

```
ipv6 interface neighbor cache max entry num
no ipv6 interface neighbor cache max entry [num]
```

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *num*
 - [Setting value]: Maximum number of entries (256...20480)
 - [Initial value]:
 - 1024

[Explanation]

The maximum number of entries in the neighbor cache is set for each interface.
When the number of entries in the neighbor cache reaches the set maximum number of entries, old neighbor cache is deleted. When this command is executed, if the number of entries in the current neighbor cache exceeds the maximum number of entries, old neighbor cache is deleted.

[Notes]

RTX5000 and RTX3500 can be used after Rev.14.02.20.
RTX1210 can be used after Rev.14.01.40.
RTX830 can be used after Rev.15.02.20.

[Applicable model]

vRX VMware ESXi version, vRX Sakura Cloud version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.1.9Sets the amount of time to keep an IPv6 fragment packet for reconstruction.

[Format]

ipv6 reassembly hold-time sec
no ipv6 reassembly hold-time [sec]

[Setting value and initial value]

- sec
- [Setting value]:

Setting value	Description
Seconds (1 .. 60)	Time to keep an IPv6 fragment packet for reconstruction.

- [Initial value]: 60 seconds

[Explanation]

Time to keep an IPv6 fragment packet for reconstruction.
When reconstruction is not possible even after the set time has elapsed, the kept packet is discarded. Packets already kept at the time of command execution are not changed.

[Notes]

RTX5000 and RTX3500 can be used with Rev.14.00.32 or later.
RTX1210 can be used with Rev.15.02.20 or later.
RTX830 can be used with Rev.15.02.20 or later.

[Applicable model]

vRX VMware ESXi version, vRX Sakura Cloud Edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.1.10Setting Up Rewriting of DSFields in IPv6 Packets

[Format]

ipv6 dscp supersede id dscp filter_num [filter_num_list]
no ipv6 dscp supersede id [dscp]

[Setting value and Initial value]

- *id*
 - setting value: Identification number (1..65535)
 - initial value: -
- *dscp*
 - setting value:

- DSCP value to rewrite (0..63)
- The following mnemonics are available

mnemonic	DSCP value
default	0
cs6	8
cs6	16
cs7	24
cs7	32
cs7	40
cs7	48
cs7	56
af11	10
af21	12
af13	14
af22	18
af23	20
af22	22
af31	26
af32	28
af33	30
af41	34
af42	36
af43	38
ef	46

- [Initial value]: -
- *filter_num*
 - set value: Number of static filter (1..21474836)
 - [Initial value]: -
- *filter_num_list*
 - set value: Number of static filter (1..21474836)
 - [Initial value]: -

[Explanation]

DS field is rewritten to a specified value when an IPv6 packet is relayed.

The list is checked in order of identification number, and filters in the *filter_num* list are successively applied. If the first matched IPv6 filter is pass, pass-log, pass-nolog, restrict, restrict-log or restrict-nolog, the DS field is rewritten.

If reject, reject-log or reject-nolog, the process ends without rewriting.

[Notes]

RTX5000 and RTX3500 can be used in Rev. 14.00.34 or later.

RTX1300 can be used in Rev. 15.02.27 or

later. RTX830 can be used in Rev. 15.02.27

or later. RTX830 can be used in Rev.

15.02.27 or later. RTX830 can be used in

Rev. 15.02.27 or later.

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.2.1 Defining Prefixes for Dynamic Assignment in DHCPv6

[Format]

```
ipv6 dhcp prefix prefix_id dhcp-prefix@prefix_interface[sub_prefix/prefix_len]
no ipv6 dhcp prefix prefix_id
```

[Setting Values and Initial Values]

- *prefix_id*
 - *prefix_number*
- [Initial Values]: -
- *prefix_interface*
 - *prefix_name* : Interface name of the source of the DHCPv6 proxy
 - [Initial Values]: -
- *sub_prefix*
 - *prefix_number* : Lower part specified when dividing the prefix obtained from *prefix_interface*
 - [Initial Values]: -
- *prefix_len*
 - *prefix_length*
 - [Initial Values]: -

[Explanation]

Defining Prefixes for Dynamic Assignment in DHCPv6 To perform the assignment, it is necessary to set the prefix option of the **ipv6 interface dhcp service** command.

The LOOPBACK interface cannot be specified in *prefix_interface*.

[Notes]

It can be specified in RTX1300 Rev.23.00.16 or later.

[Applicable Models]

RTX1300

25.2.2 Configuring IPv6 Address of Interface

[Format]

```
ipv6 interface address ipv6_address/prefix_len [address_type]
ipv6 interface address
auto ipv6 interface
address dhcp ipv6
interface address proxy
ipv6 pp address ipv6_address/prefix_len [address_type]
ipv6 pp address
auto ipv6 pp
address dhcp ipv6
pp address proxy
ipv6 tunnel address ipv6_address/prefix_len [address_type]
ipv6 tunnel address
auto ipv6 tunnel
address dhcp ipv6
tunnel address proxy
no ipv6 interface address ipv6_address/prefix_len [address_type]
no ipv6 interface address
auto no ipv6 interface
address dhcp no ipv6
interface address proxy
no ipv6 pp address ipv6_address/prefix_len [address_type]
```

```

no ipv6 pp address
auto no ipv6 pp
address dhcp no ipv6
pp address proxy
no ipv6 tunnel address ipv6_address/prefix_len [address_type]
no ipv6 tunnel address
auto no ipv6 tunnel
address dhcp no ipv6
tunnel address proxy

```

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name, LOOPBACK interface name, bridge interface name
 - [Setting value]: -
- *ipv6_address*
 - [Setting value]: IPv6 address part
 - [Setting value]: -
- *prefix_len*
 - [Setting value]: IPv6 prefix length
 - [Setting value]: -
- *address_type*
- [Setting value]:

Setting value	Description
unicast	Unicast
Anycast	Anycast

- [Setting value]: unicast
- *auto*: Keyword indicating that an IPv6 address is generated from the prefix obtained by RA and the MAC address of the interface
 - [Setting value]: -
- *dhcp*: Keyword indicating that an IPv6 address is generated from the prefix obtained by DHCPv6 and the MAC address of the interface
 - [Setting value]: -
- *proxy*: Proxy
 - [Setting value]:
 - *prefix_type@prefix_interface[interface_id/prefix_len]*

Setting value	Description
dhcp-prefix	DHCPv6 proxy
RA-prefix	RA proxy

- *prefix_interface*

Setting value	Description
<i>prefix_interface</i>	Interface name of the source

- *interface_id*

Setting value	Description
<i>interface_id</i>	Interface ID

- *prefix_len*

Setting value	Description
<i>prefix_len</i>	IPv6 prefix length

- [Setting value]: -

Explanation

IPv6 addresses are assigned to the interface.

Notebook

The address assigned by this command can be confirmed by the **show ipv6 address** command. A function for automatically setting addresses in multiple LAN interfaces can be utilized.

Specifically, a function for generating an IPv6 address from the prefix and interface ID obtained by RA and a function for generating an IPv6 address from the prefix and interface ID obtained by DHCPv6 can be utilized.

When these are configured, the default path is directed to the last configured interface.

When the LOOPBACK interface is specified, *auto*, *dhcp*, *address_type*, and *proxy* cannot be specified.

The LOOPBACK interface cannot be specified in *prefix_interface*.

The bridge interface cannot be specified for vRX Amazon EC2 version and RTX5000/RTX3500 Rev.14.00.11 or earlier.

[Configuration Example]

- Add ::1 to the RA prefix received by LAN2 to create an IPv6 address and assign it to LAN1.

```
# ipv6 lan1 address ra-prefix@lan2::1/64
```

- LAN2 splits the /56 prefix (XXXX:XXXX:XXXX:XX00::/56) obtained by DHCPv6, and assigns it to LAN1 and LAN3. Assign an IPv6 address with a different /64 prefix to

```
IPv6 address assigned to LAN1 (XXXX:XXXX:XXXX:XX01::1/64)
```

```
IPv6 address assigned to LAN3 (XXXX:XXXX:XX02::1/64)
```

```
# ipv6 lan1 address dhcp-prefix@lan2::1:0:0:0:1/64
```

```
# ipv6 lan3 address dhcp-prefix@lan2::2:0:0:0:1/64
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.2.3 IPv6 address configuration based on interface prefix**[Format]**

```
ipv6 interface prefix ipv6_prefix/prefix_len
```

```
ipv6 interface prefix proxy
```

```
ipv6 pp prefix ipv6_prefix/prefix_len
```

```
no ipv6 pp prefix proxy
```

```
ipv6 tunnel prefix ipv6_prefix/prefix_len
```

```
ipv6 tunnel prefix proxy
```

```
no ipv6 interface prefix ipv6_prefix/prefix_len
```

```
no ipv6 interface prefix proxy
```

```
no ipv6 pp prefix ipv6_prefix/prefix_len
```

```
no ipv6 pp prefix proxy
```

```
no ipv6 tunnel prefix ipv6_prefix/prefix_len
```

```
no ipv6 tunnel prefix proxy
```

[Setting value and initial value]

- *interface*
 - Setting value: LAN interface name, bridge interface name
 - [Initial value]: -
- *ipv6_prefix*
 - Setting value: IPv6 prefix length
 - [Initial value]: -
- *prefix_len*
 - Setting value: IPv6 prefix length
 - [Initial value]: -
- *proxy*
 - Setting value:
 - *prefix_type@prefix_interface[interface_id/prefix_len]*

- *prefix_type*

Setting value	Description
dhcp-prefix	DHCPv6 proxy
ra-prefix	RA proxy

- *prefix_interface*

Setting value	Description
<i>prefix_interface</i>	Interface name of the source

- *interface_id*

Setting value	Description
<i>interface_id</i>	Interface ID

- *prefix_len*

Setting value	Description
<i>prefix_len</i>	IPv6 prefix length

- [Initial value]: -

Initial value

To assign an IPv6 address to an interface. A similar command is the **ipv6 interface address** command, which specifies only a prefix instead of an address. The part after the prefix is automatically complemented based on the MAC address. The MAC address used at this time is the one assigned to the interface to be configured. However, a PP interface or a tunnel interface without a MAC address uses the MAC address of a LAN1 interface.

Note that the **ipv6 prefix** command with a similar name defines a prefix notified in router advertisements, and does not assign an IPv6 address. However, in normal operation, since the prefix of an IPv6 address given to the interface and the prefix notified in router advertisements are the same, the same prefix is often set for both commands.

[Notes]

The address given by this command can be confirmed by a **show ipv6 address** command.

A LOOPBACK *interface* cannot be specified for a *prefix_interface*.

A bridge interface cannot be specified for vRX Amazon EC2 version and RTX5000/RTX3500 Rev.14.00.11 or earlier.

[Configuration Example]

- A RA received by LAN2 is prefixed to LAN1.

```
# ipv6 lan1 prefix ra-prefix@lan2::/64
```

- LAN2 divides the /56 prefix (XXXX:XXXX:XXXX:XX00::/56) obtained by DHCPv6, and assigns it to LAN1 and LAN3. A different /64 prefix is assigned to

```
A prefix given to LAN1 is XXXX:XXXX:XX01::/64 A prefix given
to LAN3 is XXXX:XXXX:XXXX:XX02::/64
```

```
# ipv6 lan1 prefix dhcp-prefix@lan2::1:0:0:0:1/64
# ipv6 lan3 prefix dhcp-prefix@lan2::2:0:0:0:1/64
```

```
(Note: For internal operation reasons, set "dhcp-prefix@lan2::1:0:0:0:1/64" instead of "dhcp-
prefix@lan2::1:0:0:0:0/64").
```

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.2.4

W

ether to log when IPv6 prefix changes

[Format]

```
ipv6 interface prefix change log log
```

```
ipv6 pp prefix change log log
```

```

ipv6 tunnel prefix change log log
no ipv6 interface prefix change log log
no ipv6 pp prefix change log log
no ipv6 tunnel prefix change log log

```

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name, bridge interface name
 - [Initial value]: -
- *log*
 - [Setting value]:

Setting value	Explanation
on	Logging IPv6 Prefix Changes
off	Do not log IPv6 prefix changes

- [Initial value]: off

[Explanation]

Whether to log when IPv6 prefix changes Logs are recorded at the INFO level.

When multiple addresses for the same prefix are set, the same log is displayed multiple times.

[Notes]

Bridge interface cannot be specified for vRX Amazon EC2 version and RTX5000/RTX3500 Rev.14.00.11 or earlier.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.2.5Setting DHCPv6 Operation

[Format]

```

ipv6 interface dhcp service type
ipv6 interface dhcp service client [ir=value]
ipv6 interface dhcp service server [prefix=prefix_id]
ipv6 pp dhcp service type
ipv6 pp dhcp service client [ir=value]
ipv6 tunnel dhcp service type
ipv6 tunnel dhcp service client [ir=value]
no ipv6 interface dhcp
service no ipv6 pp dhcp
service
no ipv6 tunnel dhcp service

```

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Setting value]: -
- *type*
 - [Setting value]:

Setting value	Description
off	Do not use DHCPv6
client	Client
server	Server

- [Setting value]: off

- *Value*
 - [Setting value]: off

Setting value	Description
on	When acting as a client, send Inform-Request
off	When acting as a client, send Solicit

- [Setting value]: off
- *Prefix_id*
 - [Setting value]: Prefix number
 - [Setting value]: -

Description

DHCPv6 operation in each interface is configured.

When acting as a server, always supports Inform-Request. Also, if the prefix option is configured, it corresponds to Solicit and assigns the prefix set by the **ipv6 dhcp prefix** command.

[Notes]

The ir option cannot be specified in vRX Amazon EC2 version.

The prefix option can be specified in RTX1300 Rev.23.00.16 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.2.6 Setting the number of times of Duplicate Address Detection (DAD) transmission

Format

ipv6 interface dad retry count count

ipv6 pp dad retry count count

no ipv6 interface dad retry count [count]

no ipv6 pp dad retry count [count]

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name, bridge interface name
 - [Setting value]: -
- *count*
 - Setting value: Number of times of DAD retransmission on the selected interface (0..10)
 - [Setting value]: 1

Description

Set the number of times of DAD transmission to detect address duplication when IPv6 address is set in the interface. However, if 0 is set, the address is treated as valid without sending DAD.

[Notes]

Bridge interface cannot be specified in vRX Amazon EC2 version and RTX5000 / RTX3500 Rev.14.00.11 or earlier.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.2.7 Set the maximum number of IPv6 addresses that are automatically set

[Format]

ipv6 max auto address max

no ipv6 max auto address [max]

[Setting value and initial value]

- *Max*
 - Setting value: Maximum number of IPv6 addresses per interface that are automatically set (1-256)
 - [Setting value]: 16

Explanation

Set the maximum number of IPv6 addresses per interface that are automatically set in the interface by RA.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.2.8 Setting a rule to select a starting IPv6 address

[Format]

ipv6 source address selection *rule rule*

no ipv6 source address selection *rule [rule]*

[Setting value and initial value]

- *rule*: A rule to select a starting IPv6 address
- [Setting value]:

Setting value	Description
Prefix	Longest match of prefix
lifetime	Priority is given to the one with longer life.

- [Initial value]: prefix

[Explanation]

A rule to select a starting IPv6 address is set.

If 'prefix' is set, the end IPv6 address is compared with the starting IPv6 address candidate, and the part that matches from the beginning

The one with the longest (prefix) is selected as the starting address.

If 'lifetime' is set, those with a long life of IPv6 address are selected preferentially.

[Notes]

Normally, it is sufficient to set 'prefix', but when address renumbering occurs, setting 'lifetime' may be effective.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.3 Neighbor search

25.3.1 Definition of prefixes to be distributed in r router advertisements

[Format]

ipv6 prefix *prefix_id prefix/prefix_len* [preferred_lifetime=*time*] [valid_lifetime=*time*] [*l_flag*=*switch*] [*a_flag*=*switch*]

ipv6 prefix *prefix_id proxy* [preferred_lifetime=*time*] [valid_lifetime=*time*] [*l_flag*=*switch*] [*a_flag*=*switch*]

no ipv6 prefix *prefix_id*

[Setting value and initial value]

- *prefix_id*
 - [Setting value]: Prefix number
 - [Initial value]: -
- *Prefix*
 - [Setting value]: Prefix
 - [Initial value]: -
- *prefix_len*
 - [Setting value]: Prefix length

- [Initial value]: -
- *proxy*
 - [Setting value]:
 - *prefix_type@prefix_interface[interface_id/prefix_len]*
 - *prefix_type*

Setting value	Description
dhcp-prefix	DHCPv6 proxy
RA-prefix	RA proxy

- *prefix_interface*

Setting value	Description
<i>prefix_interface</i>	Interface name of the source

- *interface_id*

Setting value	Description
<i>interface_id</i>	Interface ID

- *prefix_len*

Setting value	Description
<i>prefix_len</i>	IPv6 prefix length

- [Initial value]: -
- *preferred_lifetime*: Recommended prefix lifetime (0..4294967295)
 - [Initial value]: 604800
- *valid_lifetime*: Recommended prefix lifetime (0..4294967295)
 - [Initial value]: 2592000
- *time*: Time setting
 - [Setting value]:
 - *yyyy-mm-dd[,hh:mm[:ss]]*

Setting value	Description
yyyy	Year(1980..2079)
mm	Month(01..12)
dd	Sun(01..31)
hh	Hour(00..23)
mm	Minute(00..59)
ss	Seconds(00..59, default is 00)

- [Initial value]: -
- *l_flag* : On-link flag
 - [Initial value]: on
- *a_flag* : Autonomous address configuration flag
 - [Initial value]: on
- *switch*
 - [Setting value]:
 - on
 - off
 - [Initial value]: -

Description

Prefixes to be distributed in router advertisements are defined. To actually advertise, use the **ipv6 interface rtadv send** command.

Setting is necessary.

In *time*, the lifetime can be set to either the number of seconds or the time at which the lifetime expires. When a numerical value (0 or more and 4294967295 or less) is set as *time*, the number of seconds is advertised as the lifetime. When a *time* is set as time, the lifetime is calculated assuming that the lifetime expires at that time and is advertised. When setting the time, the above format is followed. The recommended lifetime is the time at which an address cannot be used on a new connection. Also, the on-link flag is set to on when the prefix is specific to that data link. The autonomous address configuration flag is set to on when the prefix can be used in autonomous address configuration.

The LOOPBACK *interface* cannot be specified for *prefix_interface*.

The bridge interface cannot be specified for vRX Amazon EC2 version and RTX5000 / RTX3500 Rev.14.00.11 or earlier.

[Notes]

The link-local prefix cannot be set.

[Configuration Example]

- Transfer RA received by LAN2 to LAN1
- LAN2 splits the /56 prefix (XXXX:XXXX:XXXX:XX00::/56) obtained by DHCPv6, and distributes it to LAN1 and LAN3. Distribute a different /64 prefix from to router advertisements

```
Prefix distributed in router advertisements for LAN1 :
XXXX:XXXX:XXXX:XX01::/64 Prefix distributed in router advertisements for
LAN3 : XXXX:XXXX:XXXX:XX02::/64

# ipv6 prefix 1 dhcp-prefix@lan2::1:0:0:0:1/64
# ipv6 prefix 2 dhcp-prefix@lan2::2:0:0:0:1/64
# ipv6 lan1 rtadv send 1
# ipv6 lan3 rtadv send 2

(Note: Set "dhcp-prefix@lan2::1:0:0:0:1/64" instead of "dhcp-prefix@lan2::1:0:0:0/64" for
```

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.3.2Definition of RDNSS options distributed in router advertisements

[Format]

```
ipv6 nd ra-rdnss rdns_id dns_ipv6_address [dns_ipv6_address...] [option=value]
no ipv6 nd ra-rdnss rdns_id [...]
```

[Setting value and initial value]

- rdns_id*
 - [Setting value]: RDNSS option number (1..21474836)
 - [Setting value]: -
- dns_ipv6_address*
 - [Setting value]:

Setting value	Description
dhcpv6	IPv6 address of DNS server notified by DHCPv6
ipv6_address	IPv6 address of any DNS server

- [Setting value]: -
- option=value* : Column of NAME=VALUE
- [Setting value]:

NAME	VALUE	Description
lifetime	Seconds, infinity	Effective time of DNS server (0..4294967294 seconds). infinity indicates that DNS server can be used indefinitely.

- [Setting value]:
 - lifetime = **ipv6** interface rtadv send command router advertisement maximum interval (max-rtr-adv-interval) of 3 Double

Description

Define RDNSS options to be distributed in router advertisement. Setting of rdNSS= option of **ipv6 interface rtadv send** command is necessary in order to actually advertise.
Up to three *dns_ipv6_addresses* can be specified.

[Notes]

RTX1210 Rev.14.01.41 以降、RTX830 Rev.15.02.24 以降、RTX1220 Rev.15.04.04 以降、RTX1300 Rev.23.00.05 以降のフ
Can be used with armware.

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.3.3Control of sending router advertisement

Format

ipv6 interface rtadv send *prefix_id* [*prefix_id*...] [option=value...]

ipv6 pp rtadv send *prefix_id* [*prefix_id*...] [option=value...]

no ipv6 interface rtadv send [...]

no ipv6 pp rtadv send [...]

[Setting value and initial value]

- *interface*
 - Setting value: LAN interface name
 - [Setting value]: -
- *prefix_id*
 - Setting value: Prefix number
 - [Setting value]: -
- *option=value* : Column of NAME=VALUE
 - [Setting value]:

NAME	VALUE	Description
m_flag	On, off	managed address configuration フ ラグ。 Setting whether or not to allow host to automatically set address by means other than router advertisement represented by DHCP6, in addition to automatic setting by router advertisement.
o_flag	On, off	Other stateful configuration flag. Setting whether or not to allow host to automatically set option information other than IPv6 address by means other than router advertisement.
prf_flag	high、 medium、 low	default router preference flag. Setting indicating priority of router advertisement.
max-rtr-adv-interval	Number of seconds	Maximum interval between sending router advertisement. (4-1,800 seconds)
min-rtr-adv-interval	Number of seconds	Minimum interval for sending router ads (3-1,350 seconds)
adv-default-lifetime	Number of seconds	Validity time of the terminal's default route set by the router ad (0-9,000 seconds)

NAME	VALUE	Description
adv-reachable-time	Number of milliseconds	Validity time of reachability confirmed between nodes by the terminal that received the router ad (0-3,600,000 milliseconds)
adv-retrans-time	Number of milliseconds	Interval for resending router ads (0-4,294,967,295 milliseconds)
adv-cur-hop-limit	Number of hops	Limit hops for router ads (0-255)
Mtu	Auto, off, number of bytes	Setting whether and when to include the MTU option in the router ad. In the case of auto, the MTU of the interface is adopted.
route-info	route-info, off, route information option number	Setting whether and when to include the route information option in the router ad. In the case of route-info, the route information allocated by the RA's route information option is notified.
rdnss	rdnss, off, dhcpv6, RDNSS option number	Setting whether and when to include the RDNSS option in the router ad. In the case of dnss, the server group allocated by the RA's RDNSS option is notified.
dnssl	dnssl, off, DNSSL option number	Setting whether and when to include the dnssl option in the router ad. In the case of dnssl, the server group allocated by the RA's DNSSL option is notified.

- Initial value:
 - m_flag = off
 - o_flag = off
 - prf_flag = medium
 - max-rtr-adv-interval = 600
 - min-rtr-adv-interval = 200
 - adv-default-lifetime = 1800
 - adv-reachable-time = 0
 - adv-retrans-time = 0
 - adv-cur-hop-limit = 64
 - Mtu = auto
 - route-info = route-info
 - rdnss = rdnss
 - dnssl = dnssl

Description

Control sending of the router ad for each interface. The prefix set by the **ipv6 prefix command** is used as the sent prefix. Optionally, using m_flag and o_flag, it is possible to set how a managed host interprets automatic setting information other than router ads. Optionally, it is also possible to set the transmission interval of the router ad to be sent and information included in the router ad.

Notebook

The prf_flag= option cannot be specified on vRX Amazon EC2 edition, vRX VMware ESXi edition, RTX5000 / RTX3500 Rev.14.00.31 or earlier, RTX1300 Rev.23.00.04 or earlier, RTX1220 Rev.15.04.03 or earlier, RTX1210 Rev.14.01.40 or earlier, and RTX830 Rev.15.02.21 or earlier.

The route-info= option cannot be specified on vRX Amazon EC2 edition, vRX VMware ESXi edition, RTX5000 / RTX3500, RTX3510 Rev.23.01.01 or earlier, RTX1300 Rev.23.00.11 or earlier, RTX1220 Rev.15.04.05 or earlier, RTX1210, and RTX830 Rev.15.02.30 or earlier.

The rdnss= option cannot be specified on vRX Amazon EC2 edition, vRX VMware ESXi edition, RTX5000 / RTX3500 Rev.14.00.31 or earlier, RTX1210 Rev.14.01.39 or earlier, and RTX830 Rev.15.02.19 or earlier.

The RDNSS option number cannot be specified on RTX5000, RTX3500, RTX1300 Rev.23.00.04 or earlier, RTX1220 Rev.15.04.03 or earlier, RTX1210 Rev.14.01.40 or earlier, and RTX830 Rev.15.02.23 or earlier.

The dnssl= option cannot be specified on vRX Amazon EC2 edition, vRX VMware ESXi edition, RTX5000, RTX3510 Rev.23.01.01 or earlier, RTX3500, RTX1300 Rev.23.00.11 or earlier, RTX1220 Rev.15.04.05 or earlier, RTX1210, and RTX830 Rev.15.02.29 or earlier.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.3.4 Setting up the function to retransmit router requests

[Format]

ipv6 interface rtsol max-retransmit mrt=MRT mrd=MRD mrc=MRC

ipv6 pp rtsol max-retransmit mrt=MRT mrd=MRD mrc=MRC

no ipv6 interface rtsol max-retransmit [...]

no ipv6 pp rtsol max-retransmit [...]

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *MRT*
 - [Setting value]: Maximum retransmission interval (4.3600 (seconds))
 - [Initial value]: 3600
- *MRD*
 - [Setting value]: Maximum retransmission duration (4.2147483647 (seconds) or infinity)
 - [Initial value]: infinity
- *MRC*
 - [Setting value]: Maximum retransmission interval (4.2147483647 or infinity)
 - [Initial value]: infinity

[Description]

The retransmission interval increases by a factor of two from an initial value of 4 seconds. The initial value is +10% wide and the magnification is $\pm 10\%$ wide, taking random values. If both MRD and MRC are set to values other than infinity, retransmission stops when either of the conditions of MRD and MRC are satisfied.

Retransmission is not performed when MRC is set to 0.

[Notes]

RTX3500 can be used with Rev.14.00.26 or later. RTX8300 can be used with Rev.14.00.26 or later. RTX8300 can be used with Rev.14.01.33 or later. RTX830 can be used with Rev.15.02.09 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.3.5 Defining DNSSL options to be distributed in router ads

[Format]

ipv6 nd ra-dnssl dnssl_id domain_name [domain_name...] [option=value]

no ipv6 nd ra-dnssl dnssl_id [...]

[Setting value and initial value]

- *dnssl_id*
 - [Setting value]: DNSSL option number (1..21474836)
 - [Initial value]: -
- *domain_name*
- [Setting value]:

Setting value	Explanation
<i>domain_name</i>	Domain name to be notified with DNSSL option

- [Initial value]: -
- *option=value* : column with NAME=VALUE
- [Setting value]:

Name	VALUE	Explanation
lifetime	Seconds, infinity	Time of DNS server (0..4294967294 seconds). infinity indicates that the DNS server can be used indefinitely.

- [Initial value]:
 - lifetime = **ipv6 interface** rtadv send command router ads maximum interval (max-rtr-adv-interval) of 3 Double

Description

Define the DNSSL options to be distributed in router advertisements. To actually advertise, it is necessary to set the dnssl option of the **ipv6 interface rtadv send command**.

Up to three *domain_names* can be specified.

[Notes]

Can be specified in RTX3510 Rev.23.01.02 or later. Can be specified in RTX8300 Rev.15.02 or later. RTX1220 Rev.15.04.07 以降で指定可能。 Can be specified in RTX830 Rev.15.02.30 or later.

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX840, RTX830

25.3.6Defining route information options to be distributed in router advertisements

[Format]

ipv6 nd ra-route-info *route_info_id* *prefix/prefix_len* [*option=value*]

no ipv6 nd ra-route-info *route_info_id* [...]

[Setting value and initial value]

- *route_info_id*
 - Setting value: Route information option number (1..21474836)
 - [Initial value]: -
- *Prefix*
 - Setting value: Prefix
 - [Initial value]: -
- *prefix_len*
 - Setting value: Prefix length
 - [Initial value]: -
- *Column with option=value* : NAME=VALUE
- [Setting value]:

NAME	VALUE	Explanation
prf_flag	high、medium、low	Route Preference flag. Setting indicating the priority of a route.
lifetime	Seconds, infinity	Effective time of the route information (0..4294967294 seconds). infinity indicates that the route information can be used indefinitely.

- [Initial value]:
 - prf_flag = medium
 - lifetime = **ipv6** interface rtadv send command Router advertisement maximum interval (max-rtr-adv-interval) of 3
Double

[Explanation]

Define route information options to be distributed in router advertisements. To actually advertise, it is necessary to set the route-info option of the **ipv6 interface rtadv send** command.

[Notes]

RTX3510 Rev.23.01.01 or earlier, RTX1300 Rev.23.00.11 or earlier, RTX1220 Rev.15.04.06 or earlier, and RTX830 Rev.15.02.30 or later
Cannot be used before

[Applicable model]

vRX Sakura Cloud Edition, RTX3510, RTX1300, RTX1220, RTX840, RTX830

25.4Route control

25.4.1Adding route information of IPv6

[Format]

ipv6 route *network* gateway *gateway* [*parameter*] [*gateway gateway* [*parameter*]]
no ipv6 route *network* [*gateway*...]

[Setting value and initial value]

- *network*
- [Setting value]:

Setting value	Explanation
IPv6 address/prefix length	Host to send to
Default	Default route

- [Initial value]: -
- *gateway*: Gateway
- [Setting value]:
 - IP address % Scope identifier
 - pp *peer_num* [*dlci=dlci*]: Route to the PP interface. If "dlci=dlci" is specified, Route to DLCI
 - *peer_num*
 - Counterpart number
 - anonymous
 - pp anonymous *name=name*

Setting value	Description
<i>name</i>	Name by PAP/CHAP

- Ra *interface*

Setting value	Description
<i>interface</i>	LAN interface name and bridge interface name operating as RA client when using the default gateway determined by RA (valid only when the destination is Default)

- dhcp *interface*

Setting value	Description
<i>interface</i>	LAN interface name and bridge interface name operating as a DHCP client when using the default gateway given by DHCP (valid only when the destination is Default)

- *tunnel_num*: Route to tunnel interface
- LOOPBACK interface name, NULL interface name
- [Initial value]: -
- *parameter*: The following parameters can be set multiple times separated by spaces
- [Setting value]:

Setting value	Description
<i>filter number</i> [<i>number..</i>]	Specifying filter-type routes • <i>number</i> • Filter number (1..21474836) (can be set multiple times separated by spaces)
<i>dpi number</i> [<i>number..</i>]	Specifying filter-type routes • <i>number</i> • DPI filter number (1..2147483647) (can be set multiple times separated by spaces)
<i>metric metric</i>	Metric specification • <i>metric</i> • Metric value (1..15) • If omitted, 1
<i>hide</i>	Optional only when the output interface is a LAN interface, PP interface or TUNNEL interface, meaning that the route is valid only when a line is connected

- [Initial value]: -

[Explanation]

IPv6 route information is added.

For models with multiple LAN interfaces, it is necessary to specify the interface by scope identifier. The LAN interface name is used as the scope identifier. For models with one LAN interface, if the scope identifier is omitted, it is treated as if LAN1 was specified.

When a filter-type route is specified as a *gateway* parameter, filters are applied in the order described, and a suitable gateway is selected. When there is no suitable gateway or when no gateway for which a filter-type route is specified is described, a gateway for which a filter-type route is not specified is selected. When there is also no gateway for which a filter-type route is not specified, processing is continued assuming that the route does not exist. When multiple gateways for which a filter-type route is not specified are described, selection of the route is determined by round robin at the time when those routes are used.

Note that since the LOOPBACK interface and the NULL interface are always in the up state, the hide option can be specified, but it has no meaning.

[Notes]

The *dlci=* option of the PP interface can be specified for RTX5000 and RTX3500.

The *ra interface* is available for vRX Amazon EC2 version, vRX VMware ESXi version, RTX5000, RTX3500, RTX1300 Rev.23.00.04 or earlier,

It cannot be specified for RTX1220 Rev.15.04.04 or earlier, RTX1210, and RTX830 Rev.15.02.26 or earlier.

The bridge interface cannot be specified for vRX Amazon EC2 version and RTX5000/RTX3500 Rev.14.00.11 or earlier. The filter option cannot be specified for vRX Amazon EC2 version, vRX VMware ESXi version, RTX5000, RTX3510 Rev.23.01.01 or earlier, RTX3500, RTX1300 Rev.23.00.11 or earlier, RTX1220 Rev.15.04.05 or earlier, RTX1210, and RTX830 Rev.15.02.29 or earlier. The *dpi* option can be specified for RTX1300 Rev.23.00.12 or later and RTX830 Rev.15.02.30 or later.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.4.2 Setting whether to log when there is a change in IPv6 route information

[Format]

ipv6 route change log *log*
no ipv6 route change log [*log*]

[Setting value and initial value]

- log*
- [Setting value]:

Setting value	Description
on	Logging IPv6 route changes
off	Do not log IPv6 route changes

- [Initial value]: off

[Explanation]

Whether to log when there is a change in IPv6 route information is set. Logs are recorded at the INFO level.

[Notes]

Not available with RTX1300 Rev. 23.00.04 or earlier, RTX1220 Rev. 15.04.03 or earlier, and RTX830 Rev. 15.02.26 or earlier

[Applicable model]

vRX Sakura Cloud Edition, RTX3510, RTX1300, RTX1220, RTX840, RTX830

25.5 RIPng

25.5.1 Setting up RIPng usage

[Format]

no ipv6 rip use *use*
no ipv6 rip use

[Setting value and initial value]

- Use*
- [Setting value]:

Setting value	Description
on	Using RIPng
off	No RIPng

- [Initial value]: off

[Explanation]

Setting whether to use RIPng

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.5.2 Setting up sending policy for RPng in interface

[Format]

ipv6 interface rip send *send*
ipv6 pp rip send *send*
ipv6 tunnel rip send
send no ipv6 interface
rip send no ipv6 pp rip
send
no ipv6 tunnel rip send

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *send*
 - [Setting value]:

Setting value	Description
on	Sending RIPng
off	No RIPng

- [Initial value]: on

[Explanation]

Setting up sending policy for RIPng

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.5.3 Setting up sending policy for RPng in interface

[Format]

```

ipv6 interface rip receive receive
ipv6 pp rip receive receive
ipv6 tunnel rip receive
receive no ipv6 interface rip
receive no ipv6 pp rip
receive
no ipv6 tunnel rip receive

```

[Set value and initial value]

- *interface*
 - [Set value]: LAN interface name
 - [Initial value]: -
- *receive*
 - [Set value]:

Set value	Description
on	Process received RIPng packets
off	Ignore received RIPng packets

- [Initial value]: on

[Explanation]

Set the reception policy of RIPng.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.5.4 Set the number of hops added for RIPng

[Format]

```

ipv6 interface rip hop direction hop
ipv6 pp rip hop direction hop
no ipv6 interface rip hop direction
no ipv6 pp rip hop direction

```

[Set value and initial value]

- *interface*
 - [Set value]: LAN interface name
 - [Initial value]: -

- *direction*
 - [Set value]:

Set value	Description
in	Add when receiving
out	Add when receiving

- [Initial value]: -
- *hop*
 - [Set value]: Number of hops added (0..15)
 - [Initial value]: 0

[Explanation]

Set the number of hops added to the metric of RIPng sent and received by the PP interface.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.5.5Set up a reliable RPng gateway in the interface

[Format]

```

ipv6 interface rip trust gateway [except] gateway [gateway...]
ipv6 pp rip trust gateway [except] gateway [gateway...]
no ipv6 interface rip trust gateway [[except] gateway [gateway...]]
no ipv6 pp rip trust gateway [[except] gateway [gateway...]]

```

[Set value and initial value]

- *interface*
 - [Set value]: LAN interface name
 - [Initial value]: -
- *gateway*
 - [Set value]: IPv6 address
 - [Initial value]: -

[Explanation]

Set up a reliable RIPng gateway.

If the except keyword is not specified, the listed gateways are considered trustworthy and only RIPs from them are received.

If the except keyword is specified, only RIPs from other gateways except for the gateways listed are received as trustworthy gateways.

Up to 10 *gateways* can be specified.

[Applicable model]

[Settings] vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.5.6[Settings] Setup filtering for routes sent and received by RIPng

[Format]

```

ipv6 interface rip filter direction filter_list [filter_list...]
ipv6 pp rip filter direction filter_list [filter_list...]
ipv6 tunnel rip filter direction filter_list
[filter_list...] no ipv6 interface rip filter direction
no ipv6 pp rip filter direction
no ipv6 tunnel rip filter direction

```

[Settings and initial values]

- *interface*
 - [Settings]: LAN interface name
 - [Initial values]: -

- *direction*
- [Settings]:

Settings	Description
in	Targeting inward packets
out	Targeting outward packets

- [Initial values]: -
- *filter_list*
- [Settings]: Filter number
- [Initial values]: -

[Explanation]

Setup filters to be applied to RIPng packets sent and received by the interface.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.5.7 Setting operation of RPng on the PPside when connecting a line

[Format]

```
ipv6 pp rip connect send action
no ipv6 pp rip connect send
```

[Settings and initial values]

- *action*
- [Settings]:

Settings	Description
None	Do not send RIPng
Interval	Sending RIPng at the time interval set by the ipv6 pp rip connect interval command
Update	Sending RIPng only when route information changes

- [Initial values]: update

[Explanation]

Setup conditions for sending out RIPng for a selected party when connecting a line.

[Configuration Example]

```
# ipv6 pp rip connect interval 60
# ipv6 pp rip connect send interval
```

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.5.8 Setting time interval for sending out RPng on the PPside when connecting a line

[Format]

```
ipv6 pp rip connect interval time
no ipv6 pp rip connect interval
```

[Settings and initial values]

- *time*
- Settings: Number of seconds (30..21474836)
- [Initial values]: 30

[Explanation]

Set time interval for sending out RIPng for a selected party when connecting a line.

[Configuration Example]

```
# ipv6 pp rip connect interval 60
# ipv6 pp rip connect send interval
```

[Applicable model]

[Settings] vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.5.9 Setting the behavior of RPng on the PPside when the line is disconnected**[Settings]**

```
ipv6 pp rip disconnect send action
no ipv6 pp rip disconnect send
```

[Settings and initial values]

- *action*
- [Settings]:

Settings	Description
None	Do not send RPng
Interval	Sending RPng at the time interval set by the ipv6 pp rip connect interval command
Update	Sending RPng only when route information changes

- [Initial value]: none

[Explanation]

Setting conditions for sending RPng when the line is disconnected for a selected party

[Configuration Example]

```
# ipv6 pp rip disconnect interval 1800
# ipv6 pp rip disconnect send interval
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.5.10 Setting the time interval for sending RPng on the PPside when the line is disconnected**[Settings]**

```
ipv6 pp rip disconnect interval time
no ipv6 pp rip disconnect interval
```

[Settings and initial values]

- *time*
- [Settings]: Number of seconds (30..21474836)
- [Initial value]: 3600

[Explanation]

Setting the time interval for sending RPng when the line is disconnected for a selected party

[Configuration Example]

```
# ipv6 pp rip disconnect interval 1800
# ipv6 pp rip disconnect send interval
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.5.11 Setting whether to keep the route by RPng when the line is disconnected**[Settings]**

```
ipv6 pp rip hold routing hold
no ipv6 pp rip hold routing
```

[Settings and initial values]

- *Settings*
- Settings

Settings	Description
on	Holds
off	Holds

- [Initial value]: off

[Explanation]

Set whether to hold the route obtained by RIPng from the PP interface when the line is disconnected.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.5.12 Setting the priority of the route by RIPng

[Settings]

ipv6 rip preference *preference*

no ipv6 rip preference [*preference*]

[Settings and initial values]

- *preference*
 - Settings: Priority of the route by RIPng (1-2147483647)
 - Settings: 1000

[Description]

The priority of a route by RIPng is set. The priority is expressed by a numerical value of 1 or more, and the higher the number, the higher the priority.

When a route obtained by multiple protocols such as OSPFv3 and static differs, the route with the higher priority is adopted. When the priority is the same, the route adopted earlier in time becomes effective.

[Notes]

The priority of a static route is fixed at 10000.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.6 VRRPv3 configuration

25.6.1 VRRPv3 configuration for each interface

[Format]

ipv6 interface vrrp vrid *ipv6_address* [*priority=priority*] [*preempt=preempt*] [*auth=auth*] [*advertise-interval=time1*] [*down-interval=time2*]

no ipv6 interface vrrp vrid [*vrid...*]

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *vrid*
 - [Setting value]: VRRPv3 group ID (1..255)
 - [Initial value]: -
- *ipv6_address*
 - [Setting value]: IPv6 address of virtual router
 - [Initial value]: -
- *priority*
 - [Setting value]: Priority (1..254)

- [Initial value]: 100
- *preempt*: Preempt mode
- [Setting value]:

Setting value	Explanation
on	Use
off	Not used

- [Initial value]: on
- *auth*
 - [Setting value]: Text authentication string (8 characters or less)
 - [Initial value]: -
- *time1*
 - [Setting value]: Interval between VRRPv3 ads (1..60 seconds)
 - [Initial value]: 1
- *time2*
 - setting value: Time until the master determines that it is down (3..180 seconds)
 - [Initial value]: 3

[Description]

Set to use the specified VRRPv3 group.

Routers belonging to the same VRRPv3 group must match the IPv6 address of the VRID and virtual router. Actions when these differ can not be predicted.

If the *auth* parameter is not specified, it operates as no authentication.

The *time1* and *time2* parameters set the interval between when the master sends a VRRPv3 ad and when the backup monitors it to determine that it is down. In networks with a lot of traffic, if these values are set longer than the initial value, operations may be stabilized. These values must match for all VRRPv3 routers.

[Notebook]

The setting of *priority* and *preempt* parameters is ignored when specifying the address given to its own LAN interface as the IPv6 address of the virtual router. In this case, priority is the highest 255, and it always operates in preempt mode.

Not available for RTX5000 / RTX3500 Rev.14.00.17 or earlier.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.6.2 Shutdown trigger setting

Format

```

ipv6 interface vrrp shutdown trigger vrid interface
ipv6 interface vrrp shutdown trigger vrid pp peer_num [dlci=dlci]
ipv6 interface vrrp shutdown trigger vrid tunnel tunnel_num
ipv6 interface vrrp shutdown trigger vrid route network [nexthop]
no ipv6 interface vrrp shutdown trigger vrid interface
no ipv6 interface vrrp shutdown trigger vrid pp peer_num
[...] no ipv6 interface vrrp shutdown trigger vrid tunnel
tunnel_num no ipv6 interface vrrp shutdown trigger vrid
route network

```

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *vrid*

- [Setting value]: VRRPv3 group ID (1..255)
- [Initial value]: -
- *peer_num*
 - [Setting value]: Destination information number
 - [Initial value]: -
- *dlci*
 - [Setting value]: DLCI number
 - [Initial value]: -
- *tunnel_num*
 - [Setting value]: Tunnel interface number
 - [Initial value]: -
- *network*
 - [Setting value]:
 - IPv6 Prefix/Prefix length
 - [Setting value]: Default
 - [Initial value]: -
- *nexthop*
 - [Setting value]:
 - Interface name
 - IPv6 address
 - [Initial value]: -

[Explanation]

When operating as a master router in the set VRRPv3 group, it is set to shut down according to the specified condition.

Format	Description
LAN interface format	When the specified LAN interface links down or when down is detected by lan keepalive , it shuts down.
pp format	When communication becomes impossible on a line corresponding to the specified destination information number, it shuts down. When communication becomes impossible, it is a case where layer 1 drops due to cable disconnection or the like, and the following cases. • When the line is an ISDN line, if no call is connected • When the line is a leased line, it is determined that the communication partner has fallen due to LCP keepalive • When the line is a frame relay and "dlci=<i>dlci</i>" is specified, it is determined that the DLCI number specified by the PVC status check procedure cannot communicate • When down is detected by pp keepalive use setting
tunnel format	When the specified tunnel interface is down due to the following conditions, it shuts down. • When down is detected by pptp keepalive use setting in a pptp tunnel • When down is detected by pptp keepalive use setting in any of the tunnels of L2TP/IPsec, L2TPv3, and L2TPv3/IPsec • When down is detected by pptp keepalive use setting in a pptp tunnel • When down is detected by pptp keepalive use setting in a pptp tunnel

Form	Description
route format	When the specified route does not exist in a route table or is not suitable for an interface specified by <i>nexthop</i> or a gateway specified by an IPv6 address, it shuts down. When <i>nexthop</i> is omitted, it does not shut down as long as the route faces any destination.

[Notes]

RTX5000 / RTX3500 Rev.14.00.17 or earlier cannot be used.

Tunnel interface cannot be used with RTX5000 / RTX3500 Rev.14.00.31 or earlier, RTX1210 Rev.14.01.27 or earlier, and RTX830 Rev.15.02.02 or earlier

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

25.7 Filter setting

25.7.1 IPv6 filter definition

Format

ipv6 filter *filter_num* *pass_reject* *src_addr*[/*prefix_len*] [*dest_addr*[/*prefix_len*] [*protocol* [*src_port_list* [*dest_port_list*]]]]

no ipv6 filter *filter_num* [*pass_reject*]

Setting value and initial value

- *filter_num*
 - [Set value]: Static filter number (1..21474836)
 - [Set value]: -
 - *pass_reject*
 - [Set value]: Filter type (according to **ip filter** command)
 - [Set value]: -
 - *src_addr*: IPv6 address where IPv6 packet starts
 - [Set value]:
 - IPv6 address
 - Static or dynamic IPv6 address
 - Multiple FQDNs can be set as separators.
 - FQDN
 - Arbitrary character string (within 255 single-byte characters. / : cannot be used. , cannot be used because it is used as a separator)
 - An FQDN starting with * judges strings after * as backward matching conditions. For example, *.example.co.jp matches www.example.co.jp, mail.example.co.jp, etc.
 - Multiple FQDNs can be set as separators.
 - map-e
 - Keywords representing global IPv6 addresses generated by MAP-E's map rule and configured in the MAP-E tunnel
 - hb46pp
 - Keywords representing global IPv6 addresses obtained by the domestic standard provisioning method of IPv6 migration technology
 - Mnemonic representing application name (according to **ip filter** command)
 - * (for all IPv6 addresses)
 - [Set value]: -
- *prefix_len*
 - [Set value]: Prefix length
 - [Set value]: -
- *dest_addr*: IPv6 packet end point IPv6 address

- [Set value]:
 - Same format as *src_addr*
 - Same as one * if omitted
- [Set value]: -
- *protocol* : packet type to filter (according to **ip filter** command)
- [Set value]:

icmp-nd	Keywords specifying packets related to neighbor search (ICMPv6 packets whose TYPE is one of 133, 134, 135, or 136)
ICMP4	Keywords specifying ICMPv4 packets
icmp	Keywords specifying ICMPv4 packets
icmp6	

- [Set value]: -
- *src_port_list*
 - Set value: TCP/UDP source port number or ICMPv6 type (according to **ip filter** command)
 - [Set value]: -
- *dest_port_list*
 - Set value: TCP/UDP destination port number or ICMPv6 code
 - [Set value]: -

[Explanation]

Define an IPv6 filter

[Notes]

Packets related to neighbor search mean the following four.

- 133: Router Solicitation
- 134: Router Advertisement
- 135: Neighbor Solicitation
- 136: Neighbor Advertisement

src_addr and *dest_addr* can also mix IPv6 addresses, FQDNs, map-e, hb46pp, and mnemonic representing application names.

Specifying an FQDN for *src_addr* and *dest_addr* is not possible for vRX Amazon EC2 version, vRX VMware ESXi version, RTX5000/RTX3500 Rev. 14.00.31 or earlier, RTX1220 Rev. 15.04.03 or earlier, RTX1210 Rev. 14.01.40 or earlier, and RTX830 Rev. 15.02.23 or earlier

Possible

By specifying an FQDN for *src_addr* and *dest_addr*, filtering can be performed for servers that are not fixed IP addresses or servers that have multiple fixed IP addresses against one FQDN. When using an FQDN, the router itself operates as a DNS recursive server, and terminals under the router must specify this unit as a DNS server. When communication that matches the specified FQDN occurs, information on IPv6 addresses corresponding to the set FQDN is retained. The retained period can be specified with the **ip filter fqdn timer** command.

Specifying map-e for *src_addr* and *dest_addr* is not possible for vRX series, RTX5000/RTX3500 Rev. 14.00.31 or earlier, RTX1210 Rev. 14.01.39 or earlier, and RTX830 Rev. 15.02.19 or earlier.

Specifying hb46pp for *src_addr* and *dest_addr* is not possible for vRX series, RTX5000, RTX3510 Rev. 23.01.01, RTX3500, RTX1300 Rev. 23.09.7 or earlier, RTX1220 Rev. 15.09.7 or earlier, RTX1210, and RTX830 Rev. 15.09.7 or earlier. Mnemonic designations representing application names for *src_addr* and *dest_addr* are not possible for vRX series, RTX5000,

Not possible with RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, and RTX830.

For the mnemonic representing the application name, the mnemonic described in the communication destination list is designated. In the following conditions, the mnemonic representing the application name is not evaluated.

- When the LBO state is not "normally operating"
- When the specified mnemonic is not included in the communication destination list

[Configuration Example]

- Record IPv6 Packet Too Big sent and received in PP1

```
# pp select 1
# ipv6 pp secure filter in 1 100
# ipv6 pp secure filter out 1 100
# pp enable 1
# ipv6 filter 1 pass-log * * icmp6 2
# ipv6 filter 100 pass * *
```

- Packets of Microsoft 365 and Windows Update are sent via PP1, others via TUNNEL1

```
# ipv6 route default gateway pp 1 filter 1 gateway tunnel 1
# ipv6 filter 1 pass * @m365,@windows_update * *
```

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.7.2Applying IPv6 Filters**[Format]**

ipv6 interface secure filter direction [filter_list...] [dynamic filter_list]

ipv6 pp secure filter direction [filter_list...] [dynamic filter_list]

ipv6 tunnel secure filter direction [filter_list...] [dynamic filter_list] no ipv6 interface secure filter direction

no ipv6 pp secure filter direction

no ipv6 tunnel secure filter direction

[Setting value and initial value]

- interface*
 - [Setting value]: LAN interface name, LOOPBACK interface name, NULL interface name, bridge interface name
 - [Initial value]: -
- direction*
 - [Setting value]:

Setting value	Description
in	Filtering received packets
out	Filtering packets to send

- [Initial value]: -
- filter_list*
 - [Setting value]: A sequence of filter numbers separated by spaces (up to 129 as the sum of the number of static filters and dynamic filters)
 - [Initial value]: -
- dynamic* : Describe the dynamic filter number after the keyword
 - [Initial value]: -

[Description]

Applying IPv6 filters to the interface

[Notes]

Dynamic filters cannot be used with the LOOPBACK and NULL interfaces.

Direction cannot be specified as 'in' with the NULL interface.

Bridge interfaces cannot be specified with vRX Amazon EC2 version and RTX5000/RTX3500 Rev.14.00.11 or earlier.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.7.3Defining IPv6 dynamic filters

[Format]

```
ipv6 filter dynamic dyn_filter_num srcaddr[/prefix_len] dstaddr[/prefix_len] protocol [option ...]
ipv6 filter dynamic dyn_filter_num srcaddr[/prefix_len] dstaddr[/prefix_len] filter filter_list [in filter_list] [out filter_list]
[option ...]
no ipv6 filter dynamic dyn_filter_num [srcaddr ...]
```

[Setting value and initial value]

- *dyn_filter_num*
 - [Setting value]: Dynamic filter number (1..21474836)
 - [Initial value]: -
- *srcaddr* : IPv6 address of the start of an IPv6 packet
 - [Setting value]:
 - Same format as *src_addr* in the **ipv6 filter** command
 - Same as one * if omitted
 - [Initial value]: -
- *prefix_len*
 - [Setting value]: Prefix length
 - [Initial value]: -
- *dstaddr* : IPv6 packet end point IPv6 address
 - [Setting value]:
 - Same format as *srcaddr*
 - If omitted, it is the same as one *.
 - [Setting value]: -
- *protocol*: The mnemonic of a protocol
 - [Setting value]:
 - tcp/udp/ftp/tftp/domain/www/smtp/pop3/telnet
 - echo/discard/daytime/chargen/ftp/ssh/telnet/smtp/time/whois/dns/domain/dhcps/
 - dhcpc/tftp/gopher/finger/http/www/pop3/sunrpc/ident/nntp/ntp/ms-rpc/
 - netbios_ns/netbios_dgm/netbios_ssn/imap/snmp/snmptrap/bgp/imap3/ldap/
 - https/ms-ds/ike/rlogin/rwho/rsh/syslog/printer/rip/ripng/
 - dhcpv6c/dhcpv6s/ms-sql/radius/l2tp/pptp/nfs/msblast/ipsec-nat-t/sip/
 - ping/ping6/tcp/udp
 - submission
 - [Setting value]: -
- *filter_list*
 - [Setting value]: List of filter numbers registered with the **ipv6** filter command
 - [Setting value]: -
- *option*
 - [Setting value]:
 - syslog=switch

Setting value	Description
on	Keep connection history in syslog
off	Do not keep connection history in syslog

- timeout=*time*

Setting value	Description
time	Number of seconds until connection information is released when data stops flowing

- [Setting value]:
 - syslog=on

[Explanation]

A dynamic filter of IPv6 is defined. In the first format, an application name registered with a router in advance is specified. In the second format, a user describes access control rules. After the keywords filter, in, and out, the filter number defined with the **ipv6 filter** command is set.

When a connection (trigger) corresponding to the filter described after the filter keyword is detected, subsequent connections corresponding to the filters described after the in and out keywords are passed. The in keyword controls access in the opposite direction to the trigger direction, and the out keyword controls access in the same direction as the dynamic filter. The IP address of the **ipv6 filter** command is ignored. The arguments pass/reject are also ignored.

It may be possible to handle applications that are not described here by defining them using the filter keyword. Especially, it is easy to handle protocols that do not dynamically change port numbers, such as snmp.

It may be handled by setting tcp or udp. In particular, protocols that do not dynamically change port numbers, such as telnet, can be handled by specifying tcp.

[Notes]

src_addr and dstaddr can also mix mnemonics representing IP addresses, FQDNs, map-e, hb46pp, and application names.

The specification of FQDNs to src_addr and dstaddr is not possible for vRX Amazon EC2 version, vRX VMware ESXi version, RTX5000/RTX3500 Rev. 14.00.31 or earlier, RTX1220 Rev. 15.04.03 or earlier, RTX1210 Rev. 14.01.40 or earlier, and RTX830 Rev. 15.02.23 or earlier.
Possible.

The specification of map-e to src_addr and dstaddr is not possible for vRX series, RTX5000 Rev. 14.00.31 or earlier, RTX3500 Rev. 14.00.31 or earlier, RTX1210 Rev. 14.01.39 or earlier, and RTX830 Rev. 15.02.19 or earlier.

The specification of map-e to src_addr and dstaddr is not possible for vRX series, RTX5000, RTX3510 Rev. 23.01.01, RTX3500, RTX1300 Rev. 23.00.11 or earlier, RTX1220 Rev. 15.04.06 or earlier, RTX1210, and RTX830 Rev. 15.02.30 or earlier.

The specification of mnemonics representing application names to src_addr and dstaddr is not possible for vRX series, RTX5000, not possible for RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, and RTX830.

The mnemonics representing application names are specified in the communication destination list. In the following states, the mnemonics representing application names are not evaluated.

- The LBO state is not "normal operation"
- The specified mnemonics are not included in the communication destination list

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.8 Configuring IPv6 Multicast Packet Forwarding

It provides the functions of MLDv1, MLDv2, and MLD proxies. For MLDv1 and MLDv2, it supports both the host side and router side, and the functions of the host and router can be used separately for each interface. MLDv1 corresponds to RFC2710, and MLDv2 corresponds to draft-vida-mldv2-07.txt. The MLD proxy is a function that relays information of listeners existing in the downstream interface to the upstream interface, and is implemented based on draft-ietf-magma-igmp-proxy-04.txt.

A multicast packet transmitted by a specific terminal is duplicated and delivered to multiple terminals. A terminal that transmits a multicast packet is called a source, and a terminal that receives it is called a listener. In the following description, the multicast packet is simply written as a packet.

Packets sent by a source generally reach all listeners, but if you want to change the packets received by different listeners, you can divide the listeners into groups. Terminals belonging to the same group receive the same packets, and terminals belonging to different groups receive different packets. Each group is assigned a multicast address as an identifier.

The endpoint address of the IP header of the packet stores the multicast address corresponding to the group. Routers in the network look at this multicast address to see which group the packets are being forwarded to. Routers in the network have routing tables organized into groups, and distribute packets according to those routing tables. Routing tables are typically generated automatically by routing protocols such as PIM-SM, PIM-DM, and DVMRP.

The purpose of MLD (MulticastListenerDiscovery) is for a terminal to notify the multicast network of the group it joins.

Routers in the network send a message called a Query to the terminal. The terminal that receives the query sends a report back to the router. The report stores the multicast address of the group that the terminal joins. The router that receives the report reflects that information in routing. MLDv2 allows you to restrict the source of packets you receive, but uses FilterMode and SourceList to achieve this functionality. Filter modes include INCLUDE and EXCLUDE, where INCLUDE enumerates allowed sources, and EXCLUDE enumerates disallowed sources.

For example, in the following cases, only packets originating from 2001:x:x:x:1 and 2001:x:x:x:2 are forwarded.

- Filter Mode : INCLUDE
- Source Lists: {2001:x:x:x:1, 2001:x:x:x:2 }

MLD messages cannot, in principle, cross the router. Therefore, if a router is present between the terminal and the multicast network, the router must have the function of an MLD proxy. A router with the function of an MLD proxy sends a query to the LAN side and receives a report from the LAN side. It also forwards the information contained in that report to the WAN side.

25.8.1Setting Up MLD Behavior

Format

```
ipv6 interface mld type [option ...]
ipv6 pp mld type [option ...]
ipv6 tunnel mld type [option ...]
no ipv6 interface mld [type [option ...]]
no ipv6 pp mld [type [option ...]]
no ipv6 tunnel mld [type [option ...]]
```

Setting Up Up Up Up Up Up Up Up Up Down Down Down Down Down Down Down Down

- interface
 - Setting Up Up Up Up Up Up Up Up Down Down Down down down down down down down up up up up up
 - Initial Values: -
- Type : How MLD Behavior Works
 - Setting Up Up Up Up Up Up Up Up Up Down Down Down Down Down

Setting Up Up Up Up Up Up Up Up Up Down Down Down	Explanation
off	MLD Behavior Doesn't Work
router	Operating as an MLD Router
host	Operating as an MLD Host

- Initial Values: off
- Option : Option
 - Setting Up Up Up Up Up Up Up Up Down Down Down Down Down Down Down Down
 - Version=version
 - MLD Versions

Setting Up Up Up Up Up Up Up Up Up Up Up	Explanation
1	MLDv1
MLDv2	MLDv2
MLDv2	Both MLDv1 and MLDv2 are supported. (MLDv1 Compatibility Mode)

- Syslog=switch
 - Whether Detailed Information Should be Logged to Syslog

Setting Up Up Up Up Up Up Up Up Up Up Up	Explanation
on	Display
off	Do not show

- robust-variable=VALUE(1..10)

- Set the value of Robust Variable specified by MLD.
- `report-link-local-group=switch`
- Whether to process link-local scoped groups.

Setting value	Description
on	Enables report reception for link-local scoped groups when operating as an MLD router. Enables report transmission for link-local scoped groups when operating as an MLD host.
off	Disables report reception for link-local scoped groups.

- [Initial value]:
 - version=1,2
 - syslog=off
 - robust-variable=2
 - report-link-local-group=off

Description

Static configuration of MLD

[Notes]

The report-link-local-group option cannot be specified for RTX5000 / RTX3500 Rev. 14.00.20 or earlier and RTX1210 Rev. 14.01.15 or earlier.

Applicable model

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.8.2 Static configuration of MLD

Format

```

ipv6 interface mld static group [filter_mode [source...]]
ipv6 pp mld static group [filter_mode [source...]]
ipv6 tunnel mld static group [filter_mode [source...]]
no ipv6 interface mld static group [filter_mode source...]
no ipv6 pp mld static group [filter_mode source...]
no ipv6 tunnel mld static group [filter_mode source...]

```

Setting value and initial value

- *interface*
 - Setting value: Name of LAN interface
 - [Initial value]: -
- *group*
 - Setting value: Multicast address of the group
 - [Initial value]: -
- *filter_mode*: Filter mode
 - Setting value:

Setting value	Description
include	"EXCLUDE" mode for MLD
exclude	"EXCLUDE" mode for MLD

- [Initial value]: -
- *source*
 - Setting value:

Setting value	Description
IPv6 address	Multicast packet source address

Setting value	Description
Omitted	It works the same for all source addresses when omitted.

- [Initial value]: -

Description

It is assumed that a listener always exists for the specified group. This command is set when there is no listener that supports MLD. *Filter_mode* and *source* limit the source of multicast packets. When include is specified as *filter_mode*, the source to be received is listed as *source*. When *source* is omitted, requests from all sources are not received.

When exclude is specified as *filter_mode*, requests from all sources that are not desired to be received are listed as *source*. If *source* is omitted, requests from all sources are received.

[Notes]

Listeners set by this command are notified by the interface where host is set by the **ipv6** interface *mld* command. If this interface uses MLDv1, values of *filter_mode* and *source* are ignored.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

25.9 Neighbor request

25.9.1 Neighbor request triggered by duplicate address check is set.

[Format]

ipv6 nd ns-trigger-dad on [option=*value*]

ipv6 nd ns-trigger-dad off

no ipv6 nd ns-trigger-dad [...]

[Setting value and initial value]

- on
 - Neighbor request is made.
 - [Initial value]: -
- off
 - Neighbor request is not made.
 - [Initial value]: -
- *option=value* **column**. MLD operation method
 - [Setting value]:

<i>option</i>	<i>value</i>	Description
na-proxy	all	After making a neighbor request, all neighbor advertisements to the source of duplicate address check are proxied.
	discard-one-time	After making a neighbor request, neighbor advertisements to the source of duplicate address check are discarded only once, and then proxied.

- [Initial value]: na-proxy=all

[Initial Setting]

ipv6 nd ns-trigger-dad off

[Notes]

In an RA proxy, when receiving a neighbor request of duplicate address check from downstream, it is set whether or not to transmit a neighbor request with the global address as a transmission source upstream.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 26

OSPFv3

26.1 Enable setting of OSPFv3

[Format]

ipv6 ospf configure refresh

[Explanation]

Enable setting of OSPFv3. After changing the OSPFv3-related settings, restart the router or use this command to execute.

[Notes]

When this command is input, if any of the following is true, setting of OSPFv3 is not valid.

- Router ID is not set
- Area is not set
- None of the interfaces belong to an area
- There is no area through which a virtual link passes
- No interface belongs to an area through which a virtual link passes

If this command is input while setting of OSPFv3 is already valid, the setting is read again from the initial state. Therefore, route information held by OSPFv3 and route information distributed to other protocols are temporarily discarded, and operation starts from the initial state.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

26.2 Use setting of OSPFv3

[Format]

ipv6 ospf use use

no ipv6 ospf use [use]

[Setting value and initial value]

- *Use*
- [Setting value]:

Setting value	Description
on	Use OSPFv3
off	Do not use OSPFv3

- [Initial value]: off

[Explanation]

Sets whether to use OSPFv3.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

26.3 Router ID setting for OSPFv3

[Format]

ipv6 ospf router id router-id

no ipv6 ospf router id [router-id]

[Setting value and initial value]

- *router_id*
- [Setting value]: IPv4 address notation (0.0.0.0 is not allowed)

- [Initial value]: -

[Explanation]

Router ID is set.

[Notes]

When the **ipv6 ospf configure refresh** command is input, if the router ID is not set by this command, primary IPv4 addresses given to interfaces are searched in the following order and the first found IPv4 address is used as the router ID.

- LAN interface (in order of decreasing number)
- LOOPBACK interface (in order of decreasing number)

If there is no interface to which a primary IPv4 address is given, the initial value is not set.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

26.4 OSPFv3 area setting

[Format]

ipv6 ospf area *area* [stub [cost=*cost*]]

no ipv6 ospf area *area* [stub [cost=*cost*]]

[Setting value and initial value]

- *Area*
 - [Setting value]:

Setting value	Description
backbone	Backbone area
Numbers equal to or greater than one (1...4294967295)	Non-backbone area
IPv4 address notation (0.0.0.0 is not allowed)	Non-backbone area

- [Initial value]: -
- *cost*
 - Setting value: Default route cost (0-16777215)
 - [Initial value]: 0

[Explanation]

OSPFv3 area setting

Specifying a stub keyword indicates that the area is a stub area. *Cost* is a number equal to or greater than zero and is used as the default route cost advertised by an area boundary router in the area. Advertising of the default route is not performed unless *cost* is specified.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

26.5 Route advertisement to area

[Format]

ipv6 ospf area network *area* *ipv6_prefix/prefix_len* [restrict]

no ipv6 ospf area network *area* *ipv6_prefix/prefix_len* [restrict]

[Setting value and initial value]

- *Area*
 - [Setting value]:

Setting value	Description
backbone	Backbone area
Numbers equal to or greater than one (1...4294967295)	Non-backbone area
IPv4 address notation (0.0.0.0 is not allowed)	Non-backbone area

- Initial value: -
- *ipv6_prefix/prefix_len*
 - Setting value: IPv6 prefix
 - Initial value: Subnet range is not set

Description

When an area boundary router advertises a route to another area, the route within the range of the subnet specified by this command is advertised as a single subnet route. If a restrict keyword is specified, the route within the range does not advertise a summarized route either.

Applicable model

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

26.6 OSPFv3 area setting for the specified interface

Format

```

ipv6 interface ospf area area [parameters ...]
ipv6 pp ospf area area [parameters...]
ipv6 tunnel ospf area area [parameters...]
no ipv6 interface ospf area [area [parameters...]]
no ipv6 pp ospf area [area [parameters...]]
no ipv6 tunnel ospf area [area [parameters...]]
  
```

Setting value and initial value

- *interface*
 - Setting value: LAN interface name
 - Initial value: -
- *area*
 - Setting value:

Setting value	Description
backbone	Backbone area
Numbers equal to or greater than 1 (1...4294967295)	Non-backbone area
IPv4 address notation (0.0.0.0 is not allowed)	Non-backbone area

- Initial value: Interface does not belong to OSPF area
- *Parameters*
 - Setting value: Column with NAME=VALUE
 - Initial value:
 - type=broadcast(LAN interface setting)
 - type=point-to-point(PP interface setting, tunnel interface setting)
 - passive=Interface is not passive
 - cost=1(LAN interface setting), 1562(tunnel setting), pp depends on line speed
 - priority=1
 - retransmit-interval=5 seconds
 - hello-interval=1 second
 - hello-interval=10 seconds
 - dead-interval=40 seconds

description

Set the OSPFv3 area to which the specified interface belongs. The type parameter of NAME sets what type of link the interface connects to. In *parameters*, link parameters are set. Parameters are specified in the form of NAME=VALUE and have the following types:

NAME	VALUE	description
type	broadcast	broadcast type
	point-to-point	point-point type
passive		OSPFv3 packets are not sent to the interface. Set if there is no other OSPFv3 router on the interface.
cost	Cost (1...65535)	The cost of an interface is set. The initial value is determined by the type of interface and the line speed. If 1 is set for a LAN interface, 1562 for a tunnel interface, and S [kbit/s] for a PP interface, the line speed of the bound line is set by the following formula. For example, if it is set to 64 kbit/s, it is set to 1562, and if it is set to 1.536 Mbit/s it is set to 65. cost=100000/S
priority	Priority (0...255)	Priority when selecting a designated router is set. A router with a large value is selected as a designated router. If 0 is specified, it will not be selected as a designated router.
retransmit-interval	Seconds (1...65535)	The retransmission interval when sending LSA continuously is specified in seconds.
transmit-delay	Seconds	The time from when the state of the link changes to when the LSA is sent is specified in seconds.
hello-interval	Seconds (1...65535)	Set the interval between sending HELLO packets in seconds
dead-interval	Seconds (1...65535)	The time from when HELLO cannot be received from a neighboring router to when it is determined that the neighboring router is down is specified in seconds.

[Note]

About the type of the NAME parameter

Only broadcast can be set for a LAN interface as the type of the NAME parameter. Only point-to-point can be set for a PP interface using PPP or a tunnel interface.

About passive

Passive specifies when there are no other OSPFv3 routers on the link to which the interface is connected. When passive is specified, since the interface does not send OSPFv3 packets, useless traffic can be suppressed and malfunction can be prevented on the receiver side.

In the case of a LAN interface (interface with type=broadcast), the route to the link to which the interface is connected is not advertised to other OSPFv3 routers unless the **ipv6 interface ospf area** command is set. Therefore, for a LAN interface connecting to a link that does not use OSPFv3, an **ipv6 interface ospf area** command with passive is set so that the route to the link can be advertised to other OSPFv3 routers without using OSPFv3 on that link.

If the **ipv6 pp ospf area** command is not set for the PP interface, the route to the link to which the interface is connected is treated as an external route. Since it is an external route, it is necessary to set the **ipv6 ospf import** command to advertise to other OSPFv3 routers.

About hello-interval/dead-interval

The value of hello-interval/dead-interval must be the same value between all neighboring routers that can communicate directly from that interface. If a HELLO packet different from these parameters is received, it is ignored. If dead-interval is not specified, it is set to four times the value of hello-interval.

About instance IDs

The instance ID of this machine is always 0, and only packets with the same value are received when receiving OSPFv3 packets.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

26.7 Virtual link setting

Format

```
ipv6 ospf virtual-link router_id area [parameters ...]
```

```
no ipv6 ospf virtual-link router_id [area [parameters...]]
```

[Setting value and initial value]

- *router_id*
 - Setting value: Router ID of the other party of the virtual link
 - Initial value: -
- *area*: Area via
 - Setting value:

Setting value	Description
Numbers equal to or greater than 1 (1...4294967295)	Non-backbone area
IPv4 address notation (0.0.0.0 is not allowed)	Non-backbone area

- Initial value: -
- *Parameters*
 - Setting value: Column with NAME=VALUE
 - Initial value:
 - transmit-delay=5 seconds
 - transmit-delay=1 second
 - hello-interval=10 seconds
 - dead-interval=40 seconds

Description

A virtual link is set. A virtual link is set to a router specified by *router_id* via an area specified by *area*. *Parameters* allows setting *parameters* of the virtual link. Parameters are specified in the form of NAME=VALUE, and there are the following types.

NAME	VALUE	Description
retransmit-interval	Seconds (1...65535)	When sending LSA continuously, set the retransmission interval in seconds.
transmit-delay	Seconds (1...65535)	Set the time in seconds from when the state of the link changes until the LSA is sent.
hello-interval	Seconds (1...65535)	Set the transmission interval of a HELLO packet in seconds.
dead-interval	Seconds (1...65535)	Set the time in seconds until it is determined that the other party is down when the other party cannot receive HELLO from the other party.

[Notes]**About hello-interval/dead-interval**

The values of `hello-interval` and `dead-interval` must be the same between all neighboring routers that can communicate directly from that interface. If a HELLO packet whose value of these parameters is different from the set value is received, it is ignored.

About instance IDs

The instance ID of this machine is always 0, and when receiving an OSPFv3 packet, only packets with the same value are received.

About output interface

When a virtual link is set, a virtual link cannot be used unless a global address is given to an output interface to the area through which it passes.

Applicable model

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

26.8 Setting the priority of a route by OSPFv3

Format

```
ipv6 ospf preference preference
no ipv6 ospf preference [preference]
```

Setting value and initial value

- *preference*
 - Setting value: Priority of a route by OSPFv3 (1...2147483647)
 - [Default value]: 2000

Description

Setting the priority of a route by OSPFv3 The priority is expressed by a numerical value of 1 or more, and the higher the number, the higher the priority. When a route obtained by multiple protocols such as OSPFv3 and RIPv3 is different, the route with the higher priority is adopted. When the priority is the same, a route adopted earlier becomes effective in terms of time.

Notebook

The priority of a static route is fixed at 10000.

Applicable model

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

26.9 Setting whether to reflect the route received by OSPFv3 in the routing table

Format

```
ipv6 ospf export from ospf filter filter_num ...
no ipv6 ospf export from ospf [filter filter_num...]
```

Setting value and initial value

- *filter_num*
 - Setting value: Filter number of **ipv6 ospf export filter** command (1...2147483647)
 - Initial value: All routes are reflected in the routing table

Description

Setting whether to introduce the route received by OSPFv3 into the routing table. Filters are evaluated in the specified order, and only routes determined to be introduced by the first matched filter are introduced into the routing table.

Routes determined not to be introduced or routes without matching filters are not introduced.

If this command is not set, all routes are introduced into the routing table.

Notebook

This command does not affect the OSPFv3 link state database. That is, the behavior of exchanging information with other routers in OSPFv3 does not change regardless of how this command is set. Only whether the route calculated by OSPFv3 is actually used to route packets changes.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

26.10 Setting a filter to handle routes received by OSPFv3**[Format]**

```
ipv6 ospf export filter filter_num [nr] kind ipv6_prefix/prefix_len ...
```

```
no ipv6 ospf export filter filter_num [...]
```

[Setting value and initial value]

- *filter_num*
 - [Setting value]: Filter number (1...2147483647)
 - [Setting value]: -
- *nr*: How to interpret the filter
 - [Setting value]:

Setting value	Description
not	Introduce routes that do not correspond to IPv6 prefix
reject	Do not introduce routes that correspond to IPv6 prefix

- [Setting value]: -
- *kind*: How to interpret IPv6 prefix
 - [Setting value]:

Setting value	Description
include	Routes included in the specified IPv6 prefix (including IPv6 prefix itself)
Refine	Routes included in the specified IPv6 prefix (not including IPv6 prefix itself)
equal	Routes included in the specified IPv6 prefix

- [Setting value]: -
- *ipv6_prefix/prefix_len*
 - Setting value: IPv6 prefix
 - [Setting value]: -

Description

Filters to be applied when routes received by OSPFv3 from other OSPFv3 routers are introduced into a routing table are defined. Filters defined in this command have an effect only when specified in the *filter* section of the **ipv6 ospf export from ospf** command.

IPv6 prefix is set in *ipv6_prefix/prefix_len*. Multiple settings can be made and interpreted by the method specified in *kind*.

include	Routes that correspond to IPv6 prefixes and routes included in IPv6 prefixes
Refine	Routes included in IPv6 prefixes are applicable, but routes that correspond to IPv6 prefixes are not included.
equal	Routes that correspond to IPv6 prefixes are applicable only.

When *nr* is omitted, if there is at least one corresponding IPv6 prefix, the route is assumed to match the filter and the route is introduced. When not specified, if there is no corresponding IPv6 prefix, the route is assumed to match the filter and the route is introduced. When reject specified, if there is at least one corresponding IPv6 prefix, the route is assumed to match the filter and the route is not introduced.

Note

Care must be taken when setting multiple filters specified in not by the **ipv6 ospf export from ospf** command. Since it is not determined whether IPv6 prefixes that correspond to the specified not filter are introduced or not, they are evaluated by the next filter specified in the **ipv6 ospf export from ospf** command. Therefore, for example, in the following settings, all routes are introduced and there is no meaning of filters.

```
ipv6 ospf export from ospf filter 1 2
ipv6 ospf export filter 1 not equal fec0:12ab:34cd:1::/64
ipv6 ospf export filter 2 not equal fec0:12ab:34cd:2::/64
```

The first filter matches routes other than fec0:12ab:34cd:1::/64, and the second filter matches routes other than fec0:12ab:34cd:2::/64. That is, the route fec0:12ab:34cd:1::/64 does not match the first filter but is introduced because it matches the second filter. On the other hand, the route fec0:12ab:34cd:2::/64 matches the first filter and is introduced regardless of the second filter. Therefore, there is no route that is not introduced.

If you do not want to introduce the route fec0:12ab:34cd:1::/64 and the route fec0:12ab:34cd:2::/64, you need to configure the following settings.

```
ipv6 ospf export from ospf filter 1
ipv6 ospf export filter 1 not equal fec0:12ab:34cd:1::/64 fec0:12ab:34cd:2::/64
```

Or

```
ipv6 ospf export from ospf filter 1 2 3
ipv6 ospf export filter 1 reject equal fec0:12ab:34cd:1::/64
ipv6 ospf export filter 2 reject equal fec0:12ab:34cd:2::/64
ipv6 ospf export filter 3 include ::/0
```

[Applicable models]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

26.11Route introduction by external protocol

[Format]

```
ipv6 ospf import from protocol [filter filter_num ...]
no ipv6 ospf import from protocol [filter filter_num...]
```

[Setting value and initial value]

- *protocol*: External protocol to be introduced in the OSPFv3 routing table
 - [Setting value]:

Setting value	Description
static	Static routes (not including implicit routes)
Rip	RIPng

- [Initial value]: -
- *filter_num*
 - [Setting value]: Filter number of **ipv6 ospf import filter command** (1...2147483647)
 - [Initial value]: -

[Explanation]

Set whether to introduce routes by external protocols into the OSPFv3 routing table. The introduced routes are advertised to other OSPFv3 routers as external routes.
filter_num specifies the filter number defined by the **ipv6 ospf import filter** command. Routes to be introduced from external protocols are evaluated by filters in the specified order. Routes determined to be introduced by the first matched filter are introduced into OSPFv3. Routes determined not to be introduced or routes without matching filters are not introduced. Also, all routes are introduced into OSPFv3 when filter keywords and subsequent ones are omitted.

Metric values and metric types, which are parameters for advertising routes, are those specified by the corresponding **ipv6 ospf import filter** command in the **filter** check. If filter keywords and subsequent ones are omitted, the following parameters are used.

- metric=1
- type=2

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

26.12 Filter definitions applied to introducing external routes**[Format]****ipv6 ospf import filter** *filter_num* [*nr*] *kind* *ipv6_prefix/prefix_len* ... [*parameters* ...]**no ipv6 ospf import filter** *filter_num* [[*nr*] *kind* *ipv6_prefix/prefix_len* ... [*parameters*...]]**[Setting value and initial value]**• *filter_num*

- Setting value: Filter number (1...2147483647)

- [Initial value]: -

• *nr* : How filters are interpreted

- [Setting value]:

Setting value	Description
not	Routes not corresponding to IPv6 prefixes
reject	Routes not corresponding to IPv6 prefixes

- [Initial value]: -

• *kind* : How IPv6 prefixes are interpreted

- [Setting value]:

Setting value	Description
include	Routes included in the specified IPv6 prefix (including IPv6 prefix itself)
Refuses	Routes included in the specified IPv6 prefix (not including IPv6 prefix itself)
equal	Routes included in the specified IPv6 prefix

- [Initial value]: -

• *ipv6_prefix/prefix_len*

- Setting value: IPv6 prefix

- [Initial value]: -

• *parameters* : Parameters for advertising external routes

- [Setting value]:

Setting value	Description
metric = <i>metric</i>	Metric value (1 to 16777215)
type = <i>type</i>	Metric type (one or two)

- [Default]: -

[Explanation]

Filters to be applied when introducing an external route into a route table of OSPFv3 are defined. Filters defined in this command have an effect only when specified in the filter term of the **ipv6 ospf import from** command.

The IPv6 prefix is specified in *ipv6_prefix/prefix_len*. Multiple filters can be specified and interpreted by a *kind*-specified method.

include	Routes that match the IPv6 prefix and those that match the IPv6 prefix are applicable.
Refinees	Routes that match the IPv6 prefix are applicable, but those that match the IPv6 prefix are not.
equal	Routes that match the IPv6 prefix are applicable only.

When *nr* is omitted, if at least one of the corresponding IPv6 prefixes is present, the filter is assumed to match and the route is introduced. When not specified, routes that match the filter are not introduced if they do not match any of the IPv6 prefixes.

When reject is specified, if at least one of the corresponding IPv6 prefixes is present, the filter is assumed to match and the route is not introduced.

In *parameters*, metric values and metric types can be specified by metric and type, respectively, as parameters when advertising a route to be introduced as an external route of OSPFv3. When these are omitted, the following values are adopted.

- metric=1
- type=2

[Notes]

Care must be taken when setting multiple filters specified by the **ipv6 ospf import from** command. When specifying a route that does not match the specified filter, the filter does not determine whether to introduce the route or not, so it is evaluated by the next filter specified by the **ipv6 ospf import from** command. Therefore, for example, in the following settings, all routes are introduced and there is no meaning of filters.

```
ipv6 ospf import from static filter 1 2
ipv6 ospf import filter 1 not equal fec0:12ab:34cd:1::/64
ipv6 ospf import filter 2 not equal fec0:12ab:34cd:2::/64
```

The first filter matches a route other than fec0:12ab:34cd:1::/64, and the second filter matches a route other than fec0:12ab:34cd:2::/64. That is, the route fec0:12ab:34cd:1::/64 does not match the first filter, but is introduced because it matches the second filter. On the other hand, the route fec0:12ab:34cd:2::/64 matches the first filter, so it is introduced regardless of the second filter. Therefore, there is no route that is not introduced.

If you do not want to introduce the route fec0:12ab:34cd:1::/64 and the route fec0:12ab:34cd:2::/64, you need to configure the following settings.

```
ipv6 ospf import from static filter 1
ipv6 ospf import filter 1 not equal fec0:12ab:34cd:1::/64 fec0:12ab:34cd:2::/64
```

Or

```
ipv6 ospf import from static filter 1 2 3
ipv6 ospf import filter 1 reject equal fec0:12ab:34cd:1::/64
ipv6 ospf import filter 2 reject equal fec0:12ab:34cd:2::/64
ipv6 ospf import filter 3 include ::/0
```

[Applicable models]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

26.13 OSPFv3 log output settings

Format

```
ipv6 ospf log /log...
no ipv6 ospf log [/log...]
```

Setting value and initial value

- log
 - Setting value:

Setting value	Explanation
interface	Logs related to interface status and virtual links
neighbor	Logs related to the status of neighboring routers
packet	Logs related to OSPFv3 packets

- Initial value: No logs of any kind are output.

Explanation

Set the type of log output related to OSPFv3.

[Applicable models]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 27

HTTP server function

27.1 Setting the presence or absence of HTTP server function

Format

```
httpd service switch
no httpd service
```

[Setting value and initial value]

- switch*
- [Setting value]:

Setting value	Description
on	Enable HTTP server function
off	Disable HTTP server function

- [Initial value]: on

[Explanation]

Select whether to enable HTTP server.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

27.2 Setting up hosts that can access HTTP server

[Format]

```
httpd host ip_range [ip_range...]
httpd host any
httpd host
none httpd
host lan no
httpd host
```

[Setting value and initial value]

- ip_range*: IP address or mnemonic of hosts that allow access to HTTP server
- [Setting value]:

Setting value	Description
IP address (range specification) with hyphen (-) in between, and optionally arranged	Allow access from specified hosts
lanN	Allow access from WAN interface
Wan1	Allow access from WAN interface
bridge1	Allow access from VLAN interface
vlanN	Allow access from VLAN interface
lanN/M	Allow access from tag VLAN interface

- [Initial value]: -
- any*
 - [Setting value]: Allow access from all hosts
 - [Initial value]: -
- None*

- [Setting value]: Allow access from all hosts
- [Initial value]: -
- *lan*
 - [Setting value]: Allow access from within the network on the LAN side
 - [Initial value]: lan

[Explanation]

Set hosts that allow access to HTTP server

[Notes]

If a LAN interface is specified in this command, access from IP addresses other than network address and limited broadcast address is allowed. Access is not allowed unless both primary address and secondary address are set for the specified LAN interface.

All firmware after Rev.14.01 series can specify a mixture of IP address and mnemonic. The

WAN interface can be specified by all firmware after Rev.14.01 series.

The WAN interface can be specified by firmware after Rev.14.01 series.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

27.3 Setting the session timeout period of HTTP server

[Format]

httpd timeout *time*

no httpd timeout [*time*]

[Setting value and initial value]

- *time*
 - [Setting value]: Number of seconds (1..180)
 - [Initial value]: 5

[Description]

Set the timeout period of the HTTP server.

[Notes]

If a communication timeout occurs when accessing a router via the Internet, set a large value with this command.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

27.4 Setting the listen port of the HTTP server function

[Format]

httpd listen *port*

no httpd listen

[Setting value and initial value]

- *port*
 - [Setting value]: Port number (1..65535)
 - [Setting value]: 80

[Explanation]

Set the standby port of the HTTP server.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

27.5 Setting the names of the PP interface and tunnel interface

[Format]

pp name *name*
tunnel name *name*
no pp name
no tunnel name

[Setting value and initial value]

- *Name*
 - [Setting value]: Name (up to 64 characters)
 - [Initial value]: -

[Description]

Setting the names of the PP interface and tunnel interface

[Notes]

This command is used only by the WWW browser setting support function.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER28

Netvolante-DNS Service Configuration

Netvolante-DNS is a kind of dynamic DNS function, and you can register the IP address of a router to the Netvolante-DNS server operated by Yamaha with the desired name. Therefore, it can be used for server publication and site management in a dynamic IP address environment. It is not compatible with other dynamic DNS services because it uses its own protocol for procedures such as registering and updating IP addresses.

The Netvolante-DNS server operated by Yamaha is operated under free and non-guaranteed conditions at this time. Although there is no usage fee, we cannot guarantee that a name can be registered to the Netvolante-DNS server, and that the registered name can not be retrieved. Also, please note that the Netvolante-DNS server may stop without notice.

There are two types of Netvolante-DNS: host address service and telephone number service, but the telephone number service is not available in the model described in this document.

In Netvolante-DNS, since individual RT series and Netvolante-DNS routers are identified by MAC addresses, there is no guarantee that the same name can be used as it is when equipment is replaced.

28.1 Whether or not to use the Netvolante-DNS service

[Format]

`netvolante-dns use interface switch`
`no netvolante-dns use pp switch`
`no netvolante-dns use interface [switch]`
`no netvolante-dns use pp switch`

[Setting value and initial value]

- `interface`
 - no setting value: LAN interface name, WAN interface name
 - [Initial value]: -
- `switch`
 - [Setting value]:

Setting value	Explanation
auto	automatic update
off	no automatic update

- no initial value: auto

Explanation

Set whether or not to use the Netvolante-DNS service.
Automatically update the IP address to the Netvolante-DNS server when the IP address is updated.

[Notes]

The WAN interface can be specified by firmware after Rev.14.01 series.

Applicable model

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

28.2 Manual update to the Netvolante-DNSserver

[Format]

`netvolante-dns go interface`
`no netvolante-dns go pp peer_num`

Setting value and initial value

- `interface`
 - no setting value: LAN interface name, WAN interface name
 - Initial value: -

- *peer_num*
 - no setting value: destination information number
 - no initial value: -

Explanation

Manually update the IP address to the Netvolante-DNS server.

[Notes]

The WAN interface can be specified by firmware after Rev.14.01 series.

Applicable model

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

28.3 Removal from the Netvolante-DNSserver

[Format]

netvolante-dns delete go *interface* [host]

netvolante-dns delete go pp *peer_num* [host]

No setting value and initial value

- *interface*
 - no setting value: LAN interface name, WAN interface name
 - no initial value: -
- *peer_num*
 - no setting value: destination information number
 - no initial value: -
- *host*
 - no setting value: hostname
 - [Initial value]: -

[Description]

Delete the registered IP address from the Netvolante DNS server.

Only the specified host name can be deleted by specifying the host name after the interface.

[Notes]

The WAN interface can be specified with firmware after Rev.14.01.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

28.4 Setting the port number used for the Netvolante DNS service

[Format]

netvolante-dns port

no netvolante-dns port

[Setting value and initial value]

- *port*
 - [Setting value]: Port number (1..65535)
 - [Initial value]: 2002

[Description]

Set the port number used for the Netvolante DNS service.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

28.5Get the list of host names registered in the Netvolante DNS server.

[Format]

```
netvolante-dns get hostname list
interface netvolante-dns get hostname
list pp peer_num netvolante-dns get
hostname list all
```

[Setting value and initial value]

- interface
 - [Setting value]: LAN interface name, WAN interface name
 - [Initial value]: -
- peer_num
 - [Setting value]: Counterparty information number
 - [Initial value]: -
- all: All interfaces
 - [Initial value]: -

[Description]

Gets and displays the list of host names registered in the Netvolante DNS server.

[Notes]

WAN interface can be specified with firmware after Rev.14.01.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

28.6Host name registration

[Format]

```
netvolante-dns hostname host interface [server=server_num] host [duplicate]
netvolante-dns hostname host pp [server=server_num] host [duplicate]
netvolante-dns hostname host interface [server=server_num] host ipv6 address [ipv6_address]
[duplicate] netvolante-dns hostname host pp [server=server_num] host ipv6 address
[ipv6_address] [duplicate] netvolante-dns hostname host interface [server=server_num] host
ipv6 prefix [ipv6_prefix] [duplicate] netvolante-dns hostname host pp [server=server_num]
host ipv6 prefix [ipv6_prefix] [duplicate]
no netvolante-dns hostname host interface [server=server_num] [host [duplicate]]
no netvolante-dns hostname host pp [server=server_num] [host [duplicate]]
```

[Setting value and initial value]

- interface
 - [Setting value]: LAN interface name, WAN interface name
 - [Initial value]: -
- server_num
 - [Setting value]:

Setting value	Description
One or two	Server number
Omitted	When omitted, 1 is assumed to be specified.

- [Initial value]: -
- host
 - [Setting value]: Host name (up to 63 characters)
 - [Initial value]: -
- ipv6_address
 - [Setting value]: IPv6 address
 - [Initial value]: -
- ipv6_prefix
 - [Setting value]: IPv6 prefix

[Explanation]

Set the host name used by the Netvolante DNS service (Host Address Service). The host name obtained from the Netvolante DNS server is in the form of "(host name).(subdomain).netvolante.jp". (host name) is the name set by this command, and (subdomain) is assigned from the Netvolante DNS server. (subdomain) cannot be specified by the user.

The first time this command is set, only the (host name) part is set. When registration/update to the Netvolante DNS server is successful, the command is saved in the form of the complete FQDN described above.

When duplicate is added, one router can register the same name on different interfaces.

Characters that can be used for *host* are single-byte alphanumeric characters and hyphens (-), and are specified within 63 characters.

[Notes]

The WAN interface can be specified by firmware after Rev.14.01 series.

IPv6 address and ipv6 prefix can be used with firmware of RTX5000/RTX3500 Rev.14.00.26 or later, RTX1210 Rev.14.01.33 or later, RTX830 Rev.15.02.09 or later, and Rev.15.04 or later.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

28.7 Communication timeout setting

[Format]

```
netvolante-dns timeout interface time
netvolante-dns timeout pp time
no netvolante-dns timeout interface [time]
no netvolante-dns timeout pp [time]
```

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name, WAN interface name
 - [Initial value]: -
- *time*
 - [Setting value]: Timeout seconds (1..180)
 - [Initial value]: 90

[Explanation]

Set the time in seconds until communication with a netboranch DNS server times out.

[Notebook]

WAN interface can be specified by firmware after Rev.14.01 series.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

28.8 Setting whether to automatically generate host names

[Format]

```
netvolante-dns auto hostname interface [server=server_num] switch
netvolante-dns auto hostname interface [server=server_num] ipv6 address
[ipv6_address] netvolante-dns auto hostname interface [server=server_num]
ipv6 prefix [ipv6_prefix] netvolante-dns auto hostname pp [server=server_num]
switch
netvolante-dns auto hostname pp [server=server_num] ipv6 address [ipv6_address]
netvolante-dns auto hostname pp [server=server_num] ipv6 prefix [ipv6_prefix]
no netvolante-dns auto hostname interface [switch]
no netvolante-dns auto hostname pp [switch]
```

[Setting value and initial value]

- *interface*

- [Setting value]: LAN interface name, WAN interface name
- [Initial value]: -
- *server_num*
- [Setting value]:

Setting value	Explanation
One or two	Server number
Omitted	1 is assumed to be specified when omitted.

- [Initial value]: -
- *switch*
- [Setting value]:

Setting value	Explanation
on	Generate automatically
off	Not generate automatically

- [Initial value]: off
- *ipv6_address*
- [Setting value]: IPv6 address
- [Initial value]: -
- *IPv6_prefix*
- [Setting value]: IPv6 prefix
- [Initial value]: -

[Description]

Whether or not to use the automatic host name generation function is set. The automatically generated host name is in the form of "'y'+(last 6 digits of the MAC address).auto.netvolante.jp" when the first 6 digits of the MAC address is "00:a0:de". When the first 6 digits of the MAC address is other than "00:a0:de", it is in the form of "'y'+(all 12 digits of the MAC address).auto.netvolante.jp".

When this command is set to 'on' and the **netvolante-dns go** command is executed, the above host name is assigned from the Netvolante DNS server. The assigned domain name can be confirmed by the **show status netvolante-dns** command.

[Notes]

The automatic host name generation for products other than "00:a0:de" with the first 6 digits of the MAC address is supported by firmware of RTX5000/RTX3500 Rev.14.00.21 or later, RTX1210 Rev.14.01.33 or later, and all firmware of Rev.15.02 series or later.

The WAN interface can be specified by firmware of Rev.14.01 series or later.

The ipv6 address and ipv6 prefix can be used with firmware of RTX5000/RTX3500 Rev.14.00.26 or later, RTX1210 Rev.14.01.33 or later, RTX830 Rev.15.02.09 or later, and Rev.15.04 series or later.

[Applicable models]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

28.9 Setting a host name registration command using a serial number

[Format]

netvolante-dns set hostname interface serial

[Setting value and initial value]

- *interface*
- Setting value: LAN interface name, WAN interface name or "pp"
- [Initial value]: -

[Description]

The command for utilizing the host name using the serial number of the equipment is automatically set.

When this command is executed, the **netvolante-dns hostname host** command is set.

For example, if the serial number of the equipment is D000ABCDE, when **netvolante-dns set hostname pp serial** is executed, the **netvolante-dns hostname host pp server=1 SER-D000ABCDE** is set.

[Notes]

The user cannot specify a subdomain.

The WAN interface can be specified by firmware of Rev.14.01 series or later.

[Applicable models]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

28.10 Setting up a netvolante-dns server

[Format]

netvolante-dns server ip_address

netvolante-dns server name

no netvolante-dns server [*ip_address*]

no netvolante-dns server [*name*]

[Setting value and initial value]

- *ip_address*
 - Setting value: IP address
 - [Initial value]: -
- *name*
 - Setting value: Domain name
 - [Initial value]: netvolante-dns.netvolante.jp

[Description]

Setting up the IP address or host name of the netvolante-dns server

[Applicable models]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

28.11 Setting ON/OFF of the netvolante-dns server address update function

[Format]

netvolante-dns server update address use [*server=server_num*] *switch*

no netvolante-dns server update address use [*server=server_num*]

[Setting value and initial value]

- *server_num*
 - [Setting value]:

Setting value	Description
One or two	Server number
Omitted	When omitted, 1 is assumed to be specified.

- [Initial value]: -

- *switch*
 - [Setting value]:

Setting value	Description
on	Enable the update function of the server address
off	Stop the update function of the server address

- [Initial value]: on

[Explanation]

It receives a change notification of an IP address from a Netvolante DNS server, and sets whether to automatically update the setting.

[Applicable model]
RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

28.12Setting the port number of the Netvolunte DNS server address update function

[Form]

netvolante-dns server update address port [server=server_num] *port*
no netvolante-dns server update address port [server=server_num]

[Setting value and initial value]

- *server_num*
 - [Setting value]: -

Setting value	Description
1 or 2	Server number
Omitted	When omitted, 1 is assumed to be specified.

- [Initial value]: -
- *port*
 - [Setting value]: Port number (1..65535)
 - [Initial value]: 2002

[Explanation]

Set the standby port number of the IP address update notification of the Netvolunte DNS server.

[Applicable model]
RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

28.13Setting the retry interval and the number of times when a u t o m a t i c update fails

[Form]

netvolante-dns retry interval *interface interval count*
netvolante-dns retry interval *pp interval count*
no netvolante-dns retry interval *interface [interval count]*
no netvolante-dns retry interval *pp [interval count]*

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name, WAN interface name
 - [Initial value]: -
- *Interval*
 - [Setting value]:
 - auto
 - Seconds (60-300)
 - [Initial value]: auto
- *count*
 - Setting value: Number of times (1-50)
 - [Initial value]: 10

[Explanation]

Set the interval and the number of times when automatic update fails in Netvolunte DNS.

[Notes]

When auto is set in *interval*, automatic update is performed again after a time of 30 seconds to 90 seconds when automatic update fails. If it also fails, automatic update is performed after a time interval of 60 seconds.

When manual execution is performed within a specified time after automatic update fails, subsequent automatic update is not performed.

The WAN interface can be specified by the firmware of Rev.14.01 series or later.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

28.14 Setting the periodic update interval of Netvolunte DNS registration**[Form]****netvolante-dns register timer** [server=server_num] time**no netvolante-dns register timer** [server=server_num]**[Set value and initial value]**

- server_num

- [Set value]:

Set value	Description
1 or 2	Server number
Omitted	When omitted, 1 is assumed to be specified.

- [Initial value]: -

- time

- [Set value]:

Set value	Description
3600 ... 2147483647	Seconds
off	Do not update Netvolunte DNS registration periodically

- [Initial value]: off

Description

Specify the interval at which Netvolunte DNS registration is updated periodically.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

28.15 Setting up a file to save settings when Netvolunte DNS registration is successful**[Format]****netvolante-dns auto save** [server=server_num] file**no netvolante-dns auto save** [server=server_num]**[Set value and initial value]**

- server_num

- [Set value]:

Set value	Description
1 or 2	Server number
Omitted	When omitted, 1 is assumed to be specified.

- [Initial value]: -

- file

- [Set value]:

Set value	Description
off	Do not save settings automatically
auto	Do automatic saving to the default setting file
Number	File name to be saved automatically

- [Initial value]: auto

Description

Whether or not to save settings automatically when Netvolunte DNS registration is successful and when an address notification from the Netvolunte DNS server is received, and specify a file name of a save destination in case of automatic saving are specified.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 29

Setting UPnP

29.1 Setting whether or not to use UPnP

[Format]

Upnp use *use*

no upnp use

[Set value and initial value]

- *Use*

- [Set value]:

Set value	Description
on	To be used
off	Not used

- [Initial value]: off

[Explanation]

Sets whether or not to use the UPnP function.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

29.2 Setting the interface to get the IP address used for UPnP

[Format]

upnp external address refer *interface*

upnp external address refer pp

peer_num upnp external address

refer default

no upnp external address refer [*interface*]

no upnp external address refer pp [*peer_num*]

[Setting value and initial value]

- *interface*

- [Setting value]:

Setting value	Description
LAN interface name	Get the IP address of the specified LAN interface
WAN interface name	Get the IP address of the specified WAN interface
[Default]	Default route interface

- [Initial value]: default

- *peer_num*

- [Setting value]:

- Counterpart information number
- anonymous

- [Initial value]: -

[Explanation]

Setting the interface to get the IP address used for UPnP

[Notes]

WAN interface can be specified by firmware after Rev.14.01 series.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

29.3Setting the type of erase timer for UPnP port mapping

[Format]

upnp port mapping timer type type
no upnp mapping timer type

[Setting value and initial value]

- type
- [Setting value]:

Setting value	Description
normal	Do not refer to ARP information
arp	Refer to ARP information

- [Initial value]: arp

[Explanation]

Setting the type of timer for erasing UPnP port mapping
When this command changes, the erase timer value is set to 3600 seconds. The number of seconds of the erase timer can be changed with the **upnp port mapping timer** command.

Specifying arp takes precedence over setting upnp port mapping timer off.
Specify normal to leave the port mapping unaffected by arp.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

29.4Setting UPnP port mapping erase timer

[Format]

upnp port mapping timer time
no upnp port mapping timer

[Setting value and initial value]

- time
- [Setting value]:

Setting value	Description
600..21474836	Seconds
off	Do not erase

- [Initial value]: 3600

Description

Set the time until the port mapping generated by UPnP is erased.

[Notes]

Set this command after setting with the **upnp port mapping timer type** command.
Even if it is set to off, the port mapping is erased if it is set to **upnp port mapping timer type** arp. If you do not want to erase the port mapping even if ARP times out, set it to **upnp port mapping timertype** normal.

[Applicable model]
RTX1300, RTX1220, RTX1210, RTX840, RTX830

29.5Setting whether to output UPnP syslog

[Format]
`upnp syslog syslog`
`no upnp syslog`

[Setting value and initial value]

- `syslog`
- [Setting value]:

Setting value	Description
on	Output UPnP syslog
off	Do not output UPnP syslog

- [Initial value]: off

Description
Set whether to output UPnP syslog or not. Output at the debug level.

[Applicable model]
RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER30

Setting up USB

30.1 Setting whether to use USB host function

[Format]

usbhost use *switch*
no usbhost use [*switch*]

[Setting value and initial value]

- switch*
 - [Setting value]:

Setting value	Description
on	Using USB host function
off	Do not use USB host function

- [Initial value]: on

Description

Setting whether to use USB host function
When this command is set to off, USB memory is not recognized even if it is connected to a router.
Also, if a failure occurs in USB host function due to overcurrent, it can be recovered by resetting this command while the USB memory is not connected.

[Applicable model]
RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

30.2Setting the time until overcurrent protection function is activated on the USB bus

[Format]

usbhost overcurrent duration *duration*
no usbhost overcurrent duration [*duration*]

[Setting value and initial value]

- duration*
 - [Setting value]: Time (5..100, 1 unit is 10 ms)
 - [Initial value]: 5 (50 ms)

[Explanation]

Time until the overcurrent protection function works is set. If the overcurrent is detected continuously for the time set here, the overcurrent protection function works.

[Applicable model]
RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 31

Schedule

31.1 Setting a Schedule

[Format]

```

schedule at id [date] time * command...
schedule at id [date] time pp peer_num command...
schedule at id [date] time tunnel tunnel_num
command... schedule at id [date] time switch switch
command... schedule at id +timer * command...
schedule at id +timer pp peer_num command...
schedule at id +timer tunnel tunnel_num
command... schedule at id +timer switch switch
command...
no schedule at id [[date]...]

```

[Setting value and initial value]

- *id*
 - [Setting value]: Schedule number
 - [Initial value]: -
- *date*: Date (optional)
 - [Setting value]:
 - Month/Day
 - If omitted, it is regarded as */*

Setting example of the moon	Setting contents
1,2	January and February
2	February to July
2-7	February to July
-7	January to July
*	Every month

Setting example of the moon	Setting contents
1	One day only
1,2	Day one and two
2	From two to the end of the month
2-7	From two to seven
-7	From one to seven
mon-fri	Monday only
sat, sun	Saturday and Sunday
mon-fri	Monday to Friday
fri	Sunday to Friday
*	Every day

- [Initial value]: -
- *time*: Time
 - [Setting value]:

Setting value	Explanation
hh:mm[:ss]	Hour(0..23 or *): Minutes(0..59 or *): Seconds(0..59), seconds optional
Startup	When starting
usb-attached	When recognizing a USB device (Cannot be specified for the vRX series.)
sd-attached	When recognizing a microSD device (Cannot be specified for the vRX series.)

- [Initial value]: -
- *timer*: Time until *command execution* (seconds, 1..3600)
 - [Initial value]: -
- *peer_num*
 - [Setting value]:
 - Counterpart information number
 - anonymous
 - [Initial value]: -
- *tunnel_num*
 - [Setting value]: Tunnel interface number
 - [Initial value]: -
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -
- *command*
 - [Setting value]: Command to execute (with restrictions)
 - [Initial value]: -

[Explanation]

The command specified by *command* is executed at the time specified by *time* or after the time specified by *timer*. When specified in the second, third, and fourth formats, the command is executed so that **pp select/tunnel select/switch select** commands are issued in the destination information number/tunnel number/switch specified in advance.

Multiple **schedule at** commands can be specified, and those specified at the same time are executed in descending order of *id*.

When *time* is specified in the hh:mm format, it is considered that seconds are not specified, and when time is specified in the hh:mm:ss format, it is considered that seconds are specified. It is not possible to specify ranges using "-" for seconds or specify all with "*".

The following commands cannot be specified:

administrator, administrator password, administrator password encrypted, ap select (*1), auth user, auth user group, bgp configure refresh, clear vrx license, cold start, confirm, console info and console prompt (excluding commands starting with console), copy, copy exec, date, delete, echo, embedded file, exit, export vrx license, external-memory performance-test go, help, import vrx license, http revision-up go, http revision-up schedule, interface reset, ipsec transport template, ipv6 bgp configure refresh, ipv6 ospf configure refresh, commands starting with less, load, login password, login password encrypted, login timer, login user, luac, macro, make directory, nslookup, ospf configure refresh, packetdump, ping, ping6, pp select (*2), quit, remote setup, rename, rollback timer, rfts format, rfts garbage collect, save, schedule at, scp, commands starting with show, ssh, sshd host key generate, sshd session, switch control function get FUNCTION, switch select (*1), system packet-buffer, telnet, telnetd session, time, timezone, traceroute, traceroute6, tunnel select (*2), tunnel template, user attribute, vrx license update schedule

- Commands marked with (*1) can be specified on RTX1210 Rev.14.01.26 or later, RTX830 Rev.15.02.03 or later, RTX1220, and RTX1300.

- Commands marked with (*2) can be specified on all models/revisions except:
RTX5000 / RTX3500 Rev.14.00.25 or earlier,
RTX1210 Rev.14.01.25 or earlier,
RTX830 Rev.15.02.02 or earlier.

- The load command can be specified on all models/revisions except: RTX5000 / RTX3500 Rev.14.00.25 or earlier, RTX1210 Rev.14.01.27 or earlier, RTX830 Rev.15.02.02 or earlier. [Initial value of the command.

[Notes]

When entering commands, TAB key command completion is available for the command parameter; however, syntax errors are not detected until execution.

When a command specified by the schedule at command is executed, the system outputs an INFO-type SYSLOG indicating what was attempted to be executed.

It is not possible to mix numeric date and weekday specifications in the date parameter.

A schedule specified with startup is executed when the router starts. This is useful when you want to initiate a connection immediately after powering on.

Format 4 is available on RTX1300, RTX1220, RTX1210, RTX840, and RTX830.

Formats 5–7 are not available on: RTX5000 / RTX3500 Rev.14.00.31 or earlier RTX1220 Rev.15.04.03 or earlier RTX1210 Rev.14.01.40 or earlier RTX830 Rev.15.02.02 or earlier

Format 8 is not available on: RTX5000 RTX3500 RTX1220 Rev.15.04.03 or earlier RTX1210 Rev.14.01.40 or earlier RTX830 Rev.15.02.01

[Configuration Example]

- Allow connection only on weekdays from 8:00 to 17:00:.

```
# schedule at 1 */mon-fri 8:00 pp 1 isdn auto connect on
# schedule at 2 */mon-fri 17:00 pp 1 isdn auto connect off
# schedule at 3 */mon-fri 17:05 * disconnect 1
```

- Allow connection only from minute 0 to 15 every hour:.

```
# schedule at 1 *:00 pp 1 isdn auto connect on
# schedule at 2 *:15 pp 1 isdn auto connect off
# schedule at 3 *:15 * disconnect 1
```

- Switch routing on next New Year's Day

```
# schedule at 1 1/1 0:0 * ip route NETWORK gateway pp 2
```

- Execute a Lua script every 20 seconds between 12:00 and 13:00 daily.

```
# schedule at 1 12:*:00 * lua script.lua
# schedule at 2 12:*:20 * lua script.lua
# schedule at 3 12:*:40 * lua script.lua
```

- Restart a switch every day at 3:00:.

```
# schedule at 1 */* 03:00 switch 00:a0:de:01:02:03 switch control function execute restart
# schedule at 2 */* 03:00 switch lan1:4 switch control function execute restart
```

- Restart 10 minutes after command configuratio.

```
# schedule at 1 +600 * restart
```

[Applicable model]

[Settings] vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 32

VLAN Configuration

32.1 Setting up a VLAN ID

[Format]

```
vlan interface/sub_interface 802.1q vid=vid [name=name]
no vlan interface/sub_interface 802.1q
```

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *sub_interface*
 - [Setting value]: 1-32
 - [Initial value]: -
- *vid*
 - [Setting value]: VLAN ID (IEEE802.1Q tag VID field storage value) (2-4094)
 - [Initial value]: -
- *name*
 - [Setting value]: Arbitrary name for a VLAN (within 127 single-byte characters and within 63 double-byte characters)
 - [Initial value]: -

[Description]

Setting up a VLAN ID for a VLAN to be used in a LAN interface

It is possible to handle packets with IEEE802.1Q tags that store configured VLANs.

The number of VLANs that can be configured in one LAN interface is 32.

[Notebook]

When receiving a tagged packet, if the VID of the tag is not configured in a reception LAN interface, the packet is discarded. It is not possible to use it together with a LAN partitioning function (port-based-option option of the **lan type command**) in the same LAN interface. Of both, the one entered earlier becomes valid, and the one entered later becomes a command error.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

32.2 Setting up a VLAN Interconnect Interface Group

[Format]

```
vlan interconnect group phys_lan_interface group [group...]
no vlan interconnect group phys_lan_interface [group...]
```

[Setting value and initial value]

- *phys_lan_interface*: Physical LAN interface to be configured in a group
 - [Setting value]: Physical LAN interface name
 - [Initial value]: -
- *group*: LAN interfaces that make up a group
 - [Setting value]:
 - all
 - prohibit interconnection of all LAN interfaces subordinate to *phys_lan_interface*
 - none
 - prohibit interconnection of all LAN interfaces subordinate to *phys_lan_interface* (total disconnection)
 - Specify the physical LAN interface name and virtual LAN interface name by concatenating them with "."

- Allow interconnection of consecutive virtual LAN interfaces
- Specify the virtual LAN interface name by concatenating them with "-"(dollar mark)
 - Allow interconnection of consecutive virtual LAN interfaces
- Specify the physical LAN interface name or virtual LAN interface name by adding "\$"(dollar mark)
 - Allow interconnection of all other LAN interfaces subordinate to *phys_lan_interface* to only the specified LAN interface
- [Initial value]: all for all physical LAN interfaces

[Explanation]

Set a group of mutually connectable LAN interfaces for each physical LAN interface.

When using a virtual LAN interface (LAN division interface or tag VLAN interface), communication with the physical LAN interface and communication with all virtual LAN interfaces are enabled in the initial state, but this command allows specifying groups of mutually connectable LAN interfaces.

When specifying none for *group*, interconnection of all LAN interfaces subordinate to *phys_lan_interface* is enabled. (Total disconnection) When specifying none for *group*, all LAN interfaces subordinate to *phys_lan_interface* are blocked from each other, and interconnection is disabled (total disconnection). However, even when specifying none, communication with other physical LAN interfaces and virtual LAN interfaces not subordinate to the physical LAN interface specified in *phys_lan_interface* is not blocked. Note that specifying all/none is also valid for virtual LAN interfaces created after executing this command, so it is not necessary to execute this command every time the number of virtual LAN interfaces is increased.

When specifying groups to allow interconnection, specify a group of multiple physical LAN interface names for each group and a *group of* LAN interfaces whose virtual LAN interface names are connected by "-"(hyphen) or ","(comma).

A "\$" (dollar mark) can be used to represent all pairs of LAN interfaces in a simplified manner. For example, when using six (VLAN1-VLAN6) LAN division interfaces, if only the VLAN2 interface allows interconnection with all other LAN division interfaces, the group needs to specify five groups such as "vlan1, vlan2 vlan2, vlan3 vlan2, vlan4 vlan2, vlan5 vlan2, vlan6", which can be simplified to "vlan2\$". "\$" means that it is expanded to multiple groups individually paired with all LAN interfaces. Similarly, when using ten (LANI-VLANI) tag interfaces (LANI-VLANI-6), if only the lan I-VLANI interface allows interconnection with all other tag VLAN interfaces and the Native VLAN interface (LANI interface that does not use a tag VLAN), the group needs to specify ten groups such as "lan I-VLANI", which can be simplified to "lan I-VLANI". There is no need to execute this command every time the number of virtual LAN interfaces is increased, because "\$" is also valid for virtual LAN interfaces created after executing this command in the same way as specifying all / none.

A function similar to this command is a port separation function of a LAN division extension function, but the port separation function controls communication within the same virtual LAN interface (communication returned within a built-in switching hub), and communication across multiple virtual LAN interfaces cannot be controlled. This command can control communication across multiple virtual LAN interfaces.

Communication between a LAN interface and interfaces other than the LAN interface (PP interface, TUNNEL interface, etc.), and communication across multiple physical LAN interfaces are not controlled by this command.

When used together with an IP filter function, communication control processing by this command is performed after checking the OUT side IP filter, and packets that are permitted to communicate by both the IP filter function and this command can pass between interfaces.

[Notes]

RTX1300 is available after Rev. 23.01.02.

RTX1220 is available after Rev. 23.01.02.
RTX830 is available after Rev. 15.04.07.
RTX830 is available after Rev. 15.02.31.

[Configuration Example]

- LAN1 interface is completely opened

```
# vlan interconnect group lan1 all
```

- LAN2 interface is completely shut off

```
# vlan interconnect group lan2 none
```

- Groups of vlan1, vlan2, vlan3 and groups of vlan2, vlan3, vlan4 allow interconnection within each group

```
# vlan interconnect group lan1 vlan1-3 vlan2-4
```

- Allow interconnection with vlan1 and vlan3 to vlan8 only with vlan2

```
# vlan interconnect group lan1 vlan2$
```

- Allow interconnection with lan2/1, lan2/2, lan2/3, lan2/18

```
# vlan interconnect group lan2 lan2/1-3,lan2/18
```

- Allow interconnection with a LAN interface that is subordinate to all LAN2 interfaces with only lan2 and lan2/1

```
# vlan interconnect group lan2 lan2$ lan2/1$
```

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX840, RTX830

32.3Whether to log communication control by VLAN interconnection interface group

[Format]

vlan interconnect log *phys_lan_interface* type [type]
no vlan interconnect log *phys_lan_interface* [type [type]]

[Setting value and initial value]

- *phys_lan_interface* : Physical LAN interface to be configured for the group
 - [Setting value] : Physical LAN interface name
 - [Initial value] : -
- *type*
 - [Setting value] :

Setting value	Explanation
pass	Logs about communication between interfaces that are allowed to interconnect
reject	Logs about blocked communication between interfaces that are not allowed to interconnect

- [Initial value] : -

Explanation

Whether to log communication control by the VLAN interconnection interface group is set.
If this command is set, when communication control is performed in the VLAN interconnection interface group, NOTICE level
Outputs syslog

[Notes]

When using both of the IP filter function and communication control by the VLAN interconnection interface group together, checking processing of the IP filter is performed first. Therefore, if packets are discarded by the IP filter, logs by this command are not output.

RTX1300 can be used in Rev. 23.01.02 or later. RTX8300 can be used in Rev. 15.02.31 or later. RTX830 can be used in Rev. 15.02.31 or later. RTX830 can be used in Rev. 15.02.31 or later.

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX840, RTX830

CHAPTER 33

Survival notification function

33.1 Setting a shared key for survival notification

[Format]

heartbeat pre-shared-key *key*
no heartbeat pre-shared-key

[Setting value and initial value]

- key*
 - [Setting value]: Key represented by an ASCII string (up to 32 characters)
 - [Initial value]: -

[Description]

A shared key for performing authentication is set on the receiving side of a survival notification. The same key must be set on both the sending and receiving sides of the survival notification.
If this command is not set, log output at the time of transmission and reception of the survival notification is not performed.

[Applicable model]

[Model]: vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

33.2 Setting whether to receive the survival notification

[Format]

heartbeat receive *switch* [*option=value ...*]
no heartbeat receive [*switch*]

[Setting value and initial value]

- switch*
 - [Setting value]:

[Setting value]	Description
on	Receive the survival notification packet
off	Do not receive the survival notification packet

- [Initial value]: off
- option=value*

- [Setting value]:

<i>option</i>	[Setting value]	Description
log	on	Output the received contents to syslog.
	off	Do not output the received contents to syslog.
monitor	Monitoring time [seconds] (30..21474836)	Raise an alert when there is no notification within the specified number of seconds.
	off	Even when there is no reception of the survival notification, raise an alert.

- [Initial value]:
 - log=off
 - monitor=off

[Description]

Set whether to output the contents of the received survival notification to syslog.
When there is no survival notification within the monitoring time specified by the monitor option, output syslog and send an SNMP trap.

[Notes]

Before setting this command, it is necessary to set a shared key with the sending router **by heartbeat pre-shared-key** command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

33.3Execution of the survival notification

[Format]

heartbeat send *dest_addr* [*log=switch*]

[Setting value and initial value]

- dest_addr*
 - [Setting value]: IPv4 address or FQDN of the destination router
 - [Initial value]: -
- switch*: Output syslog
 - [Setting value]:

Setting value	Description
on	Output syslog
off	Do not output syslog

- [Initial value]: off

[Description]

Send the name and IP address of the device set by **snmp sysname** to the IP address specified by *dest_addr* to notify that it is in a communication state.
If log=on, outputs syslog when sending packets.

[Notes]

Before setting this command, it is necessary to set the shared key with the receiver router **by heartbeat pre-shared-key** command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 34

Survival notification function release 2

Survival notification function is a function that sends packets including your name and IP address from a router connected to the network to a router at another base to notify that communication is possible. A router that receives a notification packet outputs the notified name and IP address in a log and saves it. This function can be used as a means of notifying that communication is possible from a router at a base where the IP address of the WAN is undefined to a router at another base.

About releases

The conventional survival notification function described in the previous chapter is distinguished from release 1, and the survival notification function described in this chapter is distinguished from release 2. The concept of both functions is the same, but please note that the command system and operation are not compatible.

Features of release 2

- Use UDP /8512 port as a survival notification packet (both start and end points).
- A router that receives a survival notification identifies the router from which it is sent by the notified name. Therefore, it is necessary to set a unique name for each router that sends a survival notification.
- By having a common encryption key and authentication key for the sender router and the receiver router, it is possible to detect encryption and falsification of notification information.
- In order to facilitate operation management in multi-to-ground communication, multiple transmission/reception settings can be set by specifying each identifier. Here, the sender's transmission setting and the receiver's reception setting, which are paired, must each specify the same identifier. By including this configuration identifier in a notification packet, the receiver uniquely determines the reception setting to use for any notification packet.
- Periodic transmission of notifications, which was previously realized by combining with the **schedule** command, can be performed only with the transmission setting command.
- The IP address to be notified is basically the IP address set in the sending interface of the survival notification packet. Here, if NAT or IP masquerade is set in the interface, the IP address when applying the NAT /IP masquerade setting to the sending notification packet is used. However, when sending a survival notification packet using an unnumbered connection line, the IP address is preferentially selected from the younger interface among the LAN interfaces where the IP address is set (synchronized with the start address of the IP header of the notification packet).
- The received survival notification information can be displayed with the **show status heartbeat2** command.

34.1 Setting of notification name

[Format]

```
heartbeat2 myname name
no heartbeat2 myname
```

[Setting value and initial value]

- *name*
 - [Setting value]: Name used for survival notification (1-64 characters/ASCII, 1-32 characters/shift JIS)
 - [Initial value]: -

[Description]

The name of the machine to be notified in the survival notification is set.

Not only ASCII characters but also Japanese characters (excluding half-width katakana) within the range that can be expressed by shift JIS can be used for *name*. However, it can be set and displayed correctly only when the **console character** command is set to sjis, and it may not be processed as intended by other settings.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

34.2 Defining notification settings

[Format]

```
heartbeat2 transmit trans_id [crypto crypto_key] auth auth_key dest_addr ...
no heartbeat2 transmit trans_id
```

[Setting value and initial value]

- *trans_id*

- [Setting value]: Identifier of notification setting (1..65535)
- [Initial value]: -
- *crypto_key*
 - [Setting value]: Authentication key expressed as an ASCII string (1-32 characters)
 - [Initial value]: -
- *auth_key*
 - [Setting value]: Authentication key expressed as an ASCII string (1-32 characters)
 - [Initial value]: -
- *dest_addr*
 - [Setting value]: IPv4 address or FQDN of the destination router (up to four can be specified separated by spaces)
 - [Initial value]: -

[Explanation]

Define periodic transmission settings for survival notifications. Authentication information is given to a notification packet based on the *auth_key* set in this command. Further, when *crypto_key* is specified, notification contents are further encrypted.

When the **heartbeat2 receive** command is set as the corresponding receiver setting, *recv_id* must match the *trans_id* of this command. Similarly, *crypto_key* and *auth_key* must also match.

This command defines the minimum parameters required for transmission in association with *trans_id*. To actually enable transmission processing, it is necessary to set the **heartbeat2 transmit enable** command.

In order to distribute the transmission load by a plurality of notification settings, the time from when the notification settings become effective until the notification packet is first transmitted is random for each notification setting/destination (within 30 seconds).

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

34.3 Enabling notification settings

[Format]

heartbeat2 transmit enable [one-shot] *trans_id_list*

no heartbeat2 transmit

enable [Set value and initial value]

- *trans_id_list* : List of identifiers of notification settings that you want to enable.
 - [Set value]:
 - one number or numbers with a minus in between (ranged), and optionally arranged ones (up to 128).
 - [Initial value]: -

[Explanation]

Specify the one you want to actually enable from the defined notification settings.

Up to 128 identifier lists can be specified, separated by spaces.

When the 'one-shot' keyword is specified, notification processing of each setting specified by *trans_id_list* is executed only once. Commands entered in this format cannot be saved.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

34.4 Notification interval setting

[Format]

heartbeat2 transmit interval *time*

heartbeat2 transmit interval *trans_id*

time **no heartbeat2 transmit interval**

[*time*]

no heartbeat2 transmit interval *trans_id time*

[Set value and initial value]

- *trans_id*
 - Set value: Identifier of notification settings

- [Initial value]: -
- *time*
 - Set value: Notification interval seconds (30..65535)
 - [Initial value]: 30

[Explanation]

Specify the transmission interval of notification settings corresponding to *trans_id*.
If *trans_id* is omitted, all notification settings are applied.
However, settings that specify *trans_id* individually take precedence.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

34.5Setting whether to log when sending notifications

[Format]

heartbeat2 transmit log [*trans_id*] *sw*
no heartbeat2 transmit log [*trans_id*]

[Set value and initial value]

- *trans_id*
 - Set value: Identifier of notification settings
 - [Initial value]: -
- *SW*
 - [Set value]:

Set value	Explanation
on	Output transmitted contents to syslog
off	Do not output transmitted contents to syslog

- [Initial value]: off

[Explanation]

Set log output of notification settings corresponding to *trans_id*. If *sw* is set to 'on', when sending a survival notification, use INFO
Output level syslog.
If *trans_id* is omitted, all notification settings are applied. However, settings that specify *trans_id* individually take precedence.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

34.6Reception settings definition

[Format]

heartbeat2 receive *recv_id* [*crypto crypto_key*] *auth auth_key*
no heartbeat2 receive *recv_id*

[Setting value and initial value]

- *Recv_id*
 - [Setting value]: Identifier of reception setting
 - [Initial value]: -
- *crypto_key*
 - [Setting value]: Authentication key expressed as an ASCII string (1 to 32 characters)
 - [Initial value]: -
- *auth_key*
 - [Setting value]: Authentication key expressed as an ASCII string (1 to 32 characters)
 - [Initial value]: -

[Exp1]

Reception setting of survival notification is defined. When reception processing is performed, decryption and authentication check are performed using the setting of this command having the same *recv_id* based on the setting identifier (*trans_id*) of the sender included in the notification packet.

When **heartbeat2 transmit** command is set as the setting of the corresponding sender, *trans_id* must match *recv_id* of this command. Similarly, *crypto_key* and *auth_key* must also match.

This command defines the minimum parameters required for reception in association with *recv_id*. To actually enable reception processing, it is necessary to set **heartbeat2 receive enable** command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

34.7 Reception setting activation

[Format]

heartbeat2 receive enable *recv_id_list*

no heartbeat2 receive

enable **[Setting Value and**

Initial Value]

- *recv_id_list*: List of identifiers of reception setting that you want to activate.
 - **[Setting value]**:
 - One number or numbers with - in between (ranged), and optionally arranged ones (up to 128).
 - **[Initial value]**: -

[Explanation]

Specify what you want to actually activate from the defined reception setting.

The list of identifiers can be up to 128 separated by spaces.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

34.8 Reception interval monitoring setting

[Format]

heartbeat2 receive monitor time

heartbeat2 receive monitor *recv_id*

time no heartbeat2 receive monitor

[time]

no heartbeat2 receive monitor *recv_id time*

[Setting value and initial value]

- *recv_id*
 - **[Setting value]**: Identifier of reception setting
 - **[Initial value]**: -
- *time*: Monitoring time
 - **[Setting value]**:

Setting value	Explanation
30..21474836	Number of seconds
off	No monitoring of reception interval

- **[Initial value]**: off

[Explanation]

Monitoring setting of reception interval in reception setting corresponding to *recv_id* is performed. When monitoring is enabled, if survival notification does not arrive within the specified time, an SNMP trap is sent by outputting INFO level syslog.

If *recv_id* is omitted, all reception settings are applied. However, the setting that individually specifies *recv_id* takes precedence.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

34.9Setting whether to log when receiving notification

[Format]

```
heartbeat2 receive log [recv_id] sw
no heartbeat2 receive log [recv_id]
```

[Setting value and initial value]

- recv_id
 - [Setting value]: Identifier of reception setting
 - [Initial value]: -
- SW
 - [Setting value]:

Setting value	Description
on	Output received contents to syslog
off	Do not output received contents to syslog

- [Initial value]: off

[Explanation]

Set the log output of reception setting corresponding to *recv_id*. If *sw* is set to 'on', when sending survival notification, INFO
Outputs a level of syslog.
If *recv_id* is omitted, all reception settings are applied. However, the setting that individually specifies *recv_id* takes precedence.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

34.10Setting the maximum number of survival information that can be retained at the same time

[Setting value]

```
heartbeat2 receive record limit num
no heartbeat2 receive record limit
```

[Setting value and initial value]

- num
 - [Setting value]: Maximum number of survival information retained (vRX series, RTX5000, RTX3510, RTX3500: 64..10000, other models: 64..1000)
 - [Initial value]: 64

[Explanation]

Set the maximum number of received survival information that can be retained at the same time. In a state where the number of survival information reaches the maximum, it is not possible to take in new information. In such a case, it is necessary to delete unnecessary information with **clear heartbeat2** command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

34.11Display of survival notification status

[Setting value]

```
show status heartbeat2
show status heartbeat2 id recv_id
show status heartbeat2 name string
```

[Setting value and initial value]

- recv_id
 - Setting value: Identifier of reception setting
 - [Initial value]: -
- string
 - Setting value: String (1-64 characters/ASCII, 1-32 characters/shift JIS)
 - [Initial value]: -

Display information of received survival notification.

In the first format, all retained information is displayed.

In the second format, only information received according to the specified reception setting is displayed.

In the third format, only information in which the specified character string is included in a notification name is displayed.

For *string*, not only ASCII characters but also Japanese characters (excluding half-width katakana) within the range that can be expressed by shift JIS can be used. However, it works correctly only when the **console character** command is set to sjis, and it may malfunction in other settings.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

34.12 Clearing survival notification status

[Setting value]

clear heartbeat2

clear heartbeat2 id *recv_id*

clear heartbeat2 name *string*

[Setting value and initial value]

- *recv_id*
 - Setting value: Identifier of reception setting
 - [Initial value]: -
- *string*
 - Setting value: String (1-64 characters/ASCII, 1-32 characters/shift JIS)
 - [Initial value]: -

[Description]

Clear the received survival notification information.

In the first format, all information held is cleared.

In the second format, only information received by a specified reception setting is cleared.

In the third format, only information in which a specified character string is included in a notification name is cleared.

Not only ASCII characters but also Japanese characters (excluding half-width katakana) within the range that can be expressed by shift JIS can be used in *string*. However, it works correctly only when the **console character** command is set to sjis, and may malfunction in other settings.

[Applicable models]

vRX series, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER35

SNTP server function

SNTP is a protocol for synchronizing the time of computers and network devices using a network. The SNTP server function returns the value of the router's built-in clock in response to an inquiry about the time from a client. The SNTP server function implements SNTP version 4. It also supports requests for SNTP versions 1 to 3 as backward compatibility.

To obtain accurate time using the SNTP server function, it is recommended to periodically execute the **ntpdate** command to match the time of a router with that of another NTP server.

35.1 Setting whether to enable the SNTP server function

[Format]

```
sntp service switch
no sntp service
```

[Setting value and initial value]

- switch
- [Setting value]:

Setting value	Explanation
on	Enabling the SNTP server function
off	Enabling the SNTP server function

- [Initial value]: on

Explanation

Set whether to enable the SNTP server function.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

35.2Setting up hosts that allow access to the SNTP server

[Format]

```
sntp host ip_range [ip_range...]
sntp host
any sntp
host none
sntp host lan
no sntp host
```

[Setting value and initial value]

- ip_range : IP addresses or mnemonics of hosts that allow access to the SNTP server
- [Setting value]:

Setting value	Explanation
One IP address or IP addresses (ranged) with a hyphen (-) in between, and optionally arranged	Allow access from a specified host
lanN	Allow access from a WAN interface
wan1	Allow access from a WAN interface (Not available for vRX series, RTX5000, and RTX3500)
bridge1	Allow access from a bridge interface

Setting value	Explanation
vlanN	Allow access from a VLAN interface (Not available for vRX series)
lanN/M	Allow access from a tag VLAN interface (Not available for vRX series)

- [Initial value]: -
- *any*
 - [Setting value]: Allow access from all hosts
 - [Initial value]: -
- *None*
 - [Setting value]: Prohibit access from all hosts
 - [Initial value]: -
- *LAN*
 - [Setting value]: Allows access from within all LAN side networks.
 - [Initial value]: lan

[Explanation]

Set hosts that allow access to SNTP servers.

[Notes]

If a LAN interface is specified in this command, access from IPv4 addresses other than network addresses and directed broadcast addresses is allowed.
Access is not allowed unless the specified LAN interface has neither a primary address nor a secondary address.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER36

External memory function

This function operates various data between the router and external memory by connecting external memory (USB memory, microSD card) to the router body.
The external memory that can be used varies depending on the model.

If you use a model equipped with a FUNC button, replace the DOWNLOAD button with a FUNC button. This function enables the following operations.

- Command setting or operation by execution command
 - Output a SYSLOG message to external memory.
 - Copy a configuration file from external memory.
 - Copy a configuration file from external memory.
 - Copy a firmware file from external memory.
- Operation by operating the external memory button and DOWNLOAD button on the router body
 - Press and hold the external memory button and DOWNLOAD button simultaneously for three seconds or more to copy a configuration file and a firmware file from the external memory.
- Booting from External Memory
- Batch file execution

functionBatch file
execution function

This function stores a file (called a batch file) in which commands are listed in external memory, and executes the commands described in that file.
It can be executed by pressing the DOWNLOAD button depending on the setting. It can also be executed by the **execute batch** command on the console.
Command execution results and logs are written as files to external memory.

Using this function, communication confirmation with PING can be performed even in an environment without a PC. Necessary devices and work procedures can be greatly reduced when installing a router, for example.
Execution results, configuration details, router status, etc. are written as files to external memory.
Exported files can be viewed on a mobile phone by taking out the external memory.
It can also be used as a work log.

Technical information on this function is available at the URL shown below.
<https://www.rtpro.yamaha.co.jp>

36.1 Setting whether to use a microSD card slot

Format

sd use *switch*
no sd use

Setting value and initial value

- *switch*
 - Setting value

Setting value	Explanation
on	Using a microSD card slot
off	Do not use a microSD card slot

- Setting value: on

Description

Setting whether to use a microSD card slot When this command is set to off, the microSD card is not recognized even if it is inserted into the card slot.

Applicable model

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

36.2 Setting the operation mode of cache memory for external memory**Format**

external-memory cache mode *mode*

no external-memory cache mode [*mode*]

Setting value and initial value

- *Mode*
- Setting value

Setting value	Description
write-through	Write-through mode
copy-back1	Copy-back mode 1
copy-back2	Copy-back mode 2

- [Initial value]: copy-back1

[Explanation]

An operation mode of a cache memory for an external memory is set. Three types of operation modes, write-through mode, copy-back mode 1, and copy-back mode 2, are supported, and the timing at which data on each cache of FAT, DIR, and FILE is written to the external memory is different depending on each mode.

Each operation mode is described below.

When write-through is specified, the cache allocated to FAT, DIR, and FILE operates in write-through mode and is always written to the external memory. The safety is the highest.

When copy-back1 is specified, the FAT and DIR caches operate in copy-back mode, and the FILE cache operates in write-through mode. It can be operated faster than the write-through mode.

When copy-back2 is specified, the FAT, DIR, and FILE caches operate in copy-back mode. In this setting, since writing to the external memory is suppressed, it operates at the highest speed. However, since a state in which writing to the external memory is not completed continues, there is a high possibility that a file system of the external memory is damaged when an unexpected power failure occurs.

FAT : Abbreviation for File Allocation Table

DIR : Abbreviation for Directory Entry

[Notes]

Changes to this command are reflected when the external memory is connected. When a command is input in a state in which the external memory is already connected, it is necessary to reconnect it after removing it once.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

36.3 Setting the size of cache memory for file access acceleration**[Format]**

external-memory accelerator cache size *interface size*

no external-memory accelerator cache size *interface* [*size*]

[Setting value and initial value]

- *interface*
- [Setting value]:

Setting value	Description
usb1	USB port 1

Setting value	Description
sd1	microSD card slot

- [Initial value]: -
- *size*
- [Setting value]:

Setting value	Description
1-5	Size of cache memory (the larger the number, the larger the memory size)
off	Do not use a file access acceleration mechanism

- [Initial value]: 1

Description

Setting the size of cache memory used for speeding up file access

A mechanism for speeding up file access works when a numerical value is specified for *size*, and in particular, access performance to the external memory is improved in a configuration with many directories and files. When access performance is not improved, it may be improved by increasing *size*. However, the larger the *size*, the longer the time it takes to be usable after connecting the external memory.

If off is specified for *size*, cache memory for speeding up file access is not allocated.

Note that if an external memory is connected to all interfaces at the same time while setting the maximum value for *size* for all interfaces, it may affect the performance of the entire system, so it is recommended to limit the number of interfaces for setting this command to speed up file access.

[Notes]

Changes to this command are reflected when the external memory is connected. When a command is input while the external memory is already connected, it is necessary to reconnect it after removing it once.

Also, when access performance is not improved even if *size* is increased by this command, it may be improved by performing the following operation.

- Reduce directories and files in the external memory if possible
- Adjust the total number of directories in the external memory to 2,000 or less
- Adjust the total number of files (including directories) in directories accessed frequently to 20,000 or less
- Keep file names and directory names as short as possible (up to 32 characters recommended)

[Applicable models]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

36.4 Setting the prefix of file names of statistics stored in external memory

[Format]

external-memory statistics filename prefix *prefix* [*crypto password*] [**max-filenum=filenum**] [**interval=minute**]
no external-memory statistics filename prefix [*prefix* [*crypto password*] [**max-filenum=filenum**]
[interval=minute]]

[Setting value and initial value]

- *prefix* : Prefix of the file name (half-width alphanumeric characters only, no more than 15 characters without a prefix such as "usb1:")
- [Setting value]:

Setting value	Description
<i>usb1:filename</i>	Prefix of file name
<i>sd1:filename</i>	Prefix of file name

- [Initial value]: -
- *crypto* : Cryptographic algorithm when storing encrypted information
- [Setting value]:

Setting value	Description
aes128	Encrypt with AES128

Setting value	Description
aes256	Encrypt with AES256

- [Initial value]: -
- *password*
 - [Setting value] : Encryption key when storing encrypted information Password expressed as an ASCII string (half-width 8 characters or more, no more than 32 characters)
 - [Initial value]: -
- *filenum* : Upper limit of the number of files of statistics stored in external memory
- [Setting value]:

Setting value	Description
100 ... 2147483647	Upper limit of the number of files of statistics stored in external memory
infinity	Do not limit the number of files of statistics stored in external memory

- [Initial value]: infinity
- *minute* : Interval between writing statistics to external memory
- [Setting value]:

Setting value	Description
2 ... 120	Interval between writing statistics to external memory (minutes)

- [Initial value]: 12

Description

Set the prefix (prefix) of the file name for writing statistics. The actual file name is automatically determined based on this prefix.

For example, if the prefix is set to "yamaha", the traffic volume of the LAN2 interface is written. The file name will be something like "yamaha_traffic_lan2_20080708.csv".

[Notes]

When the number of files of statistics exceeds the upper limit, a new file is created by deleting the oldest file in the statistical information file of each kind and interface.

Regarding application traffic information, it is not encrypted with or without *crypto* parameters. The actual file name has a character string representing the type and date after the *prefix*.

The format of the file name follows. *prefix_type[id]_yyyymm[dd].ext*

- *Prefix*
 - Any character string set by this command
- *type*
 - Types of statistics

cpu	CPU utilization
memory	Memory Utilization
flow	Number of Fastpass flows
route	Number of routes
nat	Number of entries in the NAT table
filter	Number of sessions for dynamic filtering
traffic	Traffic volume by interface
qos	Traffic volume by QoS class
application	Application traffic information

- *id*

- The meaning of id depends on the type of statistics
 - Traffic volume by interface..... is shown.
 - Traffic volume by QoS class Represents . interfaces and classes
 - For other statistics, id is omitted.

• *yyyy*

- Western calendar (four digits)

• *mm*

- Month (two digits)

• *dd*

- Day (two digits)

- *dd* is omitted when dividing files by months

• *ext*

- Extensions

csv	CSV
rtfg	Encrypted files

Files encrypted and stored in external memory can be decrypted on a PC using RT-FileGuard. Traffic information of applications cannot be stored encrypted.

The number of files restricted by the *max-filenum* option is the total number of files for which statistics for all types and interfaces are written.

Regarding traffic information of applications, statistics are written out every minute regardless of interval settings.

RTX1210 can be used with Rev. 14.01.34 or later, and RTX830 can be used with Rev. 15.02.10 or later, and Rev. 15.04 or later firmware.

Applicable models

RTX1300, RTX1220, RTX1210, RTX840, RTX830

36.5 Specifying a SYSLOG file name to be stored in external memory

Format

external-memory syslog filename *name* [*crypto password*] [*limit=size*] [*backup=num*] [*interval=interval*] [*line=line*]
no external-memory syslog filename [*name*]

Setting value and initial value

- *name* : SYSLOG file name
- Setting value:

Setting value	Description
<i>usb1:filename</i>	File name in a USB flash drive (names with .bak extension cannot be specified)
<i>sd1:filename</i>	File name in a microSD card (names with .bak extension cannot be specified)

- Setting value: -
- *crypto* : Selection of a cryptographic algorithm when storing SYSLOG encrypted
- Setting value:

Setting value	Description
aes128	Encrypt with AES128
aes256	Encrypt with AES256

- Setting value: -
- *password*
 - [Setting value]: Password expressed as an ASCII string (8 or more half-width characters and up to 32 characters)
 - [Initial value]: -

- *size*
 - [Setting value]: Maximum size of a SYSLOG file (1-1024 units: MB)
 - [Initial value]: 10
- *num*
 - [Setting value]: Maximum number of backup files (1-100)
 - [Initial value]: 10
- *Interval*
 - [Setting value]: Interval between writing SYSLOG to external memory (2-86400 units: seconds)
 - [Initial value]: 2
- *line*
 - [Setting value]: Number of lines to write SYSLOG to external memory (1000-N units: ~~lines~~) N ... Log storage capacity of each model
 - [Initial value]: 1000

[Description]

Specify a SYSLOG file name to be saved in external memory.

A file name containing a .bak extension cannot be specified in *name*. Also, a file name containing a .rtfg extension cannot be specified in *name* when not encrypted.

When *crypto* and *password* are specified, SYSLOG is encrypted and then written to external memory. When encrypting, it is necessary to specify a name containing a .rtfg extension or an omitting extension in *name*. When the extension is omitted, the rtfg extension is automatically added to the file name.

When the SYSLOG file reaches the maximum size, a backup of the SYSLOG file is performed. The name of the backup file created at this time depends on firmware.

The backup file name represents the date and time when the backup was performed after the file name specified in *name*. A string of _yyyymmdd_hhmmss format is added.

- yyyy ... Western calendar (4 digits)
- mm ... month (2 digits)
- dd ... day (2 digits)
- hh ... hour (2 digits)
- mm ... minute (2 digits)
- ss ... second (2 digits)

When the number of backup files reaches the maximum number specified in *num*, or when there is no free space in external memory, a new backup file is created after deleting the oldest backup file.

When *name* contains an extension

- Save without encryption ... Add a .bak extension
- Save with encryption ... Add a _bak extension before it

Add a bak extension if *name* does not contain an extension

Write SYSLOG to external memory when the time specified in *interval* has elapsed or when the number of lines specified in *line* is output. The log storage capacity of each model that can be specified in *line* is as follows.

- RTX5000/RTX3510/RTX3500 20000
- RTX1300/RTX1220/RTX1210/RTX840/RTX830..... 10000

When this command is not set, SYSLOG is not written to external memory.

[Notes]

If the following changes are made, the *name* must be changed.

- Changing to save with encryption because SYSLOG is saved without encryption
- Changing to save without encryption because SYSLOG is saved with encryption
- Changing a cryptographic algorithm or password

A file stored with encryption in external memory can be decrypted using RT-FileGuard on a PC.

The name must be within 99 single-byte characters.

The *interval* and *line* options can be used with RTX5000/RTX3500 Rev.14.00.18 or later firmware and all Rev.14.01 or later firmware.

[Applicable models]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

36.6 Setting whether to allow copying of configuration files and firmware files by pressing the external memory button and DOWNLOAD button simultaneously

Format

operation external-memory download permit *switch*
no operation external-memory download permit [*switch*]

[Setting value and initial value]

- switch*
- [Setting value]

Setting value	Description
on	Allow
off	Do not allow

- [Initial value]: on

[Explanation]

Whether to allow copy operation of a setting file and a firmware file by simultaneously pressing an external memory button and a DOWNLOAD button is set.

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

36.7 W
Whether to allow startup from a file in external memory

[Format]

external-memory boot permit *switch*
no external-memory boot permit [*switch*]

[Setting value and initial value]

- switch*
- [Setting value]: on

Setting value	Explanation
on	Allow
off	Do not allow

- [Initial value]: on

[Explanation]

Whether to allow startup from a file in external memory is set. If this setting is set to OFF, startup from a file in external memory is not possible.

The names of the setting file and the firmware file to be read at startup can be set by the **external-memory config filename** command and the **external-memory exec filename** command, respectively.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

36.8Set timeout until detection of external memory at r outer startup

[Format]

external-memory boot timeout *time*
no external-memory boot timeout [*time*]

[Setting value and initial value]

- time*
 - Setting value: Timeout seconds (1..30)
 - [Initial value]:
 - 1 (RTX840, RTX830)
 - 2 (other than the above)

[Explanation]

Set timeout until detection of external memory at router startup.
This is effective when the **external-memory boot permit on** command is set to allow startup from a file in external memory.
In the case of a device with slow connection recognition, it may be recognized by increasing the timeout time.

[Notes]

It is recommended to set the time displayed by boot device attach as a guide in the external memory performance measurement command.

[Applicable model]

RTX3510, RTX1300, RTX840, RTX830

36.9 Specifying the firmware file name to be read at startup or by pressing the external memory button and the DOWNLOAD button simultaneously

[Format]

external-memory exec filename *from* [*to*]
external-memory exec filename off
no external-memory exec filename [*from*] [*to*]
no external-memory exec filename [off]

[Setting value and initial value]

- from*: External memory and firmware file name
 - [Setting value]:

Setting value	Explanation
<i>usb1:filename</i>	Firmware file name in USB memory
<i>sd1:filename</i>	Firmware file name in microSD card
<i>*:filename</i>	Firmware file name in USB memory and microSD card

- [Initial value]:
 - *: (model name).bin (models other than RTX5000 and RTX3500)
 - sd1: (model name).bin (RTX5000, RTX3500)

- to*: Copy destination file name
 - [Setting value]:

Setting value	Description
0 to 1	Executable format of internal storage (internal flash ROM, etc.) Firmware file number (default is 0)

- [Initial value]: 0

[Description]

Specifies a firmware file name on the external memory that is read when the external memory is inserted and started or when the external memory button and DOWNLOAD button are pressed simultaneously.

When the external memory button and DOWNLOAD button are pressed simultaneously, the firmware file is copied to the internal storage (internal flash ROM, etc.), but the firmware file number of the copy destination internal storage at that time can also be specified.

When "*" is specified for the external memory, the specified file is first searched from a microSD card, and if there is no specified file, a USB memory is searched. In the case of button operation, only the external memory of the corresponding button is an object of file search.

Specify *filename* using an absolute path or specify only the file name. When only the file name is specified, it is searched from the specified external memory. The *filename must be* within 99 single-byte characters.

When a plurality of files are applicable as a result of the search, a file closest to the root directory on the directory hierarchy and in the destination directory in alphabetical order is selected.

When off is specified, the firmware file is not searched or read.

[Notes]

Depending on the directory structure and the number of files in the external memory, it may take time to search for a file.

To shorten the search time, it is desirable to store a file near the root or specify the file directly with an absolute path, avoiding creating a directory with a deep hierarchy.

The timeout period for automatic search can be set by the **external-memory auto-search time command**.

[Configuration Example]

- Search for "rtx1220.bin" from the microSD card and load it as a firmware file.

```
# external-memory exec filename sd1:rtx1220.bin
```

- Search for "rtx1220.bin" from the directory "test" in the microSD card and load it as a firmware file.

```
# external-memory exec filename sd1:/test/rtx1220.bin
```

[Applicable models]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

36.10 Specifying the setting file name to be loaded at startup or by pressing the external memory button and the DOWNLOAD button simultaneously.

[Format]

external-memory config filename *from[,from]* [*to*] [*password*]
external-memory config filename off
no external-memory config filename [*from*] [*to*] [*password*]
no external-memory config filename [off]

[Setting value and initial value]

- from*: External memory and setting file name
 - [Setting value]:

Setting value	Description
<i>usb1:filename</i>	Setting file name in the USB memory
<i>sd1:filename</i>	Setting file name in the microSD card
<i>*:filename</i>	Setting file name in the USB memory and the microSD card

- [Initial value]:
 - *:config.rtf, *:config.txt (for models other than RTX5000 and RTX3500)
 - sd1:config.rtf, sd1:config.txt (RTX5000, RTX3500)
- to*: Copy destination file name
 - [Setting value]:

Setting value	Description
0 to 4	Setting file number of the internal storage (internal flash ROM, etc.)

- [Initial value]: 0
- *password*
 - Setting value: Decryption password (8 or more single-byte characters and up to 32 characters in ASCII character string)
 - [Initial value]: -

[Description]

Setting file name on the external memory to be loaded when the external memory is inserted and started or when the external memory button and the DOWNLOAD button are pressed simultaneously is specified.

When the external memory button and the DOWNLOAD button are pressed simultaneously, the setting file is copied to the internal storage (internal flash ROM, etc.), but the setting file number of the internal storage at that time can also be specified.

When "*" is specified in the external memory, the specified file is searched from the microSD card first, and if there is no specified file, the USB memory is searched. In the case of button operation, only the external memory of the corresponding button is searched.

The *filename* can be specified using an absolute path or only the file name. If only the file name is specified, it is searched from the specified external memory. The *filename must be* within 99 single-byte characters.

When a plurality of files correspond to each other as a result of searching, the file closest to the root directory on the directory hierarchy and in the first directory in alphabetical order is selected.

When decrypting and reading an encrypted configuration file by specifying a password, set the password when encrypted to *password*.

When off is specified, search and reading of the configuration file are not performed.

[Notes]

Depending on the directory structure of the external memory and the number of files, it may take time to search for a file.

To shorten the searching time, it is desirable to store a file in a position close to the root or to specify the file directly with an absolute path, avoiding creating a directory with a deep hierarchy.

The timeout period for automatic searching can be set by the **external-memory auto-search time command**.

A file encrypted and stored in the external memory can be decrypted on a PC using RT-FileGuard.

[Configuration Example]

- Search for "config.txt" from the microSD card and read it as a configuration file.

```
# external-memory config filename sd1:config.txt
```

- Search for "config.txt" from the directory "test" in the microSD card and read it as a configuration file.

```
# external-memory config filename sd1:/test/config.txt
```

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

36.11 Set the timeout period when searching for a file

[Format]

external-memory auto-search time *time*

no external-memory auto-search time [*time*]

[Setting value and initial value]

- *time*
 - [Setting value]:
 - Number of seconds (1..600)
 - [Initial value]: 300

[Explanation]

Set the timeout period when searching for a file stored in the external memory.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

36.12Execute a batch file

[Format]

execute batch

[Explanation]

Execute a batch file in the external memory. The batch file name to be executed is **external-memory batch filename**. Specify with do.

[Notes]

If you want to interrupt the batch file being executed, type Ctrl+C.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

36.13Configuration of batch file and execution result file

[Format]

external-memory batch filename *batchfile* [*logfile*]
no external-memory batch filename [*batchfile* [*logfile*]]

[Setting value and initial value]

- batchfile*: Batch file name
 - [Setting value]:

Setting value	Description
<i>usb1:filename</i>	Batch file name in a USB memory
<i>sd1:filename</i>	Batch file name in a microSD card
<i>*:filename</i>	Batch file name in a USB memory and a microSD card

- [Initial value]:
 - sd1:command.txt (for models other than RTX5000 and RTX3500)
 - sd1:command.txt (RTX5000, RTX3500)
- logfile*
 - [Setting value]:

Setting value	Description
<i>filename</i>	Execution result file name

- [Initial value]: command-log.txt

[Description]

Specify a batch file name and an execution result file name in external memory.

If "*" is specified in the external memory, the specified file is searched from the microSD card first, and if there is no specified file, the USB memory is searched.

Filename specifies a file using an absolute path or only a file name. If only a file name is specified in *filename* of a batch file, it is searched automatically from the external memory. When there are multiple files, files closest to the root directory on the directory hierarchy and in the destination directory in alphabetical order are selected.

If *logfile* is omitted, an execution result file is created with the name "batch file name -log.txt".

[Notes]

The number of characters that can be specified in *batchfile* is 99 characters or less when *logfile* is specified. If *logfile* is omitted, it is 91 characters or less excluding the extension.
The number of characters that can be specified in *batchfile* is 99 characters or less.

[Configuration Example]

- From the microSD card file, search "command_test.txt" as a batch file.

```
# external-memory batch filename sd1:command_test.txt
```

- From the microSD card directory "test", read "command_test.txt".

```
# external-memory batch filename sd1:/test/command_test.txt
```

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

36.14 External memory performance measurement command

[Format]

external-memory performance-test go *interface*

[Setting value and initial value]

- *interface*
- [Setting value]:

Setting value	Description
usb1	USB interface
sd1	microSD interface

- [Initial value]: -

[Description]

Whether or not a memory has performance that can withstand the use of an external memory function is confirmed.

The time required for recognition of the external memory and the speed of reading and writing data are confirmed, and if it is judged that the memory has performance that can withstand use after a series of tests.

- OK:succeeded

What is not?

- NG:

Display

failed.

[Notes]

The external memory is targeted at the state immediately after format.

This function must be executed without using other functions.

During execution of this command, **syslog debug** on and **no syslog host** are set. Therefore, DEBUG type SYSLOG may be output even if it is set to **syslog debug** off. Also, logs are not transferred to the SYSLOG server even if a **syslog host** command is set.

When using the external memory function of a Yamaha router, the minimum performance required for the external memory is confirmed, and the result of this function does not guarantee all operations of the external memory. When using the external memory function, it is recommended to periodically check that no write errors to the **external** memory have occurred with the **show status external-memory** command.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

36.15 Setting of functions to be executed when the DOWNLOAD button is pressed

[Format]

operation button function download *function* [*script_file* [args ...]]

no operation button function download [*function* [*script_file* [args ...]]]

[Setting value and initial value]

- *function*: Function to be executed when the DOWNLOAD button is pressed
- [Setting value]:

Setting value	Description
http revision-up	HTTP revision upgrade
execute batch	Batch file execution

Setting value	Description
mobile signal-strength	Acquisition of radio wave reception level of a portable terminal
execute lua	Lua Script Execution

- [Default]: http revision-up
- *script_file*
 - [Setting value]: Specify the script file name or bytecode file name as an absolute path or a relative path.
 - [Default]: -
- *args*
 - [Setting value]: Variable arguments to pass to *script_file*.
 - [Default]: -

[Explanation]

Set the function to be executed when the DOWNLOAD button is pressed. A lamp under the DOWNLOAD button lights up during execution of the function, and turns off when execution of the function is completed.

When execute lua is set to *function*, *script_file* must be specified. When a relative path is specified in *script_file*, it is interpreted as a path based on the environment variable PWD. PWD can be changed by the **set** command, and the default value is "/".

[Notes]

When executing a Lua script, if the environment variable LUA_INIT is set, the script of LUA_INIT is executed before *script_file*.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

36.16 Setting whether to allow batch file execution by the DOWNLOAD button

[Format]

operation execute batch permit *permit*
no operation execute batch permit [*permit*]

[Setting value and initial value]

- *permit*
 - [Setting value]:

Setting value	Explanation
on	Allow batch file execution by the DOWNLOAD button
off	Do not allow batch file execution by the DOWNLOAD button

- [Default]: off

[Explanation]

Whether to use the batch file execution function or not is set by the DOWNLOAD button.

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 37

HTTP upload function

This function allows you to upload the information (configuration file or SYSLOG) in a Yamaha router to a specified HTTP server.

It can be used for centralized management of configuration files and logs at multiple locations.

The configuration file is the **show config** command or the **show config N** command, and the execution result of the **show log** command is saved as a file for SYSLOG.

The name of the executed command is displayed at the top of the saved file.

When collecting information from multiple Yamaha routers on an HTTP server, files can be stored by specifying directories.

To specify a directory, set it with the **http upload** command.

In order to use this function, it is also necessary to deal with the HTTP server side.

It does not depend on the OS type of the HTTP server (Windows, UNIX, etc.), but when using an HTTP server on UNIX, the CGI script is executed with the nobody user privilege, so the generated file also has the nobody user privilege. The permissions of the CGI execution directory must be satisfied with [rw-].

The script file that needs to be run on the HTTP server side and technical information about this function are URLs shown below.

They are published at

<https://www.rtpro.yamaha.co.jp>

37.1 HTTP file configuration

[Format]

http upload type [*config_no*] [*directory/*] *filename*

no http upload type [...]

[Setting value and initial value]

- *type*
 - Setting value: 'config' or 'log'
 - Initial value: -
- *config_no*
 - Setting value: 0-4.2
 - Initial value: -
- *directory*
 - Setting value: Output directory name
 - [Initial value]: -
- *filename*
 - [Setting value]: File name of the output destination
 - [Initial value]: -

[Description]

Set the information to be uploaded to an HTTP server, and the directory name and file name of the save destination. Create a directory with the specified directory name, and create a file with the specified file name in that directory (e.g., dir1/dir2/config.txt).

The following can also be specified for the directory name and file name.

String	Meaning
% y	Year(yyyy)

String	Meaning
% m	Moon(mm)
% d	Sun (dd)
% H	Hour(hh)
% M	Minute(mm)
% S	Seconds(ss)
% n	Serial number
% a	MAC address of LAN1
% P	Model name

When specifying a character string including '%' in the directory or file name, it is necessary to specify '%' followed by '% '.

Only when 'config' is specified for *type*, *config_no* is enabled, and when *config_no* is omitted, the running config is targeted for upload.

Note that *config_no* can be set only for models that support the setting file multiplexing function.

[設定例]

Upload the directory and file "(model name)/(serial number)/(MAC address of LAN1)/20100101/120000.txt"

```
# http upload config %P/%n/%a/%y%m%d/%H%M%S.txt
```

Upload the file "% config.txt"

```
# http upload config %%config.txt
```

[Applicable model]

RTX1300, RTX1220, RTX1210

37.2Setting the URL of the HTTP upload destination

Format

http upload url *url*

no http upload url [*url*]

[Setting value and initial value]

- *url*
 - Setting value: URL of the upload destination
 - [Initial value]: -

[Description]

Setting the URL of the HTTP server to be used for HTTP upload

The HTTP server must be configured to allow cgi, and must execute cgi to accept the upload.

[Applicable model]

RTX1300, RTX1220, RTX1210

37.3Setting whether to allow HTTP upload

Format

http upload permit *switch*

no http upload permit [*switch*]

Setting value and initial value

- *switch*
 - Setting value:

Setting value	Explanation
on	Allow HTTP upload
off	Do not allow HTTP Uploads

- [Initial value]: off

[Explanation]

Set whether to allow HTTP Uploads.

[Applicable model]

RTX1300, RTX1220, RTX1210

37.4 Setting the timeout period for HTTP Uploads

[Format]

http upload timeout *time*

no http upload timeout [*time*]

[Setting value and initial value]

- *time*
 - [Setting value]: 1-180[seconds]
 - [Initial value]: 30

[Explanation]

Set the timeout period for HTTP Uploads.

[Applicable model]

RTX1300, RTX1220, RTX1210

37.5 Setting the retry interval and number of HTTP Uploads

[Format]

http upload retry interval *interval count*

no http upload retry interval [..]

[Setting value and initial value]

- *Interval*
 - [Setting value]: 1-60[seconds]
 - [Initial value]: 30
- *count*
 - [Setting value]: 1-10
 - [Initial value]: 5

[Explanation]

Set the retry interval and time when HTTP Uploads fail.

[Applicable model]

RTX1300, RTX1220, RTX1210

37.6 Configuring a proxy server used for HTTP Uploads

[Format]

http upload proxy *proxy* [*port*]

no http upload proxy [..]

[Setting value and initial value]

- *proxy*
 - [Setting value]: Proxy server
 - [Initial value]: -
- *port*
 - [Setting value]: 1-65535

- [Initial value]: 80

[Explanation]

Configure a proxy server used for HTTP Uploads.

[Applicable model]

RTX1300, RTX1220, RTX1210

37.7Execute HTTP Uploads

[Format]

http upload

go [Explanation]

Execute HTTP Uploads.

If the upload fails, retry based on the settings of the **http upload retry interval** command.

[Notes]

If the **alarm http upload** command is set to 'on', an alarm sound will sound depending on whether the upload is successful or not.

It can be specified with the **schedule at** command, and can be executed when startup is specified.

If startup is specified, the upload may fail because the route to the HTTP server has not been established immediately after startup. In such a case, it can be handled by retrying with the **http upload retry interval** command.

[Applicable model]

RTX1300, RTX1220, RTX1210

37.8Setting whether to sound an alarm sound related to the HTTP Upload feature.

[Format]

alarm http upload *switch*

no alarm http upload [*switch*]

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Description
on	Ring
off	Don't ring

- [Initial value]: on

[Explanation]

Select whether to sound an alarm sound related to the HTTP upload function.

[Applied model]

RTX1300, RTX1220, RTX1210

CHAPTER 38

Bridge interface (bridge function)

The bridge interface accommodates multiple interfaces in one virtual interface, and performs bridging between the accommodated interfaces.

The physical segment to which each accommodated interface connects is treated as one segment.

Notes

- The bridge processing in this function does not guarantee the wire rate.
- The QoS function is not supported. Therefore, the Dynamic Traffic Control function using the QoS function cannot be used.
- It does not support the spanning tree protocol.
- BPDU frames are transparent.
- IEEE802.1Q tagged packets are transparent (except for vRX series).

38.1 Setting interfaces accommodated in bridge interfaces

[Format]

bridge member *bridge_interface interface interface* [...]

no bridge member *bridge_interface [interface ...]*

[Setting value and initial value]

- *bridge_interface*
 - [Setting value]: Bridge interface name
 - [Initial value]: -
- *interface*
 - [Setting value]:

Setting value	Description
lanN	LAN interface name
lanN.M	LAN split interface name (Not specified for vRX series and RTX1300)
vlanN	VLAN interface name (Not specified for RTX830 and vRX series)
tunnelN	TUNNEL interface name
tunnelN-tunnelM	Scope of the TUNNEL interface (Not specified for RTX830 if an extended license is not imported)

- [Initial value]: -

[Explanation]

Designating interfaces accommodated in bridge interfaces that are virtual interfaces.

Bridge operations are performed between the accommodated interfaces. When a tunnel interface is accommodated, bridge operations are performed only at the tunnel interface where an L2TPv3 tunnel is established.

[Notes]

- About accommodating LAN interfaces

IPv4 and IPv6 addresses must not be assigned to the real interfaces accommodated. IPv6 link-local addresses of the real interfaces accommodated are deleted.

MTUs of the LAN interfaces accommodated must all have the same value.

The real interfaces accommodated in any bridge interface cannot be accommodated in other bridge interfaces.

If the interface accommodated is an interface with a switching hub, the communication between ports of the switching hub is completed.

The communication to be connected is not bridge operations by this function, but is processed inside the switching hub LSI.

In the cloud version of vRX Sakura, even if a LAN interface is accommodated, packets to be forwarded are discarded in a cloud virtual network (VPC), so they should not be accommodated.

Tunnel interfaces to be accommodated

The MTU of the accommodated tunnel interface is invalidated, fragments are not performed at the tunnel interface, and fragments are generated according to the MTU of the transmission interface of the encapsulated packet.
An interface accommodated in any bridge interface cannot be accommodated in another bridge interface.

Bridge interfaces

The link state of the bridge interface changes according to the link state of the accommodated LAN interface or tunnel interface.

If any accommodated interface is in an up state, the bridge interface is in an up state. If all interfaces are in a down state, the bridge interface is also in a down state.

The MAC address of the bridge interface uses the address of the interface with the smallest interface number among the accommodated LAN interfaces.

It cannot be used with RTX5000 / RTX3500 Rev.14.00.11 or earlier.

[Supports extended licenses]

Importing an [extended license](#) expands the maximum number of interfaces that can be accommodated in the bridge interface.

- *interface*

License name	Maximum number after expansion (Values per license)				
	1	2	3	4	5
YSL-VPN-EX1	10	-	-	-	-
YSL-VPN-EX2	30				
YSL-VPN-EX3	50				-

[Applicable models]

vRX VMware ESXi version, vRX Sakura cloud version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

38.2Setting whether to perform automatic learning

[Format]

bridge learning *bridge_interface* *switch*
no bridge learning *bridge_interface* [*switch*]

[Setting value and initial value]

- *bridge_interface*
 - Setting value: Bridge interface name
 - Initial value: -
- *switch*
 - Setting value:

Setting value	Explanation
on	Learning
off	Learning does not occur

- Initial value: on

[Description]

Setting whether to perform automatic MAC address learning by the bridge function.
The target bridge interface name is specified in bridge_interface.

When learning is performed, when a packet is received by the interface accommodated in the bridge interface, the starting point MAC address of the packet and the reception interface are learned and registered in a learning table.

The learned information is referred to when the bridge processing is performed, and packets are prevented from being output to unnecessary interfaces.

[Notebook]

When the learning table reaches the upper limit during learning, the oldest entry is deleted and registered.

When a learning table is referred to in the bridge processing, if there is no matching entry, packets are output to all accommodation interfaces except for the reception interface. This is similar to operation of a repeater.

RTX5000 can be used with Rev.14.00.12 or later.

RTX3500 can be used with Rev.14.00.12 or later.

[Applicable models]

vRX VMware ESXi Edition, vRX Sakura Cloud Edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

38.3 Setting a timer to erase information learned by the bridge.

[Format]

bridge learning *bridge_interface* **timer** *time*

no bridge learning *bridge_interface* **timer** [*time*]

[Setting value and initial value]

- *bridge_interface*
 - [Setting value]: Bridge interface name
 - [Setting value]: -
- *time*
 - [Setting value]:

Setting value	Description
30..32767	Number of seconds
off	Do not set a timer

- [Setting value]: 300

[Explanation]

Set the life span of information learned automatically by the bridge.

Specify the target bridge interface name in *bridge_interface*.

If a packet is not received from a starting MAC address within a specified time, learned information about the MAC address is deleted.

If off is specified, learned information is not automatically deleted.

[Notes]

RTX5000 can be used with Rev.14.00.12 or later.

RTX3500 can be used with Rev.14.00.12 or later.

[Applicable model]

vRX VMware ESXi version, vRX Sakura Cloud version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

38.4 Setting static learning information

[Format]

bridge learning *bridge_interface* **static mac_address** *interface*

no bridge learning *bridge_interface* **static mac_address** [*interface*]

[Setting value and initial value]

- *bridge_interface*
 - [Setting value]: Bridge interface name
 - [Setting value]: -
- *mac_address*
 - [Setting value]: MAC address
 - [Setting value]: -
- *interface*
 - [Setting value]: LAN interface name
 - [Setting value]: -

[Explanation]

Set static registration information referenced by the bridge.

Specify the target bridge interface name in *bridge_interface*.

Packets whose destination is the MAC address specified in *mac_address* are output to the interface specified in *interface*.

Specify the target LAN interface accommodated in *bridge_interface* in *interface*.

[Notes]

Statically registered information is referenced with priority over automatically learned information.

If the LAN interface specified in *interface* is not accommodated in *bridge_interface*, registered information is ignored.

RTX5000 can be used with Rev.14.00.12 or later.

RTX3500 can be used with Rev.14.00.12 or later.

[Applicable model]

vRX VMware ESXi version, vRX Sakura Cloud version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 39

Lua Scripting

It is a function to execute a script written in Lua language. By embedding an API dedicated to Yamaha routers in Lua scripts, it becomes possible to change router settings and program actions according to the router status.

39.1 Setting whether to enable the Lua scripting function

[Format]

```
lua use switch
no lua use [switch]
```

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Explanation
on	Enable
off	Disable

- [Initial value]: on

[Explanation]

Whether to enable the Lua scripting function is set.

If the Lua scripting function is disabled by this command while a Lua script is running, all running Lua scripts are forcibly terminated.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

39.2 Running Lua scripts

[Format]

```
lua [-e stat] [-l module] [-v] [--] [script_file [args ...]]
```

[Setting value and initial value]

- *stat*
 - [Setting value]: Script string
 - [Initial value]: -
- *module*
 - [Setting value]: Module name to be loaded
 - [Initial value]: -
- *script_file*
 - --Optional: Specify script file name or byte code file name as absolute path or relative path
 - [Initial value]: -
- *args*
 - [Setting value]: Variable arguments to pass to *script_file*
 - [Initial value]: -

[Explanation]

Run Lua scripts.

The basic syntax is the same as the Lua standard **lua** command, but it does not support the *-i/-* option, which uses standard input (stdin) as script input, and execution without parameters. The *-v* option outputs version information. --Option indicates that option processing ends at the point of description, and it is possible to specify a file name and character string starting with "-" in *script_file* or *args*. Note that each option of *-e/-l/-v* can be repeatedly specified, but it is indicated later than *script_file*.

It cannot be determined. Only one *script_file* can be specified, and all parameters after the point where *script_file* is written are ignored. At this time, no error message is output.

If a relative path is specified in *script_file*, it is interpreted as a path based on the environment variable PWD. PWD can be changed by the **set** command, and its initial value is */*.

[Notes]

If the environment variable LUA_INIT is set, the script is executed first.
When specifying a byte code file in *script_file*, only the byte code generated on the router can be executed, and the byte code generated on a PC with Lua installed cannot be executed.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

39.3Running the Lua compiler

[Format]

luac [-l] [-o output_file] [-p] [-s] [-v] [--] script_file [script_file ..]

[Setting value and initial value]

- *output_file*
 - [Setting value]: Specify the file name of the byte code output destination as an absolute path or a relative path.
 - [Setting value]: luac.out (relative path)
- *script_file*
 - [Setting value]: Specify the script file name to be compiled as an absolute path or a relative path.
 - [Initial value]: -

[Description]

Run the Lua compiler to generate bytecode.
The basic syntax is the same as the Lua standard **luac** command, but the - option cannot be specified. The -l option displays a list of generated bytecodes. The -p option only parses. The -s option removes debug information such as comments. The -v option outputs version information. The -- option indicates that the option processing is terminated at the described point, and a file name starting with "-" can be specified in *script_file*. It is also possible to specify multiple *script_files* and combine them into one bytecode file.

When a relative path is specified in *script_file/output_file*, it is interpreted as a path based on the environment variable PWD. The PWD can be changed with the **set** command, and the initial value is */*.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

39.4Displaying the running status of Lua scripts

[Format]

show status lua [info]

[Setting value and initial value]

- *info*: Type of information to display
 - [Setting value]:

Setting value	Explanation
running	Information about scripts running
history	Information about scripts running in the past
Omitted	View all information

- [Initial value]: -

Description

The running status of the current Lua script and the past running history are displayed. This information is cleared by disabling the Lua scripting feature with the **lua use** command.

- Lua version information
- Scripts running
 - Lua task number
 - Running status

RUN	Running
SLEEP	Sleeping
WATCH	SYSLOG monitoring (Lua task is sleeping)
COMMUNICATE	Communication in progress
TERMINATE	Forced termination

- Trigger
 - **The lua** command
 - **The luac** command
 - Schedule
 - DOWNLOAD button
- Command line
- Script file name
- Monitoring string (when monitoring SYSLOG)
- Start date/time/running time
- Scripts running in the past [history] (displayed in descending order of the latest 10 types)
 - Trigger
 - **The lua** command
 - **The luac** command
 - Schedule
 - DOWNLOAD button
 - Command line
 - Script file name
 - Number of runs/number of errors/error history (displayed in descending order of the latest 5 runs)
 - Previous start date/time/running result

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

39.5 Forced termination of Lua scripts

[Format]

terminate lua *task_id*

terminate lua file *script_file*

[Setting value and initial value]

- *task_id* : Lua task number to kill
- [Setting value]:

Setting value	Description
all	All Lua task numbers
1..10 (1..9 for models without DOWNLOAD button)	Lua task number

- [Initial value]: -
- *script_file*
 - [Setting value]: Specify script file name or byte code file name to be killed as absolute path or relative path
 - [Initial value]: -

[Explanation]

Kill specified Lua task or Lua script.

In the first format, kill Lua task specified by *task_id*. Lua task number and running script can be confirmed by **show status lua** command.

In the second format, kill all Lua tasks running a script whose path and file name exactly match that specified by *script_file*. If a relative path is specified in *script_file*, target Lua task is searched after it is replaced with absolute path based on environment variable PWD.

Use the first format when -e option of **lua** command is used to kill Lua script running without using script file.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

39.6Setting alarm sound related to Lua script function

[Format]

alarm lua *switch*

no alarm lua [*switch*]

[Setting value and initial value]

- switch*
- [Setting value]:

Setting value	Description
on	Ring
off	Don't sound

- [Initial value]: on

[Explanation]

Whether to sound alarm sound related to Lua script function can be selected.

[Notes]

This command can set whether to sound alarm sound related to Lua script execution by DOWNLOAD button. Whether to sound alarm sound by control in hardware library depends on **alarm entire** command setting.

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 40

Custom GUI

Custom GUI is a function that allows user to design and incorporate a GUI (user interface corresponding to WWW browser) for setting router. Router has interface to transfer configuration via HTTP from host, user creates GUI using JavaScript.

Yamaha router has WWW browser setting support function, but it was not possible to change the setting screen for each user. In this function, multiple custom GUI are incorporated, and it is possible to switch the screen by user who logs in.

40.1 Setting whether to use custom GUI

[Format]

```
httpd custom-gui use use
no httpd custom-gui use [use]
```

[Setting value and initial value]

- *Use*
- [Setting value]:

Setting value	Description
on	Use
off	Do not use

- [Initial value]: off

[Explanation]

Setting whether or not to use a custom GUI.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

40.2 Setting a user to use a custom GUI

[Format]

```
httpd custom-gui user [user] directory=path [index=name]
no httpd custom-gui user [user...]
```

[Setting value and initial value]

- *user*
 - [Setting value]: User name
 - [Initial value]: -
- *path*
 - [Setting value]: Absolute path or relative path of the base directory
 - [Initial value]: -
- *name*
 - [Setting value]: Output file name when accessing with a slash '/' stop URL
 - [Setting value]: index.html

[Explanation]

Setting a user to use a custom GUI Accessing `http://(router's IP address)/` and logging in with the user name registered by this command redirects to `http://(router's IP address)/custom/user/`.

Setting is for an unknown user when *user* is omitted. The URL in this case is `http://(router's IP address)/custom/anonymous.user/`.

Specify the base directory as absolute path or relative path in *path*. If specified by a relative path, the environment variable

interpreted as a path based on PWD. PWD can be changed by the set command, and the initial value is `"/`.

For *name*, specify the file name to be displayed when accessing with a '/' stop URL from the browser.

[Notes]

When setting this command, it is necessary to register a user with a **login user** command in advance except for an unknown user. Setting this command for an unregistered user results in an error.

Since an unknown user cannot be registered in RTX1300 and RTX840, the *user* cannot be omitted.

A user to whom this command is set cannot access the normal GUI built into the router.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

40.3 Setting whether or not to use a custom GUI API

[Format]

httpd custom-gui api use use

no httpd custom-gui api use [use]

[Setting value and initial value]

- *Use*
 - [Setting value]

Setting value	Explanation
on	Use
off	Not used

- [Initial value]: off

[Description]

Set whether or not to accept a POST request for the URL "http://(router's IP address)/custom/api" for API.

[Notes]

In order to use the URL for API, **httpd custom-gui use on** must be set in addition to this command.

Even if this command is turned on, the URL for API cannot be used unless **httpd custom-gui api password** command is set.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

40.4 Setting a password to access a custom GUI API

[Format]

httpd custom-gui api password password

no httpd custom-gui api password [password]

[Setting value and initial value]

- *password*
 - [Setting value]: Password
 - [Initial value]: -

[Description]

Set the password when sending a POST request to the URL for API. Half-width alphanumeric characters up to 32 characters can be used.

For example, if doremi is set as the password in this command, the URL becomes http://(router IP address)/custom/api?password=doremi.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 40

Custom GUI

Custom GUI is a function that allows user to design and incorporate a GUI (user interface corresponding to WWW browser) for setting router. Router has interface to transfer configuration via HTTP from host, user creates GUI using JavaScript.

Yamaha router has WWW browser setting support function, but it was not possible to change the setting screen for each user. In this function, multiple custom GUI are incorporated, and it is possible to switch the screen by user who logs in.

40.1 Setting whether to use custom GUI

[Format]

```
httpd custom-gui use use
no httpd custom-gui use [use]
```

[Setting value and initial value]

- *Use*
- [Setting value]:

Setting value	Description
on	Use
off	Do not use

- [Initial value]: off

[Explanation]

Setting whether or not to use a custom GUI.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

40.2 Setting a user to use a custom GUI

[Format]

```
httpd custom-gui user [user] directory=path [index=name]
no httpd custom-gui user [user...]
```

[Setting value and initial value]

- *user*
 - [Setting value]: User name
 - [Initial value]: -
- *path*
 - [Setting value]: Absolute path or relative path of the base directory
 - [Initial value]: -
- *name*
 - [Setting value]: Output file name when accessing with a slash '/' stop URL
 - [Setting value]: index.html

[Explanation]

Setting a user to use a custom GUI Accessing `http://(router's IP address)/` and logging in with the user name registered by this command redirects to `http://(router's IP address)/custom/user/`.

Setting is for an unknown user when *user* is omitted. The URL in this case is `http://(router's IP address)/custom/anonymous.user/`.

Specify the base directory as absolute path or relative path in *path*. If specified by a relative path, the environment variable

interpreted as a path based on PWD. PWD can be changed by the set command, and the initial value is `"/`.

For *name*, specify the file name to be displayed when accessing with a '/' stop URL from the browser.

[Notes]

When setting this command, it is necessary to register a user with a **login user** command in advance except for an unknown user. Setting this command for an unregistered user results in an error.

Since an unknown user cannot be registered in RTX1300 and RTX840, the *user* cannot be omitted.

A user to whom this command is set cannot access the normal GUI built into the router.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

40.3 Setting whether or not to use a custom GU API

[Format]

httpd custom-gui api use use

no httpd custom-gui api use [use]

[Setting value and initial value]

- *Use*
 - [Setting value]

Setting value	Explanation
on	Use
off	Not used

- [Initial value]: off

[Description]

Set whether or not to accept a POST request for the URL "http://(router's IP address)/custom/api" for API.

[Notes]

In order to use the URL for API, **httpd custom-gui use on** must be set in addition to this command.

Even if this command is turned on, the URL for API cannot be used unless **httpd custom-gui api password** command is set.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

40.4 Setting a password to access a custom GU API

[Format]

httpd custom-gui api password password

no httpd custom-gui api password [password]

[Setting value and initial value]

- *password*
 - [Setting value]: Password
 - [Initial value]: -

[Description]

Set the password when sending a POST request to the URL for API. Half-width alphanumeric characters up to 32 characters can be used.

For example, if doremi is set as the password in this command, the URL becomes http://(router IP address)/custom/api?password=doremi.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

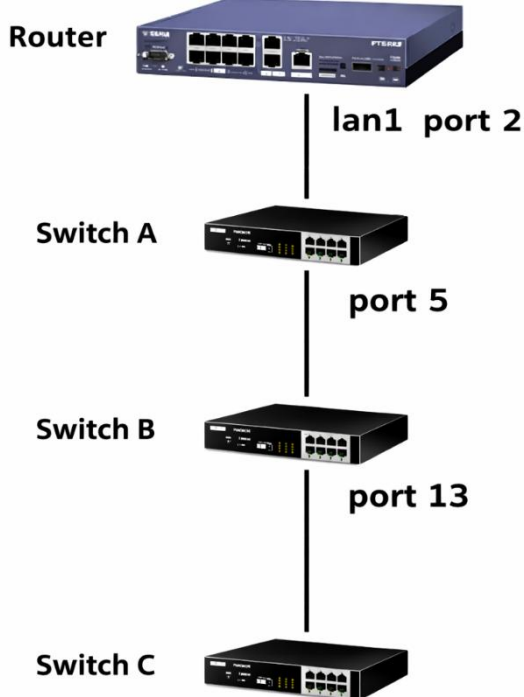
CHAPTER 41

L2MS

L2MS is a function for controlling Yamaha network equipment (switches, wireless LAN access points, routers) from a router. In L2MS, the equipment that controls is called a manager, and the equipment that is controlled by a manager is called an agent. To control an agent, refer to the control command corresponding to each equipment in addition to the common settings.

When specifying a switch or an access point in each command of this function, there are two methods: specifying by MAC address and specifying by route.

In the method of specifying by route, the port numbers of each switch in the middle are specified in order from the router as a base point.



The notation is "lan1:2-5-13" when specifying switch C in the configuration shown above.

- First specify the LAN interface of the router.
- If the LAN interface is a switching hub, specify the port number. The port number is separated by a colon ":".
- If the LAN interface is not a switching hub, it is unnecessary to specify the port number.
- Specify the port number of each switch between the router and switch C in order from the one closest to the router. Each port number is separated by a hyphen "-".

For details on the types of equipment that can be controlled by L2MS and compatible firmware revisions, please refer to the technical documentation of L2MS shown below.

<https://www.rtpro.yamaha.co.jp/RT/docs/swctl/>

41.1 Common settings

41.1.1 Setting whether to use L2MS

[Format]

switch control use *interface use* [terminal=*terminal*]

no switch control use *interface* [*use* [terminal=*terminal*]]

[Setting value and initial value]

- *interface*

- [Setting value]: LAN interface name, bridge interface name, VLAN interface
- [Initial value]: -
- *Use*
- [Setting value]:

Setting value	Explanation
on	Using L2MS
off	Do not use L2MS

- [Initial value]: off
- *terminal*
- [Setting value]:

Setting value	Explanation
on	Terminal information is acquired
off	Terminal information is not acquired

- [Initial value]: off

Explanation

Whether to use L2MS is set for each interface. Using L2MS on an interface where *use* is set to on. L2MS operates according to the setting of the **switch control use** command. When operating as a manager of L2MS, it performs communication for controlling an agent corresponding to L2MS. In addition, terminal information is acquired on an interface where the *terminal* option is set to on. Unnecessary packet transmission can be suppressed by setting *use* to off in an interface that does not use L2MS. When operating as an agent of L2MS, it returns a response packet for a search packet from the manager.

Notebook

If the mode is set to off in the **switch control mode** command, the setting of this command is not reflected.

If the mode is set to agent in the **switch control mode** command, L2MS is not enabled on a VLAN interface regardless of the setting of this command.

This command cannot be set on an interface where the port separation function is enabled.

Firmware after Rev.14.01 can set this command on an interface where the port separation function is enabled.

If a LAN interface is not accommodated in a **bridge member** command, the setting of this command to a bridge interface is not reflected. Also, if the *use* is set to on on in the bridge interface and a LAN interface accommodated in the bridge interface, only the setting to the bridge interface is reflected. Firmware after RTX1210 Rev.14.01.20 and all firmware after Rev.15.02 can set this command on a bridge interface.

The VLAN interface can be specified with RTX1210 Rev.14.01.42 or later, RTX830 Rev.15.02.30 or later, and RTX1220 Rev.15.04.07 or later.

In an interface where *use* is set to off, terminal information is not acquired even if the *terminal* option is set to on. Also, when operating as an agent of L2MS, the setting of the *terminal* option is not reflected in the operation of L2MS. The *terminal* option can be used with firmware after Rev.14.01 series.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.1.2 Setting the monitoring time interval of an agent

[Format]

switch control watch interval *time* [*count*]

no switch control watch interval

[Setting value and initial value]

- *time*
 - [Setting value]: Number of seconds (2...10)
 - [Initial value]: 3
- *count*

- [Setting value]: Number of times (2...10)
- [Initial value]: 3

[Description]

The transmission time interval of a packet for searching for an agent and the number of times of search packet transmission until it is determined that the agent is down without receiving a response packet from the agent are set.

When *time* is set to a small value, the frequency of search packet transmission decreases, but the time from when the agent is connected until the manager recognizes it becomes longer. When *time* is set to a small value, the opposite occurs, and the frequency of search packet transmission increases, but the time from when the agent is connected until the manager recognizes it becomes shorter.

When a response packet is not received from an agent even if search packets are transmitted for the number of times set in *count*, it is determined that the agent is down.

[Notes]

When manager is not set to *mode* in a **switch control mode** command, the setting of this command is not reflected in the operation of L2MS.

When an Ethernet cable connecting an agent is unplugged, it may be determined that the agent is down earlier than the setting of this command.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.1.3 Setting the monitoring time interval of terminal information

[Format]

lan-map terminal watch interval *time1* [*time2*]

no lan-map terminal watch interval [*time1* [*time2*]]

[Setting value and initial value]

- *time1*
 - setting value: Interval for acquiring terminal information under a manager/agent (seconds) (1800...86400)
 - [Initial value]: 1800
- *time2*
 - setting value: Interval for acquiring terminal information under an agent in which connection/disconnection of a terminal cannot be notified immediately (seconds) (10...86400)
 - [Initial value]: 60

[Explanation]

Setting the interval for periodically acquiring terminal information of a network managed by a LAN map.

The manager updates terminal information of a LAN map on the basis of terminal information acquired at the opportunity of immediate notification of connection/disconnection of a terminal from each agent and terminal information acquired at the opportunity of periodic acquisition processing performed to each agent at a specified interval. However, there are agents that can immediately notify connection/disconnection of a terminal and agents that cannot immediately notify connection/disconnection of a terminal, and the execution interval and purpose of periodic acquisition processing differ from each other as follows.

- Periodic acquisition 1

The manager and an agent that can immediately notify connection/disconnection of a terminal are used as target devices, and the *terminal information* is acquired every time the time set in *time1* elapses. *Periodic acquisition 1 aims at correcting terminal information. Connection/disconnection of a terminal under an agent that can immediately notify connection/disconnection of a terminal is immediately reflected on the LAN map without waiting for the elapse of time1. However, when there is no communication from a terminal and the terminal is not registered in a MAC address table of an agent or the terminal information cannot be received due to packet loss, the connection of a terminal is not immediately reflected on the LAN map. In such a case, it is reflected on the LAN map when the terminal information can be acquired by periodic acquisition performed every time time1 elapses.*
- Periodic acquisition 2

The agent that cannot immediately notify connection/disconnection of a terminal is used as the target device, and the terminal information is acquired every time the time set in *time2* elapses. The connection/disconnection of a terminal under an agent in which connection/disconnection of a terminal cannot immediately be notified is not immediately reflected on the LAN map and is reflected at intervals of *time2*.

[Notes]

The agents that cannot immediately notify connection/disconnection of a terminal are the following wireless APs.

- WLX202
- WLX302
- WLX313
- WLX402 (Firmware before Rev.17.00.09)

Other agents can immediately notify connection/disconnection of a terminal.

When *manager* is not set in *mode* in a **switch control mode** command, the setting of this command is not reflected on the operation of L2MS.

When *on* is not set in a *terminal* option in a **switch control use** command, the terminal information is not corrected or updated regardless of the setting of this command.

The *time2* option is available for RTX1210 after Rev.14.01.09.

[Applicable models]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.1.4 Setting whether to use the snapshot function

[Format]

lan-map snapshot use interface use [*terminal=terminal*]

no lan-map snapshot use interface [*use* [*terminal=terminal*]]

[Setting value and initial value]

- interface*

- [Setting value]: LAN interface name, bridge interface name, VLAN interface
- [Setting value]: -

- Use*

- [Setting value]:

Setting value	Description
on	Use
off	Do not use

- [Setting value]: off

- terminal*

- [Setting value]: off

Setting value	Description
on	Include terminal information
off	Do not include terminal information
wired-only	Include only wired terminal information

- [Setting value]: off

Description

Whether or not to use the snapshot function of a LAN map is set for each interface. In an interface where the *terminal* option is set to on, terminal information is included in the target of the snapshot function. In an interface where the *terminal* option is set to wired-only, only wired terminal information is included in the target of the snapshot function. Wirelessly connected terminal information is not included in the target of the snapshot function.

[Notes]

If *manager* is not set in *mode* by a **switch control mode** command, the setting of this command is not reflected in the operation of L2MS.

If the *terminal* option is not set to on by a **switch control use** command, terminal information is not included in the target of the snapshot function regardless of the setting of this command.

Bridge interface can be specified by RTX1210 Rev.14.01.20 or later firmware and all firmware after Rev.15.02 series.

VLAN interface can be specified by RTX1210 Rev.14.01.42 or later, RTX830 Rev.15.02.30 or later, RTX1220 Rev.15.04.07 or later, and RTX840.

wired-only can be specified by RTX1210 Rev.14.01.09 or later firmware and all firmware after Rev.15.02 series.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.1.5Create a s snapshot file

Format

take lan-map snapshot interface [update]

[Setting value and initial value]

- interface
 - [Setting value]: LAN interface name, bridge interface name, VLAN interface
 - [Initial value]: -
- update : Create a snapshot file after updating the network connection status
 - [Initial value]: -

[Description]

Create a base snapshot file by the snapshot function of a LAN map. If the *update* option is not included, save the network status currently held by the manager as a snapshot file. If the *update* option is included, update the network connection status information to the latest and save it as a snapshot file.

[Notes]

This command can be used if manager is set to *mode* by a **switch control mode** command. The following SYSLOG is output when creating a snapshot file starts.

[LANMAP] SnapShot(LAN1): Take snapshot files: Start.

The following SYSLOG is output when creating a snapshot file is completed.

[LANMAP] SnapShot(LAN1): Take snapshot files: Complete.

If the *update* option is included, the network connection status information is updated to the latest, but it may take time to complete the update depending on the configuration of the network.

The bridge interface can be specified by firmware of RTX1210 Rev. 14.01.20 or later and all firmware of Rev. 15.02 or later.

The VLAN interface can be specified by firmware of RTX1210 Rev. 14.01.42 or later, RTX830 Rev. 15.02.30 or later, RTX1220 Rev. 15.04.07 or later, and RTX840.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.1.6Setting the SYSLOG output of a LAN map

Format

lan-map log sw
no lan-map log [sw]

[Setting value and initial value]

- SW
 - [Setting value]: off

Setting value	Description
on	Output
off	Do not output

- [Setting value]: off

[Explanation]

Set the SYSLOG output related to the LAN map.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.1.7 Setting the device name used in the LAN map

[Format]

lan-map *sysname name*
no lan-map *sysname [name]*

[Setting value and initial value]

- *Name*
 - [Setting value]: Device name (one or more half-width characters, 32 or less characters)
 - [Setting value]: (product name)_(serial number)

[Explanation]

Set the device name to be displayed on the LAN map. The characters that can be used for *name* are half-width alphanumeric characters, hyphens (-), underscores (_), and spaces (). To include spaces, enclose the entire *name* in double quotes (") or single quotes (').

[Notes]

RTX1210 can be used after Rev. 14.01.20.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.2 Switch control

41.2.1 Switch selection

[Format]

switch select *switch*
no switch select

[Setting value and initial value]

- *switch*
 - [Setting value]:

Setting value	Description
Switch	MAC address or route
None	Do not select a switch

- [Initial value]: -

[Explanation]

Select the switch to be targeted. After that, the character string set in console prompt and the selected switch are displayed continuously in the prompt.

When **switch select none** or **no switch select** is executed, switches are not displayed in the prompt.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.2.2 Switch function setting

[Format]

switch control function set *function [index ...] value*
no switch control function set *function [index ...]*

[Setting value and initial value]

- *Function*
 - Setting value: Function name
 - [Initial value]: -
- *index*
 - Setting value: Index

- [Initial value]: -
- *value*
 - [Set value]: Set value
 - [Initial value]: -

[Explanation]

The function of the switch is set. The name of the function to be set and the setting value for the function are specified as a parameter. The index is specified in the function in which multiple setting objects exist.

It can be interrupted by pressing Ctrl-C during command execution. However, it can not be interrupted, when synchronization processing is started after execution.

[Notes]

It is necessary to specify the switch by **switch select** before executing this command.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.2.3 The setting contents and operation state of the function of the switch are acquired.

[Format]

switch control function get *function* [index ...] [*switch*]

[Set value and initial value]

- *Function*
 - [Set value]: The name of the function
 - [Initial value]: -
- *index*
 - [Set value]: The index
 - [Initial value]: -
- *switch*: Switch
 - [Set value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

The setting contents and operation state of the function of the switch are acquired. The name of the function to be acquired is specified as a parameter. The index is specified in the function in which multiple acquisition objects exist.

It can be interrupted by pressing Ctrl-C during command execution.

[Notes]

If *switch* is not specified, it is necessary to specify the switch by **switch select** before executing this command.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.2.4 Specific operation is executed for the switch.

[Format]

switch control function execute *function* [index ...] [*switch*]

[Set value and initial value]

- *Function*
 - [Set value]: The name of the function
 - [Initial value]: -
- *index*
 - [Set value]: The index
 - [Initial value]: -
- *switch*: Switch
 - [Set value]:

- MAC address
- Route
- [Initial value]: -

[Explanation]

Specific operation is executed for the switch. The name of the function corresponding to the operation to be executed is specified as a parameter. The index is specified in the function in which multiple execution objects exist.

It can be interrupted by pressing Ctrl-C during command execution.

[Notes]

If *switch* is not specified, it is necessary to specify the switch by **switch select** before executing this command.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.2.5 Deleting the setting of the switch

[Format]

switch control function default [both] [*switch*]

[Set value and initial value]

- Both : Deletes all applicable settings for the target switch.
 - [Initial] : -
- *switch*: Switch
 - [Setting value] :
 - MAC address
 - Route
 - [Initial] : -

[Explanation]

Delete settings on the router for the selected switch. Simultaneously, synchronization processing is performed when the router controls the switch.

When the both option is not specified, if other settings applicable to the switch exist, the switch is synchronized with that setting. For example, when this command is executed by selecting the MAC address specification setting in a state where MAC address specification and route specification settings exist, after the MAC address specification setting is deleted, the switch is synchronized with the route specification setting.

When the both option is specified, if other settings applicable to the switch exist, that setting is also deleted at the same time. In the above example, both MAC address specification and route specification settings are deleted.

That is, if you want to initialize the switch reliably, specify the both option.

[Notes]

If *switch* is not specified, it is necessary to specify the switch with **switch select** before executing this command.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.2.6 Updating the firmware of the switch

[Format]

switch control firmware upload go file [*switch*]

[Setting value and initial value]

- *file*
 - [Setting value] : Relative or absolute path of the firmware to the file
 - [Initial] : -
- *switch*: Switch
 - [Setting value] :
 - MAC address
 - Route
 - [Initial] : -

[Explanation]

Updating the firmware of the switch The firmware file is saved in flash ROM or external memory beforehand, and the path is specified in *file*. When the firmware is successfully rewritten, the switch restarts automatically.

It can be interrupted by pressing Ctrl-C during command execution.

If a relative path is specified in *file*, it is interpreted as a path based on the environment variable PWD. PWD can be changed with the **set** command, and the initial value is */*.

[Notes]

If *switch* is not specified, it is necessary to specify the switch with **switch select** before executing this command.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.2.7 Setting of LAN cable duplication function

[Format]

switch control route backup *route port*

no switch control route backup *route*

[Setting value and initial value]

- *route*
 - [Setting value] : Main route
 - [Initial] : -
- *port*
 - [Setting value] : Port number used as a backup route
 - [Initial] : -

[Explanation]

Setting of a main route and a backup route for operating the LAN cable duplication function

The LAN cable duplication function operates with the route specified in *route* as the main route and the destination route connected to *port* as the backup route.

[Notes]

The following ports cannot be set to *port*

- Port specified as a main route in *route*
- Ports already configured with LAN cable duplication function

When this command is set for a switching hub of a router, the LAN cable duplication function operates only when the **switch control use** command is set to on in the configured LAN interface.

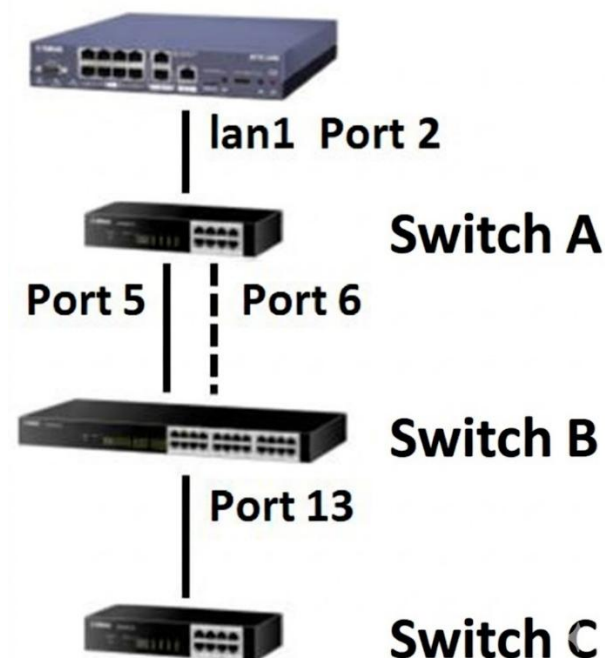
When this command is set for the switch, the link of the port temporarily goes down.

The operating state of the LAN cable duplication function can be confirmed by a **show status switch control route backup** command. If this function is not implemented in the switch, a command error occurs.

[Configuration Example]

Setting when port 5 of switch A is the main route and port 6 is the backup route as shown in the figure below.

```
switch control route backup lan1:2-5 6
```

**[Applicable model]**

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.2.8 Specifying a directory to store switch configuration files

[Format]

switch config directory *path*

no switch config directory [*path*]

[Setting value and initial value]

- *path*
 - [Setting value]: Relative path or absolute path (256 single-byte characters or less, 128 full-width characters or less)
 - [Initial value]: /sw_config

[Explanation]

Specify a directory to store switch configuration files (config).

When a relative path is specified, it is interpreted as a path starting from the environment variable PWD.

PWD can be changed with the **set** command, and the initial value is "/".

If *path* is an RTFS area, multibyte characters cannot be used in the *path*.

[Notes]

RTX1210 can be used after Rev. 14.01.28.

RTX830 can be used after Rev. 15.02.03.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.2.9 Specifying a file name to store switch settings

[Format]

switch config filename *name*

no switch config filename [*name*]

[Setting value and initial value]

- *name*
 - [Setting value]: config file name (99 single-byte characters or less, 49 full-width characters or less)
 - [Initial value]: -

[Explanation]

Specify a file name to save switch settings.

If this command is omitted, the file name is the string specified by **switch select with** .conf added. However, : (colon) is replaced by _ (underscore).

Multiple **switch select** commands can specify the same file name.

If the directory specified by **switch config directory** command is an RTFS area, multibyte characters cannot be used in the file name.

It is necessary to specify a switch with **switch select** command before executing this command.

[Notes]

RTX830 can be used after Rev. 15.02.03
RTX830 can be used after Rev. 15.02.03

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.2.10Obtaining switch settings

[Format]

switch control config get [*switch*]
switch control config get [[*interface*] all]

[Setting value and initial value]

- switch*
- [Setting value]:

Setting value	Explanation
MAC address or route	Only selected switches
all	All switches

- [Initial value]: -
- interface*
 - [Setting value]: LAN interface name, bridge interface name
 - [Initial value]: -

[Explanation]

Obtain and save switch setting files.

If the MAC address or route is specified in *switch* parameter, the specified switch setting file is obtained.

Specifying all obtains all switch setting files recognized by the manager.

When the *interface* parameter is specified, the switch connected to the specified interface is targeted.

When the *interface* parameter is omitted, it becomes the same as when all is specified.

[Notes]

For the name of the switch configuration file, use the file name specified by the **switch config directory** command. The switch configuration file is stored in the directory specified by the **switch config directory** command. It can be specified by the **schedule at** command.

RTX1210 can be used in Rev.15.02.03 or later.

RTX830 can be used in Rev.15.02.03 or later.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.2.11Restoring the switch configuration

[Format]

switch control config set [*switch*]
switch control config set [[*interface*] all]

[Setting value and initial value]

- *switch*
- [Setting value]:

Setting value	Description
MAC address or route	Selected switch only
all	All switches

- [Initial value]: -
- *interface*
 - [Setting value]: LAN interface name, bridge interface name
 - [Initial value]: -

[Description]

Restoring the switch configuration using the switch configuration file stored in the manager.

When the MAC address or route is specified in the *switch* parameter, the specified switch configuration is restored.

When all is specified, all switch configurations recognized by the manager are restored.

When *interface* parameter is specified, the switch connected to the specified interface is targeted.

When *interface* parameter is omitted, it becomes the same as when all is specified.

[Notes]

For the switch configuration file used for restoration, use the configuration file specified by the **switch config directory** command. The switch configuration file must be stored in the directory specified by the **switch config directory** command. It can be specified by the **schedule at** command.

RTX1210 can be used in Rev.15.02.03 or later.

RTX830 can be used in Rev.15.02.03 or later.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3 Switch function

41.3.1 System

41.3.1.1 Getting BootROM version

[Format]

switch control function get boot-rom-version [*switch*]

[Setting value and initial value]

- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Description]

Getting BootROM version

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.1.2 Getting firmware revision

[Format]

switch control function get firmware-revision [*switch*]

[Setting value and initial value]

- *switch*: Switch

- [Setting value]:
 - MAC address
 - Route
- [Initial value]: -

[Explanation]

Get a firmware revision.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.1.3 Get a serial number

[Format]

switch control function get serial-number [*switch*]

[Setting value and initial value]

- *switch*: switch
 - [Setting value]: -
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Get a serial number.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.1.4 Get a product name

[Format]

switch control function get model-name [*switch*]

[Setting value and initial value]

- *switch*: switch
 - [Setting value]: -
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Get a product name.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.1.5 Get a MAC address

[Format]

switch control function get system-macaddress [*switch*]

[Setting value and initial value]

- *switch*: switch
 - [Setting value]: -
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Get a MAC address.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.1.6 Set a name for the device

[Format]

switch control function set system-name
name *no switch control function set*
system-name switch control function get
system-name [*switch*]

[Setting value and initial value]

- *name*
 - Characters used for name of the device
 - Characters used for name of the device
- *switch*: switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Set the name of the device Characters used for *name* are single-byte alphanumeric characters, hyphens (-), and underscores (_).

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.1.7 Setting whether to use a power saving function

[Format]

switch control function set energy-saving
mode no switch control function set
energy-saving switch control function get
energy-saving [*switch*]

[Setting value and initial value]

- *Mode*
 - [Setting value]: off

Setting value	Description
on	Use
off	Do not use

- [Initial value]: off
 - *switch*: switch
 - [Setting value]: off
 - MAC address
 - Route
 - [Initial value]: -

Description

Whether or not to use the power saving function of a LAN port is set.

[Notes]

When the setting of this function is changed, all ports are temporarily linked down.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.1.8 LED の輝度の調整

[Format]

switch control function set led-brightness
mode no switch control function set led-
brightness switch control function get led-
brightness [*switch*]

[Setting value and initial value]

- *Mode*
 - [Setting value]: off

Setting value	Description
normal	Bright
economy	Dark

- [Initial value]: normal
- *switch*: switch
 - [Setting value]: off
 - MAC address
 - Route
 - [Initial value]: -

Description

Adjust the brightness of an LED.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.1.9 Obtaining the display mode of an LED

[Format]

switch control function get status-led-mode [*switch*]

[Setting value and initial value]

- *switch*: switch
 - [Setting value]: off
 - MAC address
 - Route
 - [Initial value]: -

Description

Obtain the current display mode of an LED for each LAN port.

Display mode	Description
link/act	Display the connection speed of each port. • Light green: Link established • Flashing green: Data transfer in progress • Off: Link lost
speed	Display the connection speed of each port. • Light green: Connected by 1000BASE-T • Solid orange: Connected via 100BASE-TX • Off: Connected via 10BASE-T
Duplex	Displays the connection status (full duplex/half duplex) of each port. • Solid orange: Connected via full duplex • Solid orange: Connected via half duplex
status	Displays the status of equipment. • Solid orange: Loop detected When a fan failure is detected by SWX2200-24G, the lower side of the mode LED blinks in orange.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.1.10 Obtaining the status of a fan

[Format]

switch control function get status-fan [*switch*]

[Setting value and initial value]

- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Obtaining the status of a fan

Condition	Description
normal	Normal
lock	Abnormalities

[Notes]

Available only for SWX2200-24G and SWX2200-8PoE

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.1.11 Obtaining the rotation speed of a fan

[Format]

switch control function get status-fan-rpm FAN [*switch*]

[Setting value and initial value]

- *FAN*
 - [Setting value]: Fan number
 - [Initial value]: -
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Obtaining the rotation speed of a fan

[Notes]

Available only for SWX2200-8PoE

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.1.12 Restart

[Format]

switch control function execute restart [*switch*]

[Setting value and initial value]

- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Restart the equipment.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.1.13 Retrieving the time since startup

[Settings]

switch control function get system-uptime [switch]

[Settings and initial values]

- switch: Switch
 - [Settings]:
 - MAC addresses
 - Routes
 - [Settings]: -

[Explanation]

Retrieving the time since startup.

[Applied models]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.2Ports

41.3.2.1 Retrieving the type of link aggregation

[Formats]

switch control function get lag-type [switch]

[Settings and initial values]

- switch: Switch
 - [Settings]:
 - MAC addresses
 - Routes
 - [Settings]: -

[Explanation]

Retrieving the type of link aggregation

Status	Description
Not bundle	Link aggregation is not configured
Type-A	Group#1: Ports 21, 22
Type-B	Group#1: Ports 21, 22 Group#2: Ports 23, 24
Type-C	Group#1: Ports 21, 22, 23, 24

[Notes]

Available only for SWX2100-24G

[Applied models]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.2.2 Setting the communication speed and operation mode of the port

[Settings]

switch control function set port-speed port
speed no switch control function set port-
speed port switch control function get port-
speed port [switch]

[Settings and initial values]

- port

- [Settings]: Port number
- [Settings]: -
- *speed*: Communication speed and operation mode
- [Settings]:

Settings	Description
Auto	Automatic speed discrimination
1000-fdx	1000BASE-T Full-duplex
100-fdx	100BASE-TX Full-duplex
100-hdx	100BASE-TX Half-duplex
10-fdx	10BASE-T Full-duplex
10-hdx	10BASE-T Half-duplex

- [Settings]: auto
- *switch*: Switch
- [Setting value]:
 - MAC address
 - Route
- [Initial value]: -

[Explanation]

Communication speed and operation mode of a port are set.

[Notes]

When the setting of this function is changed, the relevant port is temporarily linked down.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.2.3 Setting whether or not to use a port

[Format]

switch control function set port-use *port mode* **no switch control function set port-use** *port switch control function get port-use* *port* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *mode*
 - [Setting value]:

Setting value	Explanation
on	Use
off	Do not use

- [Initial value]: on
 - *switch*: switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Whether or not to use a port is set. When this function is set to off, even if a LAN cable is connected to the port, the link will not be up.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.2.4 Setting whether or not to use the auto-crossover function

[Format]

switch control function set port-auto-crossover *port*
mode no switch control function set port-auto-crossover *port switch control function get port-auto-crossover* *port* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *mode*
 - [Setting value]:

Setting value	Explanation
on	Use
off	Do not use

- [Initial value]: on
 - *switch*: switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Whether or not to use the auto-crossover function is set.

The auto-crossover function is a function for automatically determining whether a LAN cable is a straight cable or a cross cable and connecting them. When this function is set to on, it is not necessary to worry about the type of the cable.

[Notes]

When the setting of this function is changed, the link of the relevant port is temporarily linked down.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.2.5 Setting whether to use a speed downshift function

[Format]

switch control function set port-speed-downshift *port*
mode no switch control function set port-speed-downshift *port switch control function get port-speed-downshift* *port* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *Mode*
 - [Setting value]:

Setting value	Description
on	Use
off	Not used

- [Initial value]: on
 - *switch*: switch

- [Setting value]:
 - MAC address
 - Route
- [Initial value]: -

[Explanation]

Whether to use a speed downshift function is set.

The speed downshift function is a function to attempt to link by slowing down the speed when a LAN cable that cannot be used with, for example, 1000BASE-T is connected.

[Notes]

When the setting of this function is changed, the relevant port temporarily links down.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.2.6 Setting whether to use flow control**[Format]**

switch control function set port-flow-control *port*
mode **no switch control function set port-flow-**
control *port* **switch control function get port-flow-**
control *port* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *Mode*
 - [Setting value]:

Setting value	Description
on	Use
off	Not used

- [Initial value]: off
 - *switch*: switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Whether to use flow control is set.

When this function is set to on, flow control is enabled on both the receiving side and the transmitting side. Control by IEEE802.3x is performed when link-up is performed in full duplex, and control by a backpressure system is performed in half duplex.

[Notes]

When the setting of this function is changed, the relevant port temporarily links down.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.2.7 Setting whether to block L2MS packets**[Format]**

switch control function set port-blocking-control-packet *port*
mode **no switch control function set port-blocking-control-**
packet *port* **switch control function get port-blocking-control-**
packet *port* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number

- [Initial value]: -
- *Mode*
- [Setting value]:

Setting value	Description
on	Block control packets
off	Do not block control packets.

- [Setting value]: off
 - *switch*: switch
- [Setting value]: -
 - MAC address
 - Route
- [Initial value]: -

[Explanation]

Whether to block L2MS packets is set. When this function is set to on, communication for controlling a switch at the port is not performed.

[Notes]

If this function is not implemented in a Yamaha switch, a command error occurs.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.2.8 Whether to block data packets other than L2MS packets

[Format]

switch control function set port-blocking-data-packet *port*
mode **no switch control function set port-blocking-data-**
packet *port* **switch control function get port-blocking-data-**
packet *port* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *Mode*
- [Setting value]:

Setting value	Description
on	Block data packets
off	Do not block data packets

- [Initial value]: off
 - *switch*: switch
- [Setting value]:
 - MAC address
 - Route
- [Initial value]: -

[Explanation]

Whether to block data packets other than L2MS packets is set. When this function is set to on, data communication other than communication for controlling a switch at the port is not performed.

[Notes]

If this function is not implemented in a Yamaha switch, a command error occurs.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.2.9 Getting the usage of a combo port

[Format]

switch control function get status-combo-port *port* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *switch*: switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Get whether the port is used by SFP or Ethernet.

Status	Description
disable	Port not used
sfp	It is used as an SFP port.
ethernet	It is used as an e-support.

[Notes]

It can be used only with SWX2100-24G.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.2.10 Acquisition of light reception level of a port

[Format]

switch control function get status-port-sfp-rx-power *port* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

The light reception level of an SFP port is acquired.

Condition	Description
normal	Normal
low	The light reception level is below the lower threshold
high	The light reception level exceeds the upper threshold

[Notes]

It can be used only with SWX2100-24G.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.2.11 Acquisition of link status of a port

[Format]

switch control function get status-port-speed *port* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

The current link status of a port is acquired.

Condition	Description
1000-fdx	1000BASE-T full duplex
100-fdx	100BASE-TX full duplex
100-hdx	100BASE-TX half duplex
10-fdx	10BASE-T full duplex
10-hdx	10BASE-T half duplex
down	Link Down

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.3MAC address table

The size of the MAC address table of Yamaha Switch is as follows.

Model	Maximum number of entries
SWX2200-24G	8192
SWX2200-8G、SWX2200-8PoE	

41.3.3.1 Setting whether to use the MAC address aging function

[Format]

switch control function set macaddress-aging
mode no switch control function set
macaddress-aging switch control function get
macaddress-aging [*switch*]

[Setting value and initial value]

- *Mode*
 - [Setting value]:

Setting value	Description
on	Use
off	Not used

- [Initial value]: on
 - *switch*: switch
 - [Setting value]:
 - MAC address
 - Route

- [Initial value]: -

[Explanation]

Whether to use the MAC address aging function is set.

The MAC address aging function erases an entry in the MAC address table of the switch in a fixed time. When this function is set to off, the MAC address learned by the switch is not automatically erased.

The time interval to erase is set by **macaddress-aging-timer**.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.3.2 Setting the time interval for MAC address aging

[Format]

switch control function set macaddress-aging-timer *time*

no switch control function set macaddress-aging-

timer switch control function get macaddress-aging-

timer [*switch*]

[Setting value and initial value]

- *time*
 - Setting value: Number of seconds (10 .. 64800)
 - [Initial value]: 300

[Explanation]

In the MAC address aging function, the time interval for erasing the learned MAC address by the switch is set.

The time interval from when the switch learns the MAC address to when it erases the entry is the shortest number of seconds set by this function, and the longest number of seconds is twice as long. For example, if the setting value is 300 seconds, it will be a minimum of 300 seconds and a maximum of 600 seconds.

Note that when a frame from a learned MAC address is received again, the time interval until the entry is erased is reset.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.3.3 Searching the MAC address table using the MAC address as a key

[Format]

switch control function get status-macaddress-addr *mac_address* [*switch*]

[Setting value and initial value]

- *mac_address*
 - Setting value: MAC address
 - [Initial value]: -
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

A MAC address table is searched using the MAC address as a key, and a port number learned from the MAC address is acquired. When the same MAC address is learned in different VLANs, multiple port numbers may be displayed.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.3.4 Searching the MAC address table using the port number as a key

[Format]

switch control function get status-macaddress-port *port* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number

- [Initial value]: -
- *switch*: Switch
- [Setting value]:
 - MAC address
 - Route
- [Initial value]: -

[Explanation]

A MAC address table is searched using the port number as a key, and a MAC address learned in the port is acquired. When the same MAC address is learned in different VLANs, the same MAC address may be displayed in multiple ports.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.3.5 Clearing entries in the MAC address table

[Format]

switch control function execute clear-macaddress-table [*switch*]

[Setting value and initial value]

- *switch*: Switch
- [Setting value]:
 - MAC address
 - Route
- [Initial value]: -

[Explanation]

All entries in the MAC address table are cleared.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.4VLAN

When setting port VLAN/tag VLAN on a Yamaha switch, specify the VLAN registration number without directly entering the VLAN ID in the command. The VLAN registration number and the VLAN ID are linked with **vlan-id**. For example, if the following settings are made, the VLAN ID of port 2 is 4.

```
switch control function set vlan-id 10 4
switch control function set vlan-access 2 10
```

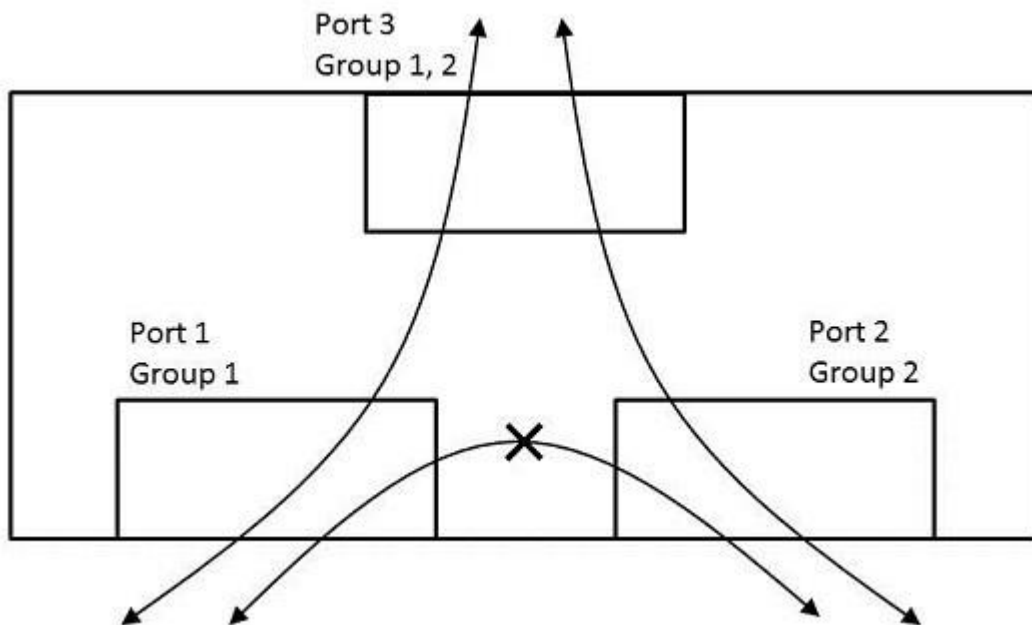
Packets received by the switch are classified into one of the VLAN IDs regardless of whether or not there is a VLAN tag, and transfer processing is performed based on that information. The VLAN operation mode of the port is set with **vlan-port-mode**.

vlan-port-mode	Behavior during reception	Behavior during reception
access	Only packets without a VLAN tag are received. The classification of the VLAN ID is based on the vlan-access setting.	When receiving, packets classified into the VLAN ID (vlan-trunk) of the port to be transmitted are sent with no VLAN tag.
trunk	Only packets with a VLAN tag are received. However, the port must be joined to the VLAN ID in the VLAN tag. The VLAN ID to which the port is joined is set with vlan-trunk . The classification of the VLAN ID is based on the information of the VLAN tag.	When receiving, packets classified into the VLAN ID (vlan-trunk) to which the port to be transmitted is joined are sent with a VLAN tag.

vlan-port-mode	Behavior during reception	Behavior during reception
hybrid	Both packets with and without a VLAN tag are received. If packets without a VLAN tag are received, the behavior is the same as for access ports. If packets with a VLAN tag are received, the behavior is the same as for trunk ports.	When receiving, packets classified into the VLAN ID (vlan-trunk) of the port to be transmitted are sent with no VLAN tag. When receiving, packets classified into the VLAN ID (vlan-trunk) to which the port to be transmitted is joined are sent with a VLAN tag. If both apply, packets are sent with no VLAN tag.

Multiple VLAN is a function that divides ports into groups and prohibits communication between groups in one switch. After enabling the function with **vlan-multiple-use**, specify the group number to which the port belongs with **vlan-multiple**. A port can belong to multiple groups. Packets received on a port are sent from other ports belonging to the same group number as the port.

As an example, consider the following case.



```
switch control function set vlan-multiple-use on
switch control function set vlan-multiple 1 1 join
switch control function set vlan-multiple 2 2 join
switch control function set vlan-multiple 3 1 join
switch control function set vlan-multiple 3 2 join
```

- Packets received on port 1 are sent from port 3 only.
- Packets received on port 2 are sent from port 3 only.
- Packets received on port 3 are sent from port 1 and port 2.

Multiple VLANs do not divide networks, so the same network address is allocated between different groups.

When port VLAN/tag VLANs and multiple VLANs are used together, communication is not possible between ports belonging to the same group in multiple VLANs if they do not belong to the same VLAN in port VLAN/tag VLANs.

41.3.4.1 Setting a VLAN ID

[Format]

```
switch control function set vlan-id vlan_register_num vid
no switch control function set vlan-id vlan_register_num
switch control function get vlan-id vlan_register_num [switch]
```

[Setting value and initial value]

- *vlan_register_num*
 - Setting value: VLAN registration number (1...256)

- [Initial value]: -
- *vid*
 - [設定値] : VLAN ID (1 .. 4094)
 - [Initial value]: Same value as VLAN registration number
- *switch*
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Setting a VLAN ID for a VLAN registration number

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.4.2 Setting the VLAN operation mode of a port

[Format]

switch control function set vlan-port-mode *port mode* **no switch control function set vlan-port-mode** *port* **switch control function get vlan-port-mode** *port* [*switch*]

[Setting value and initial value]

- *port*
 - Setting value: Port number
 - [Initial value]: -
- *mode*: VLAN operation mode
 - [Setting value]:

Setting value	Description
access	Access port
trunk	Trunk port
hybrid	Hybrid port

- [Initial value]: access
- *switch*
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Setting the VLAN operation mode of a port

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.4.3 Setting an access port

[Format]

switch control function set vlan-access *port vlan_register_num*
no switch control function set vlan-access *port*
switch control function get vlan-access *port* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Setting value]: -
- *vlan_register_num*

- [Setting value]: VLAN registration number (1 .. 256)
- [Setting value]: 1
- *switch*: Switch
 - [Setting value]: -
 - MAC address
 - Route
 - [Setting value]: -

[Explanation]

For ports where **vlan-port-mode** is access or hybrid, set the VLAN ID of the port. VLAN ID is VLAN Designated using registration number.

[Notes]

On ports where **vlan-port-mode** is trunk, changing the setting of this function does not affect operation.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.4.4 Trunk port setting**[Format]**

```
switch control function set vlan-trunk port vlan_register_num
mode no switch control function set vlan-trunk port
vlan_register_num switch control function get vlan-trunk port
vlan_register_num [switch]
```

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Setting value]: -
- *vlan_register_num*
 - [Setting value]: VLAN registration number (1 .. 256)
 - [Setting value]: -
- *mode*
 - [Setting value]:

Setting value	Explanation
join	Participate
leave	Do not participate

- [初期値] : leave
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Setting value]: -

[Explanation]

On ports where **vlan-port-mode** is trunk or hybrid, set the VLAN ID to participate. VLAN ID is VLAN Designated using registration number.

[Notes]

On ports where **vlan-port-mode** is access, changing the setting of this function does not affect operation.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.4.5 Setting whether to use multiple VLANs**[Format]**

```
switch control function set vlan-multiple-use mode
no switch control function set vlan-multiple-use
```


switch control function get vlan-multiple-use [switch]

[Setting value and initial value]

- Mode
 - [Setting value]:

Setting value	Explanation
on	Use
off	Do not use

- [Setting value]: off
 - switch: switch
 - [Setting value]: -
 - MAC address
 - Route
 - [Setting value]: -

[Explanation]

Sets whether or not multiple VLANs are used.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.4.6 Group settings for multiple VLANs

[Format]

switch control function set vlan-multiple port group_num
mode no switch control function set vlan-multiple port
group_num switch control function get vlan-multiple port
group_num [switch]

[Setting value and setting value]

- port
 - [Setting value]: Port number
 - [Setting value]: -
- group_num: Group number
 - [Setting value]:

Model	Scope
SWX2200-24G	1 .. 24
SWX2200-8G、SWX2200-8PoE	1 .. 8

- [Setting value]: -
- mode
 - [Setting value]:

Setting value	Description
join	Participate
leave	Participate

- [初期値] : leave
- switch: switch
 - [Setting value]:
 - MAC address
 - Route
 - [Setting value]: -

[Explanation]

Set the group number of the multiple VLAN to which the port belongs.

[Notes]

When **vlan-multiple-use** is set to off, changing the setting of this function does not affect operation.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.5QoS

DSCP marking is a function to rewrite the 6-bit DSCP value in the DS field of the IP header. The rewritten value is determined by the class of the port that received the packet (**qos-dscp-remark-class**) and the rewriting method of the port to be sent (**qos-dscp-remark-type**). Specifically, it is as follows.

qos-dscp-remark-type	qos-dscp-remark-class	DSCP value	PHB
af	class1	001100	AF12
	class3	010100	AF22
	class3	011100	AF32
	Class 4	100100	AF42
cs	Class 3	000000	default
	Class 2	01000	Class Selector
	Class 3	011000	
	Class 4	011000	

41.3.5.1 Setting the Rewriting Method of DSCP Marking**[Format]**

switch control function set qos-dscp-remark-type *port type*

no switch control function set qos-dscp-remark-type *port*

switch control function get qos-dscp-remark-type *port* [*switch*]

[Setting Value and Initial Value]

- *port*
 - [Setting Value]: Port number
 - [Setting Value]: off
- *type*: Rewriting method
 - [Setting Value]: off

Setting Value	Description
off	No Rewriting
af	AF (Assured Forwarding) で書き換えを行う
cs	Rewriting with CS (Class Selector)

- [Setting Value]: off
 - *switch*: switch
 - [Setting Value]: off
 - MAC Address
 - Route
 - [Setting Value]: off

[Explanation]

Setting the method for rewriting the DSCP value of an IP packet transmitted from the switch

[Applicable Model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.5.2 Setting Classification of Received Packets**[Format]**

switch control function set qos-dscp-remark-class *port class*

no switch control function set qos-dscp-remark-class *port*
switch control function get qos-dscp-remark-class *port* [*switch*]

[Setting Value and Initial Value]

- *port*
 - [Setting Value]: Port number
 - [Setting Value]: off
- *class*
 - [Setting Value]: off

Setting Value	Description
off	Not classified
Class 1	Classified into Class 1
Class 2	Classified into Class 2
Class 3	Classify into Class 4
Class 4	Classify into Class 4

- [Setting] : off
- *switch*: switch
- [Setting] : off
 - MAC address
 - Route
- [Setting] : -

[Explanation]

In DSCP marking, packets received by the switch are classified.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.5.3 Speed unit setting for bandwidth limiting

[Format]

switch control function set qos-speed-unit *unit*
no switch control function set qos-speed-unit
switch control function get qos-speed-unit [*switch*]

[Setting and initial value]

- *unit*: speed unit
 - [Setting] : off
 - 128k
 - 1m
 - 10m
 - 32m
 - [Setting] : 32m
- *switch*: switch
- [Setting] : off
 - MAC address
 - Route
- [Setting] : -

[Explanation]

Speed unit is set for policing received traffic and shaping transmitted traffic.

[Notes]

Available only for SWX2200-24G

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.5.4 Setting whether to police received traffic

[Format]

```
switch control function set qos-policing-use port
mode no switch control function set qos-policing-
use port switch control function get qos-policing-
use port [switch]
```

[Setting and initial value]

- *port*
 - [Setting] : port number
 - [Setting] : -
- *mode*
 - [Setting] : off

Setting	Explanation
on	Doing
off	Not doing

- [Setting] : off
- *switch*: switch
- [Setting] : off
 - MAC address
 - Route
- [Setting] : off

[Explanation]

Whether to police received traffic is set.

[Notes]

Available only for SWX2200-24G

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.5.5 Set bandwidth for incoming traffic

[Settings]

```
switch control function set qos-policing-speed port level
no switch control function set qos-policing-speed port
switch control function get qos-policing-speed port [switch]
```

[Settings and initial values]

- *port*
 - [Settings]: Port number
 - [Initial values]: -
- *level*
 - [Settings]: Bandwidth (1 .. 31)
 - [Settings]: 1
- *switch*: Switch
 - [Settings]:
 - MAC addresses
 - Routes
 - [Settings]: -

[Explanation]

Bandwidth for policing received traffic is set. The value obtained by multiplying the setting value of **qos-speed-unit** by *level* is the actual bandwidth.

[Notes]

Available only for SWX2200-24G

If **qos-policing-use** is set to off, changing the setting of this function does not affect operation.

[Applicable models]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.5.6 Setting whether to shape outgoing traffic

[Settings]

switch control function set qos-shaping-use *port mode*
no switch control function set qos-shaping-use *port*
switch control function get qos-shaping-use *port* [*switch*]

[Settings and initial values]

- *port*
 - [Settings]: Port number
 - [Initial values]: -
- *Mode*
 - [Settings]:

Settings	Explanation
on	Doing
off	Not doing

- [Settings]: off
- *switch*: Switch
- [Settings]:
 - MAC addresses
 - Routes
- [Initial values]: -

[Explanation]

Whether to shape outgoing traffic is set.

[Notes]

Available only for SWX2200-24G

[Applicable models]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.5.7 Set bandwidth for outgoing traffic

[Settings]

switch control function set qos-shaping-speed *port level*
no switch control function set qos-shaping-speed *port*
switch control function get qos-shaping-speed *port* [*switch*]

[Settings and initial values]

- *port*
 - [Settings]: Port number
 - [Settings]: -
- *level*
 - Settings: Bandwidth (1 .. 31)
 - [Initial values]: 1
- *Switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Description]

Bandwidth for shaping transmission traffic is set. The value obtained by multiplying the setting value of **qos-speed-unit** by *level* is the actual bandwidth.

[Notes]

Available only for SWX2200-24G.

When **qos-shaping-use** is set to off, changing the setting of this function does not affect operation.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

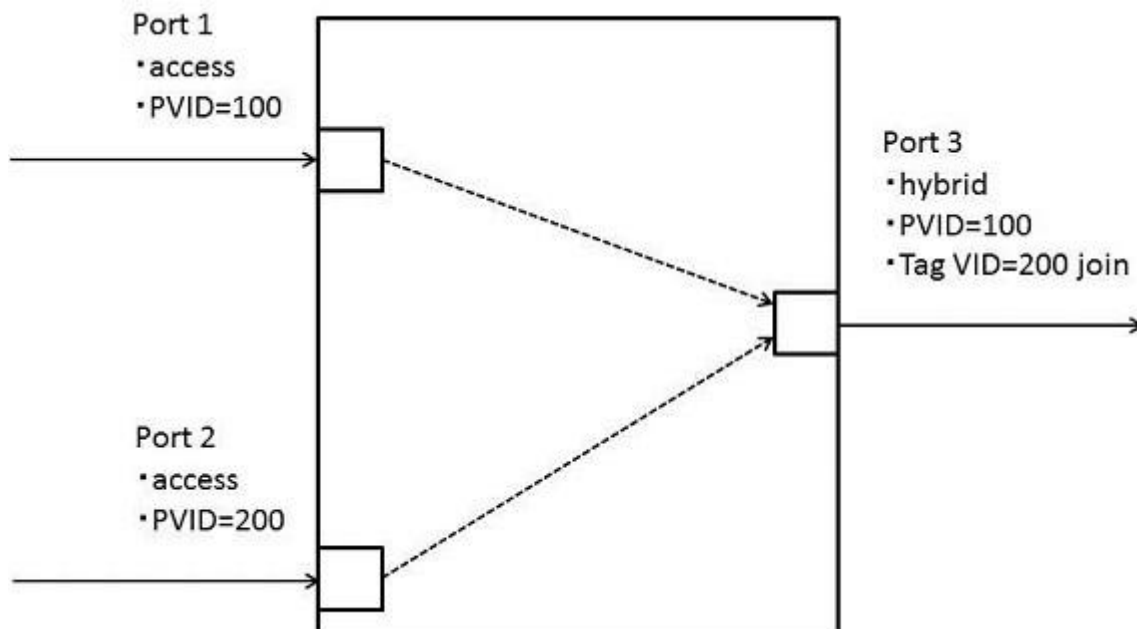
41.3.6 Mirroring

Mirroring is a function that allows you to observe communication on a specific port on other ports.

Mirroring and port blocking functions (port-blocking-control-packet and port-blocking-data-packet) cannot be used together.

When mirroring and port VLAN/tag VLAN, and multiple VLAN are used together, mirroring ports (**mirroring-src-rx** and **mirroring-src-tx**) and mirroring packet sending port (**mirroring-dest**) belong to the same VLAN or group number.

There may be a difference between mirroring packets and original packets in the presence or absence of VLAN tags. Whether or not a mirroring packet is tagged with a VLAN tag depends on the VLAN operation mode of the port sending the mirroring packet. For example, suppose you have the following settings:



- Port 1 is an access port with VLAN ID=100.
- Port 2 is an access port with VLAN ID=200.
- Port 3 is a hybrid port with VLAN ID=100 for the access port and VLAN ID=200 for the tag VLAN.
- When a packet received on port 1 and port 2 is mirrored on port 3.

```
switch control function set vlan-port-mode 3 hybrid
switch control function set vlan-access 1 100
switch control function set vlan-access 2 200
switch control function set vlan-access 3 100
switch control function set vlan-trunk 3 200 join
switch control function set mirroring-use on
switch control function set mirroring-dest 3
switch control function set mirroring-src-rx 1 on
switch control function set mirroring-src-rx 2 on
```

- When a packet received on port 1 is mirrored on port 3, no VLAN tag is added to the packet.
- When a packet received on port 2 is mirrored on port 3, a VLAN tag with VLAN ID=200 is added to the packet.

41.3.6.1 Setting whether or not to use the mirroring function

[Format]

switch control function set mirroring-use
mode **no switch control function set**
mirroring-use switch control function get
mirroring-use [*switch*]

[Setting value and initial value]

- *Mode*
 - [Setting value]:

Setting value	Description
on	Use
off	Not used

- [Initial value]: off
 - *switch*: switch
- [Setting value]:
 - MAC address
 - Route
- [Initial value]: -

[Explanation]

Whether or not to use the mirroring function is set.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.6.2 Setting up ports to send mirroring packets

[Format]

switch control function set mirroring-dest *port*
no switch control function set mirroring-dest
switch control function get mirroring-dest
[*switch*]

[Setting value and initial value]

- *port*
 - Setting value: Port number to send mirroring packets.
 - [Initial value]:

Model	Port number
SWX2200-24G	24
SWX2200-8G、SWX2200-8PoE	8

- *Switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Set a port to send a mirroring packet.

[Notes]

When **mirroring-use is set to off**, changing the setting of this function does not affect the operation.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.6.3 Setting whether to mirror received packets

[Format]

```
switch control function set mirroring-src-rx port
mode no switch control function set mirroring-src-
rx port switch control function get mirroring-src-rx
port [switch]
```

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *mode*
 - [Setting value]:

Setting value	Explanation
on	Mirroring received packets
off	Do not mirror received packets

- [Initial value]: off
 - *switch*: switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Whether to mirror the received packets is set.

[Notes]

Mirroring is not performed even if this function is set to on a port set to **mirroring-dest**.

When **mirroring-use is set to off**, changing the setting of this function does not affect the operation.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.6.4 Setting whether to mirror the packets to be sent

[Format]

```
switch control function set mirroring-src-tx port
mode no switch control function set mirroring-src-
tx port switch control function get mirroring-src-tx
port [switch]
```

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *mode*
 - [Setting value]:

Setting value	Explanation
on	Mirroring the packets to be sent
off	Do not mirror the packets to be sent

- [Initial value]: off
 - *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Whether to mirror the packets to be sent is set.

[Notes]

Mirroring is not performed even if this function is set to on a port set to **mirroring-dest**.

When **mirroring-use** is off, changing the setting of this function does not affect the operation.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.7Counter

Each port has a frame counter and an octet counter that can be counted separately for reception and transmission. The frame counter can count multiple types of packets at the same time.

When using the frame counter, set the packet type to be counted by **counter-frame-rx-type** or **counter-frame-tx-type** in advance. The counter value is obtained by **status-counter-frame-rx** or **status-counter-frame-tx**.

The octet counter value is obtained by **status-counter-octet-rx** or **status-counter-octet-tx**.

Class of packets counted by the frame counter, class-0 to class-3 are classified by DSCP marking.

(**qos-dscp-remark-class**) is supported. Correspondence is as follows.

Classification by DSCP	Class of send queue or receive queue
Class 1	class-0
Class 2	class-1
Class 3	class-2
Class 4	class-3
No classification (off)	

When sending packets received by a switch, the receive queue and the send queue classes are always the same.

41.3.7.1 Setting of frame types to be counted by the receive frame counter

Format

switch control function set counter-frame-rx-type *port counter type*

no switch control function set counter-frame-rx-type *port counter*

switch control function get counter-frame-rx-type *port counter [switch]*

Setting value and initial value

- port*
 - Setting value: Port number
 - Initial value: -
- counter*: Counter number
 - Setting value:

Model	Scope
SWX2200-24G	1 .. 5
SWX2200-8G、SWX2200-8PoE	1 .. 3

- Initial value: -
- type*: Packet type to be counted
 - Setting value:

Setting value	Description
packets	All packets
broadcast-and-multicast-packets	Broadcast packets and multicast packets
total-error-packets	Packets that contain CRC errors, alignment errors, or frame size errors

Setting value	Explanation
broadcast-packets	Broadcast packets
multicast-packets	Multicast packets
packets-64-octets	Packets of 64 octets
packets-65-to-127-octets	Packets of 65 to 127 octets
packets-128-to-255-octets	Packets between 128 and 255 octets
packets-256-to-511-octets	Packets between 256 and 1023 octets
packets-512-to-1023-octets	Packets between 512 and 1023 octets
packets-1024-to-1526-octets	Packets between 1024 and 1026 octets
Pause	PAUSE packets
Fifo-drops	Packets discarded due to receive buffer overflow
total-good-packets	Successfully received packets
class-0	Packets distributed to receive queue class-1
class-1	Packets distributed to receive queue class-2
class-2	Packets distributed to receive queue class-3
class-3	Packets distributed to receive queue class-3
backward-drops	Packets discarded due to buffer congestion
classifier-drops	Packets with source or destination MAC address of 00:00:00:00:00, packets with VLAN tag received by access port, packets without VLAN tag received by trunk port
crc-align-errors	Packets that detect CRC errors, alignment errors, or errors at the physical layer
under-size-packets	Packets less than 64 bytes and with a normal CRC
over-size-packets	Packets greater than or equal to 1519 bytes (without VLAN tag) or greater than or equal to 1523 bytes (with VLAN tag) and with a normal CRC
fragments	Packets less than 64 bytes and with a normal CRC
jabbers	Packets greater than or equal to 1519 bytes (without VLAN tag) or greater than or equal to 1523 bytes (with VLAN tag) and with a normal CRC
control-packets	Packets with Ethernet type of 0x8808

- Initial value

Model	Counter number	Types
SWX2200-24G	1	packets
	2	total-good-packets
	3	total-error-packets
	4	Fifo-drops
	5	crc-align-errors
SWX2200-8G、SWX2200-8PoE	1	packets
	2	total-good-packets
	3	total-error-packets

- *switch*
 - Initial value
 - MAC address
 - Route
 - Initial value: -

[Description]

The type of a frame to be counted by a reception frame counter is set. The value of the counter is acquired by **status-counter-frame-rx**.

[Notes]

When the setting of this function is changed, all counters (transmission, reception, frame, octet) in the port are reset.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.7.2 Setting the type of a frame to be counted by a transmission frame counter

[Format]

switch control function set counter-frame-tx-type *port counter type*
no switch control function set counter-frame-tx-type *port counter*
switch control function get counter-frame-tx-type *port counter* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- counter: Counter number
 - [Setting value]:

Model	Scope
SWX2200-24G	1 .. 5
SWX2200-8G、SWX2200-8PoE	1 .. 3

- [Initial value]: -
- *type* : Type of packet to be counted
 - [Setting value]:

Setting value	Description
packets	All packets
broadcast-and-multicast-packets	Broadcast packets and multicast packets
total-error-packets	Number of times transmission was interrupted due to an error when sending a packet
broadcast-packets	Broadcast packets
multicast-packets	Multicast packets
packets-64-octets	Packets of 64 octets
packets-65-to-127-octets	Packets of 65 to 127 octets
packets-128-to-255-octets	Packets of 128 to 255 octets
packets-256-to-511-octets	Packets of 511 to 256 octets
packets-512-to-1023-octets	Packets of 512 to 1023 octets
packets-1024-to-1526-octets	Packets of 1024 to 1026 octets
Pause	PAUSE packets

Setting value	Description
Fifo-drops	Packets discarded due to transmission buffer overflow
total-good-packets	Packets sent successfully
class-0	Packets sent from transmission queue class-1
class-1	Packets sent from transmission queue class-1
class-2	Packets sent from send queue class-2
class-3	Packets sent from send queue class-3
drops	Packets discarded due to multiple collisions, late collisions, or long stays in the send buffer
collisions	Number of collisions
cfi-drop	Packets discarded because the CFI bit is 1 (if a packet with a CFI bit of 1 is received and an attempt is made to send the packet without a tag, it will be discarded).

- [Initial value]:

Model	Counter number	Types
SWX2200-24G	1	packets
	2	total-good-packets
	3	total-error-packets
	4	Fifo-drops
	5	collisions
SWX2200-8G、SWX2200-8PoE	1	packets
	2	total-good-packets
	3	total-error-packets

- *switch*: switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Description]

The type of frames to be counted by a send frame counter is set. The value of the counter is obtained by **status-counter-frame-tx**.

[Notes]

When the setting of this function is changed, all counters (transmission, reception, frame, octet) at the port are reset.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.7.3 Acquisition of value of received frame counter

[Format]

switch control function get status-counter-frame-rx *port* counter [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- counter: Counter number

- [Setting value]:

Model	Scope
SWX2200-24G	1 .. 5
SWX2200-8G、SWX2200-8PoE	1 .. 3

- [Initial value]: -

• *switch*: Switch

- [Setting value]:

- MAC address
- Route

- [Initial value]: -

[Explanation]

The value of a reception frame counter is acquired.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.7.4 The value of a transmission frame counter is acquired.

[Format]

switch control function get status-counter-frame-tx *port* counter [*switch*]

[Setting value and initial value]

- *port*

- [Setting value]: Port number
- [Initial value]: -

• counter: Counter number

- [Setting value]:

Model	Scope
SWX2200-24G	1 .. 5
SWX2200-8G、SWX2200-8PoE	1 .. 3

- [Initial value]: -

• *switch*: Switch

- [Setting value]:

- MAC address
- Route

- [Initial value]: -

[Explanation]

The value of a transmission frame counter is acquired.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.7.5 The value of a reception octet counter is acquired.

[Format]

switch control function get status-counter-octet-rx *port* [*switch*]

[Setting value and initial value]

- *port*

- [Setting value]: Port number
- [Initial value]: -

• *switch*: Switch

- [Setting value]:

- MAC address
- Route

- [Initial value]: -

[Explanation]

The value of a reception octet counter is acquired. This counter counts the number of octets for all packets received regardless of the setting of **counter-frame-tx-type**.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.7.6 The value of a transmission octet counter is acquired.

[Format]

switch control function get status-counter-octet-tx port [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

The value of a reception octet counter is acquired. This counter counts the number of octets for all packets received regardless of the setting of **counter-frame-tx-type**.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.7.7 Counter clearing

Format

switch control function execute clear-counter [*switch*]

[Setting value and initial value]

- *switch*: switch
 - [Setting value]: -
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

All counters (all ports, transmit, receive, frame, octet) are cleared.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.8 Loop detection

Yamaha switches detect network loops in two ways: monitoring MAC address movement and monitoring L2MS packets. MAC address movement means that the same MAC address is learned on different ports. The switch monitors MAC address movement per second. It is determined that a loop has occurred if the number of movement exceeds the threshold specified by **loopdetect-count** and continues for the time set by **loopdetect-time**.

The L2MS packet monitoring method monitors the number of times the switch itself has received a control packet sent. It is determined that a loop has occurred if the number of times the control packet sent exceeds the threshold specified by **loopdetect-count** continues for the time set by **loopdetect-time**.

Regardless of which method is detected, the LED lights orange on ports where loops have occurred. For ports that use loop detection, set **loopdetect-port-use** to on.

The behavior after loop occurrence is set by **loopdetect-linkdown**. **loopdetect-linkdown** is linkdown or linkdown-recovery

In this case, links are down until the loop stops, starting from the port with the highest number among ports where loops occur.

Here they go. It is recommended to use port 1 as the uplink port so that it can communicate with routers even when loops occur.

In addition, LEDs of ports that link down due to loop occurrence will blink orange.

41.3.8.1 Threshold setting for determining that a loop has occurred per second

[Format]

```
switch control function set loopdetect-count
count no switch control function set
loopdetect-count count switch control function
get loopdetect-count [switch]
```

[Setting value and initial value]

- *count*
 - Setting value: Threshold for determining that a loop has occurred per second (3 .. 65535)
 - Initial value: 3
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Description]

Threshold for determining that a loop has occurred per second is set. It is determined that a loop has occurred if the number of times the MAC address moves or the number of times the control packet sent by the switch itself exceeds the threshold set by this function continues for the time set by **loopdetect-time**.

[Applicable models]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.8.2 Set the time until it is determined that a loop has occurred.

[Format]

```
switch control function set loopdetect-time time
no switch control function set loopdetect-time
switch control function get loopdetect-time
[switch]
```

[Setting value and initial value]

- *time*
 - Setting value: Number of seconds (2 .. 60)
 - Initial value: 3
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

-

Set the time until it is determined that a loop has occurred when the number of times the MAC address moves or the number of times the control packet sent by the switch itself continues to exceed the threshold set by **loopdetect-count**.

[Applicable models]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.8.3 Setting the operation when a loop occurs

[Settings]

```
switch control function set loopdetect-linkdown
action no switch control function set loopdetect-
linkdown switch control function get loopdetect-
linkdown [switch]
```

[Settings and initial values]

- *action*

- [Settings]:

Settings	Description
None	Nothing.
Linkdown	Link down the port where the loop occurred.
linkdown-recovery	After link down the port where the loop occurred, it is restored after a certain time has elapsed.

- [Initial values]: none
 - *switch*: switch
 - [Settings]:
 - MAC addresses
 - Routes
 - [Initial values]: -

[Description]

The operation when the loop occurs is set.

When *action* is linkdown or linkdown-recovery, the port where the loop occurs is linked down in order from the port with the largest number until the loop stops. To restore the port where the link occurred, **reset-loopdetect** is executed or a MODE button is pressed.

When *action* is linkdown-recovery, it is restored automatically after a time set by **loopdetect-recovery-timer** has elapsed after link down the port.

[Notes]

On the port where **loopdetect-port-use** is set to off, the operation set by this function is not performed because it is not detected even if the loop actually occurs.

[Applicable models]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.8.4 Setting the time from link down the port to recovery

[Settings]

switch control function set loopdetect-recovery-timer time

no switch control function set loopdetect-recovery-timer switch control function get loopdetect-recovery-timer [switch]

[Settings and initial values]

- *time*
 - Settings: Number of seconds (1 .. 86400)
 - [Initial values]: 300
- *switch*: switch
 - [Settings]:
 - MAC addresses
 - Routes
 - [Initial values]: -

[Settings]

Set the time from link down to recovery when **loopdetect-linkdown** is set to linkdown-recovery.

[Applicable models]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.8.5 Setting whether or not to use the loop detection function

[Formats]

switch control function set loopdetect-port-use port mode no switch control function set loopdetect-port-use port switch control function get loopdetect-port-use port [switch]

[Settings and initial values]

- *port*
 - Settings: Port number
 - [Initial values]: -
- *Mode*
 - Settings:

Settings	Explanation
on	Use
off	Not used

- [Initial values]: on
 - *switch*: switch
 - Settings:
 - The MAC address
 - Route
 - [Initial value]: -

[Explanation]

Whether or not to use the loop detection function is set. When a loop occurs in a port set to off and a port set to on, the loop is detected in the port set to on. When a loop occurs only in the port set to off, it is not detected.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.8.6 Setting whether or not to perform loop detection using L2MS packets

[Format]

switch control function set loopdetect-use-control-packet
mode no switch control function set loopdetect-use-
control-packet switch control function get loopdetect-use-
control-packet [*switch*]

[Setting value and initial value]

- *Mode*
 - [Setting value]:

Setting value	Explanation
on	Loop detection using control packets is performed.
off	Loop detection by control packets is not performed.

- [Initial value]: On
 - *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Whether or not to perform loop detection using L2MS packets is set. When this function is set to on, it is determined that a loop occurs when a control packet transmitted by the switch itself is received.

[Note]

If congestion occurs in hubs or switches under the switch and control packets are not forwarded, the loop may not be detected.

If this function is not implemented in Yamaha Switch, a command error occurs.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.8.7 Obtaining the state of a port related to the loop detection function

[Format]

switch control function get status-loopdetect-port *port* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Obtain the state of a port related to the loop detection function.

Condition	Explanation
normal	Normal
loopdetect	Loop occurs.
Linkdown	Link down occurs because a loop occurs.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.8.8 Obtaining the time remaining until recovery from link down state

[Format]

switch control function get status-loopdetect-recovery-timer *port* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Remaining time from link down state to recovery due to loop generation is acquired.

[Applied model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.8.9 Recovery of a port that is link down due to loop generation

[Format]

switch control function execute reset-loopdetect [*switch*]

[Setting value and initial value]

- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

All ports that are link down due to loop generation are recovered.

[Applied model]
RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.9PoE power supply

41.3.9.1 Setting the upper limit of the class that can be supplied at each port

[Format]

switch control function set poe-class *port class*
no switch control function set poe-class *port class*
switch control function get poe-class *port [switch]*

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *class*
 - [Setting value]:

Setting value	Explanation
None	No power supply
Class 3	Power supply up to 15.4W equipment
Class 4	Power supply up to 30W equipment

- [Initial value]:
 - Class 4 (1, 3, 5, 7 ports)
 - Class 3 (2, 4, 6, 8 ports)
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

The upper limit of power supply for each port is set. The upper port (1, 3, 5, 7 ports) of the switch can be set to the upper limit of class 4 (30W). The lower port (2, 4, 6, 8 ports) can be set to the upper limit of class 3 (15.4W). When a class 4 (30W) equipment is connected to the upper port with the upper and lower ports as a pair, power supply to the port located directly below it is stopped.

[Notebook]

Only available for SWX2200-8PoE.

When equipment of the set class or higher is connected, power supply is not performed even if the power actually used is equal to or less than the set class.

[Applicable model]
RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.9.2 Acquisition of power supply status of each port

[Format]

switch control function get status-poe-state *port [switch]*

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route

- [Initial value]: -

[Explanation]

Condition	Description	Notes
None	No power supply	-
terminate	Power supply stop	-
supply-class0, supply-class1, supply-class2, supply-class3, supply-class4	Power supply (power supply class)	-
overcurrent	Power supply stop due to overcurrent	-
class-failure	Power supply stop due to recognizing a class larger than the power class setting	Occurs only on SWX2200-8PoE
over-supply	Power supply stop due to power supply exceeding the maximum power supply capacity	-
over-temperature	Power supply stop due to internal temperature exceeding 60C	Occurs only on SWX2200-8PoE
fan-lock	Power supply stop due to fan stop	Occurs only on SWX2200-8PoE
forced-terminate	Power supply stop due to Class4 (30W) power supply being supplied to a port that was supplying Class3 (15.4W) power	Occurs only on SWX2200-8PoE
power-failure	Power supply stop due to power supply failure	-

[Notes]

Can be used with SWX2200-8PoE, SWX2100-10PoE, SWX2100-5PoE

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.9.3 Get the class of the device connected to each port**Format**

switch control function get status-poe-detect-class *port* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Get the class of the device connected to the port.

[Notes]

Can be used with SWX2200-8PoE, SWX2100-10PoE, SWX2100-5PoE

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.9.4 Acquisition of internal temperature of switch**[Format]**

switch control function get status-poe-temperature [*switch*]

[Setting value and initial value]

- *switch*: switch

- [Setting value]: -
 - MAC address
 - Route
- [Initial value]: -

[Explanation]

The internal temperature of the switch is acquired.

[Notes]

It can be used only with SWX2200-8PoE.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.9.5 Acquisition of supply power of each port**[Format]**

switch control function get status-poe-supply port [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *switch*: switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

The current supply power of each port is acquired.

[Notes]

It can be used with SWX2200-8PoE, SWX2100-10PoE, SWX2100-5PoE.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.9.6 The detailed supply power of each port is acquired.**[Format]**

switch control function get status-poe-supply-detail port [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

The detailed current supply power of each port is acquired.

[Notes]

It can be used with SWX2100-10PoE, SWX2100-5PoE.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.9.7 The total supply power of the switch is acquired.

[Format]

switch control function get status-poe-supply-total [*switch*]

[Setting value and initial value]

- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

The total supply power of the switch is acquired. The unit is W (watts)

[Notes]

It can be used with SWX2100-10PoE and SWX2100-5PoE.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.9.8 Power supply recovery

[Format]

switch control function execute restart-poe-supply [*switch*]

[Setting value and initial value]

- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Power supply is restored. If power supply is stopped due to some abnormality, power supply recovery by this command is not possible in the case of power supply stop due to a power supply abnormality.

[Notes]

It can be used with SWX2200-8PoE only.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.9.9 Power supply to each port is started.

[Format]

switch control function execute start-poe-supply *port* [*switch*]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Power supply to each port is started.

[Notes]

It can be used with SWX2100-10PoE and SWX2100-5PoE.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.3.9.10 Power supply to each port is stopped.

[Format]

switch control function execute stop-poe-supply *port* [*switch*]

[Setting value and initial value]

- *port*
 - Power supply: Port number
 - [Initial value]: -
- *switch*: Switch
 - [Setting value]:
 - MAC address
 - Route
 - [Initial value]: -

[Explanation]

Power supply to each port is stopped.

[Notes]

It can be used with SWX2100-10PoE and SWX2100-5PoE.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.4Access point control

41.4.1Access point selection

[Format]

ap select *ap*

no ap select

[Setting value and initial value]

- *ap*
 - [Setting value]:

Setting value	Description
MAC address or route	Selecting an access point
None	Do not select an access point

- [Initial value]: -

[Explanation]

Select an access point as an object. After that, the character string set in console prompt and the access point selected by *ap* parameter are displayed continuously in the prompt.

When **ap select** none or **no ap select** is executed, the access point is not displayed in the prompt.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.4.2Specifying a directory to store the a ccess point configuration file

[Format]

ap config directory *path*

no ap config directory [*path*]

[Setting value and initial value]

- *path*
 - [Setting value]: Relative path or absolute path (256 characters or less in half-width characters, 128 characters or less in full-width characters)

- [Initial value]: /ap_config

[Explanation]

Specify a directory to store the access point configuration file (config). When a relative path is specified, it is interpreted as a path starting from the environment variable PWD. PWD can be changed by the **set** command, and the initial value is "/".

In RTX1210 Rev.14.01.28 or later, RTX830 Rev.15.02.03 or later, and Rev.15.04 or later, full-width characters can be used in *path*, but multibyte characters cannot be used in *path* when *path* points to the RTFS area.

Full-width characters cannot be used in *path in models* other than the above and firmware.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.4.3 Specifying a file name to store the access point configuration

[Format]

ap config filename *name*

no ap config filename [*name*]

[Setting value and initial value]

- *name*
 - [Setting value]: config file name (99 characters or less in half-width characters, 49 characters or less in full-width characters)
 - [Initial value]: -

[Explanation]

Specify a file name to store the access point configuration.

If this command is omitted, the file name is the string specified by **ap select with** .conf added. However, : (colon) is replaced by _ (underscore).

The same file name can be specified by multiple **ap select** commands.

In RTX1210 Rev.14.01.28 or later, RTX830 Rev.15.02.03 or later, and Rev.15.04 or later, multibyte characters cannot be used in the file name when the directory specified by the **ap select directory** command is the RTFS area.

It is necessary to specify a switch by **ap select** command before executing this command.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.4.4 Execute backup of access point configuration

[Format]

ap control config get [*ap*]

ap control config get [[*interface*] all]

[Setting value and initial value]

- *ap*
 - [Setting value]:

Setting value	Description
MAC address or route	Only selected access point
all	All access points

- [Initial value]: -
- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -

[Description]

To perform backup operation of access point settings.

When using the *ap* parameter, only the target access point is backed up.

When all is specified, configurations of all access points recognized by a Yamaha router are saved.
When a LAN interface is specified, only the access point connected to the LAN interface is targeted. When parameters are omitted, it is the same as when all is specified.

[Notes]

It can be specified by a **schedule at** command.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.4.5Execution of restoration of a ccess point settings

[Format]

ap control config set [*ap*]
ap control config set [[*interface*] *all*]

[Setting value and initial value]

- *ap*
- [Setting value]:

Setting value	Description
MAC address or route	Only the access point selected
<i>all</i>	All access points

- [Initial value]: -
- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -

[Description]

Execution of restoration operation of access point settings is performed.

When using the *ap* parameter, only the access point selected is deleted.
When all is specified, the configuration of all access points recognized by a Yamaha router is restored.
When a LAN interface is specified, only the access point connected to the LAN interface is targeted. When parameters are omitted, it is the same as when all is specified.

[Notes]

It can be specified by a **schedule at** command.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.4.6Delete a ccess point settings

[Format]

ap control config delete [*ap*]

[Setting value and initial value]

- *ap*
- [Setting value]:

Setting value	Description
MAC address or route	Only the access point selected
<i>all</i>	All access points

- [Initial value]: -

[Description]

Execution of deletion of access point settings is performed.
When the *ap* parameter is used, only the access point selected is deleted.

When the ap parameter is omitted, all access points selected are deleted.

[Notes]

It can be specified by a **schedule at** command.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.4.7 Setting whether to use the zero config function of access point settings

[Format]

ap control config-auto-set use use

no ap control config-auto-set use [use]

[Setting value and initial value]

- Use
- [Setting value]:

Setting value	Description
on	Use
off	Do not use

- [Initial value]: on

[Explanation]

Whether to use the zero config function of access point setting is set.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.4.8 Execution of HTTP revision-up function of access point

[Format]

ap control firmware update go [ap]

[Setting value and initial value]

- ap
- [Setting value]:

Setting value	Description
MAC address or route	Only selected access point
all	All access points

- [Initial value]: -

[Explanation]

Request firmware update to the access point.

If the ap parameter is omitted, this command is executed for all access points.

[Notes]

It can be specified by the **schedule at** command.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.4.9 Using HTTP proxy for access point control

[Format]

ap control http proxy use use

no ap control http proxy use [use]

[Setting value and initial value]

- Use
- [Setting value]:

Setting value	Description
on	Use
off	Do not use

- [Initial value]: on

[Explanation]

Whether to use HTTP proxy for access point control is set.
When use is set to on, the GUI of the access point can be accessed via the router.

[Notes]

The HTTP proxy function can be used only for the access point under the management of the router in L2MS.
Also, an IP address must be assigned to the access point.
There is no need to enter authentication information for each access point, and by going through a router, VPN and static IP can be used from a remote base.
Access point can be set without using masquerade.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

41.4.10Timeout time setting of HTTP proxy for access point control

[Format]

ap control http proxy timeout *time*
no ap control http proxy *timeout [time]*

[Setting value and initial value]

- *time*
 - Setting value: Number of seconds for timeout
 - Initial value: 60

[Description]

Set the timeout period of the HTTP proxy function for access point control.
When accessing the GUI of an access point via a proxy, if there is no response from the access point within the specified time, it times out.

[Applicable models]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER42

YNO AGENT

YNO AGENT is a function for remotely managing Yamaha network equipment with "Yamaha Network Organizer (YNO)". Yamaha network equipment with the YNO AGENT function enabled connects to the YNO Manager via the Internet and performs the following processing as necessary.

- Notification of operation status of Yamaha network equipment to the YNO Manager
- CONFIG transmission, application, and storage
- Firmware update
- Command execution
- Display of Yamaha network equipment GUI using GUI Forwarder
- CONFIG automatic application by zero configuration

Technical information on this function is published at the URL shown below.
<https://www.rtpo.yamaha.co.jp/RT/docs/yno/agent/>

42.1 Setting whether to use the YNO AGENT function

[Format]

YNO use *sw*
no yno use *sw*

[Setting value and initial value]

- *sw*
 - [Setting value]:

Setting value	Description
on	Use
off	Not used

- [Initial value]: off

[Explanation]

Setting whether to use the YNO AGENT function.

[Notes]

RTX5000 and RTX3500 can be used with Rev.14.01.14 or later.
RTX1210 can be used with Rev.14.01.14 or later.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

42.2 Access code setting for YNO Manager connection

[Format]

yno access code *operator_id* *access_code*
no yno access code [*operator_id* [*access_code*]]

[Setting value and initial value]

- *operator_id*
 - [Setting value]: Access code (8 characters or more)
 - [Initial value]: -
- *access_code*
 - [Setting value]: Access code (8 characters or more and 64 characters or less)
 - [Initial value]: -

[Explanation]

Access code for YNO agent function to connect to YNO Manager is set.

Yamaha network equipment is managed by an operator specified by `operator_id`. All Yamaha network equipment managed by the same operator must be set with the same operator ID and access code.

When **yno zero-config id** command is set, this command cannot be set.

[Note]

When the access code is changed in YNO Manager, this command including new access code is automatically executed and saved in managed Yamaha network equipment.

RTX5000 and RTX3500 can be used with Rev.14.01.14 or later.

RTX1210 can be used with Rev.14.01.14 or later.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

42.3 Setting whether to output additional SYSLOG related to YNO agent function

[Format]

`no yno log type [type...]`

`no yno log [type...]`

[Setting value and initial value]

- *type*
 - [Setting value]

Setting value	Description
action-read	Outputs a SYSLOG related to the operating status of Yamaha network equipment and reading of CONFIG.
inform	SYSLOG related to periodic communication with YNO manager. Output

- [Initial value]: -

[Explanation]

Sets whether to output an additional SYSLOG related to YNO agent function.

[Notes]

RTX5000 and RTX3500 can be used after Rev.14.00.26.

RTX1210 can be used after Rev.14.01.14.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

42.4 Setup of own equipment description displayed in YNO manager.

[Format]

`description yno description`

`no description yno [description]`

[Setup value and initial value]

- *description*
 - [Setup value]: Description string (maximum 32 characters/half-width, 16 characters/full-width)
 - [Initial value]: Empty string

[Explanation]

Setup the description of Yamaha network equipment displayed in YNO manager.

[Notes]

RTX5000 and RTX3500 can be used after Rev.14.01.14.
 RTX1210 can be used after Rev.14.01.14.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

42.5 Setup of HTTPS proxy server used by YNO

[Format]

```
yno https-proxy proxy_server port
no yno https-proxy [proxy_server [port]]
```

[Setup value and initial value]

- *proxy_server*
 - [Setup value]: Host name or IP address of HTTPS proxy server
 - [Initial value]: -
- *port*
 - [Setup value]: Port number of HTTPS proxy server (1..65535)
 - [Initial value]: -

[Explanation]

Setup the HTTPS proxy server used by YNO.

In *proxy_server*, specify the host name of HTTPS proxy server in FQDN format or IP address with up to 255 single-byte alphanumeric characters and single-byte symbols.

In *port*, specify the port number of HTTPS proxy server.

[Notes]

You cannot use HTTPS proxy server that requires user authentication.

RTX5000 and RTX3500 can be used after Rev.14.01.26.
 RTX1210 can be used after Rev.14.01.26.
 RTX830 can be used after Rev.15.02.03.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

42.6 Setting Timeout Period for GUI Forwarder Connection

[Format]

```
yno gui-forwarder timeout time
no yno gui-forwarder timeout [time]
```

[Setup value and initial value]

- *time*
 - [Setup value]: Number of seconds (3..60)
 - [Initial value]:
 - 5 (RTX1210 Rev.14.01.33 or earlier, RTX830 Rev.15.02.09 or earlier)
 - 30 (other than the above)

[Description]

Set timeout period for GUI Forwarder connection.

If there is no response from GUI Forwarder server within the time set by this command, disconnect GUI Forwarder session.

[Notes]

RTX830 can be used in Rev.15.02.03 or later.
 RTX1210 can be used in Rev.14.01.26 or later.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

42.7 Setting the zero config of YNO

[Format]

```
yno zero-config id text operator_id place_id [password]
no yno zero-config id [text [operator_id [place_id [password]]]]
```

[Setting value and initial value]

- *operator_id*
 - [Setting value]: Operator ID (4 characters or more and 64 characters or less)
 - [Initial value]: -
- *place_id*
 - [Setting value]: Place ID (64 characters or less)
 - [Initial value]: -
- *password*
 - [Setting value]: Password (64 characters or less, optional)
 - [Initial value]: -

[Description]

Set the place ID and password used in the zero config of YNO agent function. When this command is set, an attempt to connect to YNO manager is made automatically, and the zero config is activated after the connection is established.

This command cannot be set when the **yno access code** command is set.

[Notebook]

RTX5000 can be used in Rev.14.01.32 or later. RTX830 can be used in Rev.14.01.32 or later. RTX830 can be used in Rev.14.01.32 or later. RTX830 can be used in Rev.15.02.08 or later.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

42.8 Display of the operating status of YNO agent function

[Format]

```
show status
```

yno [説明]

Displays the operating status of YNO agent function. The display contents differ depending on the revision of firmware.

- [新形式]
 - CWMP operating status

Display	Description
Not connected (setting incomplete)	YNO agent function is disabled or insufficiently configured
Not connected (startup processing in progress)	YNO agent function is enabled, initialization and Connecting to ACS
Not connected (end processing in progress)	YNO agent function is disabled, disconnecting with ACS

Display	Description
Normal ([session establishment date and time])	Successful connection with ACS (the date and time of session establishment is displayed in parentheses)
Abnormal ([reason])	Failed to connect with ACS (the reason for abnormality is displayed in parentheses)
Zero config processing in progress ([reason for abnormality])	Successful connection with ACS, and zero config is operating (if an abnormality occurs during processing, the reason for abnormality is displayed in parentheses)

- XMPP operating status

Display	Description
Not connected	Not connected to XMPP server
Connection	Can use XMPP
Abnormalities	Can't use XMPP

- GFW operating status (GUI Forwarder compatible firmware only)

Display	Description
Not connected	Not connected to a GFW server
Connection	Can use GFW
Abnormality	Cannot use GFW

- Operating status of LAS (only for LAS-compatible firmware)

Display	Description
Not connected	Not connected to a LAS server
Connection	Can use LAS
Abnormality	Cannot use LAS

- ID of an operator who manages Yamaha network equipment

- [Old model]

- Operating status of YNO agent function

Current status	Description
Setting incomplete	YNO agent function disabled or not configured properly
Startup processing	YNO agent function is enabled, and initialization and connection to YNO manager
termination processing	YNO agent function disabled, disconnecting with YNO manager
normal operation	successfully connected to YNO manager
Abnormal occurrence	failed to connect to YNO manager

- ID of an operator who manages Yamaha network equipment
- Session establishment date and time to YNO manager
- Can XMPP protocol be used or not
- Can GUI forwarder be used or not (only firmware compatible with GUI forwarder connection)

[Notes]

Contents of new models are displayed in the following models and firmware, and contents of old models are displayed in the others.

Model	Revision
RTX5000	Rev.14.00.32 以降
RTX3510	All revisions

Model	Revisions
RTX3500	Rev.14.00.32 以降
RTX1210	All revisions
RTX1220	All revisions
RTX1210	Rev.14.01.28 or later
RTX840	All revisions
RTX830	Rev.15.02.03 or later

RTX5000 and RTX3500 can be used with Rev.14.01.14 or later.

RTX1210 can be used with Rev.14.01.26 or later.

Example of display

- [新形式]

```

Show status yno
CWMP:           正常 (2018/03/14 14:30:21)
XMPP:           Normal
GFW:           Normal
LAS:           Normal
Operator ID:    dummy_id

```

```

show status yno
CWMP:           Abnormal (Failed to connect to ACS)
XMPP:           Not connected
GFW:           Not connected
LAS:           Not connected
Operator ID:    dummy_id

```

- [Old format]

```

show status yno
Current state:   Normal operation
Operator ID:    dummy_id
Session establishment date and time:
2016/12/18 11:46:03 XMPP connection:
Valid

```

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

42.9 LAS (Log Analysis Service)

42.9.1 SYSLOG transmission queue length setting

[Format]

```

yno las syslog queue length
no yno las syslog queue length

```

[Setting value and initial value]

- *length*
 - [Setting value]: Length
 - [Setting value]: Length
 - 1000..40000 (RTX5000 / RTX3510 / RTX3500 / RTX1300 Rev.23.00.09 or later)
 - 1000..10,000 (other than the above)
 - [Initial value]:
 - 40,000 (RTX5000 / RTX3510 / RTX3500 / RTX1300 Rev.23.00.09 or later)
 - 10,000 (other than the above)

[Description]

SYSLOG transmission queue length setting Even if a value smaller than the current transmission queue length is set, SYSLOG already stored in the transmission queue is not discarded and transmitted to the LAS server.

[Notes]

RTX5000 can be used with Rev.14.00.32 or later
 RTX3500 can be used with Rev.14.02.20 or later
 RTX1220 can be used with Rev.15.04.03 or later
 RTX1210 can be used with Rev.14.01.40 or later
 RTX830 can be used with Rev.15.02.20 or later

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

42.9.2 Timeout setting for waiting for response from the LAS server to the request sent by the LAS client

[Format]

yno las request timeout *seconds*
no yno las request timeout

[Setting value and initial value]

- *seconds*
 - Setting value: seconds (10..60)
 - Initial value: 30

[Description]

Timeout setting for waiting for response from the LAS server to the request sent by the LAS client

[Notes]

RTX1220 can be used with Rev.15.02.20 or later
 RTX830 can be used with Rev.15.02.20 or later
 RTX830 can be used with Rev.15.02.20 or later
 RTX1210 can be used with Rev.15.02.20 or later
 RTX830 can be used with Rev.15.02.20 or later

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

42.9.3 Timeout setting for the LAS client to retry sending the request

Format

yno las request retry *count*
no yno las request retry

[Setting value and initial value]

- *count*
 - [Setting value]: Number of times (0..5)
 - [Initial value]: 3

[Explanation]

Sets the number of times the LAS client retries sending a request.

[Notes]

RTX5000 can be used with Rev.14.00.32 or later.
 RTX830 can be used with Rev.14.02.20 or later.
 RTX1220 can be used with Rev.15.04.03 or later.

RTX1210 can be used with Rev.14.01.40 or later.
RTX830 can be used with Rev.15.02.20 or later.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

42.9.4 Configuring keepalives for connections with LAS servers

[Format]

yno las connection keepalive *interval* [timeout=*sw*]

no yno las connection keepalive

[Setting value and initial value]

- Interval*

- [Setting value]:

Setting value	Explanation
off	No keepalives
300	Keepalives time interval (number of seconds)

- 60

- SW*

- [Setting value]:

Setting value	Explanation
on	Disconnect a connection if there is no response from the LAS server
off	Do not disconnect a connection if there is no response from the LAS server

- [Initial value]: off

Explanation

While displaying in real time with YNO Manager, the LAS client establishes a connection with the LAS server. Keepalives packets are sent from the LAS client at *intervals* set for intervals while a connection is established. If *SW* is set to on, if there is no response from the LAS server by the time set in *interval* after keepalives packets are sent, the LAS client disconnects the connection and attempts to reconnect.

[Notebook]

RTX5000 can be used with Rev.14.00.32 or later. RTX8300 can be used with Rev.15.02.20 or later. RTX1220 can be used with Rev.15.02.20 or later. RTX1210 can be used with Rev.14.01.40 or later. RTX830 can be used with Rev.15.02.20 or later.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

42.9.5 Display of LAS operating status

[Format]

show status yno

las

Displays the operating status of LAS.

[Notebook]

RTX8300 can be used with Rev.15.02.20 or later. RTX8300 can be used with Rev.15.02.20 or later. RTX8300 can be used with Rev.15.02.20 or later.

RTX8300 can be used with Rev.15.02.20 or later.

RTX830 can be used with Rev.15.02.20 or later.

[Example of display]

```
show status yno las
Function          : Enable
Log transmission result      : Success
SYSLOG transmission speed    : 100 lines / 60 seconds
SYSLOG transmission queue length: 26
```

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

42.10 Setting the time interval for keepalive with the XMPP server

[Format]

yno xmpp connection *keepalive interval*

no yno xmpp connection keepalive [*interval*]

[Setting value and initial value]

- *Interval*
 - [Setting value]: Time interval for sending keepalive packets (30..300 seconds)
 - [Initial value]: 300

[Description]

Time interval for performing keepalive communication with the XMPP server is set.

[Notes]

If this command is executed, communication with the YNO manager may be temporarily disabled. In that case, the XMPP connection will be reconnected and automatically restored at the next execution of keepalive communication with the XMPP server.

RTX3500 can be used with Rev.14.00.32 or later. RTX830 can be used with Rev.14.00.32 or later. RTX1210 can be used with Rev.14.01.41 or later. RTX830 can be used with Rev.15.02.22 or later. RTX830 can be used with Rev.15.04.04 or later.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 43

Diagnosis

43.1 Diagnosis of open/close status of ports

[Format]

diagnose config port map interface protocol [*src_addr* [*src_port*]] *dst_addr*

[Setting value and initial value]

- *interface*
 - [Setting value]: Interface name of the receiver (LAN, PP (pp *peer_num*))
 - [Initial value]: -
- *protocol*
 - [Setting value]: Packet type to be diagnosed (multiple packets can be specified separated by commas)
 - [Setting value]:
 - Decimal number representing protocol (0..255)
 - Mnemonic representing protocol

Setting value	Description
tcp	TCP packet
udp	UDP packet
icmp	ICMP packet
gre	PPTPgre packet
esp	IPsec esp packet
ah	IPsec ah packet

- [Initial value]: -
- *src_addr*
 - [Setting value]: Source IP address of input packet
 - [Initial value]: -
- *src_port*
 - [Setting value]: Source port number of input packet
 - [Initial value]: -
- *dst_addr*
 - [Setting value]: Destination IP address to be diagnosed (multiple packets can be specified separated by commas)
 - [Initial value]: -

[Explanation]

Diagnose whether packets received from the interface specified by the *interface* parameter can pass through the router.

In tcp and udp packets, if a well-known port of a destination IP address specified by the *dst_addr* parameter exists and can pass through a router, its contents are displayed. For packets other than tcp and udp, settings related to the port are ignored, and if a packet can reach *dst_addr*, its contents are displayed.

If *src_addr* and *src_port* are omitted, a router automatically samples a combination of a source IP address and a source port number that is considered necessary from the filter settings.

[Notes]

Since this command is implemented by performing pseudo packet transfer processing only inside the router, it does not transmit a packet to be diagnosed to a host specified by *dst_addr*. Therefore, if it is possible for a port closed on the host side to pass through the router, it is determined that the port is open. This is also the case when an IP address of the router itself is specified in *dst_addr*, and it does not diagnose an open/close state of the port of the router itself.

Note that this command does not consider an ethernet filter.

[Applicable model]

RTX1300, RTX1220, RTX1210

43.2 Diagnosis of access range that can reach a port

[Format]**diagnose config port access interface** [*protocol*] *dst_addr dst_port***[Setting value and initial value]**

- *interface*
 - [Setting value]: Interface name of the receiver (LAN, PP (pp *peer_num*))
 - [Initial value]: -
- *protocol*: Packet type to be diagnosed (multiple packets can be specified separated by commas, if omitted, all types)
 - [Setting value]:

Setting value	Explanation
tcp	TCP packets
udp	UDP packets

- [Initial value]: -
- *dst_addr*
 - [Setting value]: Destination IP address to be diagnosed
 - [Initial value]: -
- *src_port*
 - [Setting value]: Destination port number to be diagnosed
 - [Initial value]: -

[Explanation]

Displays the range of source IP addresses and source port numbers that can be reached by packets specified by *protocol* parameters to the port number of the host specified by the *dst_addr/dst_port* parameter.

[Notes]

Since this command is implemented by performing packet transfer processing in a pseudo manner only inside the router, packets to be diagnosed are not transmitted to the host specified by *dst_addr*. Therefore, if it is possible to pass a router even on a closed port on the host side, it is determined that it can reach that port. This is also the case where the router's own IP address is specified in *dst_addr*, and does not depend on the open/close state of the router's own port.

The ethernet filter is not considered in this command.

[Applicable model]

RTX1300, RTX1220, RTX1210

43.3 Setting the maximum number of passing packets that can be detected by diagnosis of the open/close state of the port

[Format]**diagnosis config port max-detect** *num***[Setting value and initial value]**

- *num*
 - [Setting value]: Maximum number of passing packets that can be detected (100..1000000)
 - [Initial value]: 2000

[Explanation]

Setting the maximum number of passing packets that can be detected by diagnosis of the open/close state of the port and diagnosis of the access range that can be reached to the port. If passing packets exceeding this value are detected, diagnosis is interrupted.

[Notes]

In the diagnosis result of the open/close state of the port, transmission source address space and transmission source port number space that can be passed are aggregated and displayed as much as possible. However, since diagnosis is interrupted when the number of passing before aggregation exceeds this setting value, diagnosis may be interrupted even if the number of passing displayed in the diagnosis result is actually lower than this setting value.

[Applicable model]

RTX1300, RTX1220, RTX1210

43.4 **Setting the number of history of diagnosis results of the open/close state of the port**

[Format]

diagnosis config port history-*num num*

[Setting value and initial value]

- *num*
 - Setting value: Number of history to be saved as a diagnosis result (1..10)
 - [Initial value]: 3

[Explanation]

Setting the number of history to be saved as a diagnosis result of diagnosis of the open/close state of the port and diagnosis of the access range that can be reached to the port.

[Notes]

If a history exceeding the setting value is already saved when this command is executed, the history exceeding the setting value is deleted.

[Applicable model]

RTX1300, RTX1220, RTX1210

43.5 **Display of diagnostic result of open/close status of port**

[Format]

show diagnosis config port

map [Explanation]

Displays diagnostic result of open/close status of port.

[Applicable model]

RTX1300, RTX1220, RTX1210

43.6 **Display of diagnostic result of access range reachable to port**

[Format]

show diagnosis config port

access [Explanation]

Displays diagnostic result of access range reachable to port.

[Applicable model]

RTX1300, RTX1220, RTX1210

43.7 **Clearing diagnostic result of open/close status of port**

[Format]

clear diagnosis config

port [Explanation]

Clears all diagnostic result of diagnosis of open/close status of port and diagnosis of access range reachable to port.

[Applicable model]

RTX1300, RTX1220, RTX1210

CHAPTER44

Statistics

44.1 Setting whether to enable statistics function

[Format]

```
statistics type sw
no statistics type [sw]
```

[Setting value and initial value]

- type : Type of internal resource
 - [Setting value]

Setting value	Explanation
cpu	CPU utilization rate
memory	Memory utilization rate
traffic	Traffic volume by interface
flow	Number of fast-pass flows
nat	Number of entries in NAT table
route	Number of routes
filter	Number of sessions of dynamic filter
application	Traffic information of application

- [Initial value]: -
- SW
 - [Setting value]:

Setting value	Explanation
on	Activating statistics function
off	Activating statistics function

- [Initial value]: off

Explanation

Setting whether to enable various statistics functions.

Notes

If it is turned off, statistical information before it is cleared. Collected statistical information can be confirmed by Web GUI dashboard and YNOsLAS (log analysis service).
Application keyword of type parameter can be used in RTX1300 since Rev.15.02.13 of RTX830.
RTX3510 is available in Rev.23.01.02 or later RTX1210 is available in Rev.14.01.34 or later RTX830 is available in Rev.15.02.10 or later

[Applicable models]

RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 45

Flexible LAN/WAN port

Flexible LAN/WAN port is a function that allows a user to flexibly change the physical port configuration of a conventionally fixed LAN interface.

With this function, router resources can be used efficiently by adopting the configuration according to the usage environment, such as line speed and network configuration.

Flexible LAN/WAN port has the following advantages:

- It is possible to select a WAN port according to the line speed.
- Multiple LAN interfaces can be used.

Technical information on this function is published at the URL shown below.

<https://www.rtpo.yamaha.co.jp/RT/docs/flexible-lan/>

45.1 Port mapping to a LAN interface

[Format]

lan flexible-port interface=sw_port [interface=sw_port...]

no lan flexible-port

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *SW_PORT*
 - [Setting value]: Port number
 - Initial value]: -

[Explanation]

Port mapping to a LAN interface is configured.

The number of available LAN interfaces is as follows. A combination of interface=sw_port can be specified up to the number of maximum LAN interfaces.

Model	Maximum number of LAN interfaces
RTX1300	8

When multiple ports are mapped to one LAN interface, port numbers separated by sw_port ",", (comma), port numbers (range specification) with "-" (hyphen) between them, and their combinations are specified.

The mapping of the initial state of RTX1300 is shown in the table below.

Interface	Port number
lan1	1..8
lan2	9
lan3	10

[Note]

Even if the setting of this command is changed, the setting is not reflected unless the router is restarted. The current mapping state can be checked with the command show lan flexible-port.

Ports mapped to the same LAN interface act as switches. The setting value of this command must satisfy all of the following conditions.

- Mapping at least one port to a LAN1 interface
- Mapping all ports to one of the LAN interfaces

Note that a port cannot be mapped to multiple LAN interfaces.

[Applicable model]
RTX1300

45.2 Display of ports mapped to a LAN interface

[Format]

show lan flexible-port [interface]

[Setting value and initial value]

- *interface*
 - Setting value: LAN interface name
 - Initial value: -

[Explanation]

Display ports mapped to a LAN interface by the command lan flexible-port.
When interface is specified, ports mapped to the relevant LAN interface are displayed. When interface is omitted, mappings of all LAN interfaces are displayed.

[Example display]

- Display mappings of all LAN interfaces

```
#showlanflexible-port
LAN1: 1 2 3 4
LAN2:56
LAN3:78910

#
```

- Display ports mapped to a LAN2 interface

```
#showLanflexible-portlan2 LAN2: 5
6

#
```

[Applicable model]
RTX1300

45.3 Setting the operation type of a LAN port

[Format]

lan port type port speed [option=value...]

Lan port type port option=value [option=value...]

no lan port type port [...]

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -
- *speed: LAN speed and operation mode*
 - [Setting value]:

Setting value	Description
Auto	Automatic speed discrimination

Setting value	Description
10g-fdx	100BASE-T full duplex
5g-fdx	5GBASE-T full duplex
2.5g-fdx	2.5GBASE-T full duplex
1000-fdx	1000BASE-T full duplex
100-fdx	100BASE-TX full duplex
100-hdx	100BASE-TX half duplex
10-fdx	10BASE-T full duplex
10-hdx	10BASE-T half duplex

- [Initial value]: auto
- *option=value: optional feature*

- [Setting value]:

- auto-crossover
 - Auto crossover function

Setting value	Description
on	Enable the auto crossover function
off	Disable the auto crossover function

- speed-downshift
 - Speed downshift function

Setting value	Description
on	Speed downshift function is enabled
off	Speed downshift function is disabled

- energy-saving
 - Power saving function

Setting value	Description
on	Power saving function is enabled
off	Power saving function is disabled

- [Initial value]:
 - auto-crossover=on
 - speed-downshift=on
 - energy-saving=off

[Explanation]

Speed and operation mode types of a LAN port and optional functions are configured.

Speed and operation mode that can be specified in speed differ depending on the port. Speed and operation mode that can be specified in each port are shown below.

Model	Ports	Specifiable speed and operation mode
RTX1300	1 .. 8	• 1000-fdx • 100-fdx • 100-hdx • 10-fdx • 10-hdx
	9,10	• 10g-fdx • 5g-fdx • 2.5-fdx • 1000-fdx • 100-fdx • 100-hdx

This command is applied only to a LAN port and does not affect the operation of an SFP+ port.

[Notes]

After this command is executed, reset is automatically performed in all LAN interfaces, and the setting becomes effective afterwards.

At least one speed or option=value pair must be specified, and failure to specify any of them results in an error.

The values that can be specified in option=value are the same as those that can be specified in a lan type command. However, the following options cannot be specified.

- mtu
- macaddress-aging
- port-based-option

The mtu option can be configured with the lan type command. The macaddress-aging option can be configured with the switching-hub macaddress-aging command. Divide-network (LAN division function) of port-based-option can be substituted with the lan flexible-port command. Cannot use split-into

[Configuration Example]

1. Ports 1 and 2 are connected in full duplex to 100BASE-TX, and the other ports are connected by auto-negotiation.

```
# lan port type 1 100-fdx
# lan port type 2 100-fdx
```

[Applicable model]
RTX1300

45.4 MAC Address aging functional LAN port operation setting

[Format]

switching-hub macaddress-aging age_time
no switching-hub macaddress-aging [age_time]

[Setting value and initial value]

- age_time
 - [Setting value]: Aging time, on or off
 - [Initial value]: 300 (models whose time can be specified) / on (models whose time cannot be specified)

[Explanation]

Set the MAC address aging function.

The MAC address aging function erases an entry in the MAC address table of a switching hub in a fixed time. When the MAC address aging function is disabled by setting `age_time` to off, not only is the MAC address learned by the switching hub not automatically erased, but it is not erased even if a `clear switching-hub macaddress` command is executed. The entry is erased only when the function is re-enabled by setting `age_time` to a valid value.

In the following models, the number of seconds can be specified in the setting value. However, there may be an error between the setting value of the command and the time until it is actually erased.

Model	Setting range
RTX3510, RTX1300	4.819

When on is input in a model whose number of seconds can be specified, it is converted to the initial value of 300.

The size of the MAC address table is as follows.

Model	Maximum number of entries
RTX3510	16,376
RTX1300	16,378 (*)

* Figures when three LAN interfaces are used in the factory default state. It varies depending on the number of LAN interfaces used in the flexible LAN/WAN port. (Maximum number of entries = 16,384 - Number of LAN interfaces * 2), and when the number of LAN interfaces used is eight, the maximum number of entries is 16,374.

[Notes]

After execution of this command, reset is automatically performed on all LAN ports connected to the switching hub, and then the setting becomes effective.

[Applicable model]

RTX3510, RTX1300

45.5 LAN port operation setting

[Format]

`lan port shutdown port`

`no lan port shutdown port`

[Setting value and initial value]

- *port*
 - [Setting value]: Port number
 - [Initial value]: -

[Description]

Prevent the specified LAN port from being used. On the LAN port where this command is set, link-up is not performed even if a LAN cable is connected.

[Notes]

Reset is automatically performed on all LAN interfaces after execution of this command, and then the setting becomes effective.

[Applicable model]

RTX1300

CHAPTER 46

LBO

Local Breakout (hereinafter referred to as LBO) is a function to perform part of Internet access directly from routers installed at each site.

Yamaha Router acquires a communication destination list containing IP addresses and FQDNs used by applications subject to LBO from the outside and realizes LBO using filtered routing based on the list.

The communication destination list is provided on Yamaha's Web server, and the latest IP addresses and FQDNs are reflected for periodic maintenance by Yamaha. In addition, Yamaha Router periodically checks this communication destination list (hereinafter referred to as official list) from the Web server and automatically updates the list in use if a new version of the list has been published. Regular maintenance of the communication destination list and router settings by router administrators is unnecessary.

Technical information on this function is published at the URL shown below.

<https://www.rtpo.yamaha.co.jp/RT/docs/lbo/>

46.1 Setting whether to use LBO

[Format]

lbo use switch

no lbo use [switch]

[Setting value and initial value]

- *switch*
- [Setting value]

Setting value	Explanation
on	Using LBO
off	Do not use LBO

- [Initial value] : off

Explanation

Whether to use LBO is set.

[Applicable model]

RTX840

46.2 Primary Communication Destination List Source Settings

[Format]

lbo list primary list

no lbo list primary [list]

[Setting value and initial value]

- *list*
- [Setting value]
 - URLs starting with http:// or https://
 - RTFS or file path on external memory (relative path can be specified)
 - None
- [Initial value]: https://www.rtpo.yamaha.co.jp/lbo/address_list.xml

Explanation

Setting the URL or file path to acquire the primary communication destination list used in LBO.

When a mnemonic with the same name is specified for primary and secondary, the value defined in the primary is used.

[Applicable model]

RTX840

46.3 Secondary Communication Destination List Source Settings

[Format]

lbo list secondary list

no lbo list secondary [list]

[Setting value and initial value]

- *list*
 - [Setting value]
 - URLs starting with http:// or https://
 - RTFS or file path on external memory (relative path can be specified)
 - None
 - None.

[Explanation]

Setting the URL or file path to acquire the secondary communication destination list used in LBO.

[Note]

When a mnemonic with the same name is specified for primary and secondary, the value defined in the primary is used.

[Applicable model]

RTX840

46.4 Manual execution of acquisition of the communication destination list

[Format]

lbo list get go [no-confirm] [force]

[Setting value and initial value]

- no-confirm : Do not display a message to confirm whether to update the communication destination list when a new version of the communication destination list exists.
 - [Initial value] : -
- force : Forcibly acquires the communication destination list without checking the version of the communication destination list, and also forcibly updates the cache file stored in RTFS.
 - [Initial value] : -

[Explanation] n

Manually execute the acquisition of the communication destination list used in LBO.

[Notes]

Since the update check of the communication destination list is performed automatically, it is not necessary to execute this command normally. It is used when a retry is desired immediately when automatic acquisition fails.

[Applicable model]

RTX840

46.5 Displaying the operating status of LBO

[Format]

show status lbo

[Explanation]

Information on the operating status of LBO and the communication destination list is displayed.

- Operating status

Display	Description
Invalid	LBO is invalid.
Normal operation	LBO is operating normally.
IP address / FQDN list downloading	The communication destination list is being acquired.
IP address / FQDN list download failure (waiting for retry)	Failed to acquire the communication destination list, and is being reacquired.
IP address / FQDN list downloading and updating	The communication destination list is being updated.
Abnormal stop	An abnormality occurs, and the operation of LBO is stopped.

- Information on the communication destination list

Display	Description
Version number	Version number described in the communication destination list
Last acquisition date and time	Last date and time when the communication destination list was acquired
Last acquisition date and time	Last date and time when the update process of the communication destination list was executed
Last update result	Result of executing the update process - Updated to latest version ... Updated to the latest communication destination list - Update failure ... Skipped update because the latest communication destination list is being used. - Update failure ... Failed to acquire the latest communication destination list
Cache file usage	Cache file usage - YES ... Using - NO ... Not using

Display example

```

USER1# show status lbo
Current Status
  Working normally
IP Address / FQDN List Information

```

List Name	Primary	Secondary
Version number	2025103000	-----
Last downloaded	2025/12/04 11:26	---/--/-- --:--
Last updated	---/--/-- --:--	---/--/-- --:--
Last update result	Not executed	-----
Cache file usage	NO	-----

[Applicable model]

RTX840

46.6 Display of communication volume with route change

[Format]

show lbo traffic list [application]

[Set value and initial value]

- application*
 - [Set value]: mnemonic for applications starting with "@"
 - [Initial value]: -

[Explanation]

Displays communication volume (octet number) with route change by LBO.

[Note]

The number of octets to be displayed is the cumulative value of the length of IP packets passing through a router.

[Example]

```
#show lbo traffic list
@m365
  LAN2 6838 Octet
@google
  LAN2 1040 Octet
@windows_update
  Not_transmitted

#show lbo traffic list @m365
@m365
  LAN2 16020 Octet
```

[Applicable model]

RTX840

46.7 Clearing the amount of communication that changed the route

[Format]

```
clear lbo traffic list
```

[Explanation]

Clears the amount of communication (octet number) that changed the route by LBO.

[Applicable model]

RTX840

CHAPTER 47

Operation

47.1 Selection of destination information number

Format

Pp select peer_num

no pp select

Set value and initial value

- *Peer_num*
- Set value: -

Set value	Description
Number	Destination information number
None	Do not select the other party
anonymous	Setting of the other party whose ISDN number is unknown

- Set value: -

Description

Select the destination information number to be set or displayed. After that, the character string set by console prompt command and the destination information number are displayed successively in the prompt. If none is specified, the destination information number is not displayed in the prompt.

Notes

This operation command can be executed even by a general user.

The no pp select command behaves like the pp select none command. Refer to 1.6 for the difference between models of the destination information number that can be selected.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.2 Selection of tunnel interface number

Format

tunnel select tunnel_num

no tunnel select

Set value and initial value

- *tunnel_num*
- Set value:

Set value	Description
Number	Tunnel interface number
None	Do not select tunnel interface

- Set value: -

Explanation

Select the tunnel interface number to be set or displayed in the tunnel mode.

Notes

The operation of this command can be executed even by a general user.

If the prompt is tunnel, pp related commands cannot be entered.

The **no tunnel select** command behaves like the **tunnel select none** command.

Refer to "IPsec settings" for the difference between models of the tunnel interface number that can be selected.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.3 Operation related to setting

47.3.1 Transition to administrative user

Format

administrato

r [Explanation]

The router settings cannot be changed until this command is issued. Also operation commands cannot be executed. There are no parameters, and an administrative password can be entered again according to the prompt after command input. The password entered is not displayed on the screen.

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.3.2 End

Format

quit

quit save

exit

exit save

[Setting value and initial value]

- **save:** If specified when exiting from the management user, save the setting contents to non-volatile memory and exit.
 - [Initial value]: -

[Explanation]

Login to the router is finished or exit from the management user.

When leaving from the management user without saving by changing the setting, it inquires whether or not to save the new setting contents to non-volatile memory. If it is saved in non-volatile memory, starting with the same setting becomes possible even after restarting.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.3.3 Saving setting contents

[Format]

save [filename [comment]]

[Setting value and initial value]

- **filename:** File name to save the setting
- [Setting value]:

Setting value	Description
0 to 4	Setting file number of internal storage (internal flash ROM, etc.)
usb1:filename	Setting file name in USB memory (Not specified for vRX series, RTX5000, and RTX3500)
sd1:filename	Setting file name in microSD card (Not specified for vRX series)

- [Initial value]: -
- *comment*
 - Setting value: Comment of setting file (within 200 characters)
 - [Initial value]: -

[Explanation]

Current setting contents are saved in non-volatile memory.

If file specification is omitted, it is saved in the setting file used at startup.

File name is within 99 characters.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.3.4 Duplicate setting file

[Format]

copy config from to

copy config from to crypto [password]

copy config from to [password]

[Setting value and initial value]

- *from: Copy source file name*
- [Setting value]:

Setting value	Description
0 to 4.2	Setting file number in internal storage (internal flash ROM, etc.)
usb1:filename	Setting file name in microSD card (Not specified for vRX series, RTX5000, and RTX3500)
sd1:filename	Setting file name in microSD card (Not specified for vRX series)
*:filename	Setting file name in microSD card (Not specified for vRX series)
<i>prefix:filepath</i>	Setting file name in external storage (Not specified for vRX series except for vRX Amazon EC2 version)
emfs:filename	Setting file name in EMFS

- [Initial value]: -
- *to: Copy destination file name*
- [Setting value]:

Setting value	Description
0 to 4	Setting file number for internal storage (internal flash ROM, etc.)
usb1:filename	Setting file name in USB memory (Cannot be specified for vRX series, RTX5000, and RTX3500)
sd1:filename	Setting file name in microSD card (Cannot be specified for vRX series)

Setting value	Description
<i>prefix:filepath</i>	Setting file name in external storage (Can be specified for vRX series except for vRX Amazon EC2 version)

- [Initial value]: -
- *Crypto: Choice of cryptographic algorithm*
- [Setting value]:

Setting value	Description
aes128	Encrypt with AES 256.
aes256	Encrypt with AES 256.

- [Initial value]: -
- *password*
 - [Setting value]: Password expressed as an ASCII string (8 or more half-width characters and up to 32 characters)
 - [Initial value]: -

Description

Duplicate the saved setting file.

External memory, external storage, and EMFS files cannot be specified for both copy source and copy destination. Since there is no setting file in internal storage (internal flash ROM, etc.) immediately after cold start, it is not possible to copy the setting file to external memory, external storage, and EMFS. In this case, it is necessary to save the setting once with the save command and then execute it.

In order to reflect the contents copied to internal storage (internal flash ROM, etc.) in actual operation, it is necessary to restart the router after executing this command.

When "*" is specified for external memory, the specified file is searched from the microSD card first, and if there is no specified file, the USB memory is searched. File name specifies a file using an absolute path or only a file name. When only a file name is specified for filename, it is searched automatically from external memory.

When there are multiple files, the file in the directory closest to the root directory on the directory hierarchy and in the first directory in alphabetical order is selected.

When specifying an external memory as the copy destination, specify a file using an absolute path for filename. File name is within 99 half-width characters.

When specifying a file on external storage as the copy source and copy destination, specify the prefix when mounting the external storage with the mount command in prefix, and specify the absolute path of the file in filepath. The directory name and file name must be specified with a maximum of 255 characters.

Encryption functions can be used for external memory and external storage.

When CRYPTO is specified, the setting file is encrypted and then copied to external memory or external storage. When copying by encryption, the file name must include the .rtfg extension or specify a name that omits the extension. When the extension is omitted, the .rtfg extension is automatically added to the file name.

Encryption in which a password is omitted can be performed.

Notes

External memory and internal storage without decrypting encrypted setting files on external storage
Cannot be copied to ROM, etc.)

The second format can be used only when copying a setting file of internal storage (internal flash ROM, etc.) by encryption to external memory or external storage. The third format can be used only when copying an encrypted setting file on external memory or external storage by decrypting it to internal storage (internal flash ROM, etc.). Since the encryption algorithm at the time of decryption is automatically determined, it is not necessary to specify the encryption algorithm at the time of decryption.

When setting file number of internal storage (internal flash ROM, etc.) is used as a copy destination file, the original copy destination file becomes a saved file after executing this command.

Depending on directory structure and the number of files in external memory, it may take time to search for a file. To shorten the search time, it is desirable to store a file near the root or directly specify the file by absolute path, avoiding creating a directory with a deep hierarchy.

The timeout period for automatic search can be set by external-memory auto-search time command.

A file encrypted and stored in external memory can be decrypted on a PC using RT-FileGuard.

Encryption functions cannot be used with vRX Amazon EC2 version.
Files on EMFS cannot be specified with RTX5000 / RTX3500 Rev.14.00.25 or earlier, RTX1210 Rev.14.01.27 or earlier, and RTX830 Rev.15.02.02 or earlier.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.3.5 Firmware file is copied to internal storage (internal flash ROM, etc.)

[Format]

copy exec from to

[Setting value and initial value]

- *from*: Copy source file name
- [Setting value]:

Setting value	Description
Number	Execution format of internal storage (internal flash ROM, etc.) Firmware file number (can be specified for models other than RTX840 and RTX830), only 0 can be specified
usb1:filename	Firmware file name in USB memory (only for models with USB interface)
sd1:filename	Firmware file name in microSD card (only for models with microSD interface)
*:filename	Firmware file name in USB memory and microSD card

- [Initial value]: -
- *to*: Copy destination file name
- [Setting value]:

Setting value	Description
Number	Executable firmware file number of internal storage (internal flash ROM, etc.) (RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210) In this case, 0 and 1 can be specified, only 0 can be specified for RTX840 and RTX830, and only 1 can be specified for models other than those listed on the left)

- [Initial value]: -

[Description]

Executable firmware file is copied to internal storage (internal flash ROM, etc.)

In order to reflect the contents copied to internal storage (internal flash ROM, etc.) in actual operation, it is necessary to restart the router after executing this command.

When "*" is specified for external memory, the specified file is searched from the microSD card first, and if there is no specified file, the USB memory is searched.

File name specifies a file using an absolute path or only a file name. When only the file name is specified in filename, it is searched automatically from external memory. File name is within 99 characters.

When multiple files are found as a result of the search, the file closest to the root directory on the directory hierarchy and in the first directory in alphabetical order is selected.

[Notes]

Only models with an external memory interface can specify a file in external memory.

Only models with a firmware multiplexing function can specify a copy destination firmware file number other than 0.

Depending on the directory structure of external memory and the number of files, it may take time to search for a file. In order to shorten the search time, it is desirable to avoid creating a directory with a deep hierarchy and store the file close to the root directory.

It is desirable to specify the file directly with an absolute path.

The timeout of automatic search can be set by external-memory auto-search time command.

[Applicable models]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.3.6 Deleting a configuration file

[Format]

delete config filename

[Setting value and initial value]

- *filename*: File name to delete
- [Setting value]:

Setting value	Description
all	All configuration files in internal storage (internal flash ROM, etc.)
0 to 4.2	Setting file number of internal storage (internal flash ROM, etc.)

- [Initial value]: -

[Description]

Deleting a saved configuration file

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.3.7 Deleting an executable firmware file

[Format]

delete exec filename

[Setting value and initial value]

- *filename*: File name to delete
- [Setting value]:

Setting value	Description
Number	Executable firmware file number (only 1 can be specified)

- [Initial value]: -

[Explanation]

Saved executable firmware file is deleted.

[Applied model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210

47.3.8 Setting the default configuration file

[Format]

set-default-config filename

[Setting value and initial value]

- *filename*
 - [Setting value]: Setting file number (0..4.2)
 - [Initial value]: -

[Explanation]

Setting the configuration file to be used at startup.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.3.9 Setting the default firmware file

[Format]**set-default-exec filename****[Setting value and initial value]**

- *filename*
 - [Setting value]: Executable firmware file number (0..1)
 - [Initial value]: -

[Explanation]

Setting the firmware file to be used at startup.

[Applied model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210

47.3.10 Setting the baud rate of the serial port

[Format]**set-serial-baudrate rate****[Setting value and initial value]**

- *rate*
 - [Setting value]: Baud rate (9600/19200/38400/57600/115200)
 - [Initial value]: 9600

[Explanation]

Setting the baud rate of the serial port

[Applied model]

vRX Sakura Cloud Edition, RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.3.11 Initializing the settings

[Format]**cold****start****[Explanation]****n]**

Return to the initial settings at the time of factory shipment or deployment and restart. It is necessary to enter the management password at the time of command execution.

If an extension license has been imported, it will ask you to confirm "Do you want to maintain the extension by extension license (Ex-license) (Y/N)?", so it is necessary to enter "Y" to activate the extension license after initialization is completed, and "N" to delete the extension license along with initialization.

[Notes]

Note that all configuration files on internal storage (internal flash ROM, etc.) will be deleted.

Whether to maintain the extension by extension license can be specified by firmware of RTX1300 Rev.23.00.14 or later and RTX3510.

The extension license of RTX830 is forcibly deleted along with initialization by this command.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.3.12 Restrictions on configuration from remote routers

[Format]**remote setup accept tel_num [tel_num_list]****remote setup accept any****remote setup accept none**

no remote setup accept

[Setting value and initial value]

- *tel_num*
 - [Setting value]: Phone number
 - [Initial value]: -
- *tel_num_list*
 - [Setting value]: Phone number separated by spaces
 - [Initial value]: -
- any: Keyword indicating that configuration from all remote routers is allowed
 - [Initial value]: any
- none: Keyword indicating that configuration from all remote routers is denied
 - [Initial value]: -

[Explanation]

Set a destination to allow the configuration of your own router.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4 Clearing dynamic information

47.4.1 Clearing account

[Format]

clear account
clear account interface

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - BRI interface name
 - PRI interface name
 - [Initial value]: -

[Explanation]

Clears the account for the specified interface (total of all in the first format).

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.2 Clear PP account

[Format]

clear account pp [peer_num]

[Setting value and initial value]

- *peer_num*
 - [Setting value]:
 - Counterpart information number
 - If omitted, the currently selected destination
 - [Initial value]: -

[Explanation]

Clear the account for the specified PP interface.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.3 Clearing TUNNEL account

[Format]

clear account tunnel [tunnel_num]

[Setting value and initial value]

- *tunnel_num*
 - [Setting value]:
 - Counterpart information number
 - If omitted, the selected counterpart is displayed.
 - [Initial value]: -

[Explanation]

Clear the account for the tunnel interface for which the specified data connect connection setting is set.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210

47.4.4 Clearing Data Connect account

[Format]

clear account ngn

data [Explanation]

Clear Data Connect account

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.5 Clearing ARP table

[Format]

clear

arp

[Explanation]

n]

Clear the ARP table.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.6 Clearing dynamic IP routing information

[Format]

clear ip dynamic

routing [Explanation]

Clears dynamically set IP routing information.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.7 Clear peak values of connections managed by dynamic filters.

[Format]

clear ip connection

peak [Explanation]

Clear peak values of IPv4 connections managed by dynamic filters.

[Applicable model]

RTX1300

47.4.8 Clear learning information for bridges

[Format]

clear bridge learning bridge_interface

[Setting value and initial value]

- *bridge_interface*
 - [Setting value]: Bridge interface name
- [Initial value]: -

[Explanation]

All dynamically received bridge learning information is erased.

[Notes]

Registration information set statically is not erased.

RTX3500 can be used with Rev.14.00.12 or later.

RTX3500 can be used with Rev.14.00.12 or later.

[Applicable model]

vRX VMware ESXi version, vRX Sakura Cloud Edition, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.9 Clearing logs

[Format]

clear log [saved]

[Setting value and initial value]

- *saved*
 - [Setting value]: Clear logs just before reboot
- [Initial value]: -

[Explanation]

Clear logs

[Notes]

The saved option cannot be specified with RTX5000 / RTX3500 Rev.14.00.17 or earlier and RTX1210 Rev.14.01.10 or earlier.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.10 Clearing DNS cache

[Format]

clear dns

cache

[Explanation]

Clear the cache held by the DNS recursive server.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.11 Clear counter information of interface

[Format]

clear status interface

clear status pp peer_num

clear status tunnel tunnel_num

[Setting value and initial value]

- *interface*
 - [Setting value]:

- WAN interface name
- WAN interface name
 - Not specified with vRX series, RTX5000, and RTX3500
- Bridge interface name
- [Initial value]: -
- *peer_num*
 - [Setting value]: Counterpart information number
 - [Initial value]: -
- *tunnel_num*
 - [Setting value]: Tunnel interface number
 - [Initial value]: -

[Explanation]

Counter information of the specified interface is cleared.

[Notes]

Cumulative reception, cumulative transmission, and cumulative error of the interface used in the mobile Internet function are not cleared in order to prevent operations related to transmission restriction from being performed. Counter information of these cumulative can be cleared by using clear mobile access limitation command.

Bridge interface cannot be specified in vRX Amazon EC2 version and RTX5000 / RTX3500 Rev.14.00.11 or earlier.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.12 Clear NAT address table

[Format]

clear nat descriptor dynamic nat_descriptor

[Setting value and initial value]

- *nat_descriptor*
- [Setting value]:

Setting value	Explanation
1..2147483647	NAT descriptor number
all	All NAT descriptor numbers

- [Initial value]: -

[Explanation]

Clear NAT address table

[Notes]

Communication may become unstable temporarily when the address management table is cleared during communication.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.13 Clear NAT address table of interface

[Format]

clear nat descriptor interface dynamic interface

clear nat descriptor interface dynamic pp [peer_num]

clear nat descriptor interface dynamic tunnel [tunnel_num]

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name

- Not specified in vRX series, RTX5000 and RTX3500
- [Initial value]: -
- *peer_num*
 - [Setting value]:
 - Counterpart information number
 - anonymous
 - Counterpart currently selected if omitted
 - [Initial value]: -
- *tunnel_num*
 - [Setting value]:
 - Tunnel interface number
 - Tunnel interface currently selected if omitted
 - [Initial value]: -

[Explanation]

Clear NAT address table applied to interface

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.14 Clear statistics of session managed by IP masquerade

[Format]

clear nat descriptor masquerade session statistics [nat_descriptor]

[Setting value and initial value]

- *nat_descriptor*
- [Setting value]:
 - NAT descriptor number (1..2147483647)
 - *nat_descriptor* When omitted, statistics are cleared for all NAT descriptors.
- [Initial value]: -

[Explanation]

Statistics of sessions managed by IP masquerade are cleared.

[Notes]

RTX5000 / RTX3500 Rev.14.00.32 or later, RTX1210 Rev.14.01.33 or later, RTX830 Rev.15.02.09 or later are available.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.15 Peak values of sessions managed by IP masquerade are cleared.

[Format]

clear nat descriptor masquerade session peak [nat_descriptor]

[Setting value and initial value]

- *nat_descriptor*
- [Setting value]:
 - NAT descriptor number (1..2147483647)
 - *nat_descriptor* When omitted, peak values of sessions managed by all NAT descriptors are cleared.
- [Initial value]: -

[Explanation]

Peak values of sessions managed by IP masquerade are cleared.

[Notes]

This command is available only when the type parameter is set to 2 or 3 in the nat descriptor backward-compatibility command.

RTX1300 is available in Rev.23.00.17 or later.

[Applicable model]

RTX1300

47.4.16 PPPoE pass-through function clears learned information.

[Format]

clear pppoe pass-through

learning [Explanation]

PPPoE pass-through function erases learned information.

[Notes]

PPPoE session does not expire even if this command is executed.

RTX830 is available in Rev.15.02.03 or later.

RTX1210 is available in Rev.14.01.26 or later.

RTX5000 and RTX3500 are available in Rev.14.01.26 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.17 IPv6 dynamic routing information erasure

[Format]

clear ipv6 dynamic

routing [Explanation]

IPv6 routing information obtained by the routing protocol is erased.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.18 IPv6 dynamic filter clears the peak value of the connection managed.

[Format]

clear ipv6 connection

peak [Explanation]

IPv6 connection peak value managed by the dynamic filter is cleared.

[Applicable model]

RTX1300

47.4.19 Neighbor cache erasure

[Format]

clear ipv6 neighbor cache [interface]

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -

[Description]

Neighbor cache is erased.

When interface is specified, only the neighbor cache obtained via the interface is erased.

[Notebook]

The interface parameter is vRX Amazon EC2 version, vRX VMware ESXi version, RTX5000 / RTX3500 Rev.14.01.39 or earlier,

It is not possible to specify it in RTX1210 Rev.14.01.39 or earlier and RTX830 Rev.15.02.19 or earlier.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.20 Delete the history of startup information

[Format]

clear boot

list

[Explanation]

Delete the history of startup information.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.4.21 Clearing SYSLOG saved in external memory and deleting backup files

[Format]

clear external-memory

syslog **[Explanation]**

Clears the log in the currently written SYSLOG file saved in external memory and deletes all backup files of SYSLOG. The backup file of SYSLOG to be deleted is a file existing in the path specified by the external-memory syslog filename command.

Note that this command operates only when the SYSLOG file name is set by the external-memory syslog filename command and the external memory is connected to the specified external storage interface.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.5 Manipulation of files and directories

47.5.1 Creating directories

[Format]

make directory path

[Setting values and initial values]

- path
 - [Setting values]: Relative path or absolute path
 - [Initial value]: -

[Explanation]

Create a directory with the specified name.

When a relative path is specified in path, it is interpreted as a path based on the environment variable PWD. PWD can be changed by the set command, and the initial value is "/".

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.5.2 Delete files or directories

[Format]

delete path

[Setting values and initial values]

- path
 - [Setting values]: Relative path or absolute path
 - [Initial value]: -

[Explanation]

Delete specified files or directories

If the directory is not empty, subordinate files and directories are deleted at the same time.

When a relative path is specified in path, it is interpreted as a path based on the environment variable PWD. PWD can be changed by the set command, and the initial value is "/".

[Notes]

When "config" or "exec" is specified as a relative path in path, delete config command or delete exec command is executed instead of this command. In such cases, a file or directory is specified as an absolute path without using a relative path.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.5.3 Duplicate files or directories

[Format]

copy from to

[Setting values and initial values]

- from
 - [Setting values]: Source file name or directory name
 - [Initial value]: -
- to
 - [Setting values]: Source file name or directory name
 - [Initial value]: -

[Explanation]

Duplicate files or directories When from is a directory, all subordinate files and directories are recursively duplicated. From and to are specified as relative paths or absolute paths, respectively.

When from is a file, the following operations are performed.

When a directory with the same name as to exists, the data of to is overwritten by the data of from.

When a directory with the same name as to exists, a file with the same name as from is created under that directory.

When a directory with the same name as to exists, a file with the same name as from is created.

The following operations are performed when from is a directory.

Duplicate cannot be executed if a file with the same name as to exists.

If a directory with the same name as to exists, a directory with the same name as from is created under that directory.

If there is no file or directory with the same name as to, a to is created.

If a relative path is specified for from and to, it is interpreted as a path based on the environment variable PWD.

The PWD can be changed with the set command, and the initial value is "/".

[Notes]

If "config" or "exec" is specified as a relative path for from, the copy config command or copy exec command is executed instead of this command. In such cases, the relative path is not used, and a file or directory is specified as an absolute path.

Since this command does not create a parent directory according to necessity, an error occurs if a directory that does not exist in the path of to is included.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.5.4 Changing the name of a file or directory

[Format]

rename path name

[Setting value and initial value]

- path
 - Setting value: Relative or absolute path of the file or directory to be changed

- [Initial value]: -
- *name*
 - Setting value: Name after change
 - [Initial value]: -

[Description]

Changing the name of a specified file or directory

If a relative path is specified for path, it is interpreted as a path based on the environment variable PWD. The PWD can be changed with the set command, and the initial value is "/".

[Notes]

If a new name is specified for the name parameter, a name containing a slash '/' cannot be specified.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6 Other operations

47.6.1 Setting permission to use the other party

[Format]

pp enable peer_num [peer_num ...]
no pp enable peer_num

[Setting value and initial value]

- *peer_num*
 - [Setting value]:

Setting value	Description
Number	Other party information number
Number 1-Number 2	Other party information number from number 1 to number 2
Number 1-	Other party information number from number 1 to number 2
Number 1	Other party information number from number 1 to number 2
anonymous	Anonymous interface
all	Other party information number

- Initial value: -

[Description]

The other party information number can be used. Since all other parties are disabled at the time of shipment from the factory, this command must be used to enable it.

If multiple names are specified, all of them can be used. Multiple designations are RTX5000 / RTX3500 Rev.14.00.25 or earlier

Not available for RTX1210 Rev.14.01.20 or earlier and RTX830 Rev.15.02.01

[Notebook]

Be sure to change the setting by following the steps of 1. pp disable, 2. disconnect, 3. change the setting of pp, 4. enable pp, and 5. connect. When the pp enable command is executed, internal information is initialized. When a pp enable is executed while a pp is connected regardless of whether the setting of pp is changed or not, a tunnel or the like associated with a pp may be disconnected by initialization of internal information.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.2 Setting permission not to use the other party

[Settings]

pp disable peer_num [peer_num ...]

[Settings and initial values]

- *peer_num*
- [Settings]:

Settings	Description
Numbers	Other party numbers
Number 1-Number 2	Other party numbers from number 1 to number 2
Number 1-	Other party numbers from number 1 to number 2
Number 1	Other party numbers from number 1 to number 2
anonymous	Anonymous interface
all	Other party numbers

- [Initials]: -

Description

The other party is set to be disabled.
When setting the other party, it is desirable to be disabled.
If more than one is specified, all of them cannot be used. Multiple designations are available for RTX5000 / RTX3500 Rev. 14.00.25 or earlier
Not available for RTX1210 Rev. 14.01.20 or earlier and RTX830 Rev. 15.02.01

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.3 Restart

[Settings]

- restart [binary [config]]
- restart [config]

Settings and initial values

- *binary*
 - Settings: Executable firmware file number (0 to 1)
 - [Initials]: -
- *Config*
 - Settings: Setting file number of internal storage (internal flash ROM, etc.) (0 to 4.2)
 - [Initials]: -

Description

Restart the router.
A setting file and an executable firmware file at startup can be specified.
Binary is set to the default firmware file.
Config is set to the default configuration file.

Notes

Only the second format can be used for vRX series and RTX840 and RTX830. Only the first format can be used for models other than the above.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.4 Restart the interface

[Settings]

- interface reset interface [interface ...]

Settings and initial values

- *interface*
 - Settings:
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - BRI interface name
 - Not specified for RTX5000, RTX3500, and RTX1210
 - PRI interface name
 - Not specified for RTX5000, RTX3500, and RTX1210
 - USB interface name
 - Cannot be specified on the vRX series, RTX5000, and RTX3500
 - SD Interface Name
 - Cannot be specified on the vRX series
 - [Default]: -

[Description]

Restart the specified interface.

In the LAN interface, if it is set to auto-negotiate, the auto-negotiation procedure is activated.

If the line type is changed with the line type command while using the BRI and PRI interfaces, it is necessary to restart the interface with this command.

When using MP on the BRI and PRI interfaces, use the interface reset pp command.

In the USB and SD interfaces, power supply of a port is turned OFF and ON, and a USB device or a microSD card is reattached.

[Notes]

On the RTX5000, RTX3510, RTX3500, and RTX1300, when this command is executed, all LAN interfaces are reset simultaneously.

On the RTX840 and RTX830, when this command is executed for lan1 or lan2, the lan1 and lan2 interfaces are reset simultaneously.

On other models, when this command is executed, only the specified LAN interface is reset.

The USB interface cannot be specified on the RTX1210 Rev. 14.01.08 or earlier.

The SD interface cannot be specified on the RTX5000 / RTX3500 Rev. 14.00.17 or earlier and on the RTX1210 Rev. 14.01.08 or earlier.

After setting all the settings such as the line type command, pp bind command, and route information, execute it. It shall be executed in a state where communication of all destination information numbers to which the target interface is bound is stopped, and in a state where the line type is changed.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.5 Outgoing

[Format]

```
connect interface
connect peer_num
connect pp
peer_num
connect tunnel tunnel_num
```

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - Not available on the vRX series, RTX5000, and RTX3500
 - [Initial value]: -

- *peer_num*
 - Setting value: Destination information number of the destination
 - [Initial value]: -
- *tunnel_num*
 - Setting value: Tunnel number via NGN network or L2TPv3 tunnel number
 - [Initial value]: -

[Description]

Outgoing is done manually.

[Notes]

Connect tunnel command cannot be used for tunnels other than inter-site connection using data connect. Connect pp command cannot be used on models that do not implement the data connect connection function.

Connect tunnel command cannot be used on models that do not implement the data connect connection function and the L2TPv3 function.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.6 Cutting

[Format]

disconnect interface
disconnect peer_num
disconnect pp peer_num
disconnect tunnel
tunnel_num

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - Not available on the vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *peer_num*
 - [Setting value]:

Setting value	Description
Number	Destination information number to disconnect
all	All destination information numbers
anonymous	Anonymous everything
anonymous1 ..	The specified anonymous

- [Initial value]: -
- *tunnel_num*
 - [Setting value]: Tunnel number via NGN network or L2TPv3 tunnel number
 - [Initial value]: -

[Explanation]

It is manually cut.

[Notes]

The disconnect tunnel command cannot be used for tunnels other than the connection between bases using data connect. The disconnect pp command cannot be used for models that do not implement the data connect connection function.

The disconnect tunnel command cannot be used for models that do not implement the data connect connection function and the L2TPv3 function.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.7 ping

[Format]

ping [-s datalen] [-c count] [-sa ip_address] [-w wait] host

[Setting value and initial value]

- *datalen*: Data length (1..65535 bytes)
 - [Initial value]: 64
- *count*
 - [Setting value]: Number of executions (1..21474836)
 - [Initial value]: Repeat until the Ctrl+c key is entered
- *ip_address*
 - [Setting value]: Starting IP address (xxx.xxx.xxx.xxx (xxx is a decimal number))
 - [Initial value]: Select from addresses assigned to the router interface
- *wait*: Number of seconds between packet transmissions
 - [Setting value]:

Setting value	Explanation
0.1 .. 99.9	RTX5000 / RTX3500 Rev.14.00.17 or earlier, RTX1210 Rev.14.01.08 or earlier
0.1 .. 3600.0	Other than the above

- [Initial value]: 1
- *host*
 - [Setting value]:
 - The IP address of the host to ping (xxx.xxx.xxx.xxx (xxx is a decimal number))
 - The name of the host to ping
 - [Initial value]: -

[Explanation]

Send an ICMP Echo to the specified host and wait for an ICMP Echo Reply to be sent. If it is sent, indicate so. Simple statistical information is displayed when the command ends.

If the count parameter is omitted, execution continues until the Ctrl+c key is entered.

If the -w option is specified, if a reply from the other party cannot be confirmed before sending the next packet, a message to that effect is displayed. If the -w option is not specified, no message is displayed even if the packet cannot be received.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.8 Execution of ping6

[Format]

ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination

ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait]

destination%scope_id ping6 [-s datalen] [-c count] [-sa ipv6_address]

[-w wait] destination interface ping6 [-s datalen] [-c count] [-sa

ipv6_address] [-w wait] destination pp peer_num

ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination tunnel tunnel_num

[Setting value and initial value]

- *datalen*
 - [Setting value]: Data length (1..65535 bytes)
 - [Initial value]: 64
- *count*
 - [Setting value]: Number of executions (1..21474836)
 - [Initial value]: Repeat until the Ctrl+c key is entered
- *ipv6_address*
 - [Setting value]: Starting point IPv6 address

- [Initial value]: Select from addresses assigned to the router interface
- *wait*: Number of seconds between packet transmissions
- [Setting value]:

Setting value	Description
0.1 .. 99.9	[Settings]: RTX5000 / RTX3500 Rev.14.00.17 or earlier, RTX1210 Rev.14.01.08 or earlier
0.1 .. 3600.0	Other than the above

- [Setting value]: 1
- *destination*
 - [Setting value]: IPv6 address or name of the destination to be transmitted
 - [Setting value]: -
- *scope_id*
 - [Setting value]: Scope identifier
 - [Setting value]: -
- *interface*
 - [Setting value]: Name of the LAN interface
 - [Setting value]: -
- *peer_num*
 - [Setting value]: Destination information number
 - [Setting value]: -
- *tunnel_num*
 - [Setting value]: Tunnel interface number
 - [Setting value]: -

[Explanation]

Send an ICMPv6 Echo Request to the specified destination.

The scope identifier is the name of the LAN interface, the LOOPBACK interface name, or the number displayed by the show ipv6 address command (the number of the show ipv6 address command cannot be used in vRX series).

If the count parameter is omitted, execution is continued until a Ctrl+c key is input.

When the -w option is specified, if a reply from the other party cannot be confirmed before sending the next packet, a message to that effect is displayed. When the -w option is not specified, no message is displayed even if the packet cannot be received.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.9 traceroute

[Format]

traceroute host [noresolv] [-sa source]

[Setting value and initial value]

- *host*
 - [Setting value]:
 - IP address of the host to which traceroute is applied (xxx.xxx.xxx.xxx)
 - Name of the host to which traceroute is applied
 - [Setting value]: -
- *noresolv* : Keyword indicating no DNS resolution
 - [Setting value]: -
- *source*
 - [Setting value]: Starting IP address
 - [Setting value]: -

[Explanation]

Examine and display the route to the specified host.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.10 Execution of traceroute6

[Format]

traceroute6 destination [noresolv] [-sa source]

[Setting value and initial value]

- *destination*
 - [Setting value]: Starting IPv6 address or name of the destination to send
 - [Setting value]: -
- *noresolv*
 - Setting value : Keyword indicating no DNS resolution
 - [Setting value]: -
- *source*
 - Setting value]: Starting IPv6 address
 - [Setting value]: -

[Description]

The route to the specified destination is examined and displayed.

[Notes]

The noresolv and -sa options are not available for RTX5000/RTX3500 before Rev. 14.00.25, RTX1210 before Rev. 14.01.32, and RTX830 before Rev. 15.02.08

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.11 nslookup

[Format]

nslookup host [server=server [edns=edns]] [type=type] [cache=cache]

[Setting value and initial value]

- *host*
 - [Setting value]:
 - IP address
 - IPv6 address
 - Host name
 - [Initial value]: -
- *server*
 - [Setting value]: IPv4 address or IPv6 address of DNS server used for name resolution
 - [Initial value]: -
- *edns*
 - [Setting value]:

Setting value	Description
on	Communication to the target DNS server is performed by DNS
off	Communication to the target DNS server is performed by DNS

- [Initial value]: off
- *type*
 - [Setting value]:

Setting value	Description
A	Obtain IPv6 address
AAAA	Obtain IPv6 address
A+AAAA	Obtain IPv6 address
PTR	Obtain domain name from IP address
auto	Operates according to the setting value of HOST

- [Initial value]: auto
- *Cache*
- [Setting value]:

Setting value	Description
on	Name resolution prioritizes DNS cache
off	Name resolution ignores DNS cache

- [Initial value]: on

[Explanation]

Name resolution by DNS When type is set to auto, A and AAAA are obtained when host setting value is IPv4 address or IPv6 address, and PTR is obtained when FQDN. Do not use DNS cache if dns cache use is off even when cache is set to on.

[Notes]

The AAAA record and PTR record of IPv6 address are not available for the following models and revisions.

RTX830 Rev.15.02.08 and earlier

RTX1210 Rev.14.01.32 以前

RTX5000 / RTX3500 Rev.14.00.25 and earlier

The server option, edns option, type option, and cache option are not available for the following models and revisions.

RTX830 Rev.15.02.33

and earlier RTX1210

Rev.14.01.42 and earlier

RTX1220 Rev.15.04.07

and earlier RTX1300

Rev.23.00.16 and earlier

RTX3510 Rev.23.01.03

and earlier

RTX5000 / RTX3500 Rev.14.00.34 and earlier

[Applicable model]

[Model No.] vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.12 Deleting Connection Management Information for IPv4 Dynamic Filters

[Format]

disconnect ip connection session_id [channel_id]

[Setting value and initial value]

- *session_id*
 - [Setting value]: Identifier of a session
 - [Initial value]: -
- *channel_id*
 - [Setting value]: Identifier of a channel
 - [Initial value]: -

[Explanation]

A specific channel belonging to a specified session is deleted. When no channel is specified, all channels belonging to the session are deleted.

[Applicable model]

[Model No.] vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.13 TELNET client

[Format]

telnet host [port [mode [negotiation [abort]]]]

[Setting value and initial value]

- *host*
 - [Setting value]: IP address, host name or NGN network phone number of the person to whom TELNET is to be connected
 - [Initial value]: -
- *port: Port number to use*
 - [Setting value]:
 - Decimal number
 - Port number mnemonic
 - 23 (TELNET)
 - [Initial value]: 23
- *mode: Operation mode of TELNET communication (transmission)*
 - [Setting value]:

Setting value	Description
character	Communicate on a line-by-line basis
line	Communicate on a line-by-line basis
auto	Select character/line according to the setting value of the port parameter
Omitted	Auto

- [Initial value]: auto
- *negotiation : Negotiation selection for TELNET option*
 - [Setting value]:

Setting value	Description
on	Negotiate
off	No negotiation
auto	On/off selected according to the setting value of the port parameter
Omitted	Auto

- [Initial value]: auto
- *abort : Abort key to force termination of TELNET client*
 - [Setting value]:
 - Decimal number ASCII code
 - 29(^)
 - [Initial value]: 29

Description

Run the TELNET client

[Notes]

Only A record (IPv4) is supported for connection by host name.

Character mode performs transparent communication for connection to normal TELNET servers.

Line mode edits input lines and performs line-by-line communication. Completion of line editing is determined by input of a line feed code (CR:0x0d or LF:0x0a).

Automatic selection of function by port number

1. Automatic selection of operation mode for TELNET communication

Character-by-character mode is used when the port number is 23, and line-by-line mode is used when the port number is not.

2. Automatic selection of TELNET option negotiation

Negotiate when the port number is 23, otherwise do not negotiate.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.14 Deleting Connection Management Information for IPv6 Dynamic Filter

[Format]

disconnect ipv6 connection session_id [channel_id]

[Setting value and initial value]

- *session_id*
 - [Setting value]: Identifier of a session
 - [Initial value]: -
- *channel_id*
 - [Setting value]: Identifier of a channel
 - [Initial value]: -

[Explanation]

Deleting a specific channel belonging to a specified session When no channel is specified, all channels belonging to that session are deleted.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.15 Erasure of Switching Hub MAC Address Table

[Format]

clear switching-hub macaddress [interface]

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -

[Explanation]

Erases a dynamic MAC address table held inside a switching hub LSI.

[Notes]

When the macaddress-aging parameter of the lan type command is set to off, even if this command is executed, the table entry information is not erased, but is erased when the macaddress-aging parameter is set to on.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.16 Sending Magic Packet

[Format]

wol send [-i interval] [-c count] interface mac_address [ip_address [udp port]]
wol send [-i interval] [-c count] interface mac_address ethernet type

[Setting value and initial value]

- *Interval*
 - Interval between packets
 - [Initial value]: 1
- *count*
 - Interval between packets
 - [Initial value]: 4
- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -

- *mac_address*
 - [Setting value]: MAC address
 - [Initial value]: -
- *ip_address*
 - [Setting value]: IPv4 address
 - [Initial value]: -
- *port*
 - [Setting value]: UDP port number
 - [Initial value]: -
- *type*
 - [Setting value]: Ethernet type field value (1501..65535)
 - [Initial value]: -

[Description]

Magic Packet is sent to a specified LAN interface.

In the first format, packets containing Magic Packet data sequences are sent to a UDP payload as IPv4 UDP packets. Endpoint IP addresses and endpoint UDP port numbers can be specified, but if they are omitted, the directed broadcast address of the interface is used as the endpoint IP address and 9 (discard) is used as the endpoint port number. Also, packets are sent by unicast when the endpoint IP address is specified. In that case, normal routing and ARP procedures are not followed, and the endpoint MAC address is specified by a command. Packets are sent by broadcast when the endpoint IP address is omitted.

In the second format, packets in which Magic Packet data sequences begin immediately after an Ethernet header are sent.

In both formats, the transmission interval and number of times of Magic Packets can be specified by the *-i* and *-c* options. While sending packets, Commands can be interrupted with the ^C key.

[Notes]

Magic Packets cannot be sent to anything other than a LAN interface directly connected to a Yamaha router itself.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.17 Checking firmware and performing revision updates using HTTP

[Formats]

http revision-up go [no-confirm [prompt]]

[Setting values and initial values]

- *no-confirm*: Does not check whether to update firmware when there is a rewritable revision of firmware
 - [Initial value]: -
- *prompt*: Display prompt immediately after command execution so that other commands can be executed
 - [Initial value]: -

[Description]

Firmware placed on a web server and revisions of currently running firmware are checked, and if they can be rewritten, the firmware is revised up. If there is a rewritable revision of firmware, the system asks for confirmation "Do you want to update? (Y/N)", so it is necessary to enter "Y" when updating, and "N" when not updating.

If the "no-confirm" option is specified, the firmware is rewritten without confirming the update. Additionally, if the "prompt" option is specified, a prompt will be displayed immediately after command execution and other commands can be executed. However, other operations cannot be performed while firmware is being written to internal storage (internal flash ROM, etc.).

If the http revision-up permit command does not allow HTTP revision updates, the firmware is not rewritten.

If revision down is allowed by the http revision-down permit command, the firmware is rewritten even if a certain firmware in the web server has an older revision than the current firmware.

If a certain firmware in the web server has the same revision as the current firmware, the firmware is not rewritten.

[Notes]

RTX5000 and RTX3500 can be used with Rev.14.00.26 or later.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.18 URL filter statistics cleared

[Format]

clear url filter

clear url filter [interface]

clear url filter pp [peer_num]

clear url filter tunnel [tunnel_num]

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name, WAN interface name
 - [Initial value]: -
- *peer_num*
 - [Setting value]: Counterparty information number
 - [Initial value]: -
- *tunnel_num*
 - [Setting value]: Tunnel interface number
 - [Initial value]: -

[Description]

URL filter statistics are cleared. If no interface is specified, all interface information is cleared.

[Notes]

WAN interface can be specified with Rev.14.01 or later firmware.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.19 Email notification execution

[Format]

mail notify status exec id

[Setting value and initial value]

- *ID*
 - [Setting value]: Setting number (1..10)
 - [Initial value]: -

[Explanation]

Status information is transmitted by mail.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.20 Rotate (backup) a SYSLOG file stored in external memory.

[Format]

rotate external-memory syslog

[Explanation]

Rotate (backup) a SYSLOG file stored in external memory.

Save a SYSLOG file currently being written to a backup file, and create a new SYSLOG file for writing. This command is not executed when there is already a backup file with the same name.

When creating a backup file, if the number of backup files reaches the upper limit specified by the external-memory syslog filename command, or if there is no free space in external memory, the oldest backup file is deleted and then a new backup file is created.

Refer to the external-memory syslog filename command for the format of the backup file name.

This command operates only when the SYSLOG file name is set by the external-memory syslog filename command and the external memory is connected to the specified external storage interface.

[Notes]

If this command is executed periodically by the schedule at command, it becomes possible to automatically create a backup file of SYSLOG every day, week, or month.

[Configuration Example]

```
schedule at 1 */* 00:00 * rotate external-memory syslog      # Backup every day
schedule at 1 */mon 00:00 * rotate external-memory syslog   # Backup every Monday
schedule at 1 */1 00:00 * * rotate external-memory syslog   # Backup 1st day of the month
```

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.21 License authentication

[Format]

license authentication

go [Explanation]

License authentication is performed to the LMS server. It can be interrupted by pressing Ctrl-C during execution.

[Notes]

RTX830 can be used after Rev.15.02.13.

[Applicable model]

RTX1300, RTX840, RTX830

47.6.22 Interval and number of times of activation

[Format]

license authentication retry interval interval count

no license authentication retry interval [interval count]

[Setting value and initial value]

- *interval*
 - Interval (seconds) before activation (1...3600)
 - Initial value: 30
- *count*
 - Interval (seconds): Number of times to retry activation (1-10)
 - [Initial value]: 5

[Description]

Set the retry interval and number of times when license authentication fails.

When license authentication fails, license authentication is retried at intervals set in interval. When license authentication fails continuously for the number of times set in count, retry is stopped.

When manual authentication by a license authentication go command fails regardless of the setting of this command, license authentication is not retried.

[Notes]

When manual authentication by a license authentication go command is performed while waiting for license authentication retry, license authentication is stopped.

RTX830 can be used after Rev.15.02.14.

[Applicable model]

RTX1300, RTX840, RTX830

47.6.23 Batch update of settings

[Format]

load [config-type] config [difference] [silent | interactive] [no-configure-refresh] [no-key-generate] [rollback-timer=timer]

[Setting value and initial value]

- *config-type* : indicates the type of argument config
- [Setting value]:

Setting value	Description
config	config number
file	RTFS, EMFS, file names of files stored in external memory

- [Initial value]: -
- *config*
 - config number or file name
 - [Initial value]: -
- *timer*
 - Setting value: restore timer value (120...21474836)
 - [Initial value]: -

[Description]

Restores/updates settings to a specified configuration file.

If config-type is omitted, config is interpreted in the following order.

- If it matches the stored config number, its setting
- If it matches an existing file name, there are two

types of file update methods: replacement and difference.

- Replacement: All current settings are deleted once and replaced with the settings in the configuration file.
- Difference: Execute a minimal command to change the current settings to the settings in the configuration file. The default behavior is replacement update, and difference update is performed by specifying the difference option.

By default, commands to be executed to replace settings are displayed in the console. If silent option is specified, the settings are rewritten without displaying commands. If interactive option is specified, the settings can be updated while checking whether to execute commands one by one. The interactive option cannot be used from a non-interactive interface (such as command input during Web GUI configuration). Silent and interactive options cannot be specified at the same time.

If the configuration is replaced with a load command, additional commands such as 'ospf configure refresh', 'bgp configure refresh' or 'ipv6 ospf configure refresh' are executed as needed. This behavior can be suppressed by specifying the no-configure-refresh option.

If the sshd host key generate command is set in the configuration file before and after the update, if no-key-generate option is specified, host key regeneration is not performed and the settings of the host key before the update can be inherited.

The restore timer can be set with rollback-timer option. In the following cases, settings are automatically restored to the contents before executing the load command.

- The restore timer times out.
- The login timer times out.

One of the following operations is required to stop the restore timer.

- **Execute confirm command.**
- **Save configuration in non-volatile memory with save command.**
- **Logout with quit or exit command.**

- **Restart equipment with restart command.**
- Execute load command without rollback-timer option.

Only one restore timer per console is enabled. If the load command with rollback-timer option or rollback timer command is executed multiple times, only the restore timer of the last command is enabled. If rollback-timer option is omitted, the restore timer does not operate.

[Notes]

Encrypted configuration files are not supported.

RTX5000 and RTX3500 can be used with Rev.14.01.26 or later.

RTX1210 can be used with Rev.14.01.26 or later. However, the no-key-generate option can be used with Rev.14.01.28 or later.

RTX830 can be used after Rev.15.02.03.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.24 Starting a rollback timer

[Format]

rollback timer timer

[Setting value and initial value]

- *timer*
 - [Setting value]: The value of the restore timer (seconds, 1..21474836)
 - [Initial value]: -

[Description]

Only the restore timer is set. In the following cases, the settings are automatically restored to the contents before executing the rollback timer command.

- The restore timer times out.
- The login timer times out. The restore

timer stops in the following cases.

- **Execute a confirm command.**
- **Save settings to nonvolatile memory with a save command.**
- **Log out with a quit or exit command.**
- **Restart equipment with a restart command.**
- Execute a load command without the rollback-timer option.

Only one restore timer runs per console. If a load command or rollback timer command with the rollback-timer option is executed multiple times, only the restore timer of the last command is valid.

[Notes]

This command can be used as a safe net when manually changing settings.

RTX5000 and RTX3500 can be used after Rev.14.01.26.

RTX1210 can be used after Rev.14.01.26.

RTX830 can be used after Rev.14.01.26.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.25 Check settings

[Format]

confir

m

[Explanati

on]

Stop the restore timer started by the load command or rollback timer command to confirm the contents of the setting change.

[Notes]

RTX5000 and RTX3500 can be used after Rev.14.01.26.

RTX1210 can be used after Rev.14.01.26.

RTX830 can be used after Rev.14.01.26.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.26 Execute files as macros

[Format]

call [-v] [-x] filename [parameter..]

[Setting value and initial value]

- *filename*
 - [Setting value]: File name
 - [Initial value]: -
- *Parameter*
 - [Setting value]: Macro argument
 - [Initial value]: -

[Description]

Execute a file specified by filename as a macro.

Arguments can be passed to the macro. If the argument is of the form NAME=VALUE, it can refer to VALUE as a variable NAME in the macro. Other forms of arguments can be accessed as positional arguments in the order specified by \$1, \$2, etc. \$0 is a file name and \$* is a string obtained by concatenating all positional arguments with spaces. All the arguments are variables available only in the macro.

If the -v option is specified, each line to be executed when executing the macro will be executed while displaying the contents before expanding variables and aliases.

The -x option executes the macro while displaying the lines after expanding variables and aliases.

[Notes]

RTX5000 and RTX3500 can be used after Rev.14.00.26.

RTX830 can be used after Rev.14.01.26.

RTX830 can be used after Rev.15.02.03.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

47.6.27 Echo

[Format]

echo [string]

[Setting value and initial value]

- *String*
 - [Setting value]: Character string to display
 - [Initial value]: -

[Description]

Display the specified character string.

[Notes]

RTX5000 and RTX3500 can be used with Rev.14.00.26 or later.

RTX1210 can be used with Rev.14.01.26 or later.

RTX830 can be used with Rev.15.02.03 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

CHAPTER 48

Display of settings

48.1 Display of device settings

[Format]

show environment [detail]

[Explanation]

The following items are displayed.

- Revision of the system
- CPU usage (%)
 - The following values are displayed for multi-core models (each model except RTX1220 and RTX1210).
 - Usage rate per core (%)
 - Usage rate per core (%)
 - vRX Amazon EC2 version、vRX VMware ESXi version、RTX5000、RTX3500、RTX1300 Rev.23.00.04 or before On RTX830, it is displayed only when the detail option is specified.
- Memory usage (%)
- Packet buffer usage (%)
- Firmware and configuration files running
- Firmware used at startup
 - Not displayed on vRX series
- Configuration files used at startup
- Baud rate of serial port
 - Not displayed on vRX Amazon EC2 version and vRX VMware ESXi version
- Fan status
 - Displayed on RTX5000, RTX3500, RTX1220, RTX1210
- Internal temperature status
 - Displayed on RTX5000, RTX3510, RTX1220, and RTX1210

[Applicable model]

Displayed on vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

48.2 Display of all settings

[Format]

show config

show config filename

less config

less config filename

Setting value and initial value

- *filename*
 - Setting value: Setting file name or save file name (0..4.2)
 - Initial value: -

[Explanation]

Display all settings that have been set.

When the file is specified, a login password and an administration password are queried.

[Applicable model]

Displayed on vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830

48.3

Display of settings for a specified AP

[Format]

```
show config ap [ap]
less config ap [ap]
```

Setting value and initial value

- *ap*
 - Setting value:
 - MAC address or routing
 - If omitted, the selected AP is displayed.
 - Initial value: -

[Explanation]

Show config, display only those related to the specified AP from the display of less config commands.

[Notebook]

RTX1210 can be used after Rev. 14.01.09.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, and RTX830

48.4 Display of settings for a specified PP

[Format]

```
show config pp [peer_num]
show config pp [peer_num-peer_num]
less config pp [peer_num]
less config pp [peer_num-peer_num]
```

[Setting value and initial value]

- *Peer_num*
 - [Setting value]:
 - Counterpart number
 - anonymous
 - If omitted, the selected counterpart is displayed.
 - [Initial value]: -

[Explanation].

Only the counterpart number related to the specified counterpart number is displayed from the display of show config and less config commands.

When a range is specified by inserting a hyphen (-) between counterpart numbers, the counterpart number related to the specified range is displayed.

[Applicable model].

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

48.5 Display of the setting contents of the specified switch

[Format].

```
show config switch [switch]
less config switch [switch]
```

[Setting value and initial value].

- *switch*
 - [Setting value]: -
 - MAC address or route
 - If omitted, the selected switch is displayed.
 - [Initial value]: -

[Explanation].

Only the one related to the specified switch is displayed from the display of **show config** and **less config** commands.

[Notes].

RTX1210 can be used after Rev. 14.01.09.

[Applicable model].

RTX1300, RTX1220, RTX1210, RTX840, RTX830

48.6 Display of the setting contents of the specified tunnel

[Format].

```
show config tunnel [tunnel_num] [expand]
show config tunnel [tunnel_num-tunnel_num] [expand]
less config tunnel [tunnel_num] [expand]
less config tunnel [tunnel_num-tunnel_num] [expand]
```

[Setting value and initial value].

- *tunnel_num*
 - [Setting value].
 - Tunnel number
 - If omitted, the selected tunnel is displayed.
 - [Initial value]: -

[Explanation].

Only the one related to the specified tunnel number is displayed from the display of **show config** and **less config** commands.

When a range is specified by inserting a hyphen (-) between tunnel numbers, the one related to the tunnel number of the specified range is displayed.

If an **expand** keyword is specified, the setting that is actually referred to when the router operates after the tunnel template specified by the tunnel template command is applied is displayed.

[Applicable model].

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

48.7 Display of setting difference.

[Format].

```
show config difference [[config-type1] config1] [config-type2] config2
```

[Setting value and initial value].

- *config-type1/2*: Indicates the type of arguments *config1* and *config2*.
 - [Setting value].

Setting value.	Explanation.
config	config number
file	RTFS, EMFS, file names stored in external memory

- [Initial value]: -
- *config1/2*
 - *config-type1/2*: '-' (current setting), config number, or file name.
 - [Initial value]: -

[Explanation].

The difference between *config1* and *config2* is displayed in the form of a command string for converting *config1* to *config2*.

Commands that are in *config1* but not in *config2* are displayed in no format, and commands that are not in *config1* but are in *config2* are displayed in normal format.

If *config1* is omitted, it is assumed that '-' (currently running setting) is specified.

If config-type1/2 is omitted, config1/2 is interpreted in the following order.

- If it matches an existing config number, its setting
- If it matches an existing file name, its setting

[Notes]

If a config number is specified in config1/2 and the saved settings include login password, login password encrypted, administrator password, and administrator password encrypted commands, it is necessary to input those passwords before operation.

This command works only in administrator mode.

RTX5000 and RTX3500 can be used with Rev.14.01.26 or later.

RTX1210 can be used with Rev.14.01.26 or later.

RTX830 can be used with Rev.15.02.03 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

48.8 List of configuration files

Format

- show config
- list less config
- list

[Description]

Displays a list of file names, dates and times, and comments of configuration files stored in internal storage (internal flash ROM, etc.).

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

48.9 Display of a list of file information

Format

- show file list location [all] [file-only]
- less file list location [all] [file-only]

[Setting value and initial value]

- location : The location where the file to be displayed is.
- [Setting value]:

Setting value	Explanation
internal	List of configuration files stored in internal storage (internal flash ROM, etc.)
Absolute path or relative path	RTFS for internal storage (internal flash ROM, etc.) Region, external memory, external storage

- [Initial value]: -
- all : Target all directories under it
 - [Initial value]: -
- file-only : Display only file names
 - [Initial value]: -

[Description]

Displays a list of file information stored in a specified location.

If a relative path is specified for location, it is interpreted as a path based on the environment variable PWD. PWD can be changed with the set command, and the initial value is "/".

[Notes]

All and file-only can be used only if location specifies an absolute path or a relative path.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

48.10 Display of IPv6 addresses assigned to the interface

Format**show ipv6 address [interface]****show ipv6 address pp [peer_num]****show ipv6 address tunnel [tunnel_num]****[Setting value and initial value]**

- *interface*
 - Setting value: LAN interface name, LOOPBACK interface name, NULL interface, bridge interface name
 - [Initial value]: -
- *peer_num*
 - [Setting value]:
 - Counterpart information number
 - anonymous
 - If omitted, the selected party is displayed.
 - [Initial value]: -
- *tunnel_num*
 - [Setting value]: Tunnel interface number
 - [Initial value]: -

[Explanation]

The IPv6 address given to each interface is displayed.

When no interface is specified, information is displayed for all interfaces.

[Notes]

Bridge interface cannot be specified in vRX Amazon EC2 version and RTX5000 / RTX3500 Rev.14.00.11 or earlier.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

48.11 Display of SSH server public key

[Format]**show sshd public key [fingerprint]****[Setting value and initial value]**

- Fingerprint: Key keyword indicating display of fingerprint
 - [Initial value]: -

[Explanation]

Displays the public key of the SSH server.

When fingerprint keyword is specified, key length and key fingerprint of the public key are displayed.

[Notes]

Fingerprint keyword cannot be used in RTX5000 / RTX3500 Rev.14.00.20 or earlier and RTX1210 Rev.14.01.10 or earlier.

[Example display]

```
>show sshd publickey
ssh-dss
XXXXXXXXXX1kc3MAAAEBAPTb9YYdgvE+4bbhF4mtoIJri+ujdAIfgr4hL/0w7Jlvc50eXgsXJoCq1Pl
sLRGH0OzxVYbOouPCUV/jPFcatgOIii8eJNzUqSBle6MOftGjmESrdYiafyIUhps+YWqd
TlIo0AFnVUKMqAbYODA3Cy7kNVptYRK8rcKWk1ChbatWnT/Z7RcmEVEou0qlOyp79b3DcpFM7ofa4d
9ySb6mj06Y/Ok8lL5qFhCHmGOGtqJTKZsqb5VnPz8FYC8t1s6/tpyrUa5aG2af/yTEa5U5BDYAuc88
wNIUG9alGo/8WIHiBJAm432o7UPqTHWO/5nYEQu44gmEPQrPGJ65GT8AAAAVAOpjE0Jyei+4c5qWSF
```

```
ARypDjhpL1a37SDezx8yClQ5vh+4SPLdS1hdSSzXXE+MXIICXnOVPdiKC4ia10n81tMxW/EPw4SqFP
77r7VvCE/JpXv82AN2JTJ/HAn3X7lvMyCsKZLoWrEcEcBH5anvAQKByVt7RerToZ4vSgodskv7nyXX
XXXXXX
ssh-rsa XXXXXXXXXXXX1yc2EAAAABiWAAAEAwvAZK18jKTCHIHQfRV4r7UOYChX0oeKjBbuuLSDhSH
WmhpG3xxJO0pDIedSF3KnB7LX2SfymQYJ7XYIqMjmU0oziV/zi+De/z3M7wJHQUwfMZEADaR6Mx39w
6Q04/ehQcaszjXi+0Al2wG/kk56lAU23CW/i2lo//5GZTzkFKyEJUWauHWEW9glF5Yy7F64PesqoH
6h5oDNK7LhlT7s4QXRnUJphIlINrW278Dnvryy3liR+tgTJAq3cGHfYsaQCdankDilIQhUazUY0vJO
/gjYcJmUwH6Ek/cst+Pctgnt0XV5Bl079uRUmcACs2pDX5EWrbPXXXXXXXXXX==

>show sshd public key fingerprint
ssh-dss 2048 XX:XX:77:c5:f9:48:fd:62:85:fb:27:a8:0a:c1:XX:XX
ssh-rsa 2048 XX:XX:58:89:e2:0b:ec:d9:6b:49:11:d2:a3:9d:XX:XX
```

[Applicable model]
RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

48.12 **Display of filter contents of specified interface**

[Format]

show ip secure filter interface [dir]
show ip secure filter pp [peer_num] [dir]
show ip secure filter tunnel [tunnel_num] [dir]

[Setting value and initial value]

- *interface*
 - [Setting value]: Filtered interface name
 - [Initial value]: -
- *peer_num*
 - [Setting value]: Counterpart information number
 - [Initial value]: -
- *tunnel_num*
 - [Setting value]: Tunnel interface number
 - [Initial value]: -
- *[Dir]*
 - [Setting value]: Filtered direction applied, 'in' or 'out'
 - [Initial value]: -

[Explanation]

Displays the contents of the filter definition applied to the specified interface.

[Applicable model]

[Setting value]: Setting value of a filter definition applied to the specified interface

48.13 **Displaying IPv6 filter contents of the specified interface**

[Format]

show ipv6 secure filter interface [dir]
show ipv6 secure filter pp [peer_num] [dir]
show ipv6 secure filter tunnel [tunnel_num] [dir]

[Setting value and initial value]

- *interface*
 - [Setting value]: Filtered interface name applied
 - [Initial value]: -
- *peer_num*
 - [Setting value]: Counterparty information number
 - [Initial value]: -
- *tunnel_num*
 - [Setting value]: Tunnel interface number
 - [Initial value]: -
- *dir*

- [Setting value]: Filtered direction applied, 'in' or 'out'
- [Initial value]: -

[Explanation]

Displays the contents of the IPv6 filter definition applied to the specified interface.

[Notes]

Not available for RTX5000 / RTX3500 Rev. 14.00.25 or earlier, RTX1210 Rev. 14.01.32 or earlier, and RTX830 Rev. 15.02.08 or earlier

Noh

[Applicable model]

[Model]: vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

48.14 List of firmware files

[Format]

```
show exec list
less exec list
```

[Explanation]

Information on executable firmware files stored in internal storage (internal flash ROM, etc.) is displayed. The executable firmware file being started is marked with '*'. When an external memory in which an executable firmware file is stored is connected, information on the firmware file is also displayed.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

48.15 Display of environment variables

[Format]

```
show set [name]
```

[Setting value and initial value]

- Name
 - Setting value: Environment variable name
 - Initial value: -

[Explanation]

Display the value of the specified environment variable.

If name is omitted, all set environment variables are displayed.

[Notes]

RTX5000 and RTX3500 can be used after Rev. 14.01.26.

RTX1210 can be used after Rev. 14.01.26.

RTX830 can be used after Rev. 15.02.03.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210

48.16 Display of aliases

[Format]

```
show alias [name]
```

[Setting value and initial value]

- Name
 - Setting value: Alias name
 - Initial value: -

[Description]

Displays the value of the specified alias.
When name is omitted, all set aliases are displayed.

[Notes]

RTX5000 and RTX3500 can be used with Rev.14.00.26 or later.
RTX1210 can be used with Rev.14.01.26 or later.
RTX830 can be used with Rev.15.02.03 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840 and RTX830

48.17 **Display of macros**

Format

show macro [name]

Setting value and initial value

- name
 - Setting value: Macro name
 - Initial value: -

[Description]

Display the value of the specified macro.
When name is omitted, all set macros are displayed.

[Notes]

RTX5000 and RTX3500 can be used with Rev.14.02.03 or later.
RTX1210 can be used with Rev.14.01.26 or later.
RTX830 can be used with Rev.15.02.03 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840 and RTX830

CHAPTER 49

Status Display

49.1 Displaying the ARP Table

Format

show arp [interface]

Setting Value and Initial Value

- *interface*
 - Setting Value:
 - LAN Interface Name
 - Tag LAN Interface Name
 - Cannot be specified in the vRX Series
 - Initial Value: -

Description

Display the ARP Table. When an interface name is specified, only the ARP table information obtained via the interface is displayed.

Applicable Model

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840 and RTX830

49.2 Status Display

Format

show status interface

Setting Value and Initial Value

- *interface*
 - Setting Value:
 - LAN Interface Name
 - WAN Interface Name
 - Cannot be specified in the vRX Series, RTX5000 and RTX3500
 - PRI Interface Name
 - Can be specified in the RTX5000, RTX3500 and RTX1210
 - PRI Interface Name
 - Can be specified in the RTX5000, RTX3500 and RTX1210
 - Bridge Interface Name
 - Initial Value: -

Explanation

Status Display

Notes

Bridge Interface can not be specified in the vRX Amazon EC2 Edition and RTX5000/RTX3500 Rev. 14.00.11 or earlier

Applicable Model

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840 and RTX830

49.3 Status Display

Format

show status pp [peer_num]

Setting Value and Initial Value

- *Peer_num*

- Setting Value:
 - Counterpart Information Number
 - anonymous
 - When omitted, selected Counterparts are displayed
- Initial Value: -

Description

Status Displays the status of each Counterpart during connection or when it is connected last.

- Are they connected or not?
- Status of Last Call
- Date and Time of Connection
- Line Type
- Communication Time
- Reason for Disconnection
- Communication Charges
- Counterpart IP address
- Number of packets successfully transmitted
- Number and Breakdown of Transmission Errors
- Number of packets successfully received
- Number and Breakdown of Reception Errors
- Status of PPP
- Status of CCP
- Others

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.4 Displaying an IP routing table

[Format]

show ip route [destination]

show ip route detail

show ip route summary

[Setting value and initial value]

- *destination*
 - [Setting value]:
 - Destination IP address
 - When omitted, the entire routing table is displayed.
 - [Initial value]: -
- detail : Displays static routes hidden by routes obtained by a dynamic routing protocol in addition to currently valid IPv4 routes.
 - [Initial value]: -
- summary : Displays the total number of IPv4 routes for each protocol.
 - [Initial value]: -

[Description]

Displays an IP routing table or a gateway to the destination IP address. A net mask is expressed by a continuous number of bits regardless of the expression at the time of setting.

DLCI values are displayed when frame relays are used.

When detail is specified, in addition to currently valid IPv4 routes, static routes hidden by comparison of preference values with routes obtained by a dynamic routing protocol are also displayed.

When summary is specified, the total number of IPv4 routes for each protocol is displayed.

[Notes]

For routes obtained by a dynamic routing protocol, additional information is displayed according to the protocol. Additional information to be displayed is as follows.

Protocols	Metric values
RIP	Metric values
OSPF	Internal/external routes, cost values, metric values (external routes only) For external routes of Type 1, the cost value is the cost value to a route including a metric value. For external routes of Type 2, the cost value is the cost value to an ASBR.
BGP	None

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.5 Display of routing information obtained by RIP

[Format]

show ip rip

table

[Explanation]

Display of routing information obtained by RIP.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.6 Display of IPv6 routing information

[Format]

show ipv6 route

show ipv6 route detail

show ipv6 route summary

[Setting values and initial values]

- detail : In addition to currently valid IPv6 routes, static routes hidden by routes obtained by a dynamic routing protocol are also displayed.
 - Default : -
- summary : Total number of IPv6 routes for each protocol is displayed
 - Default : -

[Description]

IPv6 routing information is displayed.

When detail is specified, in addition to currently valid IPv6 routes, IPv6 routes hidden by comparison of preference values are also displayed.

When detail is specified, the total number of IPv6 routes for each protocol is displayed.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.7 Display of IPv6 RIP tables

[Format]

show ipv6 rip

table **[Explanation]**

View the IPv6 RIP table.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.8 Display of neighbor cache

[Format]**show ipv6 neighbor cache [interface]****show ipv6 neighbor cache [interface] summary****[Setting value and initial value]**

- *interface*
 - [Setting value]: LAN interface name
- [Initial value]: -

[Explanation]

Display the status of the neighbor cache.

When interface is specified, only the status of the neighbor cache obtained via the interface is displayed.

When summary is specified, only the number of entries in the neighbor cache is displayed.

[Notes]

The interface parameter and second format cannot be specified for vRX Amazon EC2 version, vRX VMware ESXi version, RTX5000 / RTX3500 Rev.14.00.31 or earlier, RTX1210 Rev.14.01.39 or earlier, and RTX830 Rev.15.02.19 or earlier.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.9 Display of learning information of the bridge

[Format]**show bridge learning bridge_interface****[Setting value and initial value]**

- *bridge_interface*
 - [Setting value]: Bridge interface name
- [Initial value]: -

[Explanation]

Display learning information of the MAC address of the bridge.

[Notes]

RTX3500 can be used with Rev.14.00.12 or later.

RTX3500 can be used with Rev.14.00.12 or later.

[Applicable model]

vRX VMware ESXi version, vRX Sakura Cloud version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.10 Display of SA in IPsec

[Format]**show ipsec sa [id]****show ipsec sa gateway [gateway_id] [detail]****[Setting value and initial value]**

- *ID*
 - [Setting value]:
 - Identifier of SA
 - When omitted, all SAs are displayed.
 - [Initial value]: -
- *gateway_id*

- [Setting value]:
 - Identifier of security gateway
 - When omitted, a summary of SAs of all security gateways is displayed.
- [Initial value]: -
- detail : Detailed information of SAs is displayed.
- [Initial value]: -

[Explanation]

Displays the SA status of IPsec.

Displays information of SAs with identifiers given by id.

[Notebook]

User name used for authentication when XAUTH authentication was performed when generating the corresponding SA

- Did RADIUS authentication or not?
- Internal IP address notified
- Added route information
- Displays information of

applied filters

simultaneously.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.11 Display of information of certificates

[Format]

show pki certificate summary [cert_id]

[Setting value and initial value]

- *cert_id*
- [Setting value]: -

Setting value	Description
1..8	Certificate file identifier

- [Initial value]: -

[Explanation]

Display information of a certificate. Displayed information is as follows.

- Subject
- SubjectAltName
- Usable period (Not Before, Not After)
- Certificate type (CA certificate / equipment certificate)

When cert_id is specified, only the information of the certificate of the specified file identifier is displayed.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.12 Displaying information of a CRL file

[Format]

show pki crl [crl_id]

[Setting value and initial value]

- *crl_id*
- [Setting value]: -

Setting value	Description
1..8	CRL file identifier

- [Initial value]: -

[Explanation]

Display information of a CRL file.
Displayed information is as follows.

- Version
- Publisher
- Update date and time
- Next update date and time

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.13 Displaying information of a VRRP

[Format]

show status vrrp [interface [vrid]]

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *vrid*
 - [Setting value]: VRRP group ID (1..255)
 - [Initial value]: -

[Explanation]

Display information of a VRRP.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.14 Display of a dynamic NAT descriptor address map

[Format]

show nat descriptor address [nat_descriptor] [detail]

[Setting value and initial value]

- *nat_descriptor*
- [Setting value]:

Setting value	Explanation
1..2147483647	NAT descriptor number
all	All NAT descriptor numbers

- [Initial value]: -
- detail: Displays all entries of a dynamic IP masquerade.
- [Initial value]: -

[Description]

Displays an address map of a dynamic NAT descriptor.
When nat_descriptor is omitted, all NAT descriptor numbers are displayed.

[Notes]

When the detail option is omitted, dynamic IP masquerade entries are displayed aggregated for each inner IP address.

An IP masquerade entry generated by deriving from a static IP masquerade entry is not displayed. Therefore, the detail option is added from the same series as an option to display in all entry display formats before that.

When there are a large number of entries of an IP masquerade, specifying the detail option may take time to display all entries and may affect communication. Therefore, when you want to check the number of ports or the number of sessions in an IP masquerade, it is recommended not to specify the detail option, or to use the show nat descriptor masquerade port summary command or the show nat descriptor masquerade session summary command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.15 Displaying an Application List of an Active NAT Descriptor

[Format]

```
show nat descriptor interface bind interface
show nat descriptor interface bind pp
show nat descriptor interface bind
tunnel
```

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -

[Description]

Displays a list of NAT descriptors and application interfaces.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.16 Displaying an Address Map of a NAT Descriptor in a LAN Interface

[Format]

```
show nat descriptor interface address interface
show nat descriptor interface address pp peer_num
show nat descriptor interface address tunnel tunnel_num
```

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *peer_num*
 - [Setting value]: Destination information number
 - [Initial value]: -
- *tunnel_num*
 - [Setting value]: Tunnel interface number
 - [Initial value]: -

[Description]

Displays an address map of the NAT descriptor applied to the interface.

[Notebook]

Dynamic IP masquerade entries are displayed aggregately for each inner IP address, and IP masquerade entries generated by deriving from static IP masquerade entries are not displayed.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.17 Display of the number of port numbers used in IP masquerade

[Format]

show nat descriptor masquerade port [nat_descriptor] summary

[Setting value and initial value]

- *nat_descriptor*
- [Setting value]:
 - NAT Descriptor Number (1..2147483647)
 - *nat_descriptor* When omitted, displays for all NAT descriptors.
- [Initial value]: -

[Description]

Displays the number of port numbers used in dynamic IP masquerade. It does not include the number of port numbers secured in static IP masquerade.

[Notes]

This command cannot be used when the type parameter is set to 2 or 3 with the nat descriptor backward-compatibility command.

Instead, the number of sessions being managed can be displayed with the show nat descriptor masquerade session summary command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.18 Display of the number of sessions being managed by IP masquerade

[Format]

show nat descriptor masquerade session [nat_descriptor] summary

[Setting value and initial value]

- *nat_descriptor*
- [Setting value]:
 - NAT descriptor number (1..2147483647)
 - *nat_descriptor* When omitted, all NAT descriptors are displayed.
- [Initial value]: -

[Description]

The number of sessions managed by IP masquerade and the peak value of the number of sessions are displayed. The peak value of the number of sessions is cleared by changing the configuration of NAT descriptor or restarting router, and is not cleared by deleting session by clear nat descriptor dynamic command.

[Notes]

This command can be used only when the type parameter is set to 2 or 3 with the nat descriptor backward-compatibility command.

RTX3500 can be used with Rev.14.00.32 or later.

RTX3500 can be used with Rev.14.00.32 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.19 Display of session statistics managed by IP masquerade

[Format]

show nat descriptor masquerade session statistics [nat_descriptor]

[Setting value and initial value]

- *nat_descriptor*
- [Setting value]:
 - NAT descriptor number (1..2147483647)
 - *nat_descriptor* When omitted, all NAT descriptors are displayed.
- [Initial value]: -

[Description]

The number of sessions, peak value, limited number of times and time are displayed for each host identified by the starting IP address as session statistics managed by IP masquerade. The limit value of the number of sessions follows the setting value of the nat descriptor masquerade session limit command.

[Notes]

Not available with RTX5000/RTX3500 Rev.14.00.31 or earlier, RTX1210 Rev.14.01.32 or earlier, and RTX830 Rev.15.02.08 or earlier
Noh

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.20 The peak value of the session used by IP masquerade is displayed.

[Format]

show nat descriptor masquerade session peak [nat_descriptor]

[Setting value and initial value]

- *nat_descriptor*
- [Setting value]:
 - NAT descriptor number (1..2147483647)
 - *nat_descriptor* When omitted, all NAT descriptors are displayed.
- [Initial value]: -

[Description]

The number of sessions and time when the session managed by IP masquerade recorded the peak are displayed. Also, the top 5 hosts with the highest number of sessions when the peak was recorded are displayed.

The peak value is cleared by the following operation.

- When you restart your router
- When you change the setting of NAT descriptor
- clear nat descriptor masquerade session peak When you execute the command
- When you execute "Clear peak value" with the dashboard's [Live]-[Number of NAT sessions] gadget for models that support Web GUI

[Notebook]

An IP masquerade entry generated by deriving from a static IP masquerade entry is not displayed.

This command can be used only when the type parameter is set to 2 or 3 with the nat descriptor backward-compatibility command.

RTX1300 can be used with Rev.23.00.17 or later.

[Applicable model]

RTX1300

49.21 Display of L2TP status

[Format]

show status l2tp [tunnel tunnel_num]

[Setting value and initial value]

- *tunnel_num*
 - [Setting value]: Tunnel number
 - [Initial value]: -

[Explanation]

Displays the status of L2TP.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.22 Displaying the status of PPTP

[Format]

show status

pptp [Explanation]

Displays information such as the status of PPTP and statistics of GRE.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.23 Displaying the status of IP/IP tunneling

[Format]

show status ipip [tunnel tunnel_num]

[Setting value and initial value]

- *tunnel_num*
 - [Setting value]: Tunnel number
 - [Initial value]: -

[Explanation]

Displays the status of IP/IP tunneling.

[Notes]

RTX5000 / RTX3500 can be used after Rev.14.01.20.
RTX1210 can be used after Rev.14.01.20.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.24 Displaying OSPF information

[Format]

show status ospf info

[Setting value and initial value]

- *info: Type of information to display*
 - [Setting value]:

Setting value	Explanation
Database	Database of OSPF
neighbor	Neighbor router
interface	Status of each interface
virtual-link	Status of virtual link

- [Initial value]: -

[Explanation]

Various information of OSPF is displayed.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.25 Displaying BGP status

[Format]

show status bgp neighbor [ip-address]

show status bgp neighbor ip-address route-type

[Setting value and initial value]

- *ip-address*
 - [Setting value]: IP address of adjacent router
 - [Initial value]: -
- *route-type*: Display of route information
 - [Setting value]:

Setting value	Explanation
advertised-routes	Display routes advertised on adjacent routers.
received-routes	Display routes received from adjacent routers.
routes	Valid routes received from adjacent routers are displayed.

- [Initial value]: -

[Explanation].

Display information on adjacent routers of BGP.

When ip-address is specified, information on specific adjacent routers is displayed. When ip-address is omitted, information on all adjacent routers is displayed.

When route-type is specified, information on routes exchanged with adjacent routers is displayed. When advertised-routes is specified, routes advertised to adjacent routers are displayed. When received-routes is specified, all routes received from adjacent routers are displayed. When routes are specified, only routes accepted by bgp export filter or the like are displayed out of routes received from adjacent routers.

[Applicable model].

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.26 Display of DHCP server status

[Format].

show status dhcp [summary] [scope_n]

[Setting value and initial value].

- *summary* : Displays an overview of the IP address allocation status of each DHCP scope.
 - [Initial value]: -
- *scope_n*
 - [Setting value]: Scope number (1-65535).
 - [Initial value]: -

[Explanation].

Display the lease status of each DHCP scope. The following items are displayed.

- Lease status of DHCP scope.
- DHCP scope number
- Network address
- Assigning IP address
- Assigning client MAC address
- Lease remaining time

- Reserved (unused) IP address
- Total number of IP addresses in DHCP scope
- Number of excluded IP addresses
- Number of allocated IP addresses
- Number of available addresses (of which reserved IP addresses)

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.27 Display of DHCP client status

[Format]

show status

dhcpc

[Explanation]

Displays the status of DHCP client.

- Client status
 - Interface
 - IP address (state if not available)
 - DHCP server
 - Lease remaining time
 - Client ID
 - Host name (when set)
- Common information
 - DNS server
 - Gateway

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.28 Display of DHCPv6 status

[Format]

show status ipv6

dhcpc **[Explanation]**

Displays the status related to DHCPv6.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.29 Display of backup status

[Format]

show status

backup

[Explanation]

Displays the backup status of interfaces configured for backup.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.30 Display of connections managed by dynamic filters

[Format]

show ip connection

show ip connection interface [direction] [ip_address]

show ip connection pp peer_num [direction]

[ip_address] show ip connection tunnel tunnel_num

[direction] [ip_address] show ip connection summary

show ip connection detail

show ip connection detail interface [direction]
show ip connection detail pp peer_num [direction]
show ip connection detail tunnel tunnel_num [direction]

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Not specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *peer_num*
 - [Setting value]: Destination information number
 - [Initial value]: -
- *tunnel_num*
 - [Setting value]: Tunnel interface number
 - [Initial value]: -
- *direction*
 - [Setting value]:

Setting value	Description
in	Input direction
out	Output direction

- [Initial value]: -
- *ip_address*
 - [Setting value]: IP address xxx.xxx.xxx.xxx (xxx is a decimal number)
 - [Initial value]: -
- summary: Displays the number of managed connections per interface/direction and the total of the whole
 - [Initial value]: -
- detail: Displays all connections managed by dynamic filters
 - [Initial value]: -

[Explanation]

For specified interfaces, connections managed by dynamic filters are displayed. When no interfaces are specified, information on all interfaces is displayed.

When detail is not specified, managed connections are aggregated and displayed for each source IP address. However, when ip_address is specified, information whose source address matches ip_address is displayed out of information when detail is specified.

[Applicable models]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.31 Peak values of connections managed by dynamic filters are displayed.

[Format]

show ip connection

peak [Explanation]

Peak values of IPv4 connections managed by dynamic filters are displayed. Peak values are cleared by the following operations.

- When you restart your router
- When you change the setting of an IP filter
- When you execute "Clear peak value" in the dashboard's [Live]-[Number of dynamic filter sessions] gadget for models that support Web GUI.
- **When you run the clear ip connection peak command**

[Applicable models]
RTX1300

49.32 Display of connections managed by dynamic filters of IPv6

[Format]

```
show ipv6 connection
show ipv6 connection interface [direction] [ipv6_address]
show ipv6 connection pp peer_num [direction]
[ipv6_address] show ipv6 connection tunnel tunnel_num
[direction] [ipv6_address] show ipv6 connection summary
show ipv6 connection detail
show ipv6 connection detail interface [direction]
show ipv6 connection detail pp peer_num [direction]
show ipv6 connection detail tunnel tunnel_num [direction]
```

[Set value and initial value]

- *interface*
 - [Set value]: LAN interface name
 - [Set value]: -
 - *peer_num*
 - [Set value]: Destination information number
 - [Set value]: -
 - *tunnel_num*
 - [Set value]: Tunnel interface number
 - [Set value]: -
 - *direction*
 - [Set value]: -
Set value	Description
in	Input direction
out	Output direction
- [Set value]: -
 - *ipv6_address*
 - [Set value]: IPv6 address part
 - [Set value]: -
 - *summary*: Displays the number of managed connections per interface/direction and the total of the whole
 - [Set value]: -
 - *detail*: Displays all connections managed by dynamic filters
 - [Set value]: -

[Explanation]

Displays connections managed by dynamic filters for specified interfaces. When no interfaces are specified, information on all interfaces is displayed.

When detail is not specified, managed connections are aggregated and displayed for each source IP address. However, when *ipv6_address* is specified, the information whose source address matches *ipv6_address* is displayed among the information when detail is specified.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.33 Displays the peak value of connections managed by dynamic filters of IPv6.

[Format]

```
show ipv6 connection peak
```

[Explanation]

Displays the peak value of IPv6 connections managed by dynamic filters. The peak value is cleared by the following operation.

- When you restart your router
- When you change the settings of an IPv6 filter
- When you execute "Clear peak value" on the dashboard's [Live]-[Number of dynamic filter sessions] gadget for models that support Web GUI.
- **When you execute the clear ipv6 connection peak command**

[Applicable model]

RTX1300

49.34 Displaying the status of network monitoring functions

[Format]

show status ip

keepalive [Explanation]

Displays the status of network monitoring functions.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.35 Displaying the history of intrusion information

[Format]

show ip intrusion detection

show ip intrusion detection interface [direction]

show ip intrusion detection pp [peer_num [direction]]

show ip intrusion detection tunnel [tunnel_num [direction]]

[Setting value and initial value]

- *interface*
 - [Setting value]:
 - WAN interface name
 - WAN interface name
 - Cannot be specified for vRX series, RTX5000, and RTX3500
 - [Initial value]: -
- *peer_num*
 - [Setting value]: Destination information number
 - [Initial value]: -
- *tunnel_num*
 - [Setting value]: Tunnel interface number
 - [Initial value]: -
- *direction*
 - [Setting value]:

Setting value	Description
in	Input direction
out	Output direction

- [Initial value]: -

[Explanation]

Recent intrusion information is displayed. Intrusion information is displayed for each direction of each interface, and the maximum number of displayed cases is the number set by the ip interface intrusion detection report command.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.36 PPPoE pass-through function displays learned information

[Format]

show pppoe pass-through

learning [Explanation]

PPPoE pass-through function displays learned information.

[Notes]

RTX830 can be used after Rev.15.02.03.

RTX1210 can be used after Rev.14.01.26.

RTX5000 and RTX3500 can be used after Rev.14.00.26.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.37 Display of settings related to Netvolanche DNS service

[Format]

show status netvolante-dns interface

show status netvolante-dns pp [peer_num]

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name, WAN interface name
 - [Initial value]: -
- *peer_num*
 - [Setting value]:
 - Destination information number
 - If omitted, selected party is displayed.
 - [Initial value]: -

[Explanation]

Display settings related to dynamic DNS. Display contents

Netvolanche DNS service	AUTO/OFF
Interface	INTERFACE
Host address	aaa.bbb.netvolante.jp
IP address	aaa.bbb.ccc.ddd
Latest update date and time	2001/01/25 15:00:00
Timeout	90 seconds

[Notes]

The WAN interface can be specified by the firmware of Rev.14.01 series or later.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.38 Displaying the Switching Hub MAC Address Table

[Format]

show status switching-hub macaddress [interface [port]] [mac_address]

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *port*
 - [Setting value]: Port number 1..8 (RTX1220, RTX1210), 1..4 (Models other than those listed on the left)
 - [Initial value]: -
- *mac_address*
 - [Setting value]: MAC address
 - [Initial value]: -

[Explanation]

Dynamic MAC address table for each port held in the switching hub LSI is displayed. When a port number is specified, only information about the port is displayed. Only an interface with a switching hub can be specified in the LAN interface name.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.39 Displaying status information about UPnP

[Format]

show status

upnp

[Explanation]

Display status information about UPnP

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.40 Displaying the status of the tunnel interface

[Format]

show status tunnel [tunnel_num]

show status tunnel [state]

show status tunnel [name=name]

[Setting value and initial value]

- *tunnel_num*
 - [Setting value]: Tunnel interface number
- [Initial value]: -
- *state: Connection status*
 - [Setting value]:

Setting value	Explanation
up	Displaying a list of connected tunnel interfaces
down	Displaying a list of tunnel interfaces that are not connected

- [Initial value]: -
- *name*
 - [Setting value]: Name of the connection partner
- [Initial value]: -

[Explanation]

Displays the status of the tunnel interface.

The second format does not correspond to PPTP tunnels. In a model that corresponds to PPTP, a PPTP tunnel is judged as an unconnected tunnel interface. In a model that corresponds to L2TP/IPsec function and L2TPv3/IPsec function, the connection status of an L2TP tunnel is judged according to the status of the IPsec tunnel.

In the third format, information on a connection partner whose name includes a character string specified in name is extracted from a connection partner connected by a multipoint tunnel interface and displayed. The name of the connection partner is set by the other party's tunnel multipoint local name command.

Note

The third format cannot be used in RTX5000/RTX3500 Rev.14.00.25 or earlier and RTX1210 Rev.14.01.19 or earlier.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.41 Displaying the status of the VLAN interface

[Format]

show status vlan [interface/sub_interface]

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name
 - [Initial value]: -
- *sub_interface*
 - [Setting value]: 1-32
 - [Initial value]: -

[Explanation]

Displays information of a VLAN interface. When a VLAN interface name is specified, only the information of the interface is displayed.

[Applied model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.42 Display of status of mail notification function by trigger

[Format]

show status mail service [template_id] [debug]

[Setting value and initial value]

- *template_id*
 - [Setting value]: Template ID (1..10)
 - [Initial value]: -
- *debug* : Display internal information for debugging
 - [Initial value]: -

[Explanation]

Displays the internal status of mail notification function by trigger.

When template ID is not specified, the status of all template IDs is displayed.

[Applied model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.43 Display of group management information of MLD

[Format]

show status ipv6

mld [Explanation]

List information managed by MLD.

If an MLD proxy is running, the transfer destination can be confirmed by this command.

[Applied model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.44 Display of route information of IPv6 multicast

[Format]

show ipv6 mroute

fib [Explanation]

Displays the transfer path of IPv6 multicast packets.

In this command, the following contents are listed for each transfer path.

Item name	Description
Inbound IF	Input interface
Source	Source address of multicast packets
Group	Group address of multicast packets
Outbound IFs	Output interface When output to multiple interfaces, they are separated by "".

[Applied model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.45 Display of logged-in user information

[Format]

show status

user

[Explanation]

Display information of a user logged-in to a router. The following items are displayed.

- User name
- Connection type
- Log-in date and time
- Idle time
- IP address of the connection partner

Also, the following symbols are displayed in front of the user name according to the state of the user.

Symbols	Status
Asterisk (*)	User information about yourself
Plus (+)	You are in administrator mode.
@ mark (@)	You logged in with RADIUS authentication.

Example

> show status user

(*: your own user information, +: administrator mode, @: authentication with RADIUS)

User name Connection type Login idle IP address

```

-----
user-local      serial      09/16 10:21    0:00:17
@user-radius2   remote     09/16 10:22    0:00:36
*+@user-radius1 telnet1    09/16 10:22    0:00:00      192.168.0.100

```

> show status user

(*: current user, +: administrator mode, @: authenticated via RADIUS)

usernameconnection login timeidleIP address

```

-----
user-local      serial      09/16 10:21    0:02:27
@user-radius2   remote     09/16 10:22    0:02:27
*+@user-radius1 telnet1    09/16 10:22    0:00:00      192.168.0.100

```

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.46Display of login history of logged-in users

[Format]

show status user

history [Explanation]

Up to 50 login histories of logged-in users are displayed. The following items are displayed.

- User name
- Connection type
- Logged-in date and time
- Idle time
- Connected IP address

Applicable model

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.47Display of packet buffer status

[Format]

show status packet-buffer [group]

[Setting value and initial value]

- group: Specify a group of packet buffers to display
 - [Setting value]

Setting value	Description
Group name (small, middle, large, jumbo, huge)	Display the status of specified groups
Omitted	Displaying the status of all groups

- [Initial value] -

[Description]

Displays the status of packet buffers. Items to be displayed are as follows:

- Name of the group
- Packet size that can be stored
- Management parameters
- Number of packet buffers currently allocated
- Number of packet buffers connected to the free list
- Number of packets allocated (*1)
- Number of times packet buffer allocation requests were received (*2)
- Number of times packet buffer allocation was successful (*2)
- Number of times packet buffer allocation failed (*2)
- Number of times packet buffers were released (*2)
- Number of times chunks were released (*1)
- Number of times unsuccessful attempts were made to allocate packets (*2)
- Number of times chunks were released (*2)

*1 Not displayed in the vRX series.

*2 Not displayed in the vRX Sakura cloud version.

[Notes]

The jumbo group can be used only in models that support the 1000BASE-T interface as a LAN interface and can send and receive jumbo packets.

Example

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

```
#show status packet-buffer large
large group: 2048 bytes length
Parameters:max-buffer=10000max-free=2812min-free=62
            buffers-in-chunk=625 initial-chunk=4
```

```
2372buffersinfree list
128buffersareallocated, req/succ/fail/rel=137/137/0/9
4chunksareallocated, req/succ/fail/rel=4/4/0/0
```

Other models

```
#showstatuspacket-bufferlarge
large group: 2048 bytes length
Parameters:max-buffer=40000
39491 buffers in free list
509buffersareallocated
allocation history:
failuresexcludingonLANinterface:0
```

[Applicable model]

[Model] vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.48 Display of QoS status

[Format]

show status qos info [interface [class]]

[Setting value and initial value]

- *info*: Type of information to display
 - [Setting value]:

Setting value	Description
bandwidth	Bandwidth used
length	Number of packets queued
dcc	Control status of Dynamic Class Control
all	All information

- [Initial value]: -
- *interface*
 - [Setting value]: Name of LAN interface (If omitted, it is displayed for all LAN interfaces)
 - [Initial value]: -
- *class*
 - [Setting value]: Class (RTX3510: 1..250; vRX Series, RTX5000, RTX3500: 1..100; other models: 1..16)
 - [Initial value]: -

[Explanation]

QoS setting information and usage status of each class are displayed for the interface.

- LAN interface name
- Queuing algorithm
- Interface speed
- Number of classes
- Setting band, usage band, peak value of usage band and recording date of each class
- Total setting band
- Number of successful/failed enqueues, number of dequeues, number of packets held, peak value and recording date of the number of packets for each class
- Host information and control details controlled by Dynamic Class Control

[Applicable model]

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.49 Status display of cooperative operation

[Format]

show status cooperation type [id]

[Setting value and initial value]

- *type*: Cooperative operation type
- [Setting value]:

Setting value	Description
bandwidth-measuring	Line bandwidth detection
load-watch	Load monitoring notification

- [Initial value]: -
- *id*
 - [Setting value]: Counter ID number (1-100)
 - [Initial value]: -

200

Information of cooperative operation is displayed.

In the case of line bandwidth detection, the following items are displayed.

- Counter information
- Status display
 - Number of times
 - Measurement time
 - Measurement result (client operation only)
 - Current status (client operation only)
 - Configuration change history (client operation only)
 - Time remaining until the next measurement (client operation only)

In the case of load monitoring notification, the following items are displayed.

- Counterparty information
- Status display
 - Number of suppression requests
 - Number of suppression cancellations
 - History

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.50 Displaying OSPFv3 information**[Format]**

show ipv6 ospf info

[Setting value and initial value]

- *info*
 - [Setting value]:

Setting value	Description
Database	Database for OSPFv3
neighbor	Neighborhood router
interface	Status of each interface
virtual-link	Status of virtual link

- [Initial value]: -

[Explanation]

Status of OSPFv3 is displayed.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.51 Displaying URL filter information

[Format]

```
show url filter
show url filter interface
show url filter pp [peer_num]
show url filter tunnel [tunnel_num]
```

[Setting value and initial value]

- *interface*
 - [Setting value]: LAN interface name, WAN interface name
 - [Initial value]: -
- *peer_num*
 - [Setting value]: Counterparty information number
 - [Initial value]: -
- *tunnel_num*
 - [Setting value]: Tunnel interface number
 - [Initial value]: -

[Explanation]

Statistics of which and how many times the URL filter applied to the interface was matched are displayed. If no interface is specified, all interface information is displayed.

The displayed contents are as follows.

- Filter number
- Starting IP address
- Number of times the HTTP connection and filter match.

[Notes]

If a filter with "*" in both keyword and IP address is applied to the interface in the url filter command, the number of times an HTTP connection matches this filter is not displayed.

WAN interface can be specified by firmware after Rev.14.01 series.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.52 Display of survival notification status

[Format]

```
show status
heartbeat
```

[Explanation]

Information of the received survival

notification is displayed. The displayed

contents are as follows.

- Notified name
- Notified IP address
- Time when the last survival notification was received
- Reception interval (seconds)

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.53 Displays the operation status of the USB host function.

[Format]

```
show status usbhost [modem]
```

[Explanation]

Displays the operation status of the USB host function.

When modem is specified, connection information about a device connected to a USB port is displayed. Displays the current communication status, total errors generated during communication, total number of bytes transmitted and received, number of incoming and outgoing calls, latest connection information, etc.

[Applicable model]

RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.54 **Display of connection information about the remote setup function**

[Format]

show status remote

setup [Explanation]

Displays connection information about the remote setup function.

Displays the current communication status, total errors generated during communication, total number of frames transmitted and received, number of incoming and outgoing calls, latest connection information, etc.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.55 **Display of technical information**

[Format]

show techinfo

[Explanation]

Information necessary for technical support is output all at once.

Unlike other show commands, the output of the show techinfo command is output all at once while ignoring the console columns/lines command settings. Page operations in which output stops for each screen are not performed. Therefore, it is desirable to save the output as a file of a PC using the log function of terminal software.

Also, the console character command settings are ignored and output always in English mode.

If you want to output while checking the contents for each screen, use the less command as follows. However, since the less command outputs many screen control sequences, it becomes difficult to understand a log file when using the less command while recording a log.

show techinfo |

less [Note]

Accessing a router from a TFTP client running on a PC and GETing the file name 'techinfo' yields the same output of the show techinfo command.

An example using Windows TFTP.EXE:

C:\>tftp 192.168.0.1 get techinfo techinfo.txt

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.56 **Displays the operating status of a microSD slot.**

[Format]

show status

sd

[Explanation]

Displays the operating status of a microSD slot.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.57 Displays the operating status of an external memory.

[Format]

show status external-

memory [Explanation]

Displays the status and common information of an external memory connected to a USB port and a microSD slot.

[Notes]

When a portable terminal is connected to a USB port, "External memory is not connected" is displayed for the USB port.

Check the status of the portable terminal with show status usbhost modem.

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.58 Displaying the status of an RTFS

[Format]

show status

rtfs [Explanation]

Displays the status of an RTFS area of an internal storage (internal flash ROM, etc.). The contents to be displayed are as follows.

- Capacity
- Free space
- Number of entries that can be created
- Number of directories
- Number of directories

An execution example is as follows.

```
#showstatusrtfs
AppearanceQuantity    Quantity:1572864Bye. Bye.
Free space
                        Quantity:156602
5Bye.Number of entries that can be
created995
FilesNumber           Number of directories2
```

[Applicable model]

RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.59 Display startup information

Format

show status boot [num]

Set value and initial value

- *num* : History number
- Set value:

Set value	Description
0..4	Display history of specified number
Omitted	0 if omitted

- Initial value: -

- Description

Display startup information

Specifying the history number displayed by the show status boot list command displays details of the history.

If num is omitted, the history with history number = 0 is displayed.

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.60 Display history details of startup information

Format

show status boot

all [Explanation]

Displays up to 5 history details of startup information.

This history is cleared when cold start command or clear boot list command is executed.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.61 Display history details of startup information

Format

show status boot

list [Explanation]

Displays up to 5 history details of startup information.

This history is cleared when cold start command or clear boot list command is executed.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.62 Display of agent list

Format

show status switch control [interface]

Set value and initial value

- *interface*
 - Set value: LAN interface name, bridge interface name, VLAN interface
 - Initial value: -

[Description]

Displays a list of agents. If interface is omitted, information about all interfaces is displayed.

The following information is displayed according to the operation status of L2MS.

- If you are acting as an L2MS manager
 - MAC address
 - Model name
 - Device name
 - Route from the manager
 - Uplink port
 - Route specified when operating the agent
 - Settings currently in use
 - Total of terminals connected to the agent and terminals lost (only when terminal management function is enabled)
 - Displayed with RTX830 Rev.15.02.32 or later and RTX1300 Rev.23.00.17 or later
- If you are acting as an L2MS agent
 - MAC address of the manager

[Notes]

Bridge interface can be specified with firmware of RTX1210 Rev.14.01.20 or later and all firmware of Rev.15.02 or later.

VLAN interface can be specified with RTX1210 Rev.14.01.42 or later, RTX830 Rev.15.02.30 or later, and RTX1220 Rev.15.04.07 or later.

[Example]

```
> show status switch control LAN1
[Display display display display]
Model name: SWX2200-24G
Device name: SWX2200-24G_0123456
Route: lan1:1
Uplink: 1
Route for setting: lan1:1
Setting: switch select lan1:1
---
LAN2
Switch control function is not enabled
---
LAN3
Switch control function is not enabled
---
BRIDGE1
Switch control function is not enabled
```

```
> show status switch control LAN1
[Display display display display]
Model name: SWX2200-24G

Uplink: 1
Route for Config: lan1:1
Config: switch select lan1:1
---
LAN2
Switch control function is not available.
---
LAN3
Switch control function is not available.
---
BRIDGE
1
Switch control function is not available.
```

```
> show status switch control LAN1
Manager: 00:a0:de:01:02:03
---
LAN2
Switch control function is not enabled
---
LAN3
Switch control function is not enabled
---
BRIDGE1
Switch control function is not enabled
```

```
> show status switch control LAN1
Manager: 00:a0:de:01:02:03
---
LAN2
Switch control function is not available.
---
LAN3
Switch control function is not available.
---
BRIDGE
1
Switch control function is not available.
```

[Applicable Models]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.63 The operation status of the LAN cable duplication function is displayed.

[Format]**show status switch control route backup route****[Setting value and initial value]**

- *route*
 - [Setting value]: Route
 - [Initial value]: -

[Explanation]

The operation status of the LAN cable duplication function is displayed.

Status	Description
None	The LAN cable duplication function is not working.
active	It operates as a communication possible route.
force-linkdown	The link is interrupted by the LAN cable duplication function.
blocking	The communication is interrupted by the LAN cable duplication function.

[Notes]

When the main route is linked up, the main route operates in active and can communicate. Also, the backup route operates in force-linkdown and does not link up even if a cable is connected.

When the main route is linked down, the backup route operates in active and can communicate. Also, the main route operates in blocking so that a loop does not occur when the link is interrupted.

If this function is not implemented in a switch, a command error occurs.

[Applicable model]

RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.64 Displaying the DNS cache

[Format]**show dns****cache****[Explanation]**

Displays the contents of the DNS cache.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.65 Display of license information

[Format]**show status license [vrX [all]]****[Explanation]**

Displays the license or extension license acquired by the LMS client (available for RTX3510, RTX1300, RTX830) and the license of vRX (available for vRX series).

The items to be displayed are as follows.

- Part number
 - Part number of the licensed product
 - Regarding the license of vRX, the basic license is displayed as "vRX-", and if there is an option license, the type of the license and function restrictions are also indicated. The official part number can be confirmed by adding the vrX option.

- Condition
 - License status
 - Regarding the license acquired by the LMS client, one of the following is displayed.
 - Active state
 - A state in which the license is within an expiration date and an application corresponding to the part number can be used.
 - Renewal grace period
 - A state in which the expiration date has passed. Since the corresponding application cannot be used after a certain period of time from this state, a license purchase procedure is required.
 - Authentication grace period
 - A state in which the license authentication is temporarily suspended. This state occurs when the Yamaha network device restarts while holding valid license information and cannot communicate with the LMS server thereafter. The corresponding application can be used, but it is necessary to perform license authentication before the deactivation time elapses. The time until deactivation can be confirmed by a show status license authentication command.
 - Regarding other licenses, it is always displayed as "Active".
- Expiration date
 - Expiration date of the license

[Notes]

Information is not displayed even if this command is executed when the license is not held or license information is not acquired from the LMS server.

RTX830 can be used with Rev.15.02.13 or later, and extended licenses can be displayed with Rev.15.02.22 or later.

[Applicable model]

vRX series, RTX3510, RTX1300, RTX840, RTX830

49.66 Display of license authentication status

[Format]

show status license

authentication [Explanation]

Displays the status of license authentication. Items to be displayed are as follows.

Last updated:	The date and time of the last successful license authentication. Shown in the format of "year/month/day hour:minute:second".
Counts to deactivation	Remaining periodic authentication count until the application is deactivated.
Time to periodic authentication	Time to next periodic authentication. Shown in the format of "hour:minute:second".
Time to deactivation	Time to deactivation Shown in the format of "hour:minute:second". Applications can be used during this time, but license authentication must be performed before the time passes.

[Notes]

RTX830 can be used with Rev.15.02.13 or later.

[Applicable model]

RTX3510, RTX1300, RTX840, RTX830

49.67 Display of the status of CPU scheduling (packet transfer) function

[Format]

show status packet-

scheduling [Explanation]

Displays the status of the current CPU scheduling (packet transfer) function.

- CPU scheduling method
 - CPU scheduling method during operation

Method name	Description
hash	Hash method
Load-balance method	Load-balance method
lan-based	LAN interface method
fixed	Fixed method

- CPU utilization
 - Total CPU core utilization per CPU core
- Flow (IPv4/IPv6)
 - Total IPv4/IPv6 flows
 - Number of received IPv4/IPv6 flows per CPU core
- Received packets
 - Number of received packets per CPU core

When the CPU scheduling method is load-balance method, the number of received IPv4/IPv6 flows per CPU core is not displayed. The number of received packets is cleared by executing the system packet-scheduling command.

[Notes]

Cannot be used with RTX5000 / RTX3500 Rev.14.00.12 or earlier.

Example of display

```
# show status packet-scheduling CPU
scheduling method: hash CPU utilization:
    CPU0:57%(5sec) 56%(1min) 56%(5min)
    CPU1:62%(5sec) 62%(1min) 62%(5min)
    CPU2:88%(5sec) 89%(1min) 88%(5min)
    CPU3: 54% (5sec) 54% (1min) 54% (5min)
Flow (IPv4/IPv6): 2 entries / 2 entries
    CPU0: 0 entry / 1 entry
    CPU1: 1 entry / 0 entry
    CPU2: 1 entry / 0 entry
    CPU3: 0 entry / 1 entry
Received packets
    CPU0:          23155524 Packet
    CPU1:          14018842 Packet
    CPU2:          23624407 Packet
    CPU3:          22886347 Packet
```

Model

vRX Series, RTX5000, RTX3510, RTX3500, RTX1300

49.68 Display of STATUS LED information

Format

show status status-led [history]

Setting value and initial value

- history: Displays the history of status change of the STATUS LED
 - [Initial value]: -

Description

Displays information of the STATUS LED.
If it is lit, a list of interfaces for which keepalives that caused the lighting are set is displayed.
History of status change is also displayed if the history option is specified.

Model

RTX3510, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.69 Displaying the status of a LAN map

Format

show lan-map interface [detail]

Setting value and initial value

- *interface*
 - Setting value: LAN interface name, bridge interface name, VLAN interface
 - [Initial value]: -
- detail: Displays details of terminal information in addition to information of agents managed by the LAN map
 - [Initial value]: -

23624407

Displays the status of the current LAN map.

- OUI information imported into the firmware (only if the detail option is specified)
- Manager information
 - Link up port
 - Terminal information directly under the manager
- Agent information
 - Model name
 - Device name
 - Route
 - Link up port
 - Up link port
 - Down link port
 - Agent status

Condition	Description
Idle	Normal status
Search	Search request is being executed

- Detection time
- Time spent completing the most recent search request
- Terminal information under the agent
- Missing agent information
 - Model name
 - Device name
 - Detection time
 - Disappearance time
 - Terminal information under the agent
- Terminal information details (only if the detail option is specified)
 - IP address
 - Detection time
 - Time of disappearance
 - Types
 - Manufacturer's name
 - Model name
 - Device name
 - OS
 - Comments
 - Whether or not to be warned by the snapshot function

[Notes]

This command can be used when manager is set in mode by a switch control mode command.

The bridge interface can be specified with RTX1210 Rev.14.01.20 or later firmware, and all Rev.15.02 or later firmware.

The VLAN interface can be specified with RTX1210 Rev.14.01.42 or later, RTX830 Rev.15.02.30 or later, and RTX1220 Rev.15.04.07 or later.

Display example

```
# show lan-map lan1 detail [OUI]  
Generated: Sat, 04 Mar 2017 04:31:14 -0400
```

[Manager]

Link-up: lan1:1

Terminals: 0

[Agent] [00:a0:de:2a:dc:02]

Model name: SWX2200-24G

Device name: SWX1

Route: lan1:1

Link-up: 1 11

Uplink: 1

Downlink: None

Status: Idle

Detection time: 2017/05/24 11:28:59

検索時間: 1 sec (867 msec)

Terminals: 0

[Port 1]

[Port 2]

[Port 3]

[Port 4]

[Port 13]

[Port 6]

[Port 13]

[Port 8]

[Port 13]

[Port 10]

[Port 11]

[12:34:56:78:90:ab]

IP address: 192.168.0.10

検出時刻: 2017/05/24 11:29:04

Type: Desktop PC

Manufacturer: Maker1

Model name: Model1

Device name: Host1

OS: OS1

Comment: comment1

Snapshot: on [Port 12]

[Port 13]

[Port 14]

[Port 20]

[Port 16]

[Port 17]

[Port 18]

[Port 19]

[Port 20]

[Port 24]

[Port 22]

[Port 23]

[Port 24]

[Disappearing Agent]

[00:a0:de:7e:53:82]

Model name: SWX2200-24G

Device name: SWX2

Detection time: 2017/05/24 11:29:32

Time of disappea	Number of terminals:2017/05/241

Applicable model

RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.70 Show copyright information for third-party software

Format

show copyright [detail]
show copyright detail [software]
show copyright [detail [license [version]]]

Set value and initial value

- *software*
 - Set value:
 - Software name to be displayed
 - [Initial value]: -
- *license*
 - Set value: License name to display license terms
 - [Initial value]: -
- *version*
 - Set value: License version number
 - [Initial value]: -

Description

Display copyright information for installed third-party software.

When the detail option is specified, license terms are also displayed.

To display copyright information and license terms for some software in the vRX series, it is necessary to specify a software parameter. The target software name is displayed when show copyright detail is executed.

Notebook

Use show copyright common-license to display general license terms applicable to third-party software in the vRX series. However, only for vRX Amazon EC2 version Rev.19.00.01, check with the third format of this command.

The first format is not available for vRX Amazon EC2 Cloud version.

The second format is not available for RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, and RTX830.

The third format is not available for vRX Amazon EC2 version Rev.19.00.01.

It is not available for RTX5000 / RTX3500 Rev.14.00.20 or earlier and RTX1210 Rev.14.01.10 or earlier.

Applicable Models

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

49.71 Displaying SFP Module Information

[Format]

show sfp-module info [interface]
show sfp-module info detail [interface]
show sfp-module info [port]
show sfp-module info detail [port]

[Setting Value and Initial Value]

- *detail*
 - [Setting Value]: Displays DDM information
 - [Initial Value]: -
- *interface*
 - [Setting Value]: LAN Interface
 - [Initial Value]: -

- *port*
 - [Setting Value]: Port Number
 - [Initial Value]: -

[Explanation]

Displays information on an SFP module connected to an SFP port.

When a LAN interface or a port number is not specified, information on an SFP module connected to all SFP ports is displayed.

When detail is specified, DDM information which is diagnostic information of the SFP module is displayed.

[Notebook]

Formats 3 and 4 are valid only for models that support flexible LAN/WAN ports.

Applicable Models

RTX3510, RTX1300

49.72 Display of the status of the domestic standard provisioning system for IPv6 migration technology

Format

show status hb46pp [tunnel tunnel_num]

Set value and initial value

- *tunnel_num*
 - Set value: Tunnel interface number
 - Initial value: -

Description

Displays the status of the domestic standard provisioning system for IPv6 migration technology.

Notes

RTX3510 can be used with Rev. 23.01.02 or later. RTX8300 can be used with Rev. 15.02.31 or later. RTX830 can be used with Rev. 15.02.31 or later. RTX830 can be used with Rev. 15.02.31 or later.

Applicable Models

RTX3510, RTX1300, RTX1220, RTX840, RTX830

CHAPTER 50

Logging

50.1 Log display

[Format]

```
show log [saved] [reverse]
show log external-memory [backup [fileid]]
show log file [backup [fileid]]
less log [saved] [reverse]
```

[Setting value and initial value]

- saved
 - [Setting value]: Displays the log immediately before a reboot
 - [Initial value]: -
- reverse
 - [Setting value]: Displays the log in reverse order
 - [Initial value]: -
- external-memory
 - [Setting value]: Displays the contents of a SYSLOG file set by the external-memory syslog filename command
 - [Initial value]: -
- file
 - [Setting value]: Displays the contents of a SYSLOG file in the /yamaha_sys directory
 - [Initial value]: -
- backup
 - [Setting value]: Displays the contents of a SYSLOG backup file or displays a list of SYSLOG backup files
 - [Initial value]: -
- *fileid: Displays the contents of a specified SYSLOG backup file*
 - [Setting value]: yyyyymmdd_hhmmss
 - [Initial value]: -

[Explanation]

Logs recording the operating conditions of routers are displayed.

The maximum number of logs retained is shown in the table below.

Model	Revisions	Number of cases
vRX series	All revisions	20000
RTX5000	All revisions	20000
RTX3510	All revisions	20000
RTX3500	All revisions	20000
RTX1300	All revisions	10000
RTX1220	All revisions	10000
RTX1210	All revisions	10000
RTX830	All revisions	10000
RTX830	All revisions	10000

When the maximum number is exceeded, the logs with the oldest occurrence time are deleted. To save more than the maximum number of logs, you need to transfer the logs to a SYSLOG server using the syslog host command and save them there.

When an unintended reboot occurs, you can display the logs immediately before a reboot by specifying 'saved'.

In this command, logs are usually displayed in order from the oldest occurrence time. 'reverse' is new by specifying it can be displayed.

For models that do not support the power-off log saving function, the log is erased when the router is turned off.

When external-memory is specified, a SYSLOG file in the external memory is displayed. When file is specified, a SYSLOG file in the /yamaha_sys directory is displayed.

When external-memory backup or file backup is specified, a list of backup files is displayed starting from the oldest one. To display the contents of a backup file, date and time data (15 digits of a character string represented by yyyymmdd_hhmmss format) of the displayed file name can be specified as fileid.

[Notes]

Even if the router is restarted while the power is turned on due to firmware upgrade by restart command or TFTP, the log is saved as long as the power is not turned off.

When external-memory is specified, the following restrictions apply.

- Encrypted log files in the external memory cannot be displayed.
- Cannot specify redirects

When file is specified, the following restrictions apply.

- Encrypted SYSLOG files in the /yamaha_sys directory cannot be displayed.

When external-memory is specified and the external-memory syslog filename command is not set, an execution error occurs.

Format 2 cannot be used with vRX series, and format 3 can be used with vRX series.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

50.2 Viewing accounts

Format

show account

show account interface

Setting value and initial value

- *interface*
 - Setting value:
 - BRI interface name
 - PRI interface name
 - Initial value: -

Explanation

Display of the following items

- Number of calls
- Number of calls
- Total ISDN charges

[Notes]

Charging information up to that point is cleared by turning off or restarting the power.

Charges are calculated by aggregating charge information notified from NTT by ISDN at the time of disconnection of communication, so that when using discount services, etc., the final charge may differ from the charge charged from NTT. In addition, since charge information is not notified when communication is performed using a communication carrier other than NTT, it is not counted as an account.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

50.3 Viewing PP accounts

Format

show account pp [peer_num]

Setting value and initial value

- *peer_num*
 - Setting value:
 - Counterparty information number
 - anonymous
 - Display of selected counterparty when omitted
 - Initial value: -

Explanation

Display accounts related to the specified PP interface.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

50.4 Viewing a TUNNEL account

Format

show account tunnel [tunnel_num]

Setting value and initial value

- *tunnel_num*
 - Setting value:
 - Counterparty information number
 - Display of selected counterparty when omitted
 - Initial value: -

Preface

Displays the number of incoming/outgoing calls and charge information for tunnel interfaces for which specified data connect connection settings are set. The number of outgoing calls and the number of incoming calls are counted at the time of disconnection. Charge information is cleared by restarting. The calculation of whether or not a threshold value set by the account threshold command is exceeded does not include a charge for data connect.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210

50.5 Viewing Data Connect accounts

[Format]

show account ngn

data [説明]

Display incoming/outgoing calls and billing information of data connect.

[Notes]

Since billing information is calculated from connection time and a set bandwidth, it may differ from the final charge.

[Applicable model]

vRX VMware ESXi version, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

50.6 Displaying the command history

[Format]

show command history [num]

[Setting value and initial value]

- *num*
 - [Setting value]: History number (1..21474836)

[Initial value]:

[Description]

Display the command history.

When num is specified, a command of a specified number to the immediately preceding command is displayed. When num is omitted, up to 20 commands are displayed retroactively from the newest command.

[Notes]

RTX5000 and RTX3500 can be used in Rev.14.01.26 or later.

RTX1210 can be used in Rev.14.01.26 or later.

RTX830 can be used in Rev.15.02.03 or later.

[Applicable model]

vRX series, RTX5000, RTX3510, RTX3500, RTX1300, RTX1220, RTX1210, RTX840, RTX830

Index

Symbols

>41
>> 41

A

administrator 565
 administrator password 44
 administrator password encrypted 44
 administrator radius auth 45
 alarm batch 98
 alarm entire 96
 alarm http revision-up 98
 alarm http upload 476
 alarm lua 484
 alarm sd 97
 alarm startup 98
 alarm usbhost 97
 alias 99
 ap config directory 537
 ap config filename 538
 ap control config delete
 539 ap control config get
 538 ap control config set
 539
 ap control config-auto-set use 540
 ap control firmware update go 540
 ap control http proxy timeout 541
 ap control http proxy use 540
 ap select 537
 auth user 250
 auth user attribute 250
 auth user group 251
 auth user group attribute 252

B

bgp aggregate 368
 bgp aggregate filter 368
 bgp autonomous-system 369
 bgp configure refresh 373
 bgp default med 378
 bgp export 371
 bgp export aspath 371
 bgp export filter 372
 bgp export route selection rule 378
 bgp force-to-advertise 376
 bgp import 373
 bgp import filter 374
 bgp log 376
 bgp neighbor 375
 bgp neighbor pre-shared-key 376
 bgp preference 370
 bgp reric interval
 377 bgp router id
 370 bgp use 368
 bridge learning 478
 bridge learning bridge_interface static 479
 bridge learning bridge_interface timer 479
 bridge member 477

C

call 594
 clear account 571
 clear account ngn data 572
 clear account pp 571

clear account tunnel 572
 clear arp 572
 clear boot list 577
 clear bridge learning 573
 clear diagnosis config port 553
 clear dns cache 573
 clear external-memory syslog 577
 clear heartbeat2 457
 clear heartbeat2 id 457
 clear heartbeat2 name 457
 clear ip connection peak 572
 clear ip dynamic routing 572
 clear ipv6 connection peak 576
 clear ipv6 dynamic routing 576
 clear ipv6 neighbor cache 576
 clear lbo traffic list 563
 clear log 573
 clear nat descriptor dynamic 574
 clear nat descriptor interface dynamic 574
 clear nat descriptor interface dynamic pp 574
 clear nat descriptor interface dynamic tunnel 574
 clear nat descriptor masquerade session peak 575
 clear nat descriptor masquerade session statistics 575
 clear pppoe pass-through learning 576
 clear status 573
 clear switching-hub macaddress 588
 clear url filter 590
 clear url filter pp 590
 clear url filter tunnel 590
 cold start 570
 confirm 593
 connect 581
 connect pp 581
 connect tunnel 581
 console character 54
 console columns 54
 console info 55
 console lines 55
 console prompt 54
 copy 578
 copy config 566
 copy exec 568

D

date 51
 delete 577
 delete config 569
 delete exec 569
 description 75
 description yno 543
 dhcp client client-identifier 203
 dhcp client client-identifier pool 203
 dhcp client client-identifier pp 203
 dhcp client hostname 201
 dhcp client hostname pool 201
 dhcp client hostname pp 201
 dhcp client option 204
 dhcp client option pool 204
 dhcp client option pp 204
 dhcp client release linkdown 205
 dhcp convert lease to bind 196
 dhcp duplicate check 191
 dhcp manual lease 198
 dhcp manual release 198
 dhcp relay select 199
 dhcp relay server 199
 dhcp relay srcport 199

- dhcp relay threshold 200
- dhcp scope 192
- dhcp scope bind 193 dhcp
- scope lease type 195 dhcp
- scope option 197
- dhcp server rfc2131 compliant 190
- dhcp service 189
- diagnose config port access 552
- diagnose config port map 551
- diagnosis config port history-num 553
- diagnosis config port max-detect 552
- disconnect 582
- disconnect ip connection 586
- disconnect ipv6 connection 588
- disconnect pp 582
- disconnect tunnel 582
- disconnect user 49
- dns cache max entry 335
- dns cache use 334
- dns domain 325
- dns host 333
- dns notice order 327
- dns private address spoof 328
- dns server 324
- dns server dhcp 326
- dns server pp 326
- dns server select 329
- dns service 324
- dns service aaaa filter 329
- dns service fallback 335
- dns srcport 333
- dns static 332
- dns syslog resolv 329

E

- echo 594
- embedded file 101
- ethernet filter 162
- ethernet interface filter 164
- execute batch 470
- exit 565
- external-memory accelerator cache size 461
- external-memory auto-search time 469
- external-memory batch filename 470
- external-memory boot permit 466
- external-memory boot timeout 467
- external-memory cache mode 461
- external-memory config filename 468
- external-memory exec filename 467
- external-memory performance-test go 471
- external-memory statistics filename prefix 462
- external-memory syslog filename 464

G

- Grep 39

H

- heartbeat pre-shared-key 450
- heartbeat receive 450
- heartbeat send 451
- heartbeat2 myname 452
- heartbeat2 receive 454
- heartbeat2 receive enable 455
- heartbeat2 receive log 456
- heartbeat2 receive monitor 455
- heartbeat2 receive record limit 456
- heartbeat2 transmit 452
- heartbeat2 transmit enable 453

- heartbeat2 transmit interval 453
- heartbeat2 transmit log 454
- help 43
- http revision-down permit 80
- http revision-up go 589
- http revision-up permit 79
- http revision-up proxy 79
- http revision-up schedule 81
- http revision-up timeout 80
- http revision-up url 79
- http upload 473
- http upload go 476
- http upload permit 474
- http upload proxy 475
- http upload retry interval 475
- http upload timeout 475
- http upload url 474
- httpd custom-gui api password 486
- httpd custom-gui api use 486
- httpd custom-gui use 485
- httpd custom-gui user 485
- httpd host 427
- httpd listen 428
- httpd service 427
- httpd timeout 428

I

- import sshd authorized-keys 89
- interface reset 580
- ip arp timer 129
- ip dscp supersede 134
- ip filter 112
- ip filter directed-broadcast 117
- ip filter dynamic 118
- ip filter dynamic timer 119
- ip filter fqdn timer 120
- ip filter set 116
- ip filter source-route 117
- ip flow limit 133
- ip flow timer 132
- ip forward filter 158
- ip fragment remove df-bit 127
- ip host 332
- ip icmp echo-reply send 206
- ip icmp echo-reply send-only-linkup 206
- ip icmp error-decrypted-ipsec send 210
- ip icmp log 210
- ip icmp mask-reply send 206
- ip icmp parameter-problem send 207
- ip icmp redirect receive 208
- ip icmp redirect send 207
- ip icmp time-exceeded send 208
- ip icmp timestamp-reply send 209
- ip icmp unreachable send 209
- ip icmp unreachable-for-truncated send 211
- ip implicit-route preference 131
- ip interface address 105
- ip interface arp log 131
- ip interface arp mtu discovery 211
- ip interface arp queue length 130
- ip interface arp static 130
- ip interface dhcp auto default-route-add 111
- ip interface dhcp auto interface-route-add 112
- ip interface dhcp lease time 202
- ip interface dhcp retry 202
- ip interface dhcp service 200
- ip interface forward filter 159
- ip interface intrusion detection 121
- ip interface intrusion detection notice-interval 122
- ip interface intrusion detection repeat-control 123
- ip interface intrusion detection report 123

- ip interface mtu 107
- ip interface nat descriptor 313
- ip interface ospf area 362
- ip interface ospf neighbor 365
- ip interface proxyarp 128
- ip interface proxyarp vrrp 128
- ip interface rebound 108
- ip interface rip auth key 144
- ip interface rip auth key text 144
- ip interface rip auth type 143
- ip interface rip filter 142
- ip interface rip force-to-advertise 148
- ip interface rip hop 143
- ip interface rip receive 141
- ip interface rip send 141
- ip interface rip trust gateway 139
- ip interface secondary address 107
- ip interface secure filter 126
- ip interface secure filter name 126
- ip interface tcp mss limit 123
- ip interface tcp window-scale 124
- ip interface vrrp 150
- ip interface vrrp shutdown trigger 151
- ip interface wol relay 75
- ip keepalive 156
- ip local forward filter 159
- ip pp address 105
- ip pp forward filter 159
- ip pp intrusion detection 121
- ip pp intrusion detection notice-interval 122
- ip pp intrusion detection repeat-control 123
- ip pp intrusion detection report 123
- ip pp mtu 107
- ip pp nat descriptor 313
- ip pp ospf area 362
- ip pp ospf neighbor 365
- ip pp rebound 108
- ip pp remote address 135
- ip pp remote address pool 136
- ip pp rip auth key 144
- ip pp rip auth key text 144
- ip pp rip auth type 143
- ip pp rip backup interface 147
- ip pp rip connect interval 146
- ip pp rip connect send 145
- ip pp rip disconnect interval 147
- ip pp rip disconnect send 146
- ip pp rip filter 142
- ip pp rip force-to-advertise 148
- ip pp rip hold routing 145
- ip pp rip hop 143
- ip pp rip receive 141
- ip pp rip send 141
- ip pp rip trust gateway 139
- ip pp secure filter 126
- ip pp secure filter name 126
- ip pp tcp mss limit 123
- ip pp tcp window-scale 124
- ip reassembly hold-time 133
- ip route 109
- ip route change log 125
- ip routing 105
- ip routing process 64
- ip simple-service 108
- ip stealth 210
- ip tos supersede 128
- ip tunnel address 220
- ip tunnel forward filter 159
- ip tunnel intrusion detection 121
- ip tunnel intrusion detection notice-interval 122
- ip tunnel intrusion detection repeat-control 123
- ip tunnel intrusion detection report 123
- ip tunnel mtu 107
- ip tunnel nat descriptor 313
- ip tunnel ospf area 362
- ip tunnel ospf neighbor 365
- ip tunnel rebound 108
- ip tunnel remote address 221
- ip tunnel rip auth key 144
- ip tunnel rip auth key text 144
- ip tunnel rip auth type 143
- ip tunnel rip filter 142
- ip tunnel rip force-to-advertise 148
- ip tunnel rip hop 143
- ip tunnel rip receive 141
- ip tunnel rip send 141
- ip tunnel rip trust gateway 139
- ip tunnel secure filter 126
- ip tunnel secure filter name 126
- ip tunnel tcp mss limit 123
- ip tunnel tcp window-scale 124
- ipip keepalive log 283
- ipip keepalive use 282
- ipsec auto refresh 234
- ipsec ike always-on 235
- ipsec ike auth method 230
- ipsec ike auto received-id-route-add 231
- ipsec ike backward-compatibility 248
- ipsec ike child-exchange type 259
- ipsec ike duration 261
- ipsec ike eap myname 232
- ipsec ike eap request 233
- ipsec ike eap send certreq 234
- ipsec ike encryption 243
- ipsec ike esp-encapsulation 257
- ipsec ike group 245
- ipsec ike hash 246
- ipsec ike keepalive log 243
- ipsec ike keepalive use 241
- ipsec ike license-key 255
- ipsec ike license-key use 256
- ipsec ike local address 240
- ipsec ike local id 240
- ipsec ike local name 239
- ipsec ike log 257
- ipsec ike message-id-control 259
- ipsec ike mode-cfg address 255
- ipsec ike mode-cfg address pool 253
- ipsec ike mode-cfg method 254
- ipsec ike nat-traversal 266
- ipsec ike negotiate-strictly 235
- ipsec ike negotiation receive 260
- ipsec ike payload type 247
- ipsec ike pfs 249
- ipsec ike pki file 232
- ipsec ike pre-shared-key 231
- ipsec ike proposal-limitation 258
- ipsec ike queue length 244
- ipsec ike remote address 237
- ipsec ike remote id 238
- ipsec ike remote name 236
- ipsec ike restrict-dangling-sa 265
- ipsec ike retry 236
- ipsec ike send info 248
- ipsec ike version 229
- ipsec ike xauth myname 249
- ipsec ike xauth request 253
- ipsec ipcomp type 269
- ipsec log illegal-spi 246
- ipsec refresh sa 264
- ipsec sa delete 267
- ipsec sa policy 263
- ipsec transport 272
- ipsec transport template 273

- ipsec tunnel 268
- ipsec tunnel fastpath-fragment-function follow df-bit 267
- ipsec tunnel outer df-bit 268
- ipsec use 229
- ipv6 dhcp prefix 386
- ipv6 dscp supersede 384
- ipv6 filter 409
- ipv6 filter dynamic 412
- ipv6 icmp echo-reply send 212
- ipv6 icmp echo-reply send-only-linkup 212
- ipv6 icmp error-decrypted-ipsec send 216
- ipv6 icmp log 215
- ipv6 icmp packet-too-big send 215
- ipv6 icmp packet-too-big-for-truncated send 217
- ipv6 icmp parameter-problem send 213
- ipv6 icmp redirect receive 214
- ipv6 icmp redirect send 213
- ipv6 icmp time-exceeded send 214
- ipv6 icmp unreachable send 214
- ipv6 interface address 386
- ipv6 interface dad retry count 391
- ipv6 interface dhcp service 390
- ipv6 interface icmp-nd queue length 383
- ipv6 interface mld 414
- ipv6 interface mld static 415
- ipv6 interface mtu 380
- ipv6 interface neighbor cache max entry 383
- ipv6 interface ospf area 419
- ipv6 interface prefix 388
- ipv6 interface prefix change log 389
- ipv6 interface rip filter 403
- ipv6 interface rip hop 402
- ipv6 interface rip receive 402
- ipv6 interface rip send 401
- ipv6 interface rip trust gateway 403
- ipv6 interface rtadv send 395
- ipv6 interface rtsol max-retransmit 397
- ipv6 interface secure filter 411
- ipv6 interface tcp mss limit 381
- ipv6 interface tcp window-scale 381
- ipv6 interface vrrp 406
- ipv6 interface vrrp shutdown trigger 407
- ipv6 max auto address 391
- ipv6 nd ns-trigger-dad 416
- ipv6 nd ra-dnssl 397
- ipv6 nd ra-rdnss 394
- ipv6 nd ra-route-info 398
- ipv6 ospf area 418
- ipv6 ospf area network 418
- ipv6 ospf configure refresh 417
- ipv6 ospf export 423
- ipv6 ospf export from ospf 422
- ipv6 ospf import 425
- ipv6 ospf import from 424
- ipv6 ospf log 426
- ipv6 ospf preference 422
- ipv6 ospf router id 417
- ipv6 ospf use 417
- ipv6 ospf virtual-link 421
- ipv6 pp address 386
- ipv6 pp dad retry count 391
- ipv6 pp dhcp service 390
- ipv6 pp mld 414
- ipv6 pp mld static 415
- ipv6 pp mtu 380
- ipv6 pp ospf area 419
- ipv6 pp prefix 388
- ipv6 pp prefix change log 389
- ipv6 pp rip connect interval 404
- ipv6 pp rip connect send 404
- ipv6 pp rip disconnect interval 405
- ipv6 pp rip disconnect send 405

- ipv6 pp rip filter 403
- ipv6 pp rip hold routing 405
- ipv6 pp rip hop 402
- ipv6 pp rip receive 402
- ipv6 pp rip send 401
- ipv6 pp rip trust gateway 403
- ipv6 pp rtadv send 395
- ipv6 pp rtsol max-retransmit 397
- ipv6 pp secure filter 411
- ipv6 pp tcp mss limit 381
- ipv6 pp tcp window-scale 381
- ipv6 prefix 392
- ipv6 reassembly hold-time 384
- ipv6 rh0 discard 382
- ipv6 rip preference 406
- ipv6 rip use 401
- ipv6 route 399
- ipv6 route change log 401
- ipv6 routing 380
- ipv6 routing process 382
- ipv6 source address selection rule 392
- ipv6 stealth 216
- ipv6 tunnel address 386
- ipv6 tunnel dhcp service 390
- ipv6 tunnel mld 414
- ipv6 tunnel mld static 415
- ipv6 tunnel mtu 380
- ipv6 tunnel ospf area 419
- ipv6 tunnel prefix 388
- ipv6 tunnel prefix change log 389
- ipv6 tunnel rip filter 403
- ipv6 tunnel rip receive 402
- ipv6 tunnel rip send 401
- ipv6 tunnel secure filter 411
- ipv6 tunnel tcp mss limit 381
- ipv6 tunnel tcp window-scale 381

L

- l2tp always-on 279
- l2tp hostname 280
- l2tp keepalive log 278
- l2tp keepalive use 278
- l2tp local router-id 280
- l2tp remote end-id 281
- l2tp remote router-id 281
- l2tp service 276
- l2tp syslog 279
- l2tp tunnel auth 277
- l2tp tunnel disconnect time 277
- lan backup 154
- lan backup recovery time 154
- lan flexible-port 555
- lan keepalive interval 155
- lan keepalive log 156
- lan keepalive use 155
- lan link-aggregation static 72
- lan linkup send-wait-time 65
- lan pass-through ethertype 160
- lan pass-through member 161
- lan port shutdown 559
- lan port type 556
- lan port-mirroring 65
- lan receive-buffer-size 73
- lan type 66
- lan-map log 491
- lan-map snapshot use 490
- lan-map sysname 492
- lan-map terminal watch interval 489
- lbo list get go 561
- lbo list primary 560
- lbo list secondary 561

- lbo use 560
- less 41
- less config 595
- less config ap 596
- less config list 598
- less config pp 596
- less config switch 596
- less config tunnel 597
- less exec list 601
- less file list 598
- less log 637
- license authentication go 591
- license authentication retry interval 591
- load 592
- login radius use 45
- login timer 73
- login user 44
- lua 481
- lua use 481
- lua c 482

M

- macro 100
- mail notify status exec 590
- make directory 577

N

- nat descriptor address inner 315
- nat descriptor address outer 314
- nat descriptor backward-compatibility 312
- nat descriptor ftp port 320
- nat descriptor log 321
- nat descriptor masquerade incoming 318
- nat descriptor masquerade port range 319
- nat descriptor masquerade remove df-bit 322
- nat descriptor masquerade rlogin 316
- nat descriptor masquerade session limit 321
- nat descriptor masquerade session limit total 322, n.e.c., n.e.c., n.e.c., n.e.c., n.e.c.
- nat descriptor masquerade unconvertible port 320
- nat descriptor sip 321
- nat descriptor static 315
- nat descriptor timer 318
- nat descriptor type 313
- nat46 ip address pool 337
- nat46 ipv6 prefix 337
- nat46 static 338
- netvolante-dns auto hostname 433
- netvolante-dns auto hostname pp 433
- netvolante-dns auto save 437
- netvolante-dns delete go 431
- netvolante-dns delete go pp 431
- netvolante-dns get hostname list 432
- netvolante-dns get hostname list pp 432
- netvolante-dns go 430
- netvolante-dns go pp 430
- netvolante-dns hostname host 432
- netvolante-dns hostname host pp 432
- netvolante-dns port 431
- netvolante-dns register timer 437
- netvolante-dns retry interval 436
- netvolante-dns retry interval pp 436
- netvolante-dns server 435
- netvolante-dns server update address port 436
- netvolante-dns server update address use 435
- netvolante-dns set hostname 434
- netvolante-dns timeout 433
- netvolante-dns timeout pp 433
- netvolante-dns use 430
- netvolante-dns use pp 430

- nslookup 585
- ntp backward-compatibility 53
- ntp local address 53
- ntpdate 52

O

- operation button function download 471
- operation execute batch permit 472
- operation external-memory download permit 466
- operation http revision-up permit 81
- OSPF area 359
- ospf area network 359
- ospf area stubhost 360
- ospf configure refresh 353
- ospf export filter 356
- ospf export from ospf 354
- ospf import filter 357
- ospf import from 355
- ospf log 366
- ospf merge equal cost stub 365
- ospf preference 353
- OSPF reric interval 366
- OSPF router id 354
- OSPF use 353
- OSPF virtual-link 360

P

- packetdump 60
- packetdump pp 60
- ping 583
- ping6 583
- pki certificate file 274
- pki crt file 274
- pp auth accept 171
- pp auth multi connect prohibit 172
- pp auth myname 172
- pp auth request 171
- pp auth username 170
- pp backup 152
- pp backup pp 152
- pp backup recovery time 153
- pp backup tunnel 152
- pp disable 579
- pp enable 579
- pp keepalive interval 137
- pp keepalive log 139
- pp keepalive use 138
- pp name 429
- pp select 564
- ppp ccp maxconfigure 182
- ppp ccp maxfailure 183
- ppp ccp maxterminate 182
- ppp ccp restart 182
- ppp ccp type 181
- ppp chap maxchallenge 177
- ppp chap restart 177
- ppp ipcp ipaddress 178
- ppp ipcp maxconfigure 179
- ppp ipcp maxfailure 179
- ppp ipcp maxterminate 178
- ppp ipcp msex 180
- ppp ipcp remote address check 180
- ppp ipcp restart 178
- ppp ipcp vjc 177
- ppp ipv6cp use 183
- ppp lcp acfc 173
- ppp lcp magicnumber 173
- ppp lcp maxconfigure 175
- ppp lcp maxfailure 175
- ppp lcp maxterminate 175

- ppp lcp mru 174
- ppp lcp pfc 174
- ppp lcp restart 175
- ppp lcp silent 176
- ppp mp interleave 345
- ppp msccbp maxretry 181
- ppp msccbp restart 180
- ppp pap maxauthreq 176
- ppp pap restart 176
- pppoe access concentrator 184
- pppoe auto connect 184
- pppoe auto disconnect 184
- pppoe disconnect time 186
- pppoe invalid-session forced close 187
- pppoe padi maxretry 185
- pppoe padi restart 185
- pppoe padr maxretry 185
- pppoe padr restart 185
- pppoe pass-through member 187
- pppoe service-name 186
- pppoe tcp mss limit 186
- pppoe use 183

Q

- queue class filter 341
- queue interface class control 350
- queue interface class filter list 346
- queue interface class property 348
- queue interface default class 348
- queue interface length 347
- queue interface type 344
- queue pp class filter list 346
- queue pp class property 348
- queue pp default class 348
- queue pp length 347
- queue pp type 344
- queue tunnel class filter list 346
- queue tunnel default class 348
- quit 565

R

- radius account 308
- radius account port 310
- radius account server 309
- radius auth 308
- radius auth port 310
- radius auth server 309
- radius retry 311
- radius secret 311
- radius server 309
- rdate 52
- remote setup accept 570
- rename 578
- restart 580
- rip advertise mode 144
- rip filter rule 148
- rip preference 140
- rip timer 149
- rip use 139
- rollback timer 593
- rotate external-memory syslog 590
- rtfs format 104
- rtfs garbage-collect 104

S

- save 565
- schedule at 443
- scp 92

- sd use 460
- security class 50
- set 99
- set-default-config 569
- set-default-exec 570
- set-serial-baudrate 570
- sftpd host 91
- show account 638
- show account ngn data 639
- show account pp 639
- show account tunnel 639
- show alias 601
- show arp 603
- show bridge learning 606
- show command 43
- show command history 639
- show config 595
- show config ap 596
- show config difference 597
- show config list 598
- show config pp 596
- show config switch 596
- show config tunnel 597
- show copyright 635
- show diagnosis config port access 553
- show diagnosis config port map 553
- show dns cache 630
- show environment 595
- show exec list 601
- show file list 598
- show ip connection 614
- show ip connection peak 615
- show ip connection pp 614
- show ip connection tunnel 614
- show ip intrusion detection 617
- show ip intrusion detection pp 617
- show ip intrusion detection tunnel 617
- show ip rip table 605
- show ip route 604
- show ip secure filter 600
- show ip secure filter pp 600
- show ip secure filter tunnel 600
- show ipsec sa 606
- show ipsec sa gateway 606
- show ipv6 address 599
- show ipv6 address pp 599
- show ipv6 address tunnel 599
- show ipv6 connection 616
- show ipv6 connection peak 616
- show ipv6 connection pp 616
- show ipv6 connection tunnel 616
- show ipv6 mroute fib 621
- show ipv6 neighbor cache 606
- show ipv6 ospf 624
- show ipv6 rip table 605
- show ipv6 route 605
- show ipv6 secure filter 600
- show ipv6 secure filter pp 600
- show ipv6 secure filter tunnel 600
- show lan flexible-port 556
- show lan-map 633
- show lbo traffic list 562
- show log 637
- show macro 602
- show nat descriptor address 608
- show nat descriptor interface address 609
- show nat descriptor interface address pp 609
- show nat descriptor interface address tunnel 609
- show nat descriptor interface bind 609
- show nat descriptor interface bind pp 609
- show nat descriptor interface bind tunnel 609
- show nat descriptor masquerade port summary 610

show nat descriptor masquerade session peak 611
 show nat descriptor masquerade session statistics 611
 show nat descriptor masquerade session summary 610
 show pki certificate summary 607
 show pki crl 607
 show pppoe pass-through learning 618
 show set 601
 show sfp-module info 635
 show sshd authorized-keys 89
 show sshd host key 85
 show sshd public key 599
 show status 603
 show status backup 614
 show status bgp neighbor 613
 show status boot 627
 show status boot all 628
 show status boot list 628
 show status cooperation 623
 show status dhcp 613
 show status dhcpc 614
 show status ethernet filter 165
 show status external-memory 627
 show status hb46pp 636
 show status heartbeat 625
 show status heartbeat2 456
 show status heartbeat2 id 456
 show status heartbeat2 name 456
 show status ip keepalive 617
 show status ipip 612
 show status ipv6 dhcp 614
 show status ipv6 mld 620
 show status l2tp 611
 show status lbo 561
 show status license 630
 show status license authentication 631
 show status lua 482
 show status mail service 620
 show status nat46 table 338
 show status netvolante-dns 618
 show status netvolante-dns pp 618
 show status ospf 612
 show status packet-buffer 622
 show status packet-scheduling 631
 show status pp 603
 show status pptp 612
 show status qos 623
 show status remote setup 626
 show status rtfs 627
 show status sd 626
 show status status-led 632
 show status switch control 628
 show status switch control route backup 630
 show status switching-hub macaddress 618
 show status tunnel 619
 show status upnp 619
 show status usbhost 625
 show status user 621
 show status user history 622
 show status vlan 620
 show status vrrp 608
 show status yno 545
 show status yno las 549
 show techinfo 626
 show url filter 625
 show url filter pp 625
 show url filter tunnel 625
 sip 100rel 285
 sip arrive address check 287
 sip arrive ringing p-n-uateype 286
 sip arrive session timer method 287
 sip arrive session timer refresher 286
 sip ip protocol 285
 sip log 289
 sip outer address 288
 sip response code busy 288
 sip session timer 284
 sip use 284
 sip user agent 286
 snmp community read-only 291
 snmp community read-write 291
 snmp display ipcp force 303
 snmp host 290
 snmp ifindex switch static index 305
 snmp local address 298
 snmp syscontact 298
 snmp syslocation 299
 snmp sysname 299
 snmp trap community 292
 snmp trap cpu threshold 300
 snmp trap delay-timer 301
 snmp trap enable snmp 299
 snmp trap enable switch 306
 snmp trap enable switch common 307
 snmp trap host 291
 snmp trap link-updown separate-l2switch-port 304
 snmp trap memory threshold 301
 snmp trap mobile signal-strength 304
 snmp trap send linkdown 302
 snmp trap send linkdown pp 302
 snmp trap send linkdown tunnel 302
 snmp yrifppdisplayatmib2 302
 snmp yrif switchdisplayatmib2 303
 snmp yriftunneldisplayatmib2 303
 snmp yrswindex switch static index 305
 snmpv2c community read-only 293
 snmpv2c community read-write 293
 snmpv2c host 292
 snmpv2c trap community 294
 snmpv2c trap host 293
 snmpv3 context name 294
 snmpv3 engine id 294
 snmpv3 host 296
 snmpv3 trap host 298
 snmpv3 usm user 295
 snmpv3 vacm access 297
 snmpv3 vacm view 296
 snrpd host 458
 snrpd service 458
 speed 340
 speed pp 340
 ssh 92
 ssh encrypt algorithm 93
 ssh known hosts 94
 sshd auth method 87
 sshd authorized-keys filename 88
 sshd client alive 86
 sshd encrypt algorithm 85
 sshd hide openssh version 87
 sshd host 83
 sshd host key generate 84
 sshd listen 83
 sshd service 82
 sshd session 84
 statistics 554
 switch config directory 496
 switch config filename 496
 switch control config get 497
 switch control config set 497
 switch control firmware upload go 494
 switch control function default 494
 switch control function execute 493
 switch control function execute clear-counter 528
 switch control function execute clear-macaddress-table 511
 switch control function execute reset-loopdetect 532

switch control function execute restart 502
switch control function execute restart-poe-supply 536
switch control function execute start-poe-supply 536
switch control function execute stop-poe-supply 537
switch control function get 493
switch control function get boot-rom-version 498
switch control function get counter-frame-rx-type 523
switch control function get counter-frame-tx-type 525
switch control function get energy-saving 500
switch control function get firmware-revision 498
switch control function get lag-type 503
switch control function get led-brightness 500
switch control function get loopdetect-count 529
switch control function get loopdetect-linkdown 529
switch control function get loopdetect-port-use 530
switch control function get loopdetect-recovery-timer 530
switch control function get loopdetect-time 529
switch control function get loopdetect-use-control-packet 531
switch control function get macaddress-aging 509
switch control function get macaddress-aging-timer 510
switch control function get mirroring-dest 521
switch control function get mirroring-src-rx 522
switch control function get mirroring-src-tx 522
switch control function get mirroring-use 521
switch control function get model-name 499
switch control function get poe-class 533
switch control function get port-auto-crossover 505
switch control function get port-blocking-control-packet 506
switch control function get port-blocking-data-packet 507
switch control function get port-flow-control 506
switch control function get port-speed 503
switch control function get port-speed-downshift 505
switch control function get port-use 504
switch control function get qos-dscp-remark-class 516
switch control function get qos-dscp-remark-type 516
switch control function get qos-policing-speed 518
switch control function get qos-policing-use 518
switch control function get qos-shaping-speed 519
switch control function get qos-shaping-use 519
switch control function get qos-speed-unit 517
switch control function get serial-number 499
switch control function get status-combo-port 508
switch control function get status-counter-frame-rx 526
switch control function get status-counter-frame-tx 527
switch control function get status-counter-octet-rx 527
switch control function get status-counter-octet-tx 528
switch control function get status-fan 502
switch control function get status-fan-rpm 502
switch control function get status-led-mode 501
switch control function get status-loopdetect-port 532
switch control function get status-loopdetect-recovery-timer 532
switch control function get status-macaddress-addr 510
switch control function get status-macaddress-port 510
switch control function get status-poe-detect-class 534
switch control function get status-poe-state 533
switch control function get status-poe-supply 535
switch control function get status-poe-supply-detail 535
switch control function get status-poe-supply-total 536
switch control function get status-poe-temperature 534
switch control function get status-port-sfp-rx-power 508
switch control function get status-port-speed 509
switch control function get system-macaddress 499
switch control function get system-name 500
switch control function get system-uptime 503
switch control function get vlan-access 513
switch control function get vlan-id 512
switch control function get vlan-multiple 515
switch control function get vlan-multiple-use 514
switch control function get vlan-port-mode 513
switch control function get vlan-trunk 514
switch control function set 492
switch control function set counter-frame-rx-type 523

switch control function set counter-frame-tx-type 525
switch control function set energy-saving 500
switch control function set led-brightness 500
switch control function set loopdetect-count 529
switch control function set loopdetect-linkdown 529
switch control function set loopdetect-port-use 530
switch control function set loopdetect-recovery-timer 530
switch control function set loopdetect-time 529
switch control function set loopdetect-use-control-packet 531
switch control function set macaddress-aging 509
switch control function set macaddress-aging-timer 510
switch control function set mirroring-dest 521
switch control function set mirroring-src-rx 522
switch control function set mirroring-src-tx 522
switch control function set mirroring-use 521
switch control function set poe-class 533
switch control function set port-auto-crossover 505
switch control function set port-blocking-control-packet 506
switch control function set port-blocking-data-packet 507
switch control function set port-flow-control 506
switch control function set port-speed 503
switch control function set port-speed-downshift 505
switch control function set port-use 504
switch control function set qos-dscp-remark-class 516
switch control function set qos-dscp-remark-type 516
switch control function set qos-policing-speed 518
switch control function set qos-policing-use 518
switch control function set qos-shaping-speed 519
switch control function set qos-shaping-use 519
switch control function set qos-speed-unit 517
switch control function set system-name 500
switch control function set vlan-access 513
switch control function set vlan-id 512
switch control function set vlan-multiple 515
switch control function set vlan-multiple-use 514
switch control function set vlan-port-mode 513
switch control function set vlan-trunk 514
switch control route backup 495
switch control use 487
switch control watch interval 488
switch select 492
switching-hub macaddress-aging 558
syslog debug 59
syslog execute command 60
syslog facility 57
syslog format hostname 58
syslog format type 56
syslog host 56
syslog info 58
syslog local address 59
syslog notice 58
syslog srcport 60
system cpu threshold 63
system memory threshold 64
system packet-buffer 94
system packet-scheduling 102

T

take lan-map snapshot 491
tcp log 76
tcp session limit 125
telnet 587
telnetd host 62
telnetd listen 61
telnetd service 61
telnetd session 63
terminate lua 483
terminate lua file 483
tftp host 74
time 51
Timezone 51

traceroute 584
 traceroute6 585
 tunnel backup 269 tunnel
 backup pp 269 tunnel
 backup tunnel 269 tunnel
 disable 218
 Tunnel enable 218
 tunnel encapsulation 220
 tunnel endpoint address 222
 tunnel endpoint local address 222
 tunnel endpoint name 223
 tunnel endpoint remote address 221
 tunnel hb46pp auth myname 226
 tunnel hb46pp server 226
 tunnel map-e type 225
 tunnel multipoint limit 224
 tunnel multipoint local name 224
 tunnel multipoint server 223
 tunnel name 429
 tunnel select 564
 tunnel template 270
 tunnel translation 225
 tunnel type 219

U

upnp external address refer 439
 upnp external address refer pp
 439 upnp port mapping timer 440
 upnp port mapping timer type 440
 upnp syslog 441
 upnp use 439
 url filter 166
 url filter log 169
 url filter port 167
 url filter reject 168
 url filter use 168
 url interface filter 167
 url pp filter 167
 url tunnel filter 167
 usbhost overcurrent duration 442
 usbhost use 442
 user attribute 46

V

vlan interconnect group 446
 vlan interconnect log 448
 vlan interface 802.1q 446

W

wins server 179
 wol send 588

Y

YNO access code 542
 YNO GUI-forwarder timeout 544
 YNO https-proxy 544
 YNO las connection keepalive
 549 YNO las request retry 548
 YNO las request timeout 548
 YNO las syslog queue length 547
 YNO log 543
 YNO use 542
 yno xmpp connection keepalive 550
 yno zero-config id 545