

# **Command Reference**

**Rev.11.01.23, Rev.14.00.15**

# Contents

<b>Preface: Introduction .....</b>	<b>22</b>
<b>Chapter 1: How to Read the Command Reference .....</b>	<b>23</b>
1.1 Applicable Firmware Revision .....	23
1.2 How to Read the Command Reference .....	23
1.3 Interface Names .....	23
1.4 Command Syntax Starting with the Word “no” .....	24
1.5 Number of Input Characters in a Command and Escape Sequence .....	24
1.6 Range of Peer Numbers by Model .....	24
1.7 About the Factory Default Settings .....	24
<b>Chapter 2: How to Use the Commands .....</b>	<b>25</b>
2.1 Console .....	25
2.1.1 Configuration Procedure Using the Console .....	25
2.1.2 Configuration from the CONSOLE or SERIAL Port .....	26
2.1.3 Configuration Using TELNET .....	30
2.1.4 Remote Setup .....	31
2.2 About the SSH Server .....	32
2.2.1 Notes Regarding the Use of the SSH Server Function .....	32
2.2.2 Setting the SSH Server .....	32
2.3 TFTP .....	32
2.3.1 Configuration Procedure Using TFTP .....	33
2.3.2 Reading the Configuration File .....	33
2.3.3 Writing the Configuration File .....	34
2.4 Keyboard Operation When Using the Console .....	34
2.5 Commands That Start with the Word “show” .....	35
2.5.1 Extracting Only the Contents That Match the Search Pattern from the Display Contents of the Show Command .....	36
2.5.2 Making the Display Contents of the Show Command Easier to View .....	37
2.5.3 Redirection to External Memory .....	38
<b>Chapter 3: Help .....</b>	<b>40</b>
3.1 Showing a Brief Explanation of the Console .....	40
3.2 Showing a List of Commands .....	40
<b>Chapter 4: Router Configuration .....</b>	<b>41</b>
4.1 Set the Login Password .....	41
4.2 Encrypt and Save the Login Password .....	41
4.3 Set the Administrator Password .....	41
4.4 Encrypt and Save the Administrator Password .....	41
4.5 Set the Login User Name and Login Password .....	42
4.6 Setting whether to use RADIUS for password authentication when logging in .....	42
4.7 Setting whether to use RADIUS for password authentication when switching to administrator .....	43
4.8 Set User Attributes .....	43
4.9 Disconnect Another User Connection by Force .....	45
4.10 Set the Security Class .....	46
4.11 Set the Time Zone .....	46
4.12 Set the Current Date .....	47
4.13 Set the Current Time .....	47
4.14 Set the Clock through a Remote Host .....	47
4.15 Set the Clock Using NTP .....	48

4.16 Set the Source IP Address for Sending NTP Packets	48
4.17 Allow Time Synchronization with NTP Server on Stratum 0	49
4.18 Set the Console Prompt Display	49
4.19 Set the Console Language and Code	49
4.20 Set the Number of Characters Shown on the Console	50
4.21 Set the Number of Lines Shown on the Console	50
4.22 Set Whether to Show System Messages on the Console	50
4.23 Set the IP Address of the Host Receiving the SYSLOG	51
4.24 Set the SYSLOG Facility	51
4.25 Set Whether to Output SYSLOGs of NOTICE Type	51
4.26 Set the Output of SYSLOG of INFO Type	52
4.27 Set Whether to Output SYSLOGs of DEBUG Type	52
4.28 Set the Source IP Address for Sending SYSLOG	53
4.29 Set the Source Port Number for SYSLOG Packets	53
4.30 Set Whether to Output Executed Commands to the SYSLOG	53
4.31 Turn the TELNET Server Function ON/OFF	53
4.32 Set the Listen Port of the TELNET Server Function	54
4.33 Set the IP Address of the Host Allowed to Access the TELNET Server	54
4.34 Set the Number of Users That Can Connect Simultaneously to the TELNET Server	55
4.35 Setting the temperature monitoring threshold	55
4.36 Set the Fast Path Function	55
4.37 Set the LAN Interface Operation	56
4.38 Set Whether to Obtain the Number of Reception Overflows in HUB IC	56
4.39 Set How Long after Linkup through the LAN Interface to Wait before Sending	57
4.40 Set the Port Mirroring Function	57
4.41 Set the Operation Type of the LAN Interface	58
4.42 Set Static Link Aggregation	62
4.43 Set the Login Timer	63
4.44 Set the IP Address of the Host Allowed to Access the Router Using TFTP	63
4.45 Set Whether to Relay Magic Packets to the LAN	63
4.46 Set the Interface or System Description	64
4.47 Set Whether to Output the Syslog at the TCP Connection Level	65
4.48 Set Whether to Allow HTTP Revision Update	67
4.49 Set the URL for the HTTP Revision Update	67
4.50 Set the Proxy Server for HTTP Revision Update	67
4.51 Set the HTTP Revision Update Timeout	68
4.52 Set Whether to Allow Downgrade	68
4.53 Set Whether to Allow Updating Using the DOWNLOAD Button	68
4.54 Revision Update Schedule	69
4.55 Turn the SSH Server Function ON/OFF	69
4.56 Set the Listen Port of the SSH Server Function	70
4.57 Set the IP Address of the Host Allowed to Access the SSH Server	70
4.58 Set the Number of Users That Can Connect Simultaneously to the SSH Server	71
4.59 Set the SSH Server Host Key	71
4.60 Set the Encryption Algorithms That the SSH Server Can Use	71
4.61 Check Whether the SSH Client Is Alive	72
4.62 Set the IP Address of the Host Allowed to Access the SFTP Server	72
4.63 SSH Client	73
4.64 SCP client	74
4.65 Setting usable encryption algorithms in the SSH client	74
4.66 Setting the file to save the public key information of the SSH server	75
4.67 Change the Packet Buffer Parameters	75

4.68 Set Whether to Sound Active Alarms or to Not Sound Them at All	76
4.69 Set Whether to Sound Alarms for the USB Host Function	77
4.70 Set Whether to Sound Alarms for the microSD Function	77
4.71 Set Whether to Sound Alarms for the Batch File Execution Function	77
4.72 Set Whether to Sound an Alarm at Startup	78
4.73 Set Whether to Sound Alarms for the HTTP Revision Update Function	78
4.74 Adjust the LED Brightness	78
4.75 Set Environment Variables	79
4.76 Set the CPU Packet Scheduling Mode	79
4.77 Set the CPU packet scheduling filter	80
4.78 Apply the CPU Packet Scheduling Filter	82
<b>Chapter 5: File System for Yamaha router: RTFS</b>	<b>83</b>
5.1 Format the RTFS	83
5.2 Perform Garbage Collection on the RTFS	83
<b>Chapter 6: IP Configuration</b>	<b>84</b>
6.1 Common Interface Settings	84
6.1.1 Set Whether to Process IP Packets	84
6.1.2 Set the IP Address	84
6.1.3 Set the Secondary IP Address	85
6.1.4 Set the Interface MTU	86
6.1.5 Set Whether to Send Returning Packets to the Same Interface	86
6.1.6 Set Whether to Run the Echo, Discard, and Time Services	87
6.1.7 Set the Statistic IP Routing Information	87
6.1.8 Set the IP Packet Filter	89
6.1.9 Define the Filter Set	92
6.1.10 Set Whether to Filter Out IP Packets with the Source-route Option	92
6.1.11 Set Whether to Filter Out Directed Broadcast Packets	92
6.1.12 Define a Dynamic Filter	93
6.1.13 Set the Dynamic Filter Timeout	94
6.1.14 Set the Operation of the Intrusion Detection Function	95
6.1.15 Set the Frequency of Intrusion Detection Notifications in a Second	96
6.1.16 Control the Repeated Intrusion Detection Notifications	96
6.1.17 Set the Number of Maximum Displayed Notifications of the Intrusion Detection	97
6.1.18 Set the Intrusion Detection Threshold Value	97
6.1.19 Set the MSS Limit of the TCP Session	98
6.1.20 Set the Number of TCP Sessions of Which the Router Is an Endpoint	98
6.1.21 Set Whether to Log Changes in the IPv4 Route Information	99
6.1.22 Set the Security by Filtering	99
6.1.23 Set Whether to Rewrite the DF Bit of the IP Packet That Matches the Rule with 0	100
6.1.24 Set the TOS Field Overwriting of the IP Packet	101
6.1.25 Set the Proxy ARP	101
6.1.26 Set the ARP Entry Lifetime	102
6.1.27 Set a Static ARP Entry	102
6.1.28 Limit the Number of Transmission Packets That Are Held until ARP Is Resolved	103
6.1.29 Set Whether to Log ARP Entry Changes	103
6.1.30 Set the Level of Preference of Implicit Routes	104
6.1.31 Set the Lifetime of Each Flow Table Entry	104
6.1.32 Configure the number of entries in the flow table	105
6.2 Setting the Remote PP Interface	105
6.2.1 Set the IP Address on the Remote PP Interface	105
6.2.2 Set the Remote IP Address Pool	106

6.2.3 Set the Time Interval of Keepalive via the PP	107
6.2.4 Set Whether to Use Keepalive via the PP	107
6.2.5 Set Whether to Log Keepalive via the PP	108
6.2.6 Set the Action when a Leased Line Down is Detected	109
6.2.7 Set Permanent Connection	109
6.3 RIP Configuration	109
6.3.1 Set Whether to Use RIP	109
6.3.2 Set the RIP Trusted Gateway	110
6.3.3 Set the RIP Routing Preference	110
6.3.4 Set the RIP Packet Transmission	111
6.3.5 Set the RIP Packet Reception	112
6.3.6 Set the RIP Filtering	112
6.3.7 Set the Number of Hops to Be Added for RIP	113
6.3.8 Set the RIP2 Authentication	113
6.3.9 Set the RIP2 Authentication Key	114
6.3.10 Set the Route Hold When the Line Is Disconnected	114
6.3.11 Set the RIP Operation on the Remote PP Interface When the Line Is Connected	115
6.3.12 Set the RIP Transmission Interval on Remote PP Interface When the Line Is Connected	115
6.3.13 Set the RIP Operation on the Remote PP Interface When the Line Is Disconnected	115
6.3.14 Set the RIP Transmission Interval on the Remote PP Interface When the Line Is Disconnected	116
6.3.15 Set Whether to Switch the RIP Source Interface during Backup	116
6.3.16 Force RIP Route Advertisement	117
6.3.17 Method of Comparison for the RIP2 Filter	117
6.3.18 Adjust the RIP Timer	118
6.4 VRRP Configuration	119
6.4.1 Set the VRRP for Each Interface	119
6.4.2 Set the Shutdown Trigger	120
6.5 Backup Configuration	120
6.5.1 Set the Destination for PP Backup When the Provider Connection Goes Down	121
6.5.2 Set the Recovery Time from Backup	121
6.5.3 Set the Destination for Backup When the Provider Connection via the LAN Goes Down	122
6.5.4 Set the Recovery Time from Backup	122
6.5.5 Set Whether to Use Keepalive via the LAN	123
6.5.6 Set the Time Interval of Keepalive via the LAN	123
6.5.7 Set Whether to Log Keepalive via the LAN	124
6.5.8 Set the Network Monitor Function	124
6.6 PIM-SM Configuration	126
6.7 Setting of the received packet statistics	126
6.7.1 Set Whether to Record Statistical Information for Received Packets	126
6.7.2 Clear statistical information for received packets	127
6.7.3 Showing statistical information for received packets	127
6.7.4 Set the Number of Classifications for Statistical Information Recorded for Received Packets	127
6.8 Set Packet Transfer Filters	128
6.8.1 Define a Packet Transfer Filter	128
6.8.2 Applying a Packet Transfer Filter to an Interface	129
<b>Chapter 7: Ethernet Filter Configuration</b>	<b>130</b>
7.1 Define a Filter	130
7.2 Set the Application to the Interface	131
7.3 Show the Ethernet Filter Status	132

<b>Chapter 8: URL Filter Configuration</b>	<b>133</b>
8.1 Define a Filter	133
8.2 Apply a URL Filter to an Interface	133
8.3 Set the HTTP Port Numbers to Apply the URL Filter To	134
8.4 Set Whether to Use the URL Filter	134
8.5 Set the HTTP Response to the Source of a Packet Discarded by the URL Filter	135
8.6 Set Whether to Log Filter Matches	135
<b>Chapter 9: PPP Configuration</b>	<b>137</b>
9.1 Set the Peer Name and Password	137
9.2 Set the Type of Authentication to Accept	137
9.3 Set the Authentication Type to Be Requested	138
9.4 Set Its Own Name and Password	138
9.5 Set Whether to Prohibit Multiple Connections from a Peer with the Same Username	139
9.6 LCP Configuration	139
9.6.1 Set the Address and Control Field Compression Option	139
9.6.2 Set the Magic Number Option	139
9.6.3 Set the Maximum Receive Unit Option	140
9.6.4 Set the Protocol Field Compression Option	140
9.6.5 Set the lcp-restart Parameter	141
9.6.6 Set the lcp-max-terminate Parameter	141
9.6.7 Set the lcp-max-configure Parameter	141
9.6.8 Set the lcp-max-failure Parameter	141
9.6.9 Set Whether to Send Configure-Request Immediately	142
9.7 PAP Configuration	142
9.7.1 Set the pap-restart Parameter	142
9.7.2 Set the pap-max-authreq Parameter	142
9.8 CHAP Configuration	143
9.8.1 Set the chap-restart Parameter	143
9.8.2 Set the chap-max-challenge Parameter	143
9.9 IPCP Configuration	143
9.9.1 Set the Van Jacobson Compressed TCP/IP	143
9.9.2 Set the IP Address Negotiation with the Remote PP Interface	143
9.9.3 Set the ipcp-restart Parameter	144
9.9.4 Set the ipcp-max-terminate Parameter	144
9.9.5 Set the ipcp-max-configure Parameter	144
9.9.6 Set the ipcp-max-failure Parameter	145
9.9.7 Set the IP Address of the WINS Server	145
9.9.8 Set Whether to Use the IPCP MS Extension Option	145
9.9.9 Set Whether to Accept a Peer IP Address That Has a Host Route	145
9.10 MSCBCP Configuration	146
9.10.1 Set the mscbcpc-restart Parameter	146
9.10.2 Set the mscbcpc-maxretry Parameter	146
9.11 CCP Configuration	146
9.11.1 Set the Compression Type of All Packets	146
9.11.2 Set the ccp-restart Parameter	147
9.11.3 Set the ccp-max-terminate Parameter	147
9.11.4 Set the ccp-max-configure Parameter	148
9.11.5 Set the ccp-max-failure Parameter	148
9.12 IPV6CP Configuration	148
9.12.1 Set Whether to Use IPV6CP	148
9.13 PPPoE Configuration	148

9.13.1 Specify the LAN Interface Used by PPPoE	148
9.13.2 Set the Access Concentrator Name	149
9.13.3 Set the Session Auto Connection	149
9.13.4 Set the Session Auto Disconnection	149
9.13.5 Set the Maximum Retry Count of PADI Packets	150
9.13.6 Set the Retransmission Time of PADI Packets	150
9.13.7 Set the Maximum Retry Count of PADR Packets	150
9.13.8 Set the Retransmission Time of PADR Packets	150
9.13.9 Set the Disconnection Timer of PPPoE Sessions	151
9.13.10 Set the Service Name	151
9.13.11 Turn ON/OFF the MSS Limit of TCP Packets and the Size	151
9.13.12 Set Whether to Forcefully Disconnect PPPoE Sessions That Do Not Exist on the Router	152
<b>Chapter 10: DHCP Configuration</b>	<b>153</b>
10.1 DHCP Server and Relay Agent Function	153
10.1.1 Set the DHCP Operation	153
10.1.2 Set the RFC2131 Compliant Operation	154
10.1.3 Set Whether to Check Duplications in the Leased IP Address	155
10.1.4 Define the DHCP Scope	155
10.1.5 Set the Reserved DHCP Address	156
10.1.6 Set the DHCP Address Assignment Operation	158
10.1.7 Generate Reserved Settings Based on the DHCP Assignment Information	159
10.1.8 Set the DHCP Options	159
10.1.9 Manually Add DHCP Lease Information	160
10.1.10 Manually Release DHCP Lease Information	161
10.1.11 Set the DHCP Server Designation	161
10.1.12 Set the DHCP Server Selection Method	161
10.1.13 Set the Relay Reference of the DHCP BOOTREQUEST Packet	162
10.2 DHCP Client Function	162
10.2.1 Set the Host Name of the DHCP Client	162
10.2.2 Set the Interface to Obtain the DNS Server Address	163
10.2.3 Set the Lease Period of the Requested IP Address	163
10.2.4 Set the Retry Count and Interval of the IP Address Get Request	164
10.2.5 Set the DHCP Client ID Option	164
10.2.6 Set the Options to Be Stored in the Message That the DHCP Client Sends to the DHCP Server	165
10.2.7 Set Whether to Release the Information When the Link Is Down	166
<b>Chapter 11: ICMP Configuration</b>	<b>167</b>
11.1 IPv4 Configuration	167
11.1.1 Set Whether to Send ICMP Echo Reply	167
11.1.2 Set Whether to Send ICMP Echo Reply When the Link Is Down	167
11.1.3 Set Whether to Send ICMP Mask Reply	167
11.1.4 Set Whether to Send ICMP Parameter Problem	168
11.1.5 Set Whether to Send ICMP Redirect	168
11.1.6 Set the Processing When ICMP Redirect Is Received	168
11.1.7 Set Whether to Send ICMP Time Exceeded	169
11.1.8 Set Whether to Send ICMP Timestamp Reply	169
11.1.9 Set Whether to Send ICMP Destination Unreachable	169
11.1.10 Set Whether to Send ICMP Error for Packets Decoded with IPsec	170
11.1.11 Set Whether to Log Received ICMP	170
11.1.12 Set the Stealth Function	171
11.1.13 Set Whether to Perform MTU Discovery by ARP	171

11.1.14 Set Whether to Send ICMP Destination Unreachable for Truncated Packets	172
11.2 IPv6 Configuration	172
11.2.1 Set Whether to Send ICMP Echo Reply	172
11.2.2 Set Whether to Send ICMP Echo Reply When the Link Is Down	172
11.2.3 Set Whether to Send ICMP Parameter Problem	173
11.2.4 Set Whether to Send ICMP Redirect	173
11.2.5 Set the Processing When ICMP Redirect Is Received	173
11.2.6 Set Whether to Send ICMP Time Exceeded	174
11.2.7 Set Whether to Send ICMP Destination Unreachable	174
11.2.8 Set Whether to Log Received ICMP	175
11.2.9 Set Whether to Send ICMP Packet-Too-Big	175
11.2.10 Set Whether to Send ICMP Error for Packets Decoded with IPsec	175
11.2.11 Set the Stealth Function	176
11.2.12 Setting whether to send an ICMP error (Packet Too Big) for truncated frames due to a size error	176
<b>Chapter 12: Tunneling</b>	<b>178</b>
12.1 Enable the Tunnel Interface	178
12.2 Disable the Tunnel Interface	178
12.3 Set the Tunnel Interface Type	178
12.4 Set the IPv4 Address of the Tunnel Interface	179
12.5 Set the Peer IPv4 Address of the Tunnel Interface	179
12.6 Set the End Point IP Address of the Tunnel Interface	180
<b>Chapter 13: IPsec Configuration</b>	<b>181</b>
13.1 Set the IPsec Operation	181
13.2 Set the IKE Version	182
13.3 Set the IKE Authentication Method	182
13.4 Register the Pre-Shared Key	183
13.5 Set the PKI Files to Use in IKEv2 Authentication	183
13.6 Set Its Own Name and Password Used for EAP-MD5 Authentication	184
13.7 Configure EAP-MD5 User Authentication	184
13.8 Set Whether to Send the Certificate Request Payload in EAP-MD5 Authentication	185
13.9 Set Whether to Start IKE	185
13.10 Set Whether to Reject Key Exchange When the Setting Differs	186
13.11 Set Whether to Continue Key Exchange When IKE Fails	187
13.12 Set the Retry Count and Interval of Key Exchange	187
13.13 Set the Remote Security Gateway Name	188
13.14 Set the IP Address of the Remote Security Gateway	188
13.15 Set the Remote ID	189
13.16 Set the Local Security Gateway Name	189
13.17 Set the IP Address of the Local Security Gateway	190
13.18 Set the Local ID	191
13.19 Set the IKE Keepalive Function	191
13.20 Set Whether to Output SYSLOG Related to IKE Keepalive	192
13.21 Set the Encryption Algorithm That IKE Uses	193
13.22 Set the Length of the Queue That Stores the Received IKE Packets	194
13.23 Set the Group That IKE Uses	194
13.24 Set the Hash Algorithm That IKE Uses	195
13.25 Set Whether to Output to the Log When the SPI Value of the Received Packet Is Invalid	195
13.26 Set the IKE Payload Type	196
13.27 Setting the IKEv1 key exchange type	196
13.28 Set Whether to Send the IKE Information Payload	197



13.29 Set Whether to Use PFS .....	197
13.30 Set XAUTH .....	198
13.31 Set the User ID to Use in XAUTH Authentication or EAP-MD5 Authentication .....	198
13.32 Set the Attributes of the User ID to Use in XAUTH Authentication or EAP-MD5 Authentication .....	199
13.33 Set the User Group to Use in XAUTH Authentication or EAP-MD5 Authentication .....	200
13.34 Set the Attribute to Use in XAUTH Authentication or EAP-MD5 Authentication .....	200
13.35 Configure XAUTH User Authentication .....	201
13.36 Set an Internal IP Address Pool .....	202
13.37 Set the IKE XAUTH Mode-Cfg Method .....	202
13.38 Set the Internal IP Address Pool That Is Assigned to the IPsec Client .....	203
13.39 Registering the VPN client simultaneous connection control license .....	203
13.40 Application of the VPN client simultaneous connection control license .....	204
13.41 Set the IKE Log Type .....	205
13.42 Set Whether to Exchange ESP by Encapsulating It in UDP .....	205
13.43 Set Whether to Restrict or not the Negotiation Parameter .....	205
13.44 Set the Management of IKE Message ID .....	206
13.45 SA Configuration .....	207
13.45.1 Set the SA Life Time .....	207
13.45.2 Define the SA Policy .....	208
13.45.3 Manually Refresh the SA .....	209
13.45.4 Set the Dangling SA Operation .....	210
13.45.5 Configure Settings for IPsec NAT Traversal .....	210
13.45.6 Deleting SAs .....	211
13.46 Tunnel Interface Configuration .....	212
13.46.1 Set the Fragmentation of IPv4 Packets Outside of IPsec Tunnel .....	212
13.46.2 Set the DF Bit Control of the IPv4 Packet on the Outside of the IPsec Tunnel .....	212
13.46.3 Set the SA Policy to Be Used .....	213
13.46.4 Set Data Compression Using IPComp .....	213
13.46.5 Set the Tunnel Backup .....	213
13.46.6 Set a Tunnel Template .....	214
13.47 Transport Mode Configuration .....	216
13.47.1 Define the Transport Mode .....	216
13.47.2 Setting the transport mode template .....	216
13.48 PKI Configuration .....	217
13.48.1 Set the Certification File .....	217
13.48.2 Set the CRL File .....	218
<b>Chapter 14: Set the L2TP Function .....</b>	<b>219</b>
14.1 Set Whether to Run L2TP .....	219
14.2 L2TP Tunnel Authentication Configuration .....	220
14.3 Set the Disconnection Timer of L2TP Tunnel .....	220
14.4 Set the L2TP Keepalive .....	220
14.5 Set L2TP Keepalive Logging .....	221
14.6 Set Whether to Output L2TP Connection Control to the Syslog .....	221
14.7 Setting a permanent L2TPv3 connection .....	222
14.8 Setting the L2TP tunnel host name .....	222
14.9 Setting the L2TPv3 local Router ID .....	222
14.10 Setting the L2TPv3 Remote Router ID .....	223
14.11 Setting the L2TPv3 Remote End ID .....	223
<b>Chapter 15: PPTP Configuration .....</b>	<b>224</b>
15.1 Common Configuration .....	224
15.1.1 Set Whether to Operate as a PPTP Server .....	224

15.1.2 Set the Tunnel Interfaces That Are Bound to the Peer Information Number	224
15.1.3 Set the PPTP Operation Type	225
15.1.4 Set the PPTP Host Name	225
15.1.5 Set the PPTP Packet Window Size	225
15.1.6 Set the Authentication Method to Request for Creating PPTP Encryption Keys	226
15.1.7 Set the Acceptable Authentication Methods for Creating PPTP Encryption Keys	226
15.1.8 Set Whether to Output PPTP Connection Control to the Syslog	226
15.2 Remote Access VPN Function	227
15.2.1 Set the PPTP Tunnel Disconnection Timer	227
15.2.2 Set the Tunnel Endpoint Name	227
15.2.3 Set the PPTP Keepalive	228
15.2.4 Set PPTP Keepalive Logging	228
15.2.5 Set the PPTP Keepalive Interval and Count	228
15.2.6 Set Whether to Allow Connection According to the Encryption of the PPTP Connection	229
<b>Chapter 16: Set the SIP Function</b>	<b>230</b>
16.1 Common Configuration	230
16.1.1 Set Whether to Use SIP	230
16.1.2 Set the Timer Value of the SIP Session-Timer Function	230
16.1.3 Select the IP Protocol to Use at the Time of Sending Calls Using SIP	231
16.1.4 Set Whether to Support 100rel when Sending Calls Using SIP	231
16.1.5 Set the Additional User-Agent Header to SIP Packet to Be Sent	231
16.1.6 Setting When refresher Is Not Specified in INVITE at the Time of Call Reception Using SIP	232
16.1.7 Set Whether to Support P-N-UAType Header at the Time of Call Reception Using SIP	232
16.1.8 Set Session Timer Request at the Time of Call Reception Using SIP	232
16.1.9 Set Whether to Verify the User Name at the Time of SIP Reception	233
16.1.10 Set an SIP Response Code to Be Returned When No Port to Receive Calls Is Available	233
16.1.11 Set the IP Address Used by SIP	234
16.1.12 Set Whether to Log SIP Messages	234
<b>Chapter 17: SNMP Configuration</b>	<b>235</b>
17.1 Set the Host to Allow Access Using SNMPv1	235
17.2 Set the SNMPv1 Read-Only Community Name	236
17.3 Set the SNMPv1 Read-Write Community Name	236
17.4 Set the SNMPv1 Trap Transmission Destination	236
17.5 Set the SNMPv1 Trap Community Name	236
17.6 Set the Hosts to Allow Access Using SNMPv2c	237
17.7 Set the SNMPv2c Read-Only Community Name	237
17.8 Set the SNMPv2c Read-Write Community Name	238
17.9 Set the SNMPv2c Trap Transmission Destination	238
17.10 Set the SNMPv2c Trap Community Name	238
17.11 Set the SNMPv3 Engine ID	239
17.12 Set the SNMPv3 Context Name	239
17.13 Set the User Managed with SNMPv3 USM	239
17.14 Set the Host to Allow Access Using SNMPv3	240
17.15 Set the MIB View Family Managed with SNMPv3 VACM	240
17.16 Set the Access Policy Managed with SNMPv3 VACM	241
17.17 Set the SNMPv3 Trap Transmission Destination	242
17.18 Set the Source Address of the SNMP Transmission Packet	242
17.19 Set sysContact	242
17.20 Set sysLocation	243
17.21 Set sysName	243

17.22 Set Whether to Send the SNMP Standard Traps	243
17.23 Set the Transmission Control of SNMP LinkDown Traps	244
17.24 Set Whether to Display the PP Interface Information in the MIB2 Range	245
17.25 Set Whether to Display the Tunnel Interface Information in the MIB2 Range	245
17.26 Set Whether to Display the Switch Interface Information in the MIB2 Range	245
17.27 Set the Forced Display of the PP Interface Address	246
17.28 Set Whether to Send a Trap When the Link of Each Port of the LAN Interface Goes Up or Down	246
17.29 Set Whether to Send the Signal Strength Trap	247
17.30 Set the Interface Number Statically Added to the Switch	247
17.31 Set the Switch Number Statically Added to the Switch	247
17.32 Set the Conditions of SNMP Trap According to Switch Status	248
17.33 Set Conditions of Common SNMP Trap for Switches	248
<b>Chapter 18: RADIUS Configuration</b>	<b>250</b>
18.1 Set Whether to Use RADIUS Authentication	250
18.2 Set Whether to Use RADIUS Account	250
18.3 Set the RADIUS Server	250
18.4 Set the RADIUS Authentication Server	251
18.5 Set the RADIUS Account Server	251
18.6 Set the UDP Port of the RADIUS Authentication Server	252
18.7 Set the UDP Port of the RADIUS Account Server	252
18.8 Set the RADIUS Secret Key	252
18.9 Set the RADIUS Retry Parameter	252
<b>Chapter 19: NAT Function</b>	<b>254</b>
19.1 Apply the NAT Descriptor to the Interface	254
19.2 Set the Operation Type of the NAT Descriptor	254
19.3 Set the Outer IP Address of the NAT Process	255
19.4 Set the Inner IP Address of the NAT Process	256
19.5 Set a Static NAT Entry	256
19.6 Set Whether to Use rlogin, rcp, and ssh When Using IP Masquerade	257
19.7 Set the Static IP Masquerade Entry	257
19.8 Set the Timer for Clearing the NAT IP Address Map	258
19.9 Set the Action Taken When a Conversion Table Corresponding to the Packet Received from the Outside Does Not Exist	259
19.10 Set the Range of Ports Used for IP Masquerade	259
19.11 Set the Port Number Identified as FTP	260
19.12 Set the Range of Ports Not Converted by IP Masquerade	260
19.13 Set Whether to Log NAT Address Assignments	261
19.14 Set Whether to Overwrite the IP Address Included in SIP Messages	261
19.15 Set Whether to Remove the DF Bit during IP Masquerade Conversion	261
19.16 Set the Number of Sessions for every Host Converted by IP Masquerade	262
<b>Chapter 20: DNS Configuration</b>	<b>263</b>
20.1 Set Whether to Use the DNS	263
20.2 Set the IP Address of the DNS Server	263
20.3 Set the DNS Domain Name	263
20.4 Set the Peer Number from Which the DNS Server Is to Be Notified	264
20.5 Set the Order in Which the DNS Servers Are Notified in the DHCP/PCP MS Extension	264
20.6 Set Whether to Process Queries Directed at a Private Address	265
20.7 Set Whether to Resolve Names Using DNS on the SYSLOG Display	265
20.8 Select the DNS Server According to the Contents of the DNS Query	266
20.9 Register the Static DNS Record	267
20.10 Set the Source Port Number of the DNS Query Packet	268

20.11 Set the IP Address of the Host Allowed to Access the DNS Server .....	269
20.12 Set Whether to Use DNS Cache .....	269
20.13 Set the Maximum Number of DNS Cache Entries .....	270
20.14 Set Whether to Unify the DNS Fallback Operations of the Router .....	270
<b>Chapter 21: Priority Control and Bandwidth Control .....</b>	<b>271</b>
21.1 Set the Interface Speed .....	271
21.2 Set the Filter for Classification .....	271
21.3 Select the Queuing Algorithm Type .....	274
21.4 Apply the Classification Filter .....	274
21.5 Set the Queue Length for Each Class .....	275
21.6 Setting the secondary class queue length .....	275
21.7 Set the Default Class .....	276
21.8 Setting the secondary default class .....	276
21.9 Set the Class Property .....	277
21.10 Set Dynamic Class Control .....	277
<b>Chapter 22: Cooperation Function .....</b>	<b>280</b>
22.1 Set Whether to Use the Cooperation Function .....	280
22.2 Set the Port Number to Be Used by the Cooperation Function .....	280
22.3 Set the Operation of Each Peer That Is to Cooperate in the Bandwidth Measurement .....	280
22.4 Set the Operation of Each Peer That Is to Cooperate in the Load Watch Notification .....	282
22.5 Set the Operation Trigger for the Load Watch Server .....	283
22.6 Set the Operation Trigger for the Load Watch Client .....	285
22.7 Manually Execute the Cooperation Function .....	285
<b>Chapter 23: OSPF .....</b>	<b>287</b>
23.1 Apply OSPF .....	287
23.2 Enable/Disable OSPF .....	287
23.3 Set the Level of Precedence of the OSPF Routing .....	287
23.4 Set the OSPF Router ID .....	288
23.5 Set Whether to Apply the Route Received through OSPF to the Routing Table .....	288
23.6 Route Import Using External Protocol .....	288
23.7 Set the Filter for Handling the Route Received through OSPF .....	289
23.8 Define Filters Applied to the Importing of AS External Routes .....	290
23.9 Set the OSPF Area .....	292
23.10 Advertise the Route to an Area .....	292
23.11 Advertise Stub Connections .....	293
23.12 Set the Virtual Link .....	293
23.13 Set the OSPF Area of the Specified Interface .....	295
23.14 Specify the OSPF Router Connected to a Non-Broadcast Network .....	298
23.15 Set the Handling of the Network Route When Stubs Are Present .....	298
23.16 Set Whether to Log OSPF State Transitions and Packet Exchanges .....	298
<b>Chapter 24: BGP .....</b>	<b>300</b>
24.1 Set the BGP Startup .....	300
24.2 Set Aggregate Routes .....	300
24.3 Set the Filter for Route Aggregation .....	300
24.4 Set the AS Number .....	301
24.5 Set the Router ID .....	301
24.6 Set the BGP Route Preference .....	302
24.7 Apply the Filter to the Route Received with BGP .....	302
24.8 Set the Filter to Be Applied to the Routes Received with BGP .....	303
24.9 Apply the Filter to the Route to Be Imported in BGP .....	304
24.10 Activate the BGP Configuration .....	305

24.11 Set the Filter to Be Applied to the Routes to Be Imported in BGP .....	305
24.12 Set the BGP Destination .....	306
24.13 Set the BGP Log .....	307
<b>Chapter 25: IPv6 .....</b>	<b>308</b>
25.1 Common Configuration .....	308
25.1.1 Set Whether to Process IPv6 Packets .....	308
25.1.2 Set the Link MTU of the IPv6 Interface .....	308
25.1.3 Set the MSS Limit of the TCP Session .....	308
25.1.4 Set Whether to Discard IPv6 Packets with Type 0 Routing Headers .....	309
25.1.5 Set the IPv6 Fast Path Function .....	309
25.2 IPv6 Address Management .....	310
25.2.1 Set the IPv6 Address of the Interface .....	310
25.2.2 Set the IPv6 Address Based on the Prefix to the Interface .....	311
25.2.3 Set Whether to Log Changes to IPv6 Prefix .....	312
25.2.4 Set the DHCPv6 Operation .....	313
25.2.5 Set the DAD (Duplicate Address Detection) Retry Count .....	314
25.2.6 Set the Maximum Number of Automatically Set IPv6 Addresses .....	314
25.2.7 Set the Rule for Determining the Source IPv6 Address .....	314
25.3 Neighbor Discovery .....	315
25.3.1 Define the Prefix Distributed by the Router Advertisement .....	315
25.3.2 Control the Router Advertisement Transmission .....	316
25.4 Route Control .....	318
25.4.1 Add IPv6 Routing Information .....	318
25.5 RIPng .....	319
25.5.1 Set Whether to Use RIPng .....	319
25.5.2 Set the Transmission Policy of RIPng on the Interface .....	319
25.5.3 Set the Reception Policy of RIPng on the Interface .....	319
25.5.4 Set the Number of Hops to Be Added for RIPng .....	320
25.5.5 Set the Trusted RIPng Gate on the Interface .....	320
25.5.6 Set the Filtering to Be Applied to the Route Exchanging RIPng Packets .....	321
25.5.7 Set the RIPng Operation on the Remote PP Interface When the Line Is Connected .....	321
25.5.8 Set the RIPng Transmission Interval on the Remote PP Interface When the Line Is Connected .....	322
25.5.9 Set the RIPng Operation on the Remote PP Interface When the Line Is Disconnected .....	322
25.5.10 Set the RIPng Transmission Interval on the Remote PP Interface When the Line Is Disconnected .....	322
25.5.11 Set Whether to Hold the Route Obtained by RIPng When the Line Is Disconnected .....	323
25.5.12 Set the RIPng Routing Preference .....	323
25.6 Set the VRRPv3 .....	323
25.6.1 Set VRRPv3 for Each Interface .....	323
25.6.2 Set the Shutdown trigger .....	324
25.7 Filter Configuration .....	325
25.7.1 Define an IPv6 Filter .....	325
25.7.2 Apply the IPv6 Filter .....	326
25.7.3 Define a Dynamic IPv6 Filter .....	327
25.8 IPv6 Multicast Packet Forwarding Configuration .....	328
25.8.1 Set the MLD Operation .....	329
25.8.2 Set Static MLD .....	329
25.9 Neighbor Solicitation .....	330
25.9.1 Set Whether to Respond to Address Duplication Checking by Performing Neighbor Solicitation .....	330

<b>Chapter 26: OSPFv3</b> .....	<b>332</b>
26.1 Applying OSPFv3 .....	332
26.2 Enabling/disabling OSPFv3 .....	332
26.3 Setting the OSPFv3 router ID .....	332
26.4 Setting the OSPFv3 area .....	333
26.5 Advertising the route to an area .....	333
26.6 Setting the OSPFv3 area of the specified interface .....	334
26.7 Setting the virtual link .....	336
26.8 Setting the level of preference of the OSPFv3 routing .....	337
26.9 Setting whether to apply the route received through OSPFv3 to the routing table .....	337
26.10 Setting the filter for handling the route received through OSPFv3 .....	337
26.11 Route import using external protocol .....	339
26.12 Filters applied to the importing of AS external routes .....	339
26.13 Setting the OSPFv3 log output .....	341
<b>Chapter 27: Triggered Mail Notification Function</b> .....	<b>342</b>
27.1 Set the Mail Configuration ID Name .....	342
27.2 Set the SMTP Mail Server .....	342
27.3 Set the POP Mail Server .....	343
27.4 Set the Timeout Value for Mail Processing .....	343
27.5 Set the Template Used to Send Mail .....	344
27.6 Set the Mail Notification Trigger .....	345
<b>Chapter 28: HTTP Server Function</b> .....	<b>348</b>
28.1 Common Configuration .....	348
28.1.1 Enable/Disable the HTTP Server Function .....	348
28.1.2 Set the IP Address of the Host Allowed to Access the HTTP Server .....	348
28.1.3 Set the Session Timeout Value of the HTTP Server .....	349
28.1.4 Set the Listen Port of the HTTP Server Function .....	349
28.1.5 Set the GUI Language .....	349
28.1.6 Set the PP Interface and Tunnel Interface Names .....	350
28.2 Set the Basic configuration page .....	350
28.2.1 Set the Provider Connection Type .....	350
28.2.2 Associate the Provider Information to PP and Assign the Name .....	351
28.2.3 Set the Provider Connection .....	351
28.2.4 Setting the DNS Server Address of the Provider .....	351
28.2.5 Set the DNS Server Address of the LAN Interface .....	352
28.2.6 Set the Peer Number from Which the DNS Server Is to Be Notified .....	352
28.2.7 Set the Type of Filter Type Routing .....	352
28.2.8 Set the Provider Name of the LAN Interface .....	353
28.2.9 Set the NTP Server .....	353
28.2.10 Setting the NTP Server Address of the Provider .....	354
28.2.11 Set Whether to Automatically Connect When the Disconnect Button Is Pressed on the Basic configuration page .....	354
28.2.12 Set Whether to Carry Out IPv6 Connection on the Basic configuration page .....	355
28.2.13 Association Between Provider Information of a LAN Interface and Tunnel .....	355
<b>Chapter 29: NetVolante DNS Service Configuration</b> .....	<b>356</b>
29.1 Set Whether to Use the NetVolante DNS Service .....	356
29.2 Manually Update the Data on the NetVolante DNS Server .....	356
29.3 Delete Data from the NetVolante DNS Server .....	357
29.4 Set the Port Number to Use for the NetVolante DNS Service .....	357
29.5 Acquire a List of Registered Host Names from the NetVolante DNS Server .....	357
29.6 Register a Host Name .....	358

29.7 Set the Communication Timeout .....	358
29.8 Set Whether to Automatically Generate the Host Name .....	359
29.9 Register the Router's Serial Number as the Host Name .....	359
29.10 Set the NetVolante DNS Server Location .....	359
29.11 Turn the NetVolante DNS Server Address Update Function ON/OFF .....	360
29.12 Set the Port Number of the NetVolante DNS Server Address Update Function .....	360
29.13 Set How Many Times and at What Interval to Retry after Automatic Updating Fails .....	361
29.14 Set the Periodical Update Interval of NetVolante DNS Registration .....	361
29.15 Set the File for Saving the Configuration When Automatic NetVolante DNS Registration Succeed ..	362
<b>Chapter 30: UPnP Configuration .....</b>	<b>363</b>
30.1 Set Whether to Use UPnP .....	363
30.2 Set the Interface That Is to Obtain the IP Address Used for UPnP .....	363
30.3 Set the Type of Timer for Clearing the UPnP Port Mapping .....	363
30.4 Set the Timer for Clearing the UPnP Port Mapping .....	364
30.5 Set Whether to Output the UPnP Syslog .....	364
<b>Chapter 31: USB Configuration .....</b>	<b>366</b>
31.1 Set Whether to Use the USB Host Function .....	366
31.2 Set the Time Until the Excess Current Protection Function in the USB Bus Is Activated .....	366
<b>Chapter 32: Schedule .....</b>	<b>367</b>
32.1 Set the Schedule .....	367
<b>Chapter 33: VLAN Configuration .....</b>	<b>370</b>
33.1 Set VLAN ID .....	370
33.2 Assigning a Switching Hub Port to a VLAN .....	370
<b>Chapter 34: Heartbeat Function .....</b>	<b>372</b>
34.1 Set the Shared Heartbeat Key .....	372
34.2 Set Whether to Receive Heartbeats .....	372
34.3 Send a Heartbeat .....	373
<b>Chapter 35: Heartbeat Function Release 2 .....</b>	<b>374</b>
35.1 Set the Notification Name .....	374
35.2 Configure Notification Settings .....	374
35.3 Enabling a Notification Configuration .....	375
35.4 Set a Notification Interval .....	375
35.5 Set Whether to Log Notification Transmissions .....	376
35.6 Configuring Reception Settings .....	376
35.7 Enabling a Reception Configuration .....	376
35.8 Set Reception Interval Monitoring .....	377
35.9 Set Whether to Log Received Notifications .....	377
35.10 Set the Maximum Number of Heartbeats That Can Be Stored at the Same Time .....	378
35.11 Show the Heartbeat Information .....	378
35.12 Clear the Heartbeat Information .....	378
<b>Chapter 36: SNTP Server Function .....</b>	<b>380</b>
36.1 Set Whether to Enable the SNTP Server Function .....	380
36.2 Set Which Hosts to Allow Access to the SNTP Server .....	380
<b>Chapter 37: External Memory Function .....</b>	<b>382</b>
37.1 Set Whether to Use the microSD Card Slot .....	382
37.2 Set the Operational Mode of Cache Memory for the External Memory .....	382
37.3 Set the Cache Memory Size for File Access Acceleration .....	383
37.4 Specify the Name of the SYSLOG File to Save in External Memory .....	384

37.5 Set Whether to Permit Setup File and Firmware File Copying through the Simultaneous Holding Down of an External Memory Button and the DOWNLOAD button .....	385
37.6 Set Whether to Allow the Router to Start Using Files in the External Memory .....	386
37.7 Set the Timeout for External Memory Detection at Router Startup .....	386
37.8 Specify the Name of the Firmware File That the Router Loads When It Starts or When an External Memory Button and the DOWNLOAD Button Are Held Down .....	386
37.9 Specify the Name of the Setup File That the Router Loads When It Starts or When an External Memory Button and the DOWNLOAD Button Are Held Down .....	387
37.10 Set the File Search Timeout .....	388
37.11 Execute the Batch File .....	389
37.12 Set the Batch and Execution Result Files .....	389
37.13 External Memory Performance Test Command .....	390
37.14 Set the Function to Execute When the DOWNLOAD Button Is Pressed .....	390
37.15 Set Whether to Allow Batch File Execution through the Pressing of the DOWNLOAD Button .....	391

## **Chapter 38: Mobile Internet Connection Function .....392**

38.1 Set Whether to Use a Mobile Terminal .....	392
38.2 Set the PIN Code to Be Input to Mobile Terminal .....	393
38.3 Send a Direct Command to the Mobile Interface .....	393
38.4 Release the Transmission Restriction on a Specified Peer .....	394
38.5 Set the Interface Used for PP .....	394
38.6 Set Automatic Transmission from the Mobile Terminal .....	394
38.7 Set the Timer for Disconnecting from the Mobile Terminal .....	395
38.8 Set the Timer for Disconnecting from the Mobile Terminal When There Is No Input .....	395
38.9 Set the Timer for Disconnecting from the Mobile Terminal When There Is No Output .....	395
38.10 Set the Access Point to Transmit To .....	396
38.11 Set a Point to Transmit Which Is Specified to the Mobile Terminal .....	396
38.12 Set the Packet Transmission Quantity Limit .....	397
38.13 Set the Packet Transmission Time Limit .....	397
38.14 Set the Maximum Number of Consecutive Authentication Failures for a Single Peer .....	398
38.15 Set the LCP Async Control Character Map Option .....	399
38.16 Set Whether to Attach a Caller ID (186) .....	399
38.17 Set Whether to Output a Detailed Syslog .....	399
38.18 Set Whether to Sound an Alarm When the Mobile Terminal Is Connected .....	400
38.19 Set the Packet Transmission Quantity Limit for Each Connection .....	400
38.20 Set the Packet Transmission Time Limit for Each Connection .....	401
38.21 Set the Duration That the Transmission Limits Apply To .....	401
38.22 Acquire the Signal Reception Level .....	402
38.23 Configure Signal Reception Level Acquisition .....	402
38.24 Displaying Regularly Acquired Signal Reception Levels .....	403
38.25 Set the AT Commands to Use to Initialize the Device Connected to the USB Port .....	403
38.26 Set Whether to Perform Flow Control on the Device Connected to the USB Port .....	404
38.27 Set Its Own Name and Password .....	404
38.28 Set the Interface Used for WAN .....	404
38.29 Set Automatic Transmission from the Mobile Terminal .....	405
38.30 Set the Timer for Disconnecting from the Mobile Terminal .....	405
38.31 Set the Timer for Disconnecting from the Mobile Terminal When There Is No Input .....	406
38.32 Set the Timer for Disconnecting from the Mobile Terminal When There Is No Output .....	406
38.33 Set Permanent Connection .....	407
38.34 Set the Access Point to Transmit To .....	407
38.35 Set the Packet Transmission Quantity Limit .....	408
38.36 Set the Packet Transmission Time Limit .....	409
38.37 Set the Packet Transmission Quantity Limit for Each Connection .....	410



38.38 Set the Packet Transmission Time Limit for Each Connection .....	410
38.39 Set the Duration That the Transmission Limits Apply To .....	411
<b>Chapter 39: Bridge Interface(Bridge function) .....</b>	<b>412</b>
39.1 Configuring member interfaces for bridge interface .....	412
39.2 Setting whether to automatically execute learning .....	413
39.3 Setting the deletion timer for bridge learning information .....	413
39.4 Configuring the static learning information .....	414
<b>Chapter 40: Lua Script Function .....</b>	<b>415</b>
40.1 Set Whether to Enable the Lua Script Function .....	415
40.2 Execute a Lua Script .....	415
40.3 Execute the Lua Compiler .....	416
40.4 Show the Status of Running Lua Scripts .....	416
40.5 Stop a Lua Script .....	417
40.6 Set Whether to Sound Alarms for the Lua Script Function .....	417
<b>Chapter 41: Custom GUI .....</b>	<b>419</b>
41.1 Set Whether to Use the Custom GUI .....	419
41.2 Configure Custom GUI User Settings .....	419
41.3 Set Whether to Use the Custom GUI API .....	420
41.4 Set the Password for Accessing the Custom GUI API .....	420
<b>Chapter 42: Switch Control Function .....</b>	<b>421</b>
42.1 Switch Control Function .....	421
42.1.1 Set Whether to Use the Switch Control Function .....	421
42.1.2 Set the Time Interval for Watching Switch .....	422
42.1.3 Select the Switch .....	422
42.1.4 Set the Functions That the Switch Has .....	423
42.1.5 Obtain the Configuration and Operation Status of the Functions That the Switch Has .....	423
42.1.6 Execute a Specified Operation for the Switch .....	423
42.1.7 Delete the Switch Setting .....	424
42.1.8 Update the Firmware of the Switch .....	424
42.1.9 Set the Ethernet Cable Redundancy .....	425
42.2 Switch Function .....	426
42.2.1 System .....	426
42.2.1.1 Obtain the BootROM Version .....	426
42.2.1.2 Obtain the Firmware Revision .....	426
42.2.1.3 Obtain the Serial Number .....	427
42.2.1.4 Obtain the Model Name .....	427
42.2.1.5 Obtain the MAC Address .....	427
42.2.1.6 Obtain the System Name .....	427
42.2.1.7 Set Whether to Use the Energy Saving Function .....	428
42.2.1.8 Adjust the LED Brightness .....	428
42.2.1.9 Obtain the LED Display Mode .....	429
42.2.1.10 Obtain the Fan State .....	429
42.2.1.11 Restart .....	430
42.2.1.12 Obtain the Time Since the System Starts Up .....	430
42.2.2 Port .....	430
42.2.2.1 Set the Port Speed and Operation Mode .....	430
42.2.2.2 Set Whether to Use the Port .....	431
42.2.2.3 Set Whether to Use the Auto Crossover Function .....	431
42.2.2.4 Set Whether to Use the Speed-Downshift Function .....	432
42.2.2.5 Set Whether to Use the Flow Control Function .....	432
42.2.2.6 Set Whether to Block the Switch control Packet .....	433

42.2.2.7 Set Whether to Block Non-Switch Control Packet .....	433
42.2.2.8 Obtain the Port Link State .....	434
42.2.3 MAC Address Table .....	434
42.2.3.1 Set Whether to Use the MAC Address-Aging Function .....	435
42.2.3.2 Set the MAC Address-Aging Time Interval .....	435
42.2.3.3 Search the MAC Address Table According to the MAC Address .....	435
42.2.3.4 Search the MAC Address Table According to the Port Number .....	436
42.2.3.5 Clear the MAC Address Table Entries .....	436
42.2.4 VLAN .....	436
42.2.4.1 Set VLAN ID .....	438
42.2.4.2 Set the Port VLAN Operation Mode .....	438
42.2.4.3 Set the Access Port .....	438
42.2.4.4 Set the Trunk Port .....	439
42.2.4.5 Set Whether to Use Multiple VLAN .....	440
42.2.4.6 Set the Multiple VLAN Group .....	440
42.2.5 QoS .....	441
42.2.5.1 Set the DSCP Remarking Rewriting Method .....	441
42.2.5.2 Set the Received Packets Classification .....	441
42.2.5.3 Set the Speed Unit for Band Limit .....	442
42.2.5.4 Set Whether to Police Incoming Traffic .....	442
42.2.5.5 Set a Bandwidth for Incoming Traffic .....	443
42.2.5.6 Set Whether to Shape Outgoing Traffic .....	443
42.2.5.7 Set a Bandwidth for Outgoing Traffic .....	444
42.2.6 Mirroring .....	444
42.2.6.1 Set Whether to Use the Mirroring Function .....	445
42.2.6.2 Set a Destination Port for Mirroring Packets .....	446
42.2.6.3 Set Whether to Mirror Received Packets .....	446
42.2.6.4 Set Whether to Mirror Packets to Be Transmitted .....	447
42.2.7 Counter .....	447
42.2.7.1 Set a Type of Frames That the Incoming Frame Counter Counts .....	448
42.2.7.2 Set a Type of Frames That the Outgoing Frame Counter Counts .....	449
42.2.7.3 Obtain the Incoming Frame Counter Value .....	451
42.2.7.4 Obtain the Outgoing Frame Counter Value .....	451
42.2.7.5 Obtain the Incoming Octet Counter Value .....	452
42.2.7.6 Obtain the Outgoing Octet Counter Value .....	452
42.2.7.7 Clear the Counter .....	452
42.2.8 Detect a Loop .....	452
42.2.8.1 Set the Threshold for Detecting the Packet Loop Per Second .....	453
42.2.8.2 Set the Time Until the Switch Determines That the Loop Occurs .....	453
42.2.8.3 Set the Operation When a Loop Occurs .....	453
42.2.8.4 Set the Time from When a Port Link Is Down Until It Is Recovered .....	454
42.2.8.5 Set Whether to Use the Loop Detection Function .....	454
42.2.8.6 Set Whether to Use the Loop Detection Function by Using Switch Control Packet .....	455
42.2.8.7 Obtain the Port Status Related to the Loop Detection Function .....	455
42.2.8.8 Obtain the Remaining Time Until the Port Is Recovered from Linkdown .....	456
42.2.8.9 Recover the Port of Which Link Is Down due to the Loop Occurrence .....	456
<b>Chapter 43: Operation .....</b>	<b>457</b>
43.1 Select the Peer Number .....	457
43.2 Select the Tunnel Interface Number .....	457
43.3 Configuration Operation .....	458
43.3.1 Switch to Administrator .....	458
43.3.2 Quit .....	458

43.3.3 Save the Configuration	458
43.3.4 Duplicate the Configuration File	459
43.3.5 Copy the Firmware File to the Internal Flash ROM	460
43.3.6 Delete a Configuration File	461
43.3.7 Deleting an executable firmware file	461
43.3.8 Set the Default Configuration File	461
43.3.9 Setting the default firmware file	462
43.3.10 Reset the Configuration	462
43.4 Clear Operation of Dynamic Information	462
43.4.1 Clear an Account	462
43.4.2 Clear the PP Account	462
43.4.3 Clear the ARP Table	463
43.4.4 Clear the Dynamic Routing Information of IP	463
43.4.5 Clearing the bridge learning information	463
43.4.6 Clear the Log	463
43.4.7 Clear InARP	463
43.4.8 Clear the DNS Cache	463
43.4.9 Clear the Interface Counter Information	464
43.4.10 Clear the NAT Address Table	464
43.4.11 Clear the NAT Address Table of the Interface	464
43.4.12 Clear the Dynamic Routing Information of IPv6	465
43.4.13 Clear the Neighbor Cache	465
43.4.14 Delete the Startup Information History	465
43.4.15 Clear the SYSLOG Saved in the External Memory and Deleting the Backup Files	465
43.5 File and Directory Operation	466
43.5.1 Create Directories	466
43.5.2 Delete a File or Directory	466
43.5.3 Copy a File or Directory	466
43.5.4 Change a File or Directory Name	467
43.6 Other Operations	467
43.6.1 Enable the Peer	467
43.6.2 Disable the Peer	468
43.6.3 Restart	468
43.6.4 Restart the Interface	468
43.6.5 Reset the PP interface	469
43.6.6 Connect	469
43.6.7 Disconnect	470
43.6.8 ping	470
43.6.9 Execute ping6	471
43.6.10 traceroute	472
43.6.11 Execute traceroute6	472
43.6.12 nslookup	472
43.6.13 Delete the Connection Management Information of the Dynamic IPv4 Filter	473
43.6.14 TELNET Client	473
43.6.15 Delete the Connection Management Information of the Dynamic IPv6 Filter	474
43.6.16 Delete the Switching Hub MAC Address Table	474
43.6.17 Send a Magic Packet	474
43.6.18 Check and Update the Firmware by Using HTTP	475
43.6.19 Clear the Statistical Information for the URL Filter	476
43.6.20 Execute the Mail Notification	476
43.6.21 Rotate (Back Up) the SYSLOG Files Stored in the External Memory	476
<b>Chapter 44: Configuration Display</b>	<b>478</b>

44.1 Show the Router Configuration .....	478
44.2 Show All Configurations .....	478
44.3 Show the Configuration of a Specified AP .....	478
44.4 Show the Configuration of a Specified PP .....	479
44.5 Show the Configuration of a Specified Switch .....	479
44.6 Show the Configuration of a Specified Tunnel .....	479
44.7 List the Configuration Files .....	480
44.8 Show a List of File Information .....	480
44.9 Show the IPv6 Address Granted to the Interface .....	480
44.10 Showing lines acquired by masterclock .....	481
44.11 Show the SSH Server Public Key .....	481
44.12 Display the Filter Contents of the Specified Interface .....	481
44.13 List of firmware files .....	482

## **Chapter 45: Status Display .....483**

45.1 Show the ARP Table .....	483
45.2 Show the Interface Status .....	483
45.3 Show the Peer Status .....	483
45.4 Show the IP Routing Information Table .....	484
45.5 Show Routing Information Obtained by RIP .....	485
45.6 Show IPv6 Routing Information .....	485
45.7 Show the IPv6 RIP Table .....	485
45.8 Show the Neighbor Cache .....	485
45.9 Showing bridge learning information .....	485
45.10 Show IPsec SA .....	486
45.11 Show the Certificate Information .....	486
45.12 Show the CRL File Information .....	487
45.13 Show VRRP Information .....	487
45.14 Show the Address Map of the Dynamic NAT Descriptor .....	487
45.15 Show the List of Active NAT Descriptor Applications .....	488
45.16 Show the Address Map of the NAT Descriptor of the LAN Interface .....	488
45.17 Show the Number of Ports Being Used by IP Masquerading .....	489
45.18 Show the L2TP Status .....	489
45.19 Show the PPTP Status .....	489
45.20 Show OSPF Information .....	489
45.21 Show the BGP Status .....	490
45.22 Show the DHCP Server Status .....	490
45.23 Show the DHCP Client Status .....	491
45.24 Show the DHCPv6 Status .....	491
45.25 Show the Backup Status .....	491
45.26 Show the Connections Managed by Dynamic Filters .....	491
45.27 Show the Connections Managed by IPv6 Dynamic Filters .....	492
45.28 Show the Status of the Network Monitor Function .....	493
45.29 Show the History of Intrusion Information .....	493
45.30 Show the Connection Time for Each Peer .....	494
45.31 Display the Status of GUI Language Setting .....	494
45.32 Show Settings Related to the NetVolante DNS Service .....	494
45.33 Show the Switching Hub MAC Address Table .....	495
45.34 Show the UPnP Status Information .....	495
45.35 Show the Tunnel Interface Status .....	495
45.36 Show the VLAN Interface Status .....	496
45.37 Show Information Regarding the Triggered Mail Notification Function .....	496
45.38 Show MLD Group Management Information .....	496

45.39 Show IPv6 Multicast Routing Information .....	497
45.40 Show Information about the Logged in User .....	497
45.41 Show the Packet Buffer Status .....	498
45.42 Show the QoS Status .....	498
45.43 Show the Cooperation Status .....	499
45.44 Showing OSPFv3 information .....	500
45.45 Show the URL Filter Information .....	500
45.46 Show the Heartbeat Information .....	501
45.47 Show the USB Host Function Operation Status .....	501
45.48 Show Connection Information Related to the Remote Setup Function .....	501
45.49 Show Technical Info .....	501
45.50 Show the Operation Status of the microSD Slot .....	502
45.51 Show the Operation Status of the External Memory .....	502
45.52 Show the RTFS Status .....	502
45.53 Show the Startup Information .....	502
45.54 Show Detail of the Startup Information History .....	503
45.55 Show a List of the Startup Information History .....	503
45.56 Show a List of the Switches Controlled by the Router .....	503
45.57 Show the Operation Status of Ethernet Cable Redundancy .....	504
45.58 Display the DNS Cache .....	504
45.59 Show the Status of CPU Packet Scheduling .....	505
<b>Chapter 46: Logging .....</b>	<b>506</b>
46.1 Show the Log .....	506
46.2 Show the Account .....	507
46.3 Show the PP Account .....	507
46.4 Display the Tunnel Account .....	507
46.5 Show the Communication History .....	508

# Preface

---

## Introduction

---

- Copying any or all of the contents of this document without prior written consent is strictly prohibited.
- The contents of this document may change without prior notice.
- Yamaha assumes no liability for damages or loss of information that may result from using this product. The warranty covers only physical defects of the product.
- The information contained in this document has been carefully checked and is believed to be reliable. However, if you find some of the contents to be missing or have questions regarding the contents, please contact us.
- Ethernet is a registered trademark of Xerox Corporation (in the United States).
- Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.
- NetWare is a registered trademark of Novell, Inc. in the United States.
- Stac LZS is a registered trademark of Hifn Inc.
- The microSDHC logo is a trademark.

# Chapter 1

## How to Read the Command Reference

### 1.1 Applicable Firmware Revision

This command reference applies to firmware Yamaha router of Rev.11.01.23, Rev.14.00.15.

For the latest firmware released after printing of this command reference, manuals, and items that differ, access the following URL and see the information in the WWW server.

<http://www.yamaha.com/products/en/network/>

### 1.2 How to Read the Command Reference

This command reference describes the commands that you enter from the router console.

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

[Syntax]	Describes the command syntax. When entering the commands with keys, the commands are not case-sensitive.
	The name section of a command is indicated in <b>Bold face</b>
	The name section of a command is indicated in <i>Italic face</i>
	Keywords are indicated in normal characters.
	Parameters enclosed in parentheses indicate that they can be omitted.
[Setting]	Describes the type of command setting and its meaning.
[Description]	Describes the function of the command.
[Note]	Indicates items to keep in mind when using the command.
[Example]	Gives an actual example of the command.
[Models]	Indicates the models that support the command.

### 1.3 Interface Names

An interface name is used in the command syntax to specify each interface on the router.

The interface name is denoted by an interface type followed by an interface number without a space between them. There are three interface types, lan, bri, and pri. The interface number is allocated in the order in which each interface is detected at startup for each interface type.

Also, when there are multiple interfaces in one module, like the BRI enhanced module, the interface number consists of the number allocated to the module and the number in the module, concatenated with periods.

For the lan interface, if the LAN division function is applied, the divided LANs are concatenated with periods.

On an RTX810 and RTX5000, VLAN interfaces can be used to enhance the LAN division function.

Tag VLANs are concatenated with slashes.

Examples

Interface Type	Interface Name
LAN on the main module	lan1
Tab VLAN	lan1/1, lan1/2, ...
LAN with LAN division function	lan1.1, lan1.2, ...
LAN with enhanced VLAN division function	vlan1,vlan2, ...
BRI on the main module	bri1
First BRI module	bri1.1, bri1.2, ...
Second BRI module	bri2.1, bri2.2, ...
First PRI module	pri1

loopback and null virtual interfaces can be specified.

Interface Type	Interface Name
LOOPBACK	loopback1, loopback2, ...loopback9
NULL	null

## 1.4 Command Syntax Starting with the Word “no”

There are many commands that have a command syntax that starts with the word **no**. When the syntax that starts with the word **no** is used, the command setting is deleted and reset to the initial value unless explained otherwise.

Using this syntax also removes the command from the display shown by the **show config** command. In other words, the input commands are displayed by the **show config** command even when the initial value is set unless the syntax starting with the word **no** is used.

Some commands have parameters that can be omitted written in the syntax starting with the word **no**. This indicates that the command will not produce an error even if the parameter is specified. The parameter value is simply discarded.

## 1.5 Number of Input Characters in a Command and Escape Sequence

The maximum number of characters that can be entered for a command is 4095 including the command name and parameter sections.

If you are entering the following special characters in the command parameter section, enter them as indicated in the following table.

Special Character	Input
?	\?, "?", "?"
#	\#, '#', "#"
	\ , ' ', " "
>	\>, '>', ">"
\	\\
'	\', ""'
"	\", ""
Space	\ followed by a space, ' ', " "

## 1.6 Range of Peer Numbers by Model

The range of peer numbers that can be used vary depending on the model.

Model Name	Range of Peer Numbers
RTX810	1-50
RTX5000	1-150

## 1.7 About the Factory Default Settings

The RTX810 settings when shipped from the factory and after the **cold start** command is executed are not the initial values of the commands described in this reference manual, but the factory default settings indicated below.

```

timezone +00:00
ip lan1 address 192.168.100.1/24
dhcp service server
dhcp server rfc2131 compliant except remain-silent
dhcp scope 1 192.168.100.2-192.168.100.191/24

```



## Chapter 2

### How to Use the Commands

The Yamaha router supports two methods for you to configure or control the router. One method is to send the commands one by one. The other method is to send a file containing a set of necessary commands. If the LAN interface cannot be used, commands can be sent through the CONSOLE or SERIAL port to carry out necessary operations such as recovery from an error.

The method of interactively configuring the router is called a console. When using the console, the commands can be executed one by one to configure or operate the router. A file containing a set of necessary commands is called a configuration file (Config). Configuration files can be sent or received from a platform that can access the Yamaha router through TFTP.

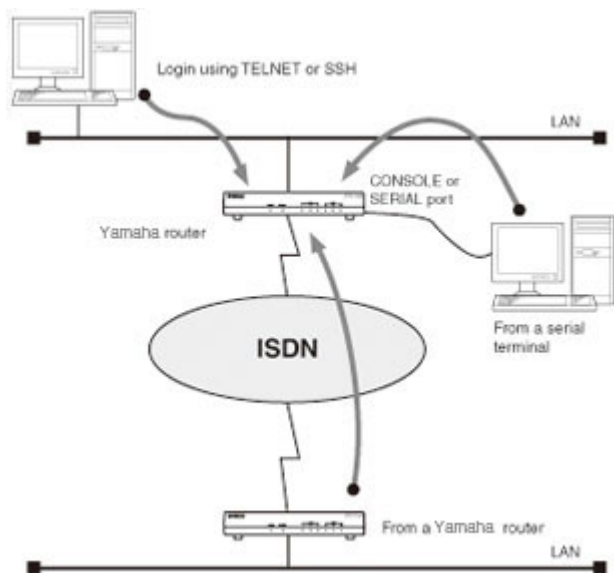
#### 2.1 Console

There are three methods for configuring the router: a method in which a serial terminal is connected to the CONSOLE port of the Yamaha router, a method in which you log in to the router using TELNET or SSH (only on models that support the SSH server function) from a host on the LAN, and a method in which you log in from another Yamaha router via an ISDN line or exclusive line.

Methods of Accessing the Yamaha router
Access from a terminal connected to the CONSOLE or SERIAL port
Log in using TELNET or SSH from a host on the LAN
Login from another Yamaha router via an ISDN line

A single user can access a Yamaha router for each method. Of those users, only a single user can be an administrator at any given time. For example, if a user accessing the router from a serial terminal is logged in as an administrator, other users cannot log in as an administrator using other access methods.

On models that support the multiple TELNET session function and SSH server function, simultaneous access from up to eight users is possible through TELNET or SSH. Multiple users can become administrators simultaneously and set the router from different hosts. In addition, each user can check the access status of all users that are accessing the router, and administrators can forcibly disconnect other users.



##### 2.1.1 Configuration Procedure Using the Console

To configure the router from the CONSOLE or SERIAL port, first, connect a PC to the CONSOLE or SERIAL port of the Yamaha router with a cross serial cable.

Use a serial cable with an appropriate connector that matches the connector on the PC side. A terminal program is used on the PC. If you are using Windows, use a terminal program such as HyperTerminal that comes with the OS. If you are using MacOS X, use the Terminal application that comes with the OS.

If you are configuring the router using TELNET, use a TELNET application on the PC. If you are using Windows, use the TELNET program that comes with the OS. If you are using MacOS X, use the Terminal application that comes with the OS and execute the telnet command.


For details on the console commands, see chapter 3 and subsequent chapters in this command reference.

Use the console commands after you thoroughly understand the operation of the commands. After issuing a command, be sure to check that the operation you intended was carried out correctly.

The character set that is displayed on the console is ASCII by default. The character set can be selected using the **console character** command according to the character display capabilities of your terminal. Note that the command input characters are always ASCII.


The basic flow of a configuration procedure is as follows:

1. After logging in as a general user, issue the **administrator** command to access the router as an administrator. If an administrator password is set, you must enter it.
2. To change the peer information of a peer that is not connected through a line, execute the **pp disable** command, and then change the contents of the peer information. If the line is connected, manually disconnect the line using the **disconnect** command.
3. Change the contents of the peer information using various commands.
4. Execute the **pp enable** command.
5. Execute the **save** command to save the configuration to the non-volatile memory.

 **Note:** Press the S key while holding down the Ctrl key to pause the console output. If you press the keys in this state, the key input is processed even though no reaction is seen on the screen. To resume the console output, press the Q key while holding down the Ctrl key.

For security reasons, the router is configured to automatically log out the user when there is no key input on the console for 300 seconds (initial value). You can change the logout time using the **login timer** command.

If you log in as an administrator and execute a configuration command, the configuration is applied immediately. However, the configuration is written to the non-volatile memory only when you execute the **save** command.

 **Caution:** When the router is started for the first time after purchase or started with the **cold start** command, the login and administrator password are not set. For security reasons, we recommend you set the login and administrator passwords.

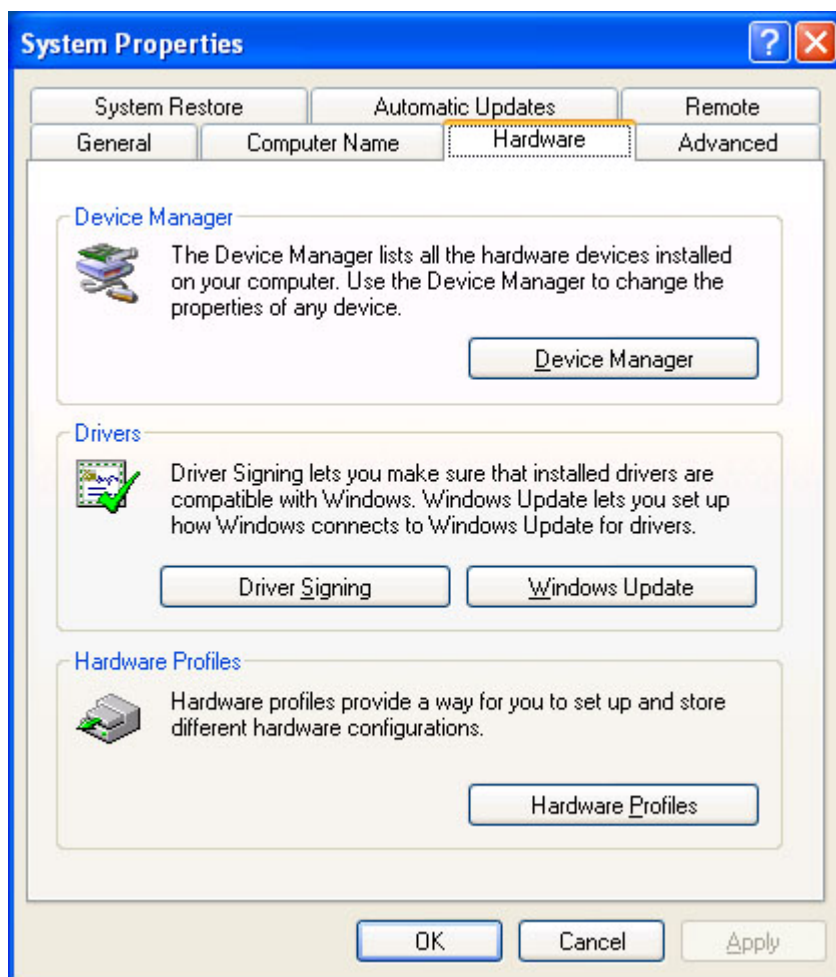
- Configuration is possible immediately after starting up the Yamaha router for the first time after purchase, but the router does not deliver actual packets.
- For details on security settings and additional settings related various parameters, follow the operation policy of your network.

### 2.1.2 Configuration from the CONSOLE or SERIAL Port

---

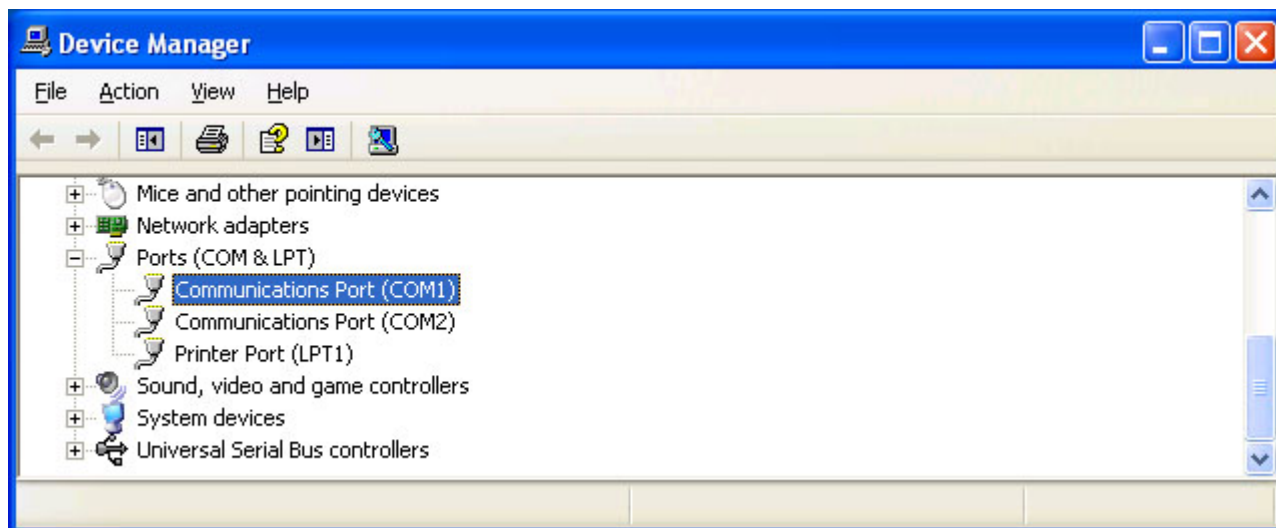
This section gives a configuration example using HyperTerminal on Windows XP. Connect the serial cable in advance.

1. On the task bar, click Start and choose My Computer. Under System Tasks, choose View system information. On the System Properties window, click the Hardware tab.



2. Click Device Manager.

Double-click the Ports (COM and LPT) icon, and check the “COMx” section of Communications Port. Normally, “COM1” is displayed. Remember this COM port number, because it is needed in step 5.



3. Close the Device Manager window.

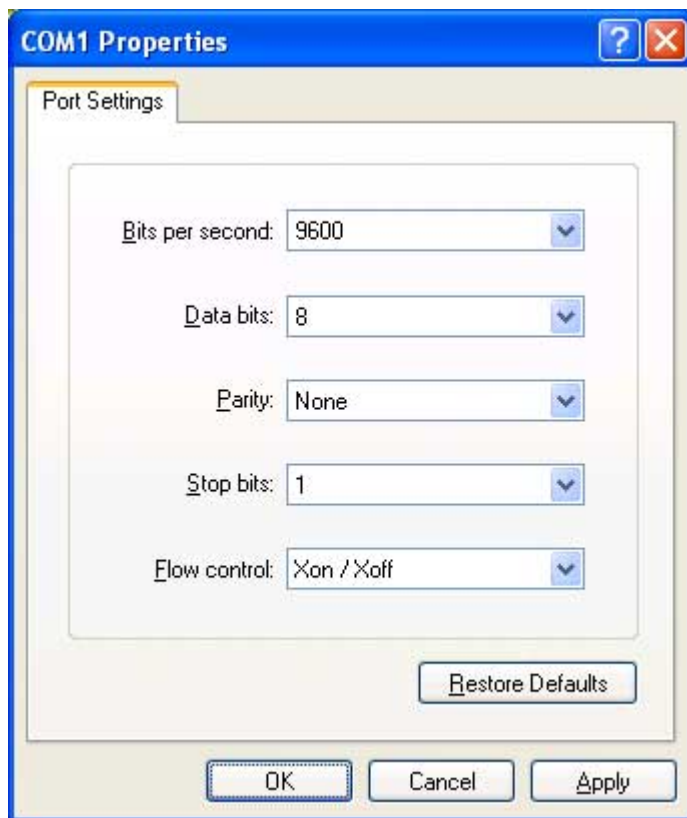
4. On the task bar, click Start, point to All Programs > Accessories > Communications, and click HyperTerminal. When the Connection Description window opens, enter an appropriate name in the Name box, and click OK.



5. From the Connect using box, 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 None, Stop bits to 1, and Flow control to Xon/Xoff. Then, click OK.



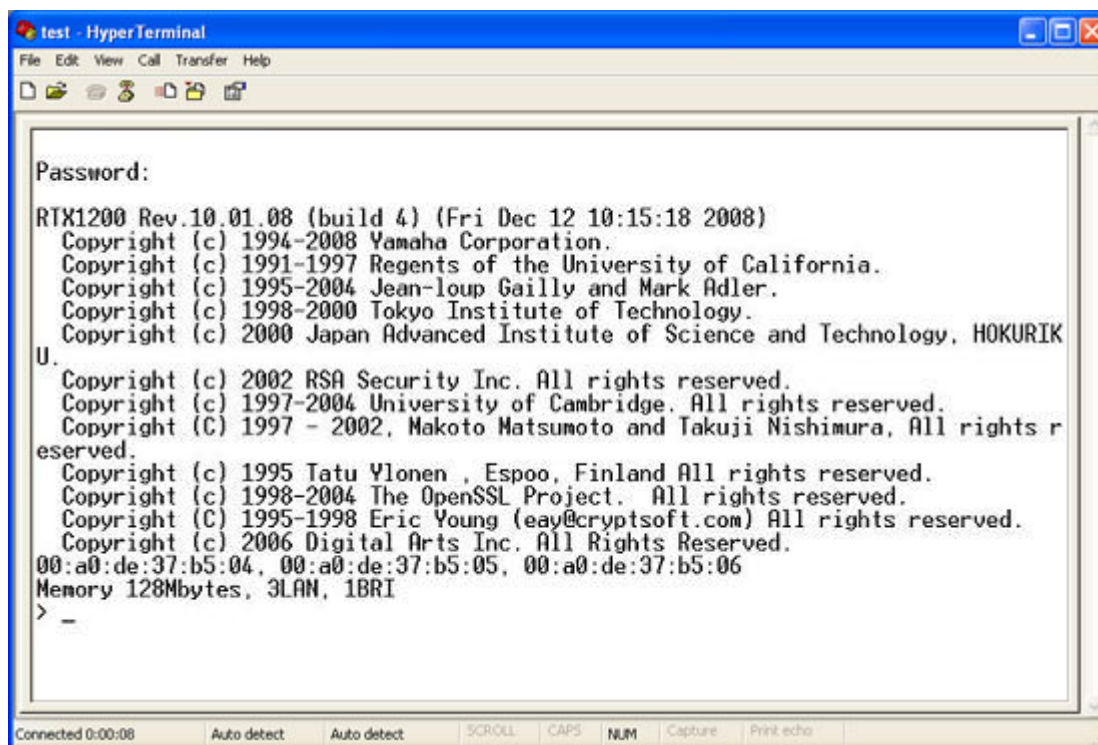
7. When “Password” is displayed, type the login password, and press the Enter key.

\* To login as a user with a registered name on models that support multiple TELNET sessions, simply press the Enter key. When “Username” is displayed, enter the registered user name, press the Enter key, and then enter the user password.

If nothing is displayed, press the Enter key once.

When > is displayed, you can enter console commands.

The following figure shows the RTX1200 login.



**Note:**

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

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

9. When “Password:” is displayed, type the administrator password.

When the character # is displayed, you can enter console commands.

10. Type console commands to configure the router.
11. When you are done, type **save** and press the Enter key.

The configuration specified with the console commands is saved to the non-volatile memory of the router.

12. To finish the configuration, type **quit** and press the Enter key.
13. To close the console screen, type **quit** again and press the Enter key.

### 2.1.3 Configuration Using TELNET

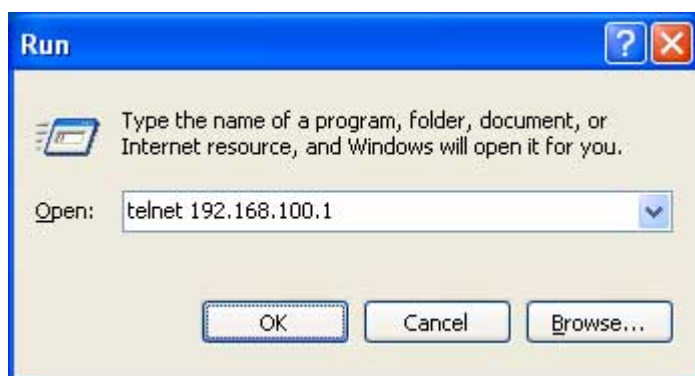
This section gives a configuration example using TELNET on Windows XP. The IP address of the Yamaha router is 192.168.100.1 in this example.

1. On the task bar, click Start and choose Run.



2. Type “telnet 192.168.100.1” and click OK.

If you are using another IP address for the router, type that address in place of “192.168.100.1”.



3. When “Password” is displayed, type the login password, and press the Enter key.

\* To login as a user with a registered name on models that support multiple TELNET sessions, simply press the Enter key. When “Username” is displayed, enter the registered user name, press the Enter key, and then enter the user password.

If nothing is displayed, press the Enter key once. When “>” is displayed, you can enter console commands.



```

Telnet 192.168.100.1
Password:
RT57i BootROM Ver. 1.01
RT57i Rev.8.00.03 (Mon Jun 18 14:31:05 2003)
Copyright (c) 1994-2003 Yamaha Corporation.
Copyright (c) 1998-2000 Tokyo Institute of Technology.
Copyright (c) 2000 Japan Advanced Institute of Science and Technology, HOKURIKI
U.
Copyright (c) 2002 RSA Security Inc. All rights reserved.
Copyright (c) 2003 VoicePump, Inc.
00:a0:de:07:f2:76, 00:a0:de:07:f2:77
Memory 18Mbytes, 2LAN, 1BRI
> administrator
Password:
#
#
# quit
>

```

#### Note:

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

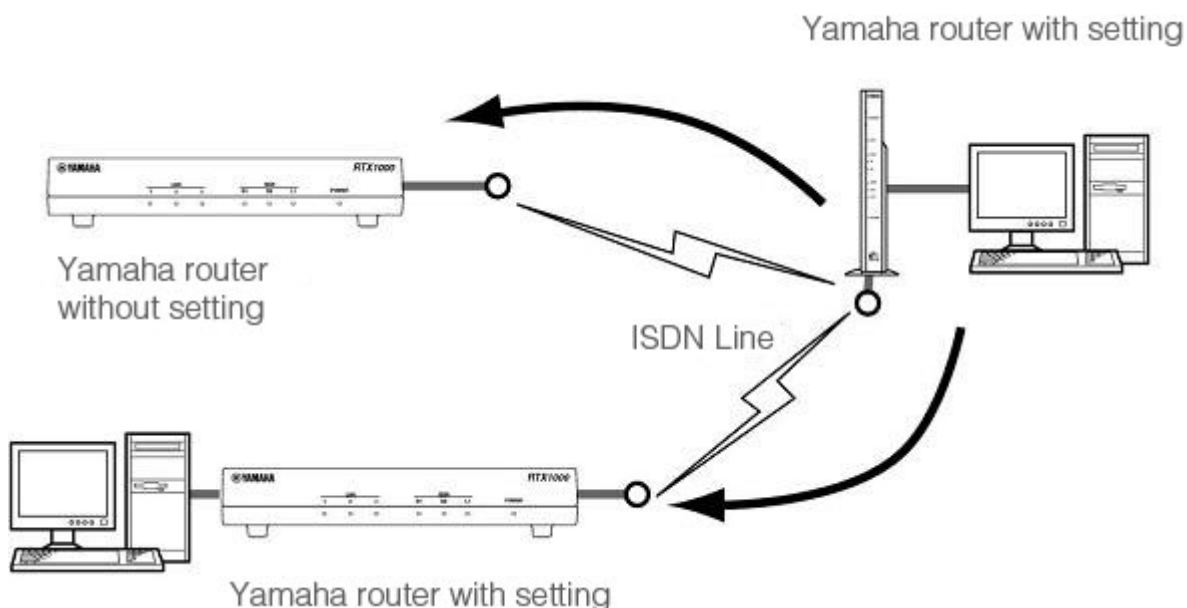
4. Type **administrator** and press the Enter key.
5. When “Password:” is displayed, type the administrator password.  
When the character # is displayed, you can enter console commands.
6. Type console commands to configure the router.
7. When you are done, type **save** and press the Enter key.

The configuration specified with the console commands is saved to the non-volatile memory of the router.

8. To finish the configuration, type **quit** and press the Enter key.
9. To close the console screen, type **quit** again and press the Enter key.

### 2.1.4 Remote Setup

If you are already using a Yamaha router, you can set up with the router in the remote site via an ISDN line or exclusive line. This operation is called “remote setup”. Since you can connect directly to the peer router via the ISDN line or exclusive line, you can set up even when you have no service contract with a provider or no access to the Internet.



You can also setup to reject the remote setup function. With this setting, you can protect accesses from unspecified parties.

The remote setup operation is available on the console. For the detailed operation, see “Configuration from the CONSOLE or SERIAL Port” or “Configuration Using TELNET” in the previous section. The command for the remote setup function is **remote setup**.

When you complete logging in to the peer Yamaha router, you can configure a router that you want to set with the console commands.



**Caution:**

- The remote setup function is only available from the Yamaha router.
- You cannot setup remotely via the WAN port such as FTTH, CATV, and ADSL.

## 2.2 About the SSH Server

---

In models that support the SSH server function, you can log in and configure the settings from the host on LAN via SSH. When doing this, the SSH client to use on the host side comes standard on MacOS X ("Terminal" application) or UNIX. However, it does not come standard in Windows operating systems. In an environment without an SSH client, use a third-party software such as a freeware with an SSH client function.

### 2.2.1 Notes Regarding the Use of the SSH Server Function

---

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

- SSH protocol version 1
- User authentication other than password authentication (host-based, public key, challenge-response, and GSSAPI authentications)
- Port forwarding (X11/TCP transmission)
- Gateway ports (port relay)
- Blank password
- scp

### 2.2.2 Setting the SSH Server

---

The SSH server function is disabled by factory default. The setup procedure to enable the SSH server function is as follows:

1. Use the **login user** command to register a user with a name. A user with a name must be registered in advance, because you must enter the user name when logging in using SSH.
2. Use the **sshd host key generate** command to generate an SSH server host key. This command generates a pair of DSA or RSA public key and secret key. This command may take more than 10 seconds to complete depending on the model.
3. Use the **sshd service** command to enable the SSH server function.

```

Telnet 192.168.100.1
> administrator
Password:
# login user RTuser himitsu
# sshd host key generate
Generating public/private dsa key pair ...
|*****
Generating public/private rsa key pair ...
|*****
# sshd service on
# save
Saving ... CONFIGO Done .
# quit
>

```

## 2.3 TFTP

---

The items configured on a Yamaha router can be read as a configuration file from a host on the LAN using TFTP. In addition, a configuration file on the host can be written to the router to configure it.

TFTP comes standard on Windows XP, Terminal application on the MacOS X, and UNIX platforms. On platforms that do not come with TFTP, obtain an application such as freeware that has a TFTP client function. The Yamaha router operates as a



TFTP server.

The configuration file contains all settings. You cannot read a portion of the configuration or write only the items that differ. The configuration file is a text file (SJIS or ASCII with CRLF line feed) that can be edited directly such as by Notepad on Windows.

TFTP can handle configuration files in plain text and encrypted configuration files. Supported encryption systems are AES128 and AES256. You cannot use a file encrypted with a specified password. RT-Tftp Client does not support encryption.



**Caution:**

- The contents of the configuration file must be written correctly such as the command syntax and parameter designation. Settings that are incorrect in terms of syntax or content are discarded and not applied to the operation.
- Note that if you are writing the configuration file to the router using TFTP and configuration is to be changed using the **line type** command, the **restart** command is needed at the end of the configuration file.

### 2.3.1 Configuration Procedure Using TFTP

---

To exchange configuration files using TFTP, the Yamaha router must be configured in advance to allow TFTP access. First, execute the **tftp host** command to set the host that is allowed to access the router. Note that the router is configured not to allow access from any host under the factory default settings.

```

Telnet 192.168.100.1
> administrator
Password:
# tftp host 192.168.100.25
# save
Saving ... CONFIGO Done .
# quit
>

```

Next, execute TFTP commands from the host on the LAN. The command syntax depends on the host operating system. Keep the following points in mind when executing commands.

- Router IP address
- Use “ascii” or “character” for the transmission mode.  
Use “binary” when handling encrypted configuration files.
- If an administrator password is set on the router, you must specify the administrator password after the file name.
- Specify “config” for the name of the activated configuration file to be exchanged.

### 2.3.2 Reading the Configuration File

---

This section gives an example in which the configuration file is read on Windows XP. Note that this operation is not a console operation of the Yamaha router. In this example, the Yamaha router IP address is 192.168.100.1, the administrator password is “himitsu”, and the name of the new file created on Windows is “OLDconfig.txt”.

1. On the task bar, click Start, point to All Programs > Accessories, and click Command Prompt.
2. Move to the directory in which the configuration file is to be saved.
3. Type **tftp 192.168.100.1 get config/himitsu OLDconfig.txt** and press the Enter key.

When encrypting a configuration file and then reading it, specify the “-encryption” option after the file name. To specify an encryption system, specify the “-aes128” option or “-aes256” option after “-encryption”. If the encryption system is omitted, AES256 is used as an encryption system. When encrypting a configuration file with the encryption system AES128 and then reading it, type the following:

Type **tftp -i 192.168.100.1 get config-encryption-aes128/himitsu OLDconfig.txt** and press the Enter key.

```

CA Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\>

D:\>cd RTX1000

D:\RTX1000>tftp 192.168.100.1 get config/himitsu OLDconfig.txt
Transfer successful: 2758 bytes in 1 second, 2758 bytes/s

D:\RTX1000>

```

### 2.3.3 Writing the Configuration File

This section gives an example in which the configuration file is written from Windows XP. Note that this operation is not a console operation of the Yamaha router. In this example, the Yamaha router IP address is 192.168.100.1, the administrator password is “himitsu”, and the name of the file on Windows that is to be written is “NEWconfig.txt”.

1. On the task bar, click Start, point to All Programs > Accessories, and click Command Prompt.
2. Move to the directory in which the configuration file is saved.
3. Type **tftp 192.168.100.1 put NEWconfig.txt config/himitsu** and press the Enter key.

When writing an encrypted and configured “NEWconfig.rtf” into the configuration file, type the following similar to writing of the normal configuration file:

Type **tftp -i 192.168.100.1 put NEWconfig.rtf config/himitsu** and press the Enter key.

```

CA Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\>

D:\>cd RTX1000

D:\RTX1000>tftp 192.168.100.1 put NEWconfig.txt config/himitsu
Transfer successful: 2726 bytes in 1 second, 2726 bytes/s

D:\RTX1000>

```

## 2.4 Keyboard Operation When Using the Console

When displaying information that does not fit on one screen, the display is stopped when the number of lines specified by **console lines** is shown, and “---more---” is shown at the bottom of the screen.

To show the rest of the information, press the space key. Press the Enter key to show a new line. When the entire information is shown by repeating these operations, the screen automatically returns to the state in which new commands can be input.

If you wish to end the display without showing the entire information, press the q key. The screen returns to the state in which new commands can be input.

If you do not want to stop the display when showing information that does not fit on one screen, execute the **console lines infinity** command.

Keyboard Operation	Description and Notes
SPACE	Advance one screen
ENTER	Advance one line

Keyboard Operation	Description and Notes
RETURN	
q	Quit
Ctrl-C	

To show the contents of **show config**, **show config list**, **show config pp**, **show config tunnel**, **show config switch**, **show config ap**, **show file list**, **show log** in a fashion similar to the **less** command on UNIX, use the **less config**, **less config list**, **less config pp**, **less config tunnel**, **less config switchl**, **less config ap**, **less file list**, **less log** commands, respectively.

Keyboard Operation	Description and Notes
{n} f	Advance {n} screens
{n} Ctrl-F	
{n} SPACE	
{n} b	Go back {n} screens
{n} Ctrl-B	
{n} j	Advance {n} lines
{n} Ctrl-J	
{n} Ctrl-E	
{n} Ctrl-M	
{n} ENTER	
{n} RETURN	
{n} k	Go back {n} lines
{n} Ctrl-K	
{n} y	
{n} Ctrl-Y	
{n} Ctrl-P	
{n} d	Advance {n} half screens
{n} Ctrl-D	
{n} u	Go back {n} half screens
{n} Ctrl-U	
{n} g	Move to line {n}
	Moves to the first line if {n} is omitted.
{n} G	Move to line {n}
	Moves to the last line if {n} is omitted.
{n} r	Redraw the current screen
{n} Ctrl-R	
{n} Ctrl-L	
q	Quit
Ctrl-C	

Description:

- n: A numerical key input representing an integer value. The value is set to 1 when omitted.
- Ctrl-X: Indicates the action of pressing the X key while holding down the Ctrl key.

## 2.5 Commands That Start with the Word “show”

You can extract and show only the contents that match a specified search pattern from the contents shown by commands that

start with the word “show”. You can also move backwards or search for contents that match a specified pattern while displaying the contents shown by commands that start with the word “show” at the page level. These functions can be used on all commands that start with the word “show”.

### 2.5.1 Extracting Only the Contents That Match the Search Pattern from the Display Contents of the Show Command

#### [Syntax]

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

#### [Setting and Initial value]

- -i : Search the string specified by *pattern* without distinguishing between lowercase and uppercase characters.
  - [Initial value] : -
- -v : Show lines that do not match the string specified by *pattern*.
  - [Initial value] : -
- -w : Show only when the string specified by *pattern* matches the word.
  - [Initial value] : -
- *pattern*
  - [Setting] : Search pattern
  - [Initial value] : -

#### [Description]

**show** Extracts and shows only the lines that match the search pattern specified by *pattern* from the display contents of the *pattern* command.

If the -i option is specified, the search is made without distinguishing between the lowercase and uppercase characters of *pattern*. For example, if you specify ‘abc’ for *pattern* when the -i option is available, ‘abc’, ‘ABC’, ‘aBc’, ‘ABc’, and so forth are considered to match the pattern. If the -i option is not specified, ‘abc’ only matches with ‘abc’.

If the -v option is specified, lines that do not match the string specified by *pattern* are shown.

If the -w option is specified, only words are matched to *pattern*. For example, if you specify ‘IP’ for *pattern* when the -w option is available, ‘ IP ’ (space before and after the word) and ‘[IP]’ are considered to match the pattern, but ‘IPv4’ and ‘IPv6’ do not. If the -w option is not specified, all the examples given above are considered to match the pattern.

The parameter *pattern* is a limited regular expression. A general regular expression allows many special characters to be used to construct a variety of search patterns. However, only the following special characters are implemented in the router.

Character	Meaning	Example	Examples of Text Strings That Match
.	Matches any character	a.b	aab, aXb, a-b
?	Matches a pattern in which the previous character appears zero times or once	b?c	ac, abc
*	Matches a pattern in which the previous character repeats zero times or more	ab*c	ac, abc, abbc, abbbbbbbbc
+	Matches a pattern in which the previous character repeats once or more	ab+c	abc, abbc, abbbbbbbbc
	Matches the previous character or the next character	ab cd	abd, acd
[ ]	Matches any character in the bracket	a[bc]d	abd, acd
[^ ]	Matches any character other than those in the bracket	a[^bc]d	aad, axd
^	Matches the beginning of the line	^abc	Any line that starts with abc
\$	Matches the end of the line	abc\$	Any line that ends with abc
()	Handle text strings as a group	(ab cd)	ab, cd

Character	Meaning	Example	Examples of Text Strings That Match
\	Cancels the effect of the following special character	a\.c	a.c

You can specify **grep** numerous times in a line. The **show** command can be used simultaneously with the **less** command. If you are using '\', '?', and '|' as characters in *pattern*, you must enter '\' before each of these characters.

the message "Searching ..." appears when the command is being executed. Enter Ctrl+C when a target character set is being searched, and you can stop the display.

```
Example)
# show command | grep nat
Searching ...
clear nat descriptor dynamic: Dynamic NAT information is deleted.
^C
#
```

#### [Example]

```
show config | grep ip | grep lan
show config | grep ip | less
```

#### [Models]

RTX810, RTX5000

## 2.5.2 Making the Display Contents of the Show Command Easier to View

### [Syntax]

```
show [...] | less
```

### [Description]

Shows the display contents of the **show** command screen by screen, and receives commands at the last line.

If the display contents are less than one screen, all of the contents are displayed, and the command ends.

Commands are executed by entering a numeric prefix and a command character. The numeric prefix can be omitted as an option. If the numeric prefix is omitted, it is considered to be 1. For search commands, a search text string can be entered after the command character.

The following commands are available.

Command	Description (Numeric Prefix Taken to Be N)
q	Quit less.
Space	Advance N screens.
b	Go back N screens.
j, ENTER	Advance N lines.
k	Go back N lines.
g	Jump to line N.
G	Jump to line N. Jumps to the last line, if the numeric prefix is omitted.
/	Searches the search pattern entered after the command character toward the front. The search pattern is the same as with the <b>grep</b> command.
?	Searches the search pattern entered after the command character toward the back. The search pattern is the same as with the <b>grep</b> command.
n	Searches the same search pattern as the previous / or ? command in the same direction.

Command	Description (Numeric Prefix Taken to Be N)
N	Searches the same search pattern as the previous / or ? command in the reverse direction.

**[Models]**

RTX810, RTX5000

**2.5.3 Redirection to External Memory****[Syntax]****show** [...] > *name***show** [...] >> *name***[Setting and Initial value]**

- *name* : File name

- [Setting] :

Setting	Description
usb1: <i>filename</i>	A file in USB memory
sd1: <i>filename</i>	A file in a microSD memory card

- [Initial value] : -

**[Description]**

A file that is specified through the redirect operator ('>'), which is an operator that enables you to save the results of the **show** command to external memory, is always created as a new file. This means that if there is a file with the same name in the external memory, it will be overwritten.

The encryption of saved files is not supported.

You can use a pipe operator ('|') with the redirect operator to save only the necessary lines to a file.

```
# show log | grep IKE > usb1:log.txt
```

you can use the redirect operator '>>' for an existing file in the external memory to add the command execution results to the existing file.

```
# show log > usb1:log.txt      ... New file
# show log >> usb1:(existing)log.txt ... Add to the end of the file.
```

Also, when you specify an existing file name as a destination file with the redirect operator '>', the message to confirm whether you overwrite the file appears.

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

However, when you execute from the command input page GUI, the custom GUI, or rt.command of Lua, the confirmation message does not appear and the file is overwritten forcefully.

**[Note]**

You cannot use a pipe operator ('|') after the redirect operator.

You cannot use multiple redirect operators.

The redirect operator can only be used with commands that start with **show** and that start with commands other than **less**.

The redirect operator cannot be used to save data to the external memory when:

- The external memory is not connected.
- A button is being pressed.
- Access has been forbidden.

When the amount of memory is insufficient, a file is created with the largest possible file size given the amount of remaining memory.

*filename* must be 99 characters or less.

**[Example]**

Save the contents of the **show log** command to USB memory.

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

Save the contents of the **show techinfo** command to a microSD card.

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

**[Models]**

RTX810, RTX5000

## Chapter 3

---

### Help

---

#### 3.1 Showing a Brief Explanation of the Console

---

**[Syntax]**

**help**

**[Description]**

Shows a brief explanation on how to use the console.

**[Models]**

RTX810, RTX5000

#### 3.2 Showing a List of Commands

---

**[Syntax]**

**show command**

**[Description]**

Lists the command names and their simple explanations.

**[Models]**

RTX810, RTX5000



---

## Chapter 4

---

### Router Configuration

---

---

#### 4.1 Set the Login Password

---

**[Syntax]**

**login password**

**[Description]**

Sets the password for logging in as a general user using up to 32 characters. There are no parameters. Enter the command, and then enter the password at the prompt.

The characters that can be used for passwords are alphanumeric characters and symbols that can be displayed in 7-bit ASCII code.

**[Models]**

RTX810, RTX5000

---

#### 4.2 Encrypt and Save the Login Password

---

**[Syntax]**

**login password encrypted**

**[Description]**

Sets the anonymous user password using up to 32 characters, encrypts, and saves the password. There are no parameters. Enter the command, and then enter the password at the prompt.

The characters that can be used for passwords are alphanumeric characters and symbols that can be displayed in 7-bit ASCII code.

**[Note]**

Use this command to encrypt and save the password. To save the password in plain text, use the **login password** command.

**[Models]**

RTX810, RTX5000

---

#### 4.3 Set the Administrator Password

---

**[Syntax]**

**administrator password**

**[Description]**

Set the administrator password for changing the router configuration as an administrator using up to 32 characters. There are no parameters. Enter the command, and then enter the password at the prompt.

The characters that can be used for passwords are alphanumeric characters and symbols that can be displayed in 7-bit ASCII code.

**[Models]**

RTX810, RTX5000

---

#### 4.4 Encrypt and Save the Administrator Password

---

**[Syntax]**

**administrator password encrypted**

**[Description]**

Set the administrator password for changing the router configuration as an administrator using up to 32 characters. There are no parameters. Enter the command, and then enter the password at the prompt.

The characters that can be used for passwords are alphanumeric characters and symbols that can be displayed in 7-bit ASCII code.

**[Note]**

Use this command to encrypt and save the password. To save the password in plain text, use the **administrator password** command.

**[Models]**

RTX810, RTX5000

## 4.5 Set the Login User Name and Login Password

---

**[Syntax]**

```
login user user [password]
login user user encrypted password
no login user user [password]
```

**[Setting and Initial value]**

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

**[Description]**

Sets the login user name and password.

Up to 32 users can be registered.

The characters that can be used for user names are alphanumeric characters, hyphen, and underscore.

In the first syntax, enter the password in plain text. The password is encrypted and saved. If the password is omitted, you enter the password at the prompt after you enter the command. The characters that can be used for passwords are alphanumeric characters and symbols that can be displayed in 7-bit ASCII code.

In the second syntax, you enter the encrypted password in *password*.

If the setting is retrieved using TFTP, the second syntax is always shown, because the password is stored using encryption.

**[Note]**

Multiple users with a same name cannot be registered.

If the command is used to set a user name that is already registered, the original setting is overwritten.

When **syslog execute command** is set to on, you should take measures to prevent the password from remaining in the log, such as using a syntax that omits the password, setting **syslog execute command** to off temporarily, or executing **clear log**.

**[Models]**

RTX810, RTX5000

## 4.6 Setting whether to use RADIUS for password authentication when logging in

---

**[Syntax]**

```
login radius use use
no login radius use
```

**[Setting and Initial value]**

- *use*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : off

**[Description]**

Sets whether to allow the use of RADIUS for password authentication when logging in.

**[Note]**

The following commands concerning the RADIUS authentication server must be specified:

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

[Models]  
RTX810, RTX5000

## 4.7 Setting whether to use RADIUS for password authentication when switching to administrator

### [Syntax]

```
administrator radius auth use
no administrator radius auth [use]
```

### [Setting and Initial value]

- *use*
- [Setting] :

Setting	Description
on	Enable local authentication together with the RADIUS authentication
only	Enable the RADIUS authentication only
off	Disable

- [Initial value] : off

### [Description]

Sets whether to use the RADIUS for password authentication when switching to the administrator with the **administrator** command.

If on is specified, an administrator password specified with the **administrator password** is compared. If the password does not match, a query is made to the RADIUS server. If only is specified, only a query is made to the RADIUS server.

### [Note]

The following commands concerning the RADIUS authentication server must be correctly specified:

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

[Models]  
RTX810, RTX5000

## 4.8 Set User Attributes

### [Syntax]

```
user attribute [user] attribute=value [attribute=value...]
no user attribute [user...]
```

### [Setting and Initial value]

- *user*
- [Setting] :

Setting	Description
User name	Registered user name
*radius	All users who log in with RADIUS authentication
*	all users

- [Initial value] : -
- *attribute=value* : User attribute
- [Setting] :
  - administrator : Attribute showing whether the administrator mode is available or not

Setting	Description
on	Allows the user to become an administrator by using the <b>administrator</b> command and allows the user to access the administrator pages GUI. Allow the user to establish SFTP connection with the administrator password.

Setting	Description
off	Does not allow the user to become an administrator by using the <b>administrator</b> command and prohibits the user from accessing the administrator pages GUI. Not allow the user to establish SFTP connection with the administrator password.

- connection : Attribute showing how to access to the router

Setting	Description
off	Prohibits all connections.
all	Allows all connections.
serial	Allows connection from the serial console.
telnet	Allows connection using TELNET.
ssh	Allows connection using SSH.
sftp	Allows connection using SFTP.
remote	Allows connection using remote setup.
http	Allows connection to the configuration GUI.

- host : Attribute specifying an access host to the router

Setting	Description
IP address	Allows connection from a specified host.
any	Allows access from all hosts.
Interface name	Allows connection from the specified interface.

- multi-session : Attribute showing whether to allow multiple sessions

Setting	Description
on	Allows multiple sessions using TELNET, SSH, or HTTP by the same user.
off	Prohibits multiple sessions using TELNET, SSH, or HTTP by the same user.

- login-timer : Login timer specification

Setting	Description
120..21474836	Number of seconds for automatically logging out when there is no key input.
clear	Disable the login timer.

- [Initial value] :
  - administrator=on
  - connection=serial,telnet,remote,ssh,sftp,http
  - host=any
  - multi-session=on
  - login-timer=300

### [Description]

Sets user attribute.

If user is omitted, anonymous *user* attributes are set.

Sets attributes of all users who log in with RADIUS authentication when \*radius is specified for *user*.

If the asterisk (\*) is set to *user*, the setting is applied to all users. However, if the user name is already registered, the settings for the specified user take precedence.

Even if the administrator attribute is changed to off against a user that is already in administrator mode, the user can remain in administrator mode until the user exits to user mode using the **exit** command or logs out.

Multiple values except off and all can be specified for the connection attribute by concatenating each value with a comma.

Even if a connection is prohibited using the connection or host attribute of this command against a user that is already connected, the user can maintain the connection until the user disconnects.

The host attribute specifies the hosts that can connect using TELNET, SSH, SFTP, and HTTP. The IP address can be a single address, two IP addresses with a hyphen in between them (range designation), or a list of these addresses separated by commas.

The multi-session attribute allows or prohibits multiple connections using TELNET, SSH or HTTP. Even if this attribute is set to off, multiple connections can be made through a same user name if the connection methods are different. Such connection examples are serial and TELNET or remote setup and SSH.

Even if the multi-session attribute is changed to off using this command against a user that already has multiple connections, the user can maintain the connection until the user disconnects.

SSH and SFTP connections cannot be allowed for anonymous users.

Multiple TELNET connections cannot be specified for anonymous users.

The timer value is taken to be 300 seconds for TELNET, SSH, SFTP, or HTTP connections even when the login-timer attribute is set to clear.

The **login timer** attribute value of this command takes precedence over the value set by the login timer command.

#### [Note]

Note that if this command is used to prohibit the connection of all users or prohibit all users from becoming administrators, you will not be able to change the router settings or check the router status.

#### [Models]

RTX810, RTX5000

## 4.9 Disconnect Another User Connection by Force

#### [Syntax]

```
disconnect user user [/connection [no]]
```

```
disconnect user [user]/connection [no]
```

#### [Setting and Initial value]

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

Setting	Description
telnet	Connection using TELNET
serial	Connection from the serial console
remote	Connection using remote setup
ssh	Connection using SSH
sftp	Connection using SFTP
http	Connection to the configuration GUI

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

#### [Description]

Disconnects other users' connections.

Specify the parameters by referring to the connection status shown by the **show status user** command.

To connect an anonymous user, use the second syntax with **user** omitted.

If a parameter is omitted, all connections that match the specified parameters are disconnected.

#### [Note]

This command cannot be used to disconnect your own session.

#### [Example]

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

```
# disconnect user test
```

Example 2) Disconnect all users connected using TELNET.

```
# disconnect user /telnet
```

**[Models]**

RTX810, RTX5000

## 4.10 Set the Security Class

**[Syntax]**

```
security class level forget [telnet]
```

```
no security class [level forget telnet]
```

**[Setting and Initial value]**

- *level*

- [Setting] :

Setting	Description
1	Allow login through serial, TELNET, SSH, and remote router.
2	Allow login from serial, TELNET, and SSH but not from a remote router.
3	Allow login only from serial.

- [Initial value] : 1

- *forget*

- [Setting] :

Setting	Description
on	Allow login with “w,lXlma” in place of the specified password and allow configuration changes. Serial connection only.
off	Allow login only when the password is entered.

- [Initial value] : on

- *telnet*

- [Setting] :

Setting	Description
on	Allow the use of the <b>telnet</b> command as a TELNET client.
off	Not allow the use of the <b>telnet</b> command.

- [Initial value] : off

**[Description]**

Sets the security class.

**[Note]**

The **remote setup accept** command can be used to place detailed access limits on logins from a remote router (**remote setup**). The login function from a remote router uses circuit switching or exclusive line. Therefore, this function is available only on models that can connect to them. If more than the specified number of users is connected when the setting is changed, the users that are already connected can maintain the connection. New connections are prohibited until the number of connected users falls below the specified number.

**[Models]**

RTX810, RTX5000

## 4.11 Set the Time Zone

**[Syntax]**

```
timezone timezone
```

```
no timezone [timezone]
```

**[Setting and Initial value]**

- *timezone* : Difference in the time of the region with respect to GMT.

- [Setting] :

Setting	Description
cct	China standard time (+08:00)
jst	Japan standard time (+09:00)
utc	GMT +(00:00)
Any hour: minute	Hour:minute (-12:00 to +11:59)

- [Initial value] : utc

**[Description]**

Sets the time zone.

**[Models]**

RTX810, RTX5000

## 4.12 Set the Current Date

---

**[Syntax]**

**date** *date*

**[Setting and Initial value]**

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

**[Description]**

Sets the current date.

**[Models]**

RTX810, RTX5000

## 4.13 Set the Current Time

---

**[Syntax]**

**time** *time*

**[Setting and Initial value]**

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

**[Description]**

Sets the current time.

**[Models]**

RTX810, RTX5000

## 4.14 Set the Clock through a Remote Host

---

**[Syntax]**

**rdate** *host* [syslog]

**[Setting and Initial value]**

- *host*
  - [Setting] :

Setting	Description
IP address	IP address of the remote host (xxx.xxx.xxx.xxx where xxx is a decimal number)
Name	Host name

- [Initial value] : -
- syslog : A keyword indicating that the output results are output to SYSLOG
- [Initial value] : -

**[Description]**

Synchronizes the router clock to the time on the host specified by the parameter.  
When this command is executed, a connection is made to TCP port 37 on the host.

**[Note]**

Yamaha router series series and many of the UNIX computers can be specified as a remote host.  
If the syslog keyword is specified, the output results of the command are output to SYSLOG at the INFO level.

**[Models]**

RTX810, RTX5000

## 4.15 Set the Clock Using NTP

---

**[Syntax]**

```
ntpdate ntp_server [syslog]
```

**[Setting and Initial value]**

- *ntp\_server*
  - [Setting] :

Setting	Description
IP address	IP address of the NTP server (xxx.xxx.xxx.xxx where xxx is a decimal number)
IPv6 address	IPv6 address of the NTP server (xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx where xxx is a hexadecimal number)
Name	NTP server name

- [Initial value] : -
- syslog : A keyword indicating that the output results are output to SYSLOG
  - [Initial value] : -

**[Description]**

Sets the router clock using NTP. When this command is executed, a connection is made to UDP port 123 on the host.

**[Note]**

When connected to the Internet, this command sets the clock more accurately than when the **rdate** command is used.  
It is better to specify an NTP server that is as close to the router as possible. Contact your provider for NTP servers that can be used.

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

**[Models]**

RTX810, RTX5000

## 4.16 Set the Source IP Address for Sending NTP Packets

---

**[Syntax]**

```
ntp local address ip_address
no ntp local address
```

**[Setting and Initial value]**

- *ip\_address*
  - [Setting] : IP address
  - [Initial value] : -

**[Description]**

Sets the source IP address for sending NTP packets.

If the source IP address is not set, the IP address of the output interface is used according to the normal UDP packet transmission rules.

**[Models]**

RTX810, RTX5000



## 4.17 Allow Time Synchronization with NTP Server on Stratum 0

---

### [Syntax]

```
ntp backward-compatibility comp
no ntp backward-compatibility [comp]
```

### [Setting and Initial value]

- *comp*
- [Setting] :

Setting	Description
accept-stratum-0	Allow time synchronization with the NTP server on stratum 0

- [Initial value] : -

### [Description]

Allows time synchronization with the NTP server on stratum 0.

### [Note]

An NTP server is not on stratum 0 unless it is synchronized with an external clock.

### [Models]

RTX810, RTX5000

## 4.18 Set the Console Prompt Display

---

### [Syntax]

```
console prompt prompt
no console prompt [prompt]
```

### [Setting and Initial value]

- *prompt*
- [Setting] : The start text string of the command prompt (up to 64 characters)
- [Initial value] : -

### [Description]

Sets the command prompt display. An empty text string can also be specified.

### [Models]

RTX810, RTX5000

## 4.19 Set the Console Language and Code

---

### [Syntax]

```
console character code
no console character [code]
```

### [Setting and Initial value]

- *code*
- [Setting] :

Setting	Description
ascii	Display in English using ASCII character codes
sjis	Display in Japanese using SJIS character codes
euc	Display in Japanese using EUC character codes

- [Initial value] : ascii

### [Description]

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

**[Note]**

The setting specified by this command is not applied to the configuration shown by the **show config** command until it is saved using the **save** command.

**[Models]**

RTX810, RTX5000

## 4.20 Set the Number of Characters Shown on the Console

---

**[Syntax]**

**console columns** *col*  
**no console columns** [*col*]

**[Setting and Initial value]**

- *col*
  - [Setting] : Number of characters shown on the console (80..200)
  - [Initial value] : 80

**[Description]**

Sets the number of characters shown per line on the console.  
 This command can also be executed by a general user.

**[Note]**

The setting specified by this command is not applied to the configuration shown by the **show config** command until it is saved using the **save** command.

**[Models]**

RTX810, RTX5000

## 4.21 Set the Number of Lines Shown on the Console

---

**[Syntax]**

**console lines** *lines*  
**no console lines** [*lines*]

**[Setting and Initial value]**

- *lines*
  - [Setting] :

Setting	Description
10..100	The number of lines
infinity	Does not stop the scrolling

- [Initial value] : 24

**[Description]**

Sets the number of lines shown on the console.  
 This command can also be executed by a general user.

**[Note]**

The setting specified by this command is not applied to the configuration shown by the **show config** command until it is saved using the **save** command.

**[Models]**

RTX810, RTX5000

## 4.22 Set Whether to Show System Messages on the Console

---

**[Syntax]**

**console info** *info*  
**no console info** [*info*]

**[Setting and Initial value]**

- *info*

- [Setting] :

Setting	Description
on	Show
off	Hide

- [Initial value] : off

**[Description]**

Sets whether to show system messages on the console.

**[Note]**

The display screen is disrupted when a system message occurs while entering a text string from a keyboard. However, the string that you are entering can be redisplayed by pressing [Ctrl]+r.

**[Models]**

RTX810, RTX5000

## 4.23 Set the IP Address of the Host Receiving the SYSLOG

---

**[Syntax]**

```
syslog host host
no syslog host [host]
```

**[Setting and Initial value]**

- *host*
  - [Setting] : IP address of the host receiving the SYSLOG (up to four locations can be specified by delimiting each location with a space)
  - [Initial value] : -

**[Description]**

Sets the IP address of the host receiving the SYSLOG.

The IP address can be IPv4 or IPv6 address.

If the **syslog debug** command is set to on, a great number of debug messages will be sent. Therefore, the host specified by this command should have efficient disk space for receiving the messages.

**[Models]**

RTX810, RTX5000

## 4.24 Set the SYSLOG Facility

---

**[Syntax]**

```
syslog facility facility
no syslog facility [facility]
```

**[Setting and Initial value]**

- *facility*
  - [Setting] :

Setting	Description
0..23	facility value
user	1
local0..local7	16..23

- [Initial value] : user

**[Description]**

Sets the SYSLOG facility.

**[Note]**

The facility numbers are to be defined by each SYSLOG server.

**[Models]**

RTX810, RTX5000

## 4.25 Set Whether to Output SYSLOGs of NOTICE Type

---

**[Syntax]**

**syslog notice** *notice*  
**no syslog notice** [*notice*]

**[Setting and Initial value]**

- *notice*
- [Setting] :

Setting	Description
on	Output
off	Not output

- [Initial value] : off

**[Description]**

Sets whether to output SYSLOGs of packet information detected by various filter functions.

**[Models]**

RTX810, RTX5000

## 4.26 Set the Output of SYSLOG of INFO Type

---

**[Syntax]**

**syslog info** *info*  
**no syslog info** [*info*]

**[Setting and Initial value]**

- *info*
- [Setting] :

Setting	Description
on	Output
off	Output but send no information to the SYSLOG host

- [Initial value] : on

**[Description]**

Sets the output of SYSLOGs related to the router operating status.

**[Note]**

The router stores the INFO type logs regardless of on/off of the *info* parameter. Sending to the host specified by the **syslog host** command is executed only when the *info* parameter is on.

**[Models]**

RTX810, RTX5000

## 4.27 Set Whether to Output SYSLOGs of DEBUG Type

---

**[Syntax]**

**syslog debug** *debug*  
**no syslog debug** [*debug*]

**[Setting and Initial value]**

- *debug*
- [Setting] :

Setting	Description
on	Output
off	Not output

- [Initial value] : off

**[Description]**

Sets whether to output SYSLOGs of DEBUG information of the router.

**[Note]**

When the *debug* parameter is turned on, a great number of debug messages is sent. Therefore, provide sufficient disk space on the host specified by the **syslog host** command, and turn debug off as soon as the necessary data is obtained.

**[Models]**  
RTX810, RTX5000

## 4.28 Set the Source IP Address for Sending SYSLOG

---

**[Syntax]**

**syslog local address** *address*  
**no syslog local address** [*address*]

**[Setting and Initial value]**

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

**[Description]**

Sets the source IP address for sending SYSLOG packets. If the source IP address is not set, the IP address of the output interface is used according to the normal UDP packet transmission rules.

**[Models]**  
RTX810, RTX5000

## 4.29 Set the Source Port Number for SYSLOG Packets

---

**[Syntax]**

**syslog sreport** *port*  
**no syslog sreport** [*port*]

**[Setting and Initial value]**

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

**[Description]**

Sets the source port number for the SYSLOG packets that the router sends.

**[Models]**  
RTX810, RTX5000

## 4.30 Set Whether to Output Executed Commands to the SYSLOG

---

**[Syntax]**

**syslog execute command** *switch*  
**no syslog execute command** [*switch*]

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Record executed commands in the log.
off	Do not record executed commands in the log.

- [Initial value] : off

**[Description]**

Sets whether to output executed commands to the SYSLOG.

**[Note]**

When a command is successfully executed, the input of that command is output to the log.

**[Models]**  
RTX810, RTX5000

## 4.31 Turn the TELNET Server Function ON/OFF

---

**[Syntax]**

**telnetd service** *service*  
**no telnetd service**

**[Setting and Initial value]**

- *service*
- [Setting] :

Setting	Description
on	Enable the TELNET server function
off	Disable the TELNET server function

- [Initial value] : on

**[Description]**

Enables or disables the TELNET server function.

**[Note]**

If the TELNET server is disabled, the TELNET server does not respond to access requests at all.

**[Models]**

RTX810, RTX5000

## 4.32 Set the Listen Port of the TELNET Server Function

---

**[Syntax]**

```
telnetd listen port
no telnetd listen
```

**[Setting and Initial value]**

- *port*
  - [Setting] : Listen port number of the TELNET server function (1..65535)
  - [Initial value] : 23

**[Description]**

Selects the listen port of the TELNET server function.

**[Note]**

The telnetd listens to TCP port 23, but the listen port can be changed with this command. If you change the listen port, you must use a TELNET client that can negotiate TELNET options even when the port number is changed.

**[Models]**

RTX810, RTX5000

## 4.33 Set the IP Address of the Host Allowed to Access the TELNET Server

---

**[Syntax]**

```
telnetd host ip_range [ip_range...]
no telnetd host
```

**[Setting and Initial value]**

- *ip\_range* : A list of IP address ranges of hosts allowed to access the TELNET server or a mnemonic
  - [Setting] :

Setting	Description
An IP address, two IP addresses with a hyphen in between them (range designation), or a list containing these addresses	Allow access from a specified host
any	Allow access from all hosts
none	Prohibit access from all hosts
LAN interface name	Allow connection of a specified interface only
Bridge interface name	Allow connection of a specified interface only

- [Initial value] : any

**[Description]**

Sets the IP address of the host allowed to access the TELNET server.

**[Note]**

A mnemonic cannot be placed in a list.

The setting is applied to subsequent TELNET connections after the change.  
RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

### 4.34 Set the Number of Users That Can Connect Simultaneously to the TELNET Server

---

**[Syntax]**

**telnetd session** *num*  
**no telnetd session**

**[Setting and Initial value]**

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

**[Description]**

Sets the number of users that can connect simultaneously to TELNET.

**[Note]**

If more than the specified number of users is connected when the setting is changed, the users that are already connected can maintain the connection. New connections are prohibited until the number of connected users falls below the specified number.

**[Models]**

RTX810, RTX5000

### 4.35 Setting the temperature monitoring threshold

---

**[Syntax]**

**system temperature threshold** *t1 t2*  
**no system temperature threshold** [*t1* [*t2*]]

**[Setting and Initial value]**

- *t1*
  - [Setting] : Temperature at which warning is generated (0..100 °C)
  - [Initial value] :
    - 70 (RTX5000)
    - 80 (for models not listed above)
- *t2*
  - [Setting] : Temperature at which warning is canceled (0..100 °C)
  - [Initial value] :
    - 65 (RTX5000)
    - 75 (for models not listed above)

**[Description]**

The internal temperature of the main unit is monitored, and if the temperature is *t1* or higher, warnings are generated via the SYSLOG and ALM lamp. Once the alarm has been triggered, the ALM lamp will remain illuminated until the temperature drops below *t2*.

**[Models]**

RTX5000

### 4.36 Set the Fast Path Function

---

**[Syntax]**

**ip routing process** *process*  
**no ip routing process**

**[Setting and Initial value]**

- *process*
  - [Setting] :

Setting	Description
fast	Use the fast path function.

Setting	Description
normal	Not use the fast path function and process all packets using normal path.

- [Initial value] : fast

**[Description]**

Sets whether to process the packet transfer using the fast path function or normal path function.

**[Note]**

There are no limitations on the functions that can be used with fast path. However, packets may be processed using normal path depending on the type of packets being handled.

**[Models]**

RTX810, RTX5000

### 4.37 Set the LAN Interface Operation

---

**[Syntax]**

```
lan shutdown interface [port...]
no lan shutdown interface [port...]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *port*
  - [Setting] : Port number (only on models with an internal switching hub)
  - [Initial value] : -

**[Description]**

Disables the LAN interface. Link is not established even when the LAN cable is connected on the LAN interface or the port on the switching hub specified by this command.

**[Models]**

RTX810, RTX5000

### 4.38 Set Whether to Obtain the Number of Reception Overflows in HUB IC

---

**[Syntax]**

```
lan count-hub-overflow switch [interval]
no lan count-hub-overflow [switch [interval]]
```

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Periodically obtain the number of reception overflows in HUB IC
off	Do not obtain the number of reception overflows in HUB IC

- [Initial value] : on
- *interval*
  - [Setting] : Time interval at which to obtain the number of reception overflows [seconds] (1..65535)
  - [Initial value] : 120

**[Description]**

Sets whether or not to periodically obtain the number of reception overflows in HUB IC.

**[Note]**

You can lighten the load from accessing the HUB IC by setting a large value for *interval* or setting *switch* to off.

Regardless of the settings on this command, the number of reception overflows in HUB IC is obtained when the **show status lan** command is executed.

**[Models]**

RTX810



## 4.39 Set How Long after Linkup through the LAN Interface to Wait before Sending

### [Syntax]

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

### [Setting and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *time*
  - [Setting] : Send wait time in seconds (0..10)
  - [Initial value] : 0 (no wait)

### [Description]

Set the amount of time after linkup to wait before sending, and restrain packet transmission. Packets whose transmission has been delayed are stored in a queue and sent after the specified amount of time has passed since linkup. The length of the queue that the packets are saved to is specified by the **queue interface length** command.

### [Note]

After linkup, if packets such as Gratuitous ARP or IPv6 neighbor solicitation packets are transmitted but the transmission is too fast and the target device is not able to receive the packets, set this wait time appropriately to delay transmission so that the target device can receive the packets.

### [Models]

RTX810, RTX5000

## 4.40 Set the Port Mirroring Function

### [Syntax]

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

### [Setting and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *mirror*
  - [Setting] : Port number from which to send the mirroring packets
  - [Initial value] : -
- *direction* : Direction of the monitored packets
  - [Setting] :

Setting	Description
in	In direction
out	Out direction

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

### [Description]

Sets the function that enables the communication on a certain port to be monitored on another port on the switching hub interface.

Only the interfaces that have a switching hub can be specified for the LAN interface name.

### [Note]

This function cannot be used simultaneously with the LAN division function.

The transmission rate of the packets delivered from the mirroring port must not exceed the line speed. If all of the mirroring packets cannot be output from the mirroring port, it may affect the communication between other ports.

**[Example]**

Example 1) Monitor the received packets of port 1 on port 4

```
# lan port-mirroring lan1 4 in 1
```

Example 2) Monitor the transmitted/received packets of port 1 and transmitted packets of port 2 on port 4

```
# lan port-mirroring lan1 4 in 1 out 1 2
```

**[Models]**

RTX810, RTX5000

## 4.41 Set the Operation Type of the LAN Interface

**[Syntax]**

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

```
lan type interface_with_swhub option=value
```

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

```
lan type interface_without_swhub option=value
```

```
no lan type interface [...]
```

**[Setting and Initial value]**

- *interface\_with\_swhub*
  - [Setting] : Name of the LAN interface with a switching hub
  - [Initial value] : -
- *interface\_without\_swhub*
  - [Setting] : Name of the LAN interface without a switching hub
  - [Initial value] : -
- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *speed* : LAN speed and operation mode
  - [Setting] :

Setting	Description
auto	Auto speed detection
1000-fdx	Full duplex 1000BASE-T
100-fdx	Full duplex 100BASE-TX
100-hdx	Half duplex 100BASE-TX
10-fdx	Full duplex 10BASE-T
10-hdx	Half duplex 10BASE-T
Omitted	auto if omitted.

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

Setting	Description
on	Enable the auto crossover function

Setting	Description
off	Disable the auto crossover function

- macaddress-aging
  - MAC address aging function

Setting	Description
Number of seconds	Aging time
on	Enable the MAC address aging function
off	Disable the MAC address aging function

- port-based-ks8995m/port-based-option
  - LAN division function and port division function

Setting	Description
divide-network	Enable the LAN division function
split-into-split_pattern	Enable the port division function (normal function)
X1,X2,X3,X4 (X1..X4 is a series of numbers 1..4 with a "+" or "-" added at the end)	Enable the port division function (enhanced function)
off	Disable the LAN division and port division functions

- speed-downshift
  - Speed-downshift function

Setting	Description
on	Enable the speed-downshift function
off	Disable the speed-downshift function

- [Initial value] :
  - mtu=1500
  - auto-crossover=on
  - macaddress-aging=300
  - port-based-option=off
  - speed-downshift=on

### [Description]

Sets the speed, the operation mode, and optional functions of the specified LAN interface.

The speed and operation mode can be specified for each port on a LAN interface with a switching hub.

#### ○ *mtu*

Specifies the maximum data length that can be transmitted or received through the interface. The data length does not include the MAC header and FCS. The tag length (4 bytes) for Tag VLAN is also not included.

The data length range that can be specified will differ depending on the LAN interface. For LAN interfaces that do not support jumbo frames, the data length range will be 64~1500. For LAN interfaces that support jumbo frames, the range is as follows:

Model	Interface	Selectable Range
RTX5000	LAN1, LAN2, LAN3, LAN4	64~9578

If the *mtu* of the interface is specified but the setting of the **ip mtu** command or the **ipv6 mtu** command is not specified (default value), the *mtu* of the interface is used for the *mtu* of IPv4 or IPv6. On the other hand, if the setting of the **ip mtu** command or the **ipv6 mtu** command is specified, the setting of the **ip mtu** command or the **ipv6 mtu** command is used as *mtu*, regardless of whether the *mtu* of the interface is specified. If none of the settings is specified, including the *mtu* of the interface, the default value of 1500 is used.

#### ○ Auto crossover function

This function automatically detects whether the LAN cable is a straight cable or a crossover cable and makes the connection accordingly. Enabling this function frees you from worrying about the cable type.

#### ○ MAC address aging function

This function can be used on LAN interfaces with a switching hub.

This function clears, at a given interval, the MAC address table entries that the switching hub stores. When this function is turned off, the MAC addresses stored by the switching hub are not cleared automatically. Moreover, the entries are not cleared even if the **clear switching-hub macaddress** command is executed. The entries are cleared only when this function is turned back on.

You can specify the number of seconds for the setting. However, there may be some margin of error between the command setting and the actual time until deletion.

Model	Selectable Range
RTX5000	1-3825
RTX810	1-3551

On models that support specifying the value in seconds, turning it on will convert it to an initial value of 300.

The size of the MAC address table is indicated below.

Model	Maximum Number of Entries
RTX5000	8192
RTX810	1024

#### o LAN division function

This function can be used on LAN interfaces with a switching hub.

There are two LAN division functions: Normal and enhanced.

In the normal LAN division function, each of the ports on the switching hub operates as a separate LAN interface. Separate IP addresses can be assigned to each interface, and routing among the interfaces is also possible. For example, the RTX810 normally has two LAN interfaces, but using the LAN division function allows five LAN interfaces to be used.

In the enhanced LAN division function, you can arrange the ports on the switching hub freely to make a single LAN interface (VLAN interface). Ports that belong to the same VLAN interface operate as switches.

The interface names that are used in LAN division are different between the normal and enhanced functions.

The name of the LAN interfaces created using the normal function is expressed as the original LAN interface name with a period and the port number.

For example, in the RTX810, lan1 is a LAN interface with a four-port switching hub, so the following LAN interfaces can be used:

Port Number	Interface Name
1	lan1.1
2	lan1.2
3	lan1.3
4	lan1.4

With the enhanced function, you can name the VLAN interfaces vlan1, vlan2, vlan3, and so on. Unlike the interfaces created with the normal function, the VLAN interfaces created with the enhanced function are not associated with specific ports. You can change the division method freely by using the **vlan port mapping** command to specify which VLAN interface each port on the switching hub belongs to.

The number of VLAN interfaces that can be used simultaneously varies by model, as indicated in the table below:

Model	Configurable VLAN Interfaces
RTX5000	vlan1-vlan4 (LAN1), vlan5-vlan8 (LAN2)
RTX810	vlan1-vlan4

When you enable the LAN division function, the settings that apply to the lan1 interface are inherited to lan1.1 (normal function) or vlan1 (enhanced function).

The LAN interfaces' MAC addresses used in LAN division are the same as the original LAN interfaces' MAC addresses. Therefore, the MAC addresses for lan1.1-lan1.4 and vlan1-vlan4 in the above example are all the same as lan1.

#### ○ Port division function

Normally, each port of a switching hub can communicate with other ports without any limitation. Using the port division function, you can restrict communication between ports.

There are two port division functions: Normal and enhanced. With the normal function, communication through the router is possible while restricting communication between ports. With the enhanced function, you can restrict communication from the specified port through the router.

With the normal function, you can divide the ports into groups, and allow communication within the group and other routers, while restricting communication with ports belonging to other groups.

In contrast to the LAN division function, the port division function does not cause the number of LAN interfaces to change. The divided ports are all considered to be part of the same LAN interface, and they share the same IP address.

To specify the port division pattern, insert colons between the port numbers that you want to divide. Examples are given below:

If the number of ports on the switching hub is 4:

split_pattern	Port				Description
	1	2	3	4	
1 : 234	↔	←	→	→	Port 1 and other ports
1 : 2 : 34	↔	↔	←	→	Ports 1, 2, and other ports
1 : 2 : 3 : 4	↔	↔	↔	↔	Divide all ports

On the same LAN interface, communication between the network of the primary address and the network of the secondary address passes through the router, so communication with other groups is possible.

In the enhanced function, by specifying the port to which you want the packets received at each port to be transferred, you can restrict communication between specific ports or with and through the router itself. Specifically, it is set up as follows:

```
lan type lan1 port-based-option=X1,X2,X3,X4
```

In Xn (n = 1..4), list the port numbers to which you want to transfer the packets received at port n, and append a "+" to the end to allow communication with and through the router, or "-" to disallow it. Note, "+" can be omitted.

If you specify "-", the packets received at that port will not be routed. Moreover, any device connected to that port will not be able to communicate with the router.

For example, in the following setup, the packets received at ports 1 - 3 are transferred to port 4 and the router; and although the packets received at port 4 is transferred to ports 1 - 3, they will not be transferred to the router. That is, the ports are divided into three groups - ports 1 and 4, ports 2 and 4, and ports 3 and 4. Ports 1 - 3 cannot communicate to each other, but only with port 4. Moreover, although ports 1 - 3 can communicate with the router, port 4 cannot communicate with the router, and the packets received are also not routed.

```
lan type lan1 port-based-option=4,4,4,123-
```

#### ○ Speed-downshift function

When set to "on", this function tries to establish a link at a reduced speed, when a cable that does not support 1000BASE-T is connected.

#### [Note]

After the execution of this command, the setting takes effect after the LAN interface is automatically reset.

#### [Example]

1. On a LAN interface with a switching hub, connect ports 1 and 2 at full duplex 100BASE-TX, and other ports using auto negotiation.

```
# lan type lan1 100-fdx 1 2
```

2. On a LAN interface with a switching hub, connect port 1 at full duplex 100BASE-TX, and other ports using auto negotiation, and use the LAN division function.

```
# lan type lan1 100-fdx 1 port-based-option=divide-network
```

- On a LAN interface with a switching hub, connect all ports using auto negotiation. Divide ports using the port division function.
  - Dividing ports 1, 2, 3, and 4 on a four-port switching hub

```
# lan type lan1 port-based-option=split-into-12:3:4
```

- On LAN1, jumbo frames (9000 bytes) can be used.

```
# lan type lan1 auto mtu=9000
```

#### [Models]

RTX810, RTX5000

## 4.42 Set Static Link Aggregation

---

### [Syntax]

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

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

### [Setting and Initial value]

- link\_id*
  - [Setting] : Link ID (1..10)
  - [Initial value] : -
- interface*
  - [Setting] : LAN interface having switching-hub
  - [Initial value] : -
- port*
  - [Setting] : Aggregation port number(s)
  - [Initial value] : -

### [Description]

Aggregates the physical links from multiple ports within the LAN interface of a switching hub and creates 1 logical link. The multiple LAN cables that are connected to the aggregated ports will be treated as 1 virtual LAN cable. In addition, among the aggregated ports, the port that actually outputs the packet is based upon the packet's receiving MAC address and sending MAC address.

Ports that belong to the same LAN interface can be aggregated. One port cannot be made subordinate to multiple logical links (multiple link IDs).

The MAC addresses learned by the aggregated ports are shared by all the ports associated with the same logical link, and normally the largest port number is saved in the MAC address table. This is the same even when the physical link for the largest port number is down. Because of this, using the **show status switching-hub macaddress** command will show the MAC addresses summarized in the largest port number column. Similar to the port number displayed by the **show arp** command and in the ARP log, when the learned MAC address ports are aggregated, it is usually the largest port number.

This can be used in conjunction with the LAN distribution feature, port separation feature and port mirroring feature. However, if the LAN distribution feature and port separation feature are used together, only ports that are attributed to the same segment of the the distributed or separated switch port can be aggregated.

### [Note]

To prevent packet loops, it is best to set up link aggregation in advance (including setting the link peer device) before connecting the LAN cables.

### [Example]

- Aggregate LAN1 Port 1 and Port 2

```
# lan link-aggregation static 1 lan1:1 lan1:2
```

- Aggregate LAN1 Port 3 and Port 4

```
# lan link-aggregation static 2 lan1:3 lan1:4
```

- Aggregate 4 ports on LAN2.

```
# lan link-aggregation static 3 lan2:1 lan2:2 lan2:3 lan2:4
```

#### [Models]

RTX5000

## 4.43 Set the Login Timer

---

### [Syntax]

**login timer** *time*  
**no login timer** [*time*]

### [Setting and Initial value]

- *time*
- [Setting] :

Setting	Description
120..21474836	The Number of seconds for automatically logging out when there is no key input
clear	Disable the login timer

- [Initial value] : 300

### [Description]

Sets the time for automatically logging out when there is no key input.

### [Note]

When logged in using TELNET or SSH, the timer value is handled as 300 seconds even if clear is specified.

### [Models]

RTX810, RTX5000

## 4.44 Set the IP Address of the Host Allowed to Access the Router Using TFTP

---

### [Syntax]

**tftp host** *host*  
**no tftp host** [*host*]

### [Setting and Initial value]

- *host*
- [Setting] :

Setting	Description
IP address	IP address (IPv6 addresses allowed) of the host allowed to access the router using TFTP
any	Allow access from all hosts using TFTP
none	Not allow access from any host using TFTP

- [Initial value] : none

### [Description]

Sets the IPv4 or IPv6 address of the host that is allowed to access the router using TFTP.

### [Note]

For security reasons, set the command to none as soon as the firmware is updated or the reading or writing of the configuration file is finished.

### [Models]

RTX810, RTX5000

## 4.45 Set Whether to Relay Magic Packets to the LAN

---

### [Syntax]

**ip interface wol relay** *relay*  
**no ip interface wol relay**

### [Setting and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *relay*

- [Setting] :

Setting	Description
broadcast	Relay Magic Packets as broadcast packets
unicast	Relay Magic Packets as unicast packets
off	Not check for Magic Packets

- [Initial value] : off

#### [Description]

Relays Magic Packets that have been constructed as IPv4 packets assigned to directed broadcast that have been transmitted from a remote location to the specified LAN interface. The destination IP address of the IPv4 packet must be addressed to a directed broadcast of the specified LAN interface.

If broadcast or unicast specified, the router checks the contents of the received packets and relays the packet 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 router extracts the MAC address from the Magic Packet data sequence, and sends the packet as a unicast packet with the source MAC address set to the extracted address.

If off is specified, the router does not check whether the packet is a Magic Packet.

#### [Note]

In all cases, the packet that is not relayed as a Magic Packet is processed based on the settings of the **ip filter directed-broadcast** command.

#### [Models]

RTX810, RTX5000

## 4.46 Set the Interface or System Description

---

#### [Syntax]

**description** *id description*

**no description** *id [description]*

**description** *interface description*

**no description** *interface [description]*

#### [Setting and Initial value]

- *id*
  - [Setting] : An ID used for the description of the entire system (1..21474836)
  - [Initial value] : -
- *interface*
  - [Setting] : The LAN interface name, WAN interface name, 'pp' or 'tunnel'
  - [Initial value] : -
- *description*
  - [Setting] : The text of the description (Up to 64 ASCII characters or 32 SJIS characters)
  - [Initial value] : -

#### [Description]

Sets the description of the entire system or the description of the interface.

The settings made with this command are just descriptions, they do not affect operation.

For the system as a whole, you can specify a multi-line description by changing the ID number.

Interface descriptions are limited to one line.

If the *interface* is set to 'pp' or 'tunnel', the description corresponds to the interface selected with **pp select** or **tunnel select**.

You can show the settings by using the **show config** command. Also, you can show the settings that have been configured for the interface by using the **show status** command.

When you execute the **show config** command, the description of the system as a whole appears before all other settings, with the lines ordered by ID number.

In the description, you can use ASCII characters or SJIS Japanese characters (except for half-width katakana). However, Japanese characters can only be specified and displayed properly when console character is set to sjis. When any other setting is selected, the Japanese characters may be garbled.



**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 4.47 Set Whether to Output the Syslog at the TCP Connection Level

**[Syntax]**

```
tcp log switch [src_addr[/mask] [dst_addr[/mask]] [tcpflag[src_port_list [dst_port_list]]]]
```

```
no tcp log [...]
```

**[Setting and Initial value]**• *switch*

- [Setting] :

Setting	Description
on	Output the syslog of the TCP connection
off	Not output the syslog of the TCP connection

- [Initial value] : off

• *src\_addr* : Source IP address

- [Setting] :

- xxx.xxx.xxx.xxx is
  - A decimal number
  - \* (the 8 bits corresponding to the net mask are zeroes)
- Two of the above items with a hyphen in between them, an above item with a hyphen in front, and an above item with a hyphen in the back indicate a range.
- \* (all IP addresses)

- [Initial value] : -

• *dst\_addr* : Destination IP address

- [Setting] :

- same format as *src\_addr*
- Same as one \* when omitted

- [Initial value] : -

• *mask* : Bit mask of the IP address. Can be specified only when *src\_addr* and *dst\_addr* are network addresses.

- [Setting] :

- Hexadecimal form such as “0xfffff00”
- Bit number form such as “/24”
- 0xffffffff when omitted.

- [Initial value] : -

• *tcpflag* : Type of TCP packets to be filtered

- [Setting] :

- Decimal indicating the protocol (6 only)
- Mnemonic indicating the protocol

Mnemonic	A decimal number	Description
tcp	6	All TCP packets
tcpsyn	-	Packets with SYN flag set
tcpfin	-	Packets with FIN flag set
tcprst	-	Packets with RST flag set
established	-	Packets with ACK flag set

- tcpflag=flag\_value/flag\_mask or tcpflag!=flag\_value/flag\_mask

- flag\_value and flag\_mask: Hexadecimal form
- Reference Flag Values

0x0001	FIN
--------	-----

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

- \*(All TCP packets. The same as when tcp is specified for the mnemonic)
- Same as \* when omitted.
- [Initial value] : -
- *src\_port\_list* : TCP source port number
- [Setting] :
  - A decimal number representing the port number and type
  - Mnemonic representing the 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
ntp	123
nntp	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540
submission	587

- Two of the above items with a hyphen in between them, an above item with a hyphen in front, and an above item with a hyphen in the back indicate a range.
- Series of above items delimited by commas (up to 10 items)
- \* (all ports or types)
- Same as \* when omitted.
- [Initial value] : -
- *dest\_port\_list* : TCP destination port number
  - [Setting] : Same format as *src\_port\_list*.
  - [Initial value] : -

#### [Description]

Outputs the TCP syslog. The **syslog debug on** command must also be specified. Supports IPv4 only. We recommend this function to be used temporarily such as when troubleshooting, because it puts stress on the system.

**[Example]**

```
tcp log on * * tcpsyn * 1723 (Whether SYN coming to the PPTP port)
tcp log on * * tcpflag!=0x0000/0x0007 (TCP packet with FIN, RST, and SYN set)
tcp log on (All TCP packets Same as tcp log on * * * * *)
```

**[Models]**

RTX810, RTX5000

## 4.48 Set Whether to Allow HTTP Revision Update

---

**[Syntax]**

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

**[Setting and Initial value]**

- *permit*
- [Setting] :

Setting	Description
on	Permit
off	Prohibit

- [Initial value] : on

**[Description]**

Sets whether to allow HTTP revision update.

**[Note]**

This command affects the direct HTTP revision update using a command, the update using the easy setup page, and update using the DOWNLOAD button.

**[Models]**

RTX810

## 4.49 Set the URL for the HTTP Revision Update

---

**[Syntax]**

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

**[Setting and Initial value]**

- *url*
- [Setting] : Set the URL where the firmware is located
- [Initial value] : [http://www.rtpro.yamaha.co.jp/firmware/revision-up/\(model name\).bin](http://www.rtpro.yamaha.co.jp/firmware/revision-up/(model name).bin)

**[Description]**

Set the URL where the firmware for the HTTP revision update is located.

The syntax is “http://IP address of the server or host name/path”.

If the port number of the server is not 80, you must specify it in the URL as in “http://IP address of the server or host name:port number/path”.

**[Models]**

RTX810

## 4.50 Set the Proxy Server for HTTP Revision Update

---

**[Syntax]**

```
http_revision-up_proxy proxy_server [port]
no http_revision-up_proxy [proxy_server [port]]
```

**[Setting and Initial value]**

- *proxy\_server*
  - [Setting] : Proxy server to be used during HTTP revision update
  - [Initial value] : -
- *port*
  - [Setting] : Proxy server port number

- [Initial value] : -

**[Description]**

Specify the host name or the IP address and port number of the Proxy server.

**[Models]**

RTX810

## 4.51 Set the HTTP Revision Update Timeout

---

**[Syntax]**

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

**[Setting and Initial value]**

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

**[Description]**

Sets the timeout value of the HTTP revision update procedure.

**[Models]**

RTX810

## 4.52 Set Whether to Allow Downgrade

---

**[Syntax]**

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

**[Setting and Initial value]**

- *permit*
  - [Setting] :

Setting	Description
on	Allow downgrading of the firmware to an older revision
off	Prohibit downgrading of the firmware to an older revision

- [Initial value] : off

**[Description]**

Sets whether to allow the firmware to be downgraded to a lower revision using the HTTP update function.

**[Models]**

RTX810

## 4.53 Set Whether to Allow Updating Using the DOWNLOAD Button

---

**[Syntax]**

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

**[Setting and Initial value]**

- *permit*
  - [Setting] :

Setting	Description
on	Allow updating using the DOWNLOAD button
off	Prohibit updating using the DOWNLOAD button

- [Initial value] : off

**[Description]**

Sets whether to allow the firmware to be updated using the DOWNLOAD button.

**[Note]**

The update function conforms to the HTTP update function.

If this command is set to off when the STATUS lamp is indicating an error, the error indication is cleared.

**[Models]**

RTX810

## 4.54 Revision Update Schedule

---

**[Syntax]**

**http revision-up schedule** *period time1 time2*

**no http revision-up schedule** [*period time1 time2*]

**[Setting and Initial value]**

- *period* : Sets the schedule at which the router tries to update the firmware.

- [Setting] :

Setting	Description
daily	daily
weekly <i>day</i>	weekly DAY Use <i>day</i> to specify the day of the week. You can set it to: sun,mon,tue,wed,thu,fri,sat
monthly <i>date</i>	monthly DATE Set <i>date</i> to a value between 1 and 31 within the month.

- [Initial value] : -
- *time1,time2* : Sets the time at which the router tries to update the firmware.
  - [Setting] : Specify *time1* and *time2* in 24-hour notation with an HH:MM format.
  - [Initial value] : -

**[Description]**

Sets the schedule at which the router tries to update the firmware.

You can use *period* to specify the period at which the router tries to update the firmware. You can set the period to daily, weekly, or monthly. You have to set the day of the week for weekly and the day of the month for monthly.

The router will not try to update the firmware if day specified for monthly does not exist in the current month. For example, if you specify 'monthly 31', the router will not try to update the firmware in months that do not have a 31st day: February, April, June, September, and November.

You can use *time1* and *time2* to set the time at which the router tries to update the firmware. The router will attempt to update the firmware once at a random time between *time1* and *time2*. If the firmware update fails, the router will not try to update the firmware again until the next day, week, or month.

When the time specified for *time1* is later than the time specified for *time2*, *time2* is interpreted as the time one day later.

If HTTP update is prohibited by the **http revision-up permit** command, the firmware is never updated.

If downgrading is permitted by the **http revision-down permit** command, the firmware is overwritten even when the firmware on the WEB server is older than the current firmware.

If the firmware on the WEB server and the current firmware are of the same revision, the firmware is not overwritten.

**[Example]**

```
http revision-up schedule daily 23:00 02:00 # Revision is performed daily at a time between 23:00 and 2:00 the next day.
http revision-up schedule weekly sun 12:00 13:00 # Revision is performed on Sundays at a time between 12:00 and 13:00.
http revision-up schedule monthly 1 23:00 0:00 # Revision is performed on the first of each month at a time between 23:00
and 24:00.
```

**[Models]**

RTX810

## 4.55 Turn the SSH Server Function ON/OFF

---

**[Syntax]**

**sshd service** *service*

**no sshd service** [*service*]

**[Setting and Initial value]**

- *service*
- [Setting] :

Setting	Description
on	Enable the SSH server function
off	SSHDisable the TELNET server function

- [Initial value] : off

**[Description]**

Enables or disables the SSH server function.

**[Note]**

If the SSH server is disabled, the SSH server does not respond to access requests at all.

**[Models]**

RTX810, RTX5000

## 4.56 Set the Listen Port of the SSH Server Function

---

**[Syntax]**

**sshd listen** *port*

**no sshd listen** [*port*]

**[Setting and Initial value]**

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

**[Description]**

Selects the listen port of the SSH server function.

**[Note]**

The SSH server listens to TCP port 22, but the listen port can be changed with this command.

**[Models]**

RTX810, RTX5000

## 4.57 Set the IP Address of the Host Allowed to Access the SSH Server

---

**[Syntax]**

**sshd host** *ip\_range* [*ip\_range* ...]

**no sshd host** [*ip\_range*...]

**[Setting and Initial value]**

- *ip\_range* : A list of IP address ranges of hosts allowed to access the SSH server or a mnemonic
- [Setting] :

Setting	Description
An IP address, two IP addresses with a hyphen in between them (range designation), or a list containing these addresses	Allow access from a specified host
any	Allow access from all hosts
none	Prohibit access from all hosts
LAN interface name	LAN interface name allowed to access to the SSH server
Bridge interface name	The bridge interface name to allow access to SSH server

- [Initial value] : any

**[Description]**

Sets the IP address of the host allowed to access the SSH server.

**[Note]**

A mnemonic cannot be placed in a list.  
The setting is applied to subsequent SSH connections after the change.

**[Models]**

RTX810, RTX5000

## 4.58 Set the Number of Users That Can Connect Simultaneously to the SSH Server

---

**[Syntax]**

```
ssh session num
no ssh session [num]
```

**[Setting and Initial value]**

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

**[Description]**

Sets the number of users that can connect simultaneously to SSH.

**[Note]**

If more than the specified number of users is connected when the setting is changed, the users that are already connected can maintain the connection. New connections are prohibited until the number of connected users falls below the specified number.

**[Models]**

RTX810, RTX5000

## 4.59 Set the SSH Server Host Key

---

**[Syntax]**

```
ssh host key generate [seed]
no ssh host key generate [seed]
```

**[Setting and Initial value]**

- *seed*
  - [Setting] : A number used to generate the host key (0..4294967295)
  - [Initial value] : -

**[Description]**

Sets the SSH server host key.

If *seed* is omitted, a random number is used to generate the key.

**[Note]**

This command must be executed in advance to generate the host key when using the SSH server function.

Since the host key generated by a *seed* is unique, different values should be assigned for each router.

If this command is executed when the host key is already set, the router asks the user whether the host key is to be updated.

The host key generation may take 30 seconds to a minute depending on the model.

If the setting is retrieved using TFTP, the keys are stored in the format **ssh host key generate** *seed* KEY1 KEY2. KEY1 and KEY2 are encrypted character strings of the RSA secret key and DSA secret key, respectively. The keys are encrypted using a router-specific method. If the stored settings are applied to other routers, the character strings are not the same as the entered KEY1 and KEY2. This is because the host key is generated from the *seed* and stored using a router-specific encryption.

**[Models]**

RTX810, RTX5000

## 4.60 Set the Encryption Algorithms That the SSH Server Can Use

---

**[Syntax]**

```
ssh encrypt algorithm [algorithm ...]
no ssh encrypt algorithm [...]
```

**[Setting and Initial value]**

- *algorithm* : Encryption algorithm (you can specify more than one algorithm by delimiting them with spaces)
  - [Setting] :

Setting	Description
aes128-ctr	AES128-CTR
aes192-ctr	AES192-CTR
aes256-ctr	AES256-CTR
aes128-cbc	AES128-CBC
aes192-cbc	AES192-CBC
aes256-cbc	AES256-CBC
3des-cbc	3DES-CBC
blowfish-cbc	Blowfish-CBC
cast128-cbc	CAST-128-CBC
arcfour	Arcfour

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

#### [Description]

Sets the encryption algorithms that the SSH server can use.

The list of algorithms that you specify for *algorithm* is proposed to the client when an SSH connection is established.

#### [Models]

RTX810, RTX5000

## 4.61 Check Whether the SSH Client Is Alive

#### [Syntax]

**ssh client alive** *switch* [*interval* [*count*]]

**no ssh client alive** [*switch* ...]

#### [Setting and Initial value]

- *switch*
- [Setting] :

Setting	Description
on	Check whether the client is alive
off	Does not check whether the client is alive

- [Initial value] : off
- *interval*
  - [Setting] : Transmission interval in seconds (1..2147483647)
  - [Initial value] : 100
- *count*
  - [Setting] : Retry count (1..2147483647)
  - [Initial value] : 3

#### [Description]

Sets whether to check whether the client is alive.

A message requesting a response is sent to the client at the specified *interval*. If there is no response after the specified retry *count*, the connection and the session are terminated.

#### [Models]

RTX810, RTX5000

## 4.62 Set the IP Address of the Host Allowed to Access the SFTP Server

#### [Syntax]

**sftpd host** *ip\_range* [*ip\_range* ...]

**no sftpd host** [*ip\_range*...]

#### [Setting and Initial value]

- *ip\_range* : A list of IP address ranges of hosts allowed to access the SFTP server or a mnemonic
  - [Setting] :



Setting	Description
An IP address, two IP addresses with a hyphen in between them (range designation), or a list containing these addresses	Allow access from a specified host
any	Allow access from all hosts
none	Prohibit access from all hosts
LAN interface name	LAN interface name allowed to access to the SFTP server
Bridge interface name	The bridge interface name to allow access to SFTP server

- [Initial value] : none

#### [Description]

Among hosts allowed to connect to the SSH server with the `sshd host` command, sets an IP address of the host that can access to the SFTP server.

#### [Note]

A mnemonic cannot be placed in a list.

The setting is applied to subsequent SFTP connections after the change.

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

#### [Models]

RTX810, RTX5000

## 4.63 SSH Client

#### [Syntax]

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

#### [Setting and Initial value]

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

#### [Description]

Executes SSH and remotely logs in to the specified host.

If *user* is omitted, access to the SSH server is attempted using the user name entered to login to the router.

If specifying an IPv6 address for *host*, enclose the IP address with "[" and "]".

The escape character specified in *escape* is recognized as an escape character only when entered at the beginning of a line. If a period (.) is entered after an escape character, connection is force-closed. When an escape character is entered twice in succession at the start of a line, this character is sent to the server only once.

The following is an example of execution:

To access remote host (192.168.1.1, port:10022):

```
# ssh -p 10022 user@192.168.1.1
```

To access remote host (2001:1::1):

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

#### [Models]

RTX810, RTX5000

## 4.64 SCP client

### [Syntax]

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

### [Setting and Initial value]

- *user*
  - [Setting] : The user name used to log in to the remote host
  - [Initial value] : -
- *host*
  - [Setting] : The host name or the IP address of the remote host
  - [Initial value] : -
- *file1*
  - [Setting] : Transfer source file name
  - [Initial value] : -
- *file2*
  - [Setting] : Transfer target file name
  - [Initial value] : -
- *port*
  - [Setting] : Port number of the remote host
  - [Initial value] : 22

### [Description]

Runs SCP.

For either *file1* or *file2*, specify a file on the remote host, and for the other, specify a file in the file system of the router.

You cannot specify files on the remote host for both *file1* and *file2*.

Similarly, you cannot specify files in the file system of the router for both *file1* and *file2*.

When specifying a file in RTFS or the external memory, omit *user* and *host*, and only specify *file* using the absolute path.

When specifying the router's configuration file (config, config0 to config4) and firmware (exec, exec0, exec1), specify only the file name, e.g. "config" or "exec0", in *file*.

If specifying an IPv6 address for *host*, enclose the IP address with "[" and "]".

The following is an example of execution:

Copying a file from a remote host (192.168.1.1) to exec0 in the router

```
# scp user@192.168.1.1:rtx810_en.bin exec0
```

Copying a file usb1:/log.txt on the router to a remote host (2001:1::1)

```
# scp usb1:/log.txt user@[2001:1::1]:log.txt
```

### [Models]

RTX810, RTX5000

## 4.65 Setting usable encryption algorithms in the SSH client

### [Syntax]

```
ssh encrypt algorithm [algorithm...]
```

```
no ssh encrypt algorithm [algorithm...]
```

### [Setting and Initial value]

- *algorithm* : Encryption algorithm (multiple specification allowed, using spaces as delimiters)
  - [Setting] :

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

Setting	Description
aes192-cbc	AES192-CBC
aes256-cbc	AES256-CBC
3des-cbc	3DES-CBC
blowfish-cbc	Blowfish-CBC
cast128-cbc	CAST-128-CBC
arcfour	Arcfour

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

#### [Description]

Sets the encryption algorithms that can be used in the SCP client.

The list of encryption algorithms specified with *algorithm* is proposed to the server at the time of SSH connection.

#### [Note]

If the server does not support the encryption algorithms specified in *algorithm*, SSH connection with the server cannot be established.

#### [Models]

RTX810, RTX5000

## 4.66 Setting the file to save the public key information of the SSH server

---

#### [Syntax]

```
ssh known hosts file
no ssh known hosts [file]
```

#### [Setting and Initial value]

- *file*
  - [Setting] : File name to save the public key information of the SSH server
  - [Initial value] : /ssh/known\_hosts

#### [Description]

Sets the file to save the public key information for the SSH server.

#### [Models]

RTX810, RTX5000

## 4.67 Change the Packet Buffer Parameters

---

#### [Syntax]

```
system packet-buffer group parameter=value [parameter=value ...]
no system packet-buffer group [parameter=value ...]
```

#### [Setting and Initial value]

- *group* : Specify the packet buffer group.
  - [Setting] : Group name (small, middle, large, jumbo, huge)
  - [Initial value] : -
- *parameter* : Specifies the parameter to be changed.
  - [Setting] :

Setting	Description
max-buffer	Maximum assigned number of the packet buffer
max-free	Maximum value of the free list
min-free	Minimum value of the free list
buffer-in-chunk	Number of packet buffers in the chunk
init-chunk	Number of chunks to allocate at startup

- [Initial value] : -
- *value*
  - [Setting] : Specifies the value to be changed.
  - [Initial value] :

## RTX810

group	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
small	1248	468	31	312	1
middle	3332	1249	83	833	1
large	4992	1404	31	312	4
huge	20	0	0	1	0

## RTX5000

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

**[Description]**

Changes the packet buffer management parameters.

The values that can be specified for the parameters vary between a huge block and other blocks. For blocks other than the huge block, whole numbers can be specified for the parameters. The parameters must satisfy all the conditions indicated below.

- $\text{max-buffer} \geq \text{max-free}$
- $\text{max-free} > \text{min-free}$
- $\text{max\_free} \geq \text{buffer-in-chunk}$
- $\text{max\_free} \geq \text{buffer-in-chunk} \times \text{init-chunk}$

For a huge block, non-negative integers can be specified for max-free, min-free, init-chunk and whole numbers can be specified for max-buffer and buffer-in-chunk. If any of the max-free, min-free, and init-chunk parameters are set to zero, all three parameters must be set to zero. If max-free, min-free, and init-chunk are set to whole numbers, the parameters must satisfy the conditions indicated above as with other groups.

**[Note]**

Jumbo groups can only be used on models that support the 1000BASE-T LAN interface and can send and received jumbo packets.

**[Example]**

```
# system packet-buffer small max-buffer=1000 max-free=500
# system packet-buffer large min-free=100
```

**[Models]**

RTX810, RTX5000

## 4.68 Set Whether to Sound Active Alarms or to Not Sound Them at All

**[Syntax]**

**alarm entire** *switch*  
**no alarm entire**

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	Sound alarms.
off	Do not sound alarms.

- [Initial value] : on

**[Description]**

Sets whether to sound active alarms or to not sound them at all.

**[Models]**  
RTX810, RTX5000

## 4.69 Set Whether to Sound Alarms for the USB Host Function

---

**[Syntax]**

**alarm usbhost** *switch*  
**no alarm usbhost**

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Sound alarms.
off	Do not sound alarms.

- [Initial value] : on

**[Description]**

Sets whether to sound alarms for the USB host function.

**[Models]**  
RTX810

## 4.70 Set Whether to Sound Alarms for the microSD Function

---

**[Syntax]**

**alarm sd** *switch*  
**no alarm sd** [*switch*]

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Sound alarms.
off	Do not sound alarms.

- [Initial value] : on

**[Description]**

Set whether to sound alarms for the microSD function.

**[Models]**  
RTX810, RTX5000

## 4.71 Set Whether to Sound Alarms for the Batch File Execution Function

---

**[Syntax]**

**alarm batch** *switch*  
**no alarm batch**

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Sound alarms.
off	Do not sound alarms.

- [Initial value] : on

**[Description]**

Sets whether to sound alarms for the batch file execution function.

**[Models]**  
RTX810, RTX5000

## 4.72 Set Whether to Sound an Alarm at Startup

---

### [Syntax]

**alarm startup** *switch* [*pattern*]

**no alarm startup** [*switch*]

### [Setting and Initial value]

- *switch*
- [Setting] :

Setting	Description
on	Sound alarms.
off	Do not sound alarms.

- [Initial value] : off
- *pattern*
  - [Setting] : The alarm pattern (1...3, 1 when omitted.)
  - [Initial value] : -

### [Description]

Sets whether to sound an alarm at startup.

### [Models]

RTX810, RTX5000

## 4.73 Set Whether to Sound Alarms for the HTTP Revision Update Function

---

### [Syntax]

**alarm http revision-up** *switch*

**no alarm http revision-up** [*switch*]

### [Setting and Initial value]

- *switch*
- [Setting] :

Setting	Description
on	Sound alarms.
off	Do not sound alarms.

- [Initial value] : on

### [Description]

Set whether to sound alarms for the HTTP revision update function.

### [Models]

RTX810

## 4.74 Adjust the LED Brightness

---

### [Syntax]

**system led brightness** *mode*

**no system led brightness** [*mode*]

### [Setting and Initial value]

- *mode*
- [Setting] :

Setting	Description
0	Bright
1	Dark

- [Initial value] : 0

### [Description]

Adjusts the LED brightness.

[Models]  
RTX810

## 4.75 Set Environment Variables

### [Syntax]

```
set name=value
no set name[=value]
```

### [Setting and Initial value]

- *name*
  - [Setting] : Environment variable name
  - [Initial value] : -
- *value*
  - [Setting] : Setting
  - [Initial value] : -

### [Description]

Sets the routers environment variables.

The environment variable naming rules are listed below.

Alphanumeric characters and underscores can be used, but names cannot start with underscores or numbers.

There is no variable name length limit, but the **set** command cannot be executed if it exceeds the maximum command line length (4095 characters).

Names are case-sensitive. For example, “abc” and “Abc” are treated as different variables.

### [Models]

RTX810, RTX5000

## 4.76 Set the CPU Packet Scheduling Mode

### [Syntax]

```
system packet-scheduling mode
no system packet-scheduling [mode]
```

### [Setting and Initial value]

- *mode* : CPU packet scheduling mode
  - [Setting] :

Setting	Description
hash	Hash base
load-balance	Load balance base
lan-based	LAN interface base

- [Initial value] : hash

### [Description]

Set the packet scheduling mode.

When the *hash* is set, CPU core for processing the packet is assigned by hash value from received packet.

When the *load-balance* is set, CPU core for processing the packet is assigned dynamically so that the load for each CPU core is evenly.

When the *lan-based* is set, CPU core for processing the packet is assigned as follow by LAN interface the packet received.

LAN interface the packet received	CPU core
LAN1	CPU0
LAN2	CPU1
LAN3	CPU2
LAN4	CPU3

### [Note]

The received packet on BRI/PRI interface is not included in the target of this command.

When this command is executed, all LAN interface link down temporarily to initialize all LAN interface.

The packet processed by normal-pass is received on a CPU core assigned by this command, but the sending process is executed on CPU1. When the **ip routing process normal** is set, all packets match this condition.

When the *hash* is set, the received packet which does not have IPv4/IPv6 header is processed on CPU0.

When the *load-balance* is set, the order of packets may be replaced. In this case, some problems may occur on the application which uses UDP packet. The replacement of packet order can be inhibited by fixing the processing CPU core using **system packet-scheduling filter** command. In the TCP connection, there is no problem if the replacement of packet order occur.

In the IPsec data transmission, ESP packet may not be sent in sequence of ESP sequence number even in any mode. Therefore, ESP sequence error occur in the receiving process at opposite side and the ESP packet is discarded. ESP sequence error can be inhibited by setting *anti-replay-check* with 'off' on the **ipsec sa policy** command.

#### [Models]

RTX5000

## 4.77 Set the CPU packet scheduling filter

---

### [Syntax]

```
system packet-scheduling filter filter_num cpu_num ip src_ipv4_address[/mask] [dest_ipv4_address[/mask]] [protocol [src_port [dest_port]]]
```

```
system packet-scheduling filter filter_num cpu_num ipv6 src_ipv6_address[/prefix_len] [dest_ipv6_address[/prefix_len]] [protocol [src_port [dest_port]]]
```

```
no system packet-scheduling filter filter_num [cpu_num ip src_ipv4_address[/mask] [dest_ipv4_address[/mask]] [protocol [src_port [dest_port]]]
```

```
no system packet-scheduling filter filter_num [cpu_num ipv6 src_ipv6_address[/prefix_len] [dest_ipv6_address[/prefix_len]] [protocol [src_port [dest_port]]]
```

### [Setting and Initial value]

- *filter\_num*
  - [Setting] : Filter number (1..40)
  - [Initial value] : -
- *cpu\_num*
  - [Setting] : CPU number (0..3)
  - [Initial value] : -
- *src\_ipv4\_address* : Source IPv4 address
  - [Setting] :
    - A.B.C.D (A-D: 0-255 or \*)
      - When the '\*' is set to A-D, All IPv4 address is target.
    - \* (All IPv4 address is target.)
  - [Initial value] : -
- *dest\_ipv4\_address* : Destination IPv4 address
  - [Setting] :
    - Same format with *src\_ipv4\_address*
    - When it is omitted, it means '\*'
  - [Initial value] : -
- *mask* : Netmask (It is possible to be configured when the *src\_ipv4\_address* and *dest\_ipv4\_address* parameter is network address)
  - [Setting] :
    - A.B.C.D (A-D: 0-255)
    - Hexadecimal value (0xXX)
    - Number of mask bit
    - When it is omitted, it means 0xffffffff
  - [Initial value] : -
- *src\_ipv6\_address* : Source IPv6 address
  - [Setting] :
    - IPv6 address
    - \* (All IP address is target)
  - [Initial value] : -
- *dest\_ipv6\_address* : Destination IPv6 address
  - [Setting] :
    - Same format with *src\_ipv6\_address*
    - When it is omitted, it means '\*'
  - [Initial value] : -



- *prefix\_len* : Prefix length (It is possible to configured when the *src\_ipv6\_address* and *dest\_ipv6\_address* is network address)
  - [Setting] :
    - Prefix length
    - When it is omitted, it means 128
  - [Initial value] : -
- *protocol* : Kind of packet scheduling
  - [Setting] :
    - Decimal number indicating the protocol
    - Mnemonic indicating the protocol (Partially)

Mnemonic	Protocol number
icmp	1 (IPv4)、 58 (IPv6)
tcp	6
udp	17
gre	47
esp	50

- \* (All protocol)
- When it is omitted, it means '\*'
- [Initial value] : -
- *src\_port* : Source port number of UDP or TCP
  - [Setting] :
    - Decimal number indicating the port number
    - Mnemonic indicating the port number (Partially)

Mnemonic	Port number
ftp	21
ftpdata	20
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

- \* (All port number)
- When it is omitted, it means '\*'
- [Initial value] : -
- *dest\_port*

- [Setting] : Same format with *src\_port*
- [Initial value] : -

**[Description]**

Set the filter for fixing the CPU core to transmit the packet.

The received packet which is matched to the filter is transmitted by CPU core specified by *cpu\_num* parameter.

**[Note]**

The received packet on BRI/PRI interface is not included in the target of this command.

The packet processed by normal-pass is received on a CPU core assigned by this command, but the sending process is executed on CPU1. When the **ip routing process normal** is set, all packets match this condition.

The received packet which does not have IPv4/IPv6 header is not included in the target of this command.

**[Example]**

```
# system packet-scheduling filter 1 0 ip 192.168.100.1
# system packet-scheduling filter 2 1 ip 172.16.1.1 172.16.2.1 icmp
# system packet-scheduling filter 3 2 ip * * 6 21
# system packet-scheduling filter 4 3 ip 10.10.10.0/24 * udp * *
# system packet-scheduling filter 5 0 ip 192.168.* *
# system packet-scheduling filter 6 1 ipv6 2001:240:10::1
# system packet-scheduling filter 7 2 ipv6 * 2001:240:100::
# system packet-scheduling filter 8 3 ipv6 2002::/32 * tcp
```

**[Models]**

RTX5000

## 4.78 Apply the CPU Packet Scheduling Filter

---

**[Syntax]**

```
system packet-scheduling filter list filter_list
no system packet-scheduling filter list [filter_list]
```

**[Setting and Initial value]**

- *filter\_list*
  - [Setting] : Filter list (separated by blank)
  - [Initial value] : -

**[Description]**

Set the order of applying filter which is configured by **system packet-scheduling filter** command.

The received packet which matches the filter is transmitted by CPU core specified by filter settings. The received packet which does not match any filter is transmitted by CPU core specified by **system packet-scheduling** command.

**[Models]**

RTX5000

---

## Chapter 5

---

### File System for Yamaha router: RTFS

---

RTFS is a file system configured in the router's internal flash ROM. Similar to general PC file systems, RTFS stores any data in the internal flash ROM and manage them with attached file names. It also has a directory structure. The internal flash ROM has a storage area for firmware (exec), configuration files (config), and other various data, but RTFS uses another independent and special area in the ROM.

When entering a command to specify a file or directory with a path without a prefix and starting from "/", you can refer the RTFS area.

Use RTFS for storing reading-only data such as scrip files of the Lua script function and HTML files of the custom GUI. Periodical writing of log files and others to the RTFS area deteriorates the flash ROM. If frequent writing causes failure of the flash ROM, we cannot provide free repair service even within the warranty period.

---

#### 5.1 Format the RTFS

---

**[Syntax]**

**rtfs format**

**[Description]**

Formats the RTFS area of the internal flash ROM and deletes all data.  
The router also formats the RTFS when it is reset to its factory default settings.

**[Note]**

Formatting deletes the data completely. You cannot recover the data after it has been deleted through formatting.

**[Models]**

RTX810, RTX5000

---

#### 5.2 Perform Garbage Collection on the RTFS

---

**[Syntax]**

**rtfs garbage-collect**

**[Description]**

Deletes unnecessary data in the internal flash ROM RTFS and increases the amount of available memory.  
Garbage collection is normally performed automatically when it is necessary, but because it takes a few tens of seconds to complete, you may want to use this command to perform it in advance.

**[Note]**

Garbage collection does not involve the deletion or overwriting of files.

**[Models]**

RTX810, RTX5000

## Chapter 6

### IP Configuration

#### 6.1 Common Interface Settings

##### 6.1.1 Set Whether to Process IP Packets

###### [Syntax]

```
ip routing routing
no ip routing [routing]
```

###### [Setting and Initial value]

- *routing*
- [Setting] :

Setting	Description
on	Process IP packets
off	Not process IP packets

- [Initial value] : on

###### [Description]

Sets whether to route IP packets.

###### [Note]

Configuration using TELNET, access using TFTP, PING, and so forth can be used even when IP routing is turned off.

###### [Models]

RTX810, RTX5000

##### 6.1.2 Set the IP Address

###### [Syntax]

```
ip interface address ip_address/mask [broadcast broadcast_ip]
ip interface 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 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 and Initial value]

- *interface*
  - [Setting] : LAN interface name, WAN interface name
  - [Initial value] : -
- *loopback*
  - [Setting] : Loopback interface name
  - [Initial value] : -
- *bridge\_interface*
  - [Setting] : Bridge interface name
  - [Initial value] : -
- *ip\_addres*
  - [Setting] : IP address xxx.xxx.xxx.xxx where xxx is a decimal number
  - [Initial value] : -
- *dhcp* : Keyword indicating that the IP address is obtained as a DHCP client
  - [Initial value] : -

- *mask*
  - [Setting] :
    - xxx.xxx.xxx.xxx where xxx is a decimal number
    - Hexadecimal number following 0x
    - Number of mask bits
  - [Initial value] : -
- *broadcast\_ip*
  - [Setting] : Broadcast IP address
  - [Initial value] : -
- *switch*
  - [Setting] :

Setting	Description
on	Use the AutoIP function
off	Not use the AutoIP function

- [Initial value] : off

#### [Description]

Sets the IP address and netmask of the interface. A broadcast address can be specified by specifying “broadcast *broadcast\_ip*”. If omitted, a directed broadcast address is used. If *dhcp* is specified, the IP address is obtained as a DHCP client immediately after this command is set. If **no ip interface address** is entered when *dhcp* is specified, a release message of the obtained IP address is sent to the DHCP server.

When “Use the AutoIP function” is set, and the retry count of *dhcp* in the **ip bridge\_interface dhcp retry** setting is finite, the 169.254.0.0/16 address is automatically decided when *dhcp* fails to allocate an address.

#### [Note]

If an IP address is not set on a LAN interface, the router tries to obtain the IP address through RARP.

If an IP address is not set on a PP interface, the interface operates as unnumbered.

The client ID that is obtained when the router is operated as a DHCP client can be checked using the **show status dhcpc** command.

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

RTX5000 does not support WAN interface for *interface* parameter.

For the default settings of this command when it is shipped from the factory and when the **cold start** command is executed, see section 1.7, “About the Factory Default Settings”.

#### [Models]

RTX810, RTX5000

### 6.1.3 Set the Secondary IP Address

#### [Syntax]

```
ip interface secondary address ip_address[/mask]
ip interface secondary address dhcp
no ip interface secondary address [ip_address/mask]
```

#### [Setting and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *ip\_address*
  - [Setting] : Secondary IP address xxx.xxx.xxx.xxx where xxx is a decimal number
  - [Initial value] : -
- *dhcp* : Keyword indicating that the IP address is obtained as a DHCP client
  - [Initial value] : -
- *mask*
  - [Setting] :
    - xxx.xxx.xxx.xxx where xxx is a decimal number
    - Hexadecimal number following 0x
    - Number of mask bits
  - [Initial value] : -

**[Description]**

Sets the secondary IP address and netmask on the LAN side.

If dhcp is specified, the IP address is obtained as a DHCP client immediately after this command is set.

**[Note]**

The broadcast address on the secondary network always uses a directed broadcast address.

**[Models]**

RTX810, RTX5000

**6.1.4 Set the Interface MTU**

---

**[Syntax]**

```
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 and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *mtu0,mtu1,mtu2*
  - [Setting] : MTU value (RTX810:64..1500, RTX5000:64..9578)
  - [Initial value] :
    - mtu0=1500
    - mtu1=1500
    - mtu2=1280

**[Description]**

Sets the MTU value of each interface.

**[Note]**

Actually, this setting applies only to IP packets. It is not applied to other protocols, and the default 1500 MTU is used for them. RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

**6.1.5 Set Whether to Send Returning Packets to the Same Interface**

---

**[Syntax]**

```
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 and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *switch*
  - [Setting] :

Setting	Description
on	Send returning packets
off	Not send returning packets

- [Initial value] :
  - off (for a PP interface)

- on (for other interfaces)

#### [Description]

Sets whether to send returning packets to the same interface.

When “Not send returning packets” is set, a relevant packet is discarded and “ICMP Destination Unreachable” is sent to the transmission source.

#### [Models]

RTX810, RTX5000

### 6.1.6 Set Whether to Run the Echo, Discard, and Time Services

#### [Syntax]

**ip simple-service** *service*

**no ip simple-service** [*service*]

#### [Setting and Initial value]

- *service*
  - [Setting] :

Setting	Description
on	Run the various TCP/UDP services
off	Stop the services

- [Initial value] : off

#### [Description]

Sets whether to run the TCP/UDP echo (7), discard (9), and time (37) services. If the services are stopped, the corresponding ports are also closed.

#### [Models]

RTX810, RTX5000

### 6.1.7 Set the Statistic IP Routing Information

#### [Syntax]

**ip route** *network* *gateway gateway1* [*parameter*] [*gateway gateway2* [*parameter*]...]

**no ip route** *network* [*gateway*...]

#### [Setting and Initial value]

- *network*
  - [Setting] :

Setting	Description
default	Default route
IP address	Destination host/number of mask bits (32 when omitted)

- [Initial value] : -
- *gateway1*, *gateway2*
  - [Setting] :
    - IP address
      - xxx.xxx.xxx.xxx where xxx is a decimal number
    - pp *peer\_num* [*dlci=dlci*] : Route to the PP interface. When “dlci=dlci” is specified, a route to the frame relay DLCI.
      - *peer\_num* : Peer number
    - pp anonymous name=*name*

Setting	Description
<i>name</i>	Name specified by PAP/CHAP authentication

- *dhcp interface*

Setting	Description
<i>interface</i>	Name of the LAN interface or WAN interface operating as DHCP client when using the default gateway provided by DHCP

- tunnel *tunnel\_num* : Route to the tunnel interface

- Loopback interface name, null interface name
- [Initial value] : -
- *parameter* : Multiple parameters below can be specified by delimiting each parameter with a space
- [Setting] :

Setting	Description
filter <i>number</i> [ <i>number..</i> ]	Set a filter-type route <ul style="list-style-type: none"> <li>• <i>number</i> <ul style="list-style-type: none"> <li>• Filter number (1..21474836) (multiple numbers can be specified by delimiting each number with a space)</li> </ul> </li> </ul>
metric <i>metric</i>	Specify the metric <ul style="list-style-type: none"> <li>• <i>metric</i> <ul style="list-style-type: none"> <li>• Metric value (1..15)</li> <li>• 1 when omitted.</li> </ul> </li> </ul>
hide	An option that is valid only when the output interface is LAN, WAN, PP, or TUNNEL and indicates that the route is valid only when the destination is connected
weight <i>weight</i>	Value indicating the ratio between different routes <ul style="list-style-type: none"> <li>• <i>weight</i> <ul style="list-style-type: none"> <li>• Weight on the route (0..2147483647)</li> <li>• 1 when omitted.</li> </ul> </li> </ul>
keepalive	Valid only when there is reachability to <i>gateway1</i>

- [Initial value] : -

### [Description]

Sets the statistic IP route.

If a filter-type route is specified for the *gateway* parameter, the filter is applied in the order written, and the matched gateway is selected.

If a matching gateway does not exist or there is no gateway that has filter-type route specified, a gateway that does not have filter-type route specified is selected.

If a gateway that does not have filter-type route specified also does not exist, the processing continues assuming that the route does not exist.

If multiple gateways that do not have filter-type route specified are written, the route is selected using the round robin method at the time the routes are to be used.

If multiple gateways that do not have a filter specified are written, the route that is used when it is to be used is determined by a stream that is identified by the source/destination IP address, protocol, and source/destination port number. The same stream packets are always delivered to the same gateway. If a value is specified for *weight* (for example the ratio of the line speeds), the ratio of the stream delivered to the route increases in proportion to the ratio of this value with respect to the *weight* values of other gateways.

In all cases, gateways that have the hide keyword specified are valid only when the line is connected. The gateways are not evaluated, if the line is not connected. The loopback and null interfaces are always up, so while you can specify the hide keyword for them, doing so has no meaning.

If you wish to use a certain gateway with higher priority without balancing the load when multiple gateways are set, set the *weight* option to 0.

### [Note]

An already existing route can be overwritten.

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

RTX5000 does not support WAN interface for *interface* parameter.

### [Example]

- Set the default gateway to 192.168.0.1.

```
# ip route default gateway 192.168.0.1
```

- The remote network connected through PP1 is 192.168.1.0/24.



```
# ip route 192.168.1.0/24 gateway pp 1
```

- Load sharing by multihoming: There are two routes as a default gateway: the 128k exclusive line for connecting PP1, and the 64k exclusive line for connecting PP2. Also, when each exclusive line goes down, the route at that time is disabled to prevent loss of packets.

```
* Simultaneous use of the NAT function and the exclusive line keepalive function is necessary.
```

```
# ip route default gateway pp 1 weight 2 hide gateway pp 2 weight 1 hide
```

- If PP1 is active, only PP1 is used. When PP1 is down, PP2 is used.

```
# ip route 192.168.0.1/24 gateway pp 1 hide gateway pp 2 weight 0
```

#### [Models]

RTX810, RTX5000

### 6.1.8 Set the IP Packet Filter

#### [Syntax]

```
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 and Initial value]

- *filter\_num*
  - [Setting] : Static filter number (1..21474836)
  - [Initial value] : -
- *pass\_reject*
  - [Setting] :

Setting	Description
pass	Pass if matched (not record in the log)
pass-log	Pass if matched (record in the log)
pass-nolog	Pass if matched (not record in the log)
reject	Discard if matched (record in the log)
reject-log	Discard if matched (record in the log)
reject-nolog	Discard if matched (not record in the log)
restrict	Pass if the line is connected and discard if it is disconnected (not record in the log)
restrict-log	Pass if the line is connected and discard if it is disconnected (record in the log)
restrict-nolog	Pass if the line is connected and discard if it is disconnected (not record in the log)

- [Initial value] : -
- *src\_addr* : Source IP address of the IP packet
  - [Setting] :
    - A.B.C.D (A-D: 0-255 or \*)
      - In the above notation, if "\*" is used for A thru D, the applicable 8 bits accept all values.
    - \* (All IP addresses are supported)
    - Two of the above items with a hyphen in between them, an above item with a hyphen in front, and an above item with a hyphen in the back indicate a range.
  - [Initial value] : -
- *dest\_addr*
  - [Setting] : Destination IP address of the IP packet.
  - [Setting] :
    - Same format as *src\_addr*
    - Same as one \* when omitted.
  - [Initial value] : -
- *mask* : IP address bit mask (can be specified only when *src\_addr* and *dest\_addr* are network addresses)
  - [Setting] :

- A.B.C.D (A-D: 0-255 or \*)
- Hexadecimal number following 0x
- Number of mask bits
- Same as 0xffffffff when omitted
- [Initial value] :-
- *protocol* : Type of packets to be filtered
- [Setting] :
  - Decimal number indicating the protocol (0..255)
  - Mnemonic indicating the protocol

Mnemonic	Decimal Number	Description
icmp	1	ICMP packet
tcp	6	TCP packet
udp	17	UDP packet
ipv6	41	IPv6 packet
gre	47	GRE packet
esp	50	ESP packet
ah	51	AH packet
icmp6	58	ICMP6 packet

- Series of above items delimited by commas (up to 5 items)
- Special settings

icmp-error	ICMP packet whose type is 3, 4, 5, 11, 12, 31, or 32
icmp-info	ICMP packet whose type is 0, 8 to 10, 13 to 18, 30, or 33 to 36
tcpsyn	tcp packet with SYN flag set
tcpfin	tcp packet with FIN flag set
tcprst	tcp packet with RST flag set
established	tcp packet with ACK flag set Function that permits connections from the inside to the outside but rejects connections from the outside to the inside
tcpflag= <i>value/mask</i>	A TCP packet for which the logical AND of the TCP flag value and <i>mask</i> value is the same as <i>value</i> or different than <i>value</i> Specify <i>value</i> and <i>mask</i> as hexadecimal values following 0x (0x0000 to 0xffff).
tcpflag! <i>=value/mask</i>	
*	All protocols

- Same as \* when omitted.
- [Initial value] :-
- *src\_port\_list* : When TCP (tcp/tcpfin/tcprst/established/tcpflag) or UDP (udp) is contained in *protocol*, the TCP or UDP source port number. When *protocol* is just ICMP (icmp), the ICMP type.
- [Setting] :
  - A decimal number representing the port number
  - Mnemonic representing the port number (a section)

Mnemonic	Port Number
ftp	20,21
ftpdata	20
telnet	23
smtp	25
domain	53

Mnemonic	Port Number
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 of the above items with a hyphen in between them, an above item with a hyphen in front, and an above item with a hyphen in the back indicate a range.
- Series of above items delimited by commas (up to 10 items)
- \* (all ports or types)
- Same as \* when omitted.
- [Initial value] : -
- *dest\_port\_list*
  - [Setting] : When TCP (tcp/tcpfin/tcprst/established/tcpflag) or UDP (udp) is contained in *protocol*, the TCP or UDP destination port number. When *protocol* is just ICMP (icmp), the ICMP code.
  - [Initial value] : -

#### [Description]

Sets the IP packet filter. The filter specified with this command is used in the **ip interface secure filter**, **ip filter set**, **ip filter dynamic**, and **ip interface rip filter** commands.

#### [Note]

Filters using restrict-log and restrict-nolog are effective for packets that need to be passed only when the line is connected and do not really require the line to be called for this purpose. One such example is the NTP packet used to synchronize the clock. When you want to check the ICMP types and codes of ICMP packets using a filter, set *protocol* to just 'icmp.' When *protocol* is set to just 'icmp', *src\_port\_list* is treated as a list of the ICMP types and *dest\_port\_list* is treated as a list of the ICMP codes. When 'icmp' and other protocols are listed for *protocol*, *src\_port\_list* and *dest\_port\_list* are treated as TCP/UDP port numbers, and ICMP packet comparison does not take place. Also, when 'icmp-error' or 'icmp-info' is specified for *protocol*, the *src\_port\_list* and *dest\_port\_list* are ignored. When *protocol* is set to '\*' or to multiple protocol that include TCP/UDP, *src\_port\_list* and *dest\_port\_list* are treated as TCP/UDP port numbers, and only the port numbers of TCP or UDP packets are compared and filtered. Other types of packets (including ICMP) are filtered and compared as if *src\_port\_list* and *dst\_port\_list* do not exist.

#### [Example]

Records the IPv4 ICMP ECHO/REPLY sent and received over LAN1 in the 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 the IPv4 redirects sent from LAN2, only "for the host" redirects are blocked.

```
# ip lan2 secure filter out 1 100
# ip filter 1 reject * * icmp 5 1
# ip filter 100 pass * *
```

#### [Models]

RTX810, RTX5000

### 6.1.9 Define the Filter Set

---

#### [Syntax]

```
ip filter set name direction filter_list [filter_list ...]
no ip filter set name [direction ...]
```

#### [Setting and Initial value]

- *name*
  - [Setting] : Text string indicating the filter set name
  - [Initial value] : -
- *direction*
  - [Setting] :

Setting	Description
in	Input filter
out	Output filter

- [Initial value] : -
- *filter\_list*
  - [Setting] : Series of filter numbers delimited by spaces (up to 1000)
  - [Initial value] : -

#### [Description]

Defines the filter set. A filter set specifies the in and out filters and is applied to an interface through RADIUS designation and the **ip interface secure filter** command.

#### [Models]

RTX810, RTX5000

### 6.1.10 Set Whether to Filter Out IP Packets with the Source-route Option

---

#### [Syntax]

```
ip filter source-route filter_out
no ip filter source-route [filter_out]
```

#### [Setting and Initial value]

- *filter\_out*
  - [Setting] :

Setting	Description
on	Filter the packets out
off	Not filter the packets out

- [Initial value] : on

#### [Description]

Sets whether to filter out IP packets with the Source-route option.

#### [Models]

RTX810, RTX5000

### 6.1.11 Set Whether to Filter Out Directed Broadcast Packets

---

#### [Syntax]

```
ip filter directed-broadcast filter_out
ip filter directed-broadcast filter filter_num [filter_num ...]
no ip filter directed-broadcast
```

#### [Setting and Initial value]

- *filter\_out*
  - [Setting] :

Setting	Description
on	Filter the packets out

Setting	Description
off	Not filter the packets out

- [Initial value] : on
- *filter\_num*
  - [Setting] : Static filter number (1..21474836)
  - [Initial value] : -

**[Description]**

Sets whether to broadcast IP packets whose destination IP address is set to a directed broadcast address to the networks to which the router is connected.

If on is specified, all directed broadcast packets are discarded.

If off is specified, all directed broadcast packets are passed.

If filter is specified, the router checks the packet using the filter specified by the **ip filter** command and passes the packet only if it matches the PASS filter.

**[Note]**

The check by the **ip interface wol relay** command takes precedence over the check by this command. Only the packets that could not pass the check by the **ip interface wol relay** command are checked with this command. Specify on to prevent so-called smurf attacks.

**[Models]**

RTX810, RTX5000

## 6.1.12 Define a Dynamic Filter

---

**[Syntax]**

**ip filter dynamic** *dyn\_filter\_num srcaddr dstaddr protocol* [*option ...*]

**ip filter dynamic** *dyn\_filter\_num srcaddr dstaddr filter filter\_list* [*in\_filter\_list*] [*out\_filter\_list*] [*option...*]

**no ip filter dynamic** *dyn\_filter\_num*

**[Setting and Initial value]**

- *dyn\_filter\_num*
  - [Setting] : Dynamic filter number (1..21474836)
  - [Initial value] : -
- *srcaddr*
  - [Setting] : Source IP address
  - [Initial value] : -
- *dstaddr*
  - [Setting] : Destination IP address
  - [Initial value] : -
- *mask* : Bit mask for IP address (can be specified only when *src\_addr* and *dest\_addr* are network addresses)
  - [Initial value] : -
- *protocol* : Protocol mnemonic
  - [Setting] :
    - tcp/udp/ftp/tftp/domain/www/smtp/pop3/telnet/netmeeting
    - 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
  - [Initial value] : -
- *filter\_list*
  - [Setting] : List of filter numbers registered by the **ip filter** command
  - [Initial value] : -
- *option*
  - [Setting] :
    - syslog=*switch*

Setting	Description
on	Keep the communication log of the connection in SYSLOG
off	Not keep the communication log of the connection in SYSLOG

- `timeout=time`

Setting	Description
time	Number of seconds until the connection information is released after the data stops flowing

- [Initial value] : `syslog=on`

### [Description]

Defines a dynamic filter. In the first syntax, an application name registered in the router in advance is specified.

In the second syntax, the user specifies the access control rules. Following the keywords `filter`, `in`, and `out`, set a filter number defined by the `ip filter` command.

If a connection (trigger) that corresponds to the filter specified after the filter keyword is detected, subsequent connections that correspond to the filter specified after the `in` keyword and `out` keyword are passed. The `in` keyword controls accesses in the reverse direction to the trigger direction, and the `out` keyword controls accesses in the same direction as the dynamic filter. The IP address in the `ip filter` command is ignored. The `pass/reject` parameter is also ignored.

If `tcp` or `udp` is specified for the protocol, filtering specific to an application is not carried out. If a certain application must be handled, specify the application name.

### [Example]

```
# ip filter 10 pass * * udp * snmp
# ip filter dynamic 1 * * filter 10
```

### [Models]

RTX810, RTX5000

## 6.1.13 Set the Dynamic Filter Timeout

### [Syntax]

**ip filter dynamic timer** [*option=timeout* [*option...*]]

**no ip filter dynamic timer**

### [Setting and Initial value]

- *option* : Option name
- [Setting] :

Setting	Description
<code>tcp-syn-timeout</code>	Drop the session if a connection is not established within the specified time after receiving SYN
<code>tcp-fin-timeout</code>	Release the connection if the specified time elapses after receiving FIN
<code>tcp-idle-time</code>	Drop the connection if no TCP connection data flows within the specified time
<code>udp-idle-time</code>	Drop the connection if no UDP connection data flows within the specified time
<code>dns-timeout</code>	Drop the connection if no response is received within the specified 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] : Wait time (seconds)
- [Initial value] : -

**[Description]**

Sets the dynamic filter timeout.

**[Note]**

This setting is used in common in all checks.

**[Models]**

RTX810, RTX5000

### 6.1.14 Set the Operation of the Intrusion Detection Function

**[Syntax]**

```
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 and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *direction* : Packet connection direction to be monitored
  - [Setting] :

Setting	Description
in	Into the interface
out	Out of the interface

- [Initial value] : -
- *type* : Packet connection type to be monitored
  - [Setting] :

Setting	Description
ip	IP header
ip-option	IP option header
fragment	Fragment
icmp	ICMP
udp	UDP
tcp	TCP
ftp	FTP
winny	Winny
share	Share
default	All unspecified types

- [Initial value] : -
- *switch*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] :
  - When TYPE is not specified=off
  - When TYPE is specified=on

- *option*
  - [Setting] :

Setting	Description
reject=on	Discards invalid packets
reject=off	Not discard invalid packets

- [Initial value] : off

**[Description]**

Detects intrusion in packets of the specified direction on the specified interface.  
When the *type* option is omitted, the settings apply to all types of intrusion detection.

**[Note]**

For high-risk attacks, the router always discards the packet regardless of the reject option setting.

Concerning Winny, the version 2 can be detected, but no other previous versions are covered.

Concerning Share, the version 1.0 EX2 (Share TCP version) can be detected, but no other previous versions are covered.  
RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

### 6.1.15 Set the Frequency of Intrusion Detection Notifications in a Second

---

**[Syntax]**

**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 and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *frequency*
  - [Setting] : Frequency (1...1000)
  - [Initial value] : 1

**[Description]**

Sets the frequency of intrusion detection notifications in a second.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

### 6.1.16 Control the Repeated Intrusion Detection Notifications

---

**[Syntax]**

**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 and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *time*
  - [Setting] : Number of seconds (1..1000)



- [Initial value] : 60

#### [Description]

Controls the notifications so that the same type of intrusions against a host is notified only once per the number of seconds specified by *time*.

#### [Note]

RTX5000 does not support WAN interface for *interface* parameter.

#### [Models]

RTX810, RTX5000

### 6.1.17 Set the Number of Maximum Displayed Notifications of the Intrusion Detection

---

#### [Syntax]

```
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 and Initial value]

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *num*
  - [Setting] : Number of notifications (1..1000)
  - [Initial value] : 50

#### [Description]

Sets the number of intrusion detection notifications that are displayed by the **show ip intrusion detection** command.

#### [Note]

RTX5000 does not support WAN interface for *interface* parameter.

#### [Models]

RTX810, RTX5000

### 6.1.18 Set the Intrusion Detection Threshold Value

---

#### [Syntax]

```
ip interface intrusion detection threshold type count
ip pp intrusion detection threshold type count
ip tunnel intrusion detection threshold type count
no ip interface intrusion detection threshold type
no ip pp intrusion detection threshold type
no ip tunnel intrusion detection threshold type
```

#### [Setting and Initial value]

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *type* : Intrusion type for setting the threshold value
  - [Setting] :

Setting	Description
port-scan.	Port scan
syn-flood	SYN flood

- [Initial value] :
  - port-scan=64
  - syn-flood=100
- *count*
  - [Setting] : Threshold value (1..65535)

- [Initial value] : -

**[Description]**

Sets the threshold value used by the intrusion detection. The meaning of the intrusion type and the specified threshold value are as follows:

<i>type</i>	Meaning of the <i>count</i> Value
port-scan	If the <i>count</i> types of different ports are accessed within a second on the same host, the router determines that it is a port scan.
syn-flood	If the number of detected SYN packets within a second is greater than or equal to <i>count</i> against the same host, the router determines that it is a SYN flood.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

### 6.1.19 Set the MSS Limit of the TCP Session

---

**[Syntax]**

```
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]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *mss*
  - [Setting] :

Setting	Description
536..1460	Maximum length of MSS
auto	Auto setting
off	Not set

- [Initial value] : off

**[Description]**

Limits the MSS of the TCP session passing the interface. The router monitors the TCP packets that pass the interface, and overwrites the MSS option value with the specified value if it exceeds the specified value. If the auto keyword is specified, the MSS value is overwritten with a value calculated from the interface MTU or the MRU if the remote MRU value is known on the PP interface.

**[Note]**

For a PP interface for PPPoE, the **pppoe tcp mss limit** command can also be used to limit the MSS of the TCP session. If this command and the **pppoe tcp mss limit** command are both valid, the MSS is limited to the smaller of the two values. RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

### 6.1.20 Set the Number of TCP Sessions of Which the Router Is an Endpoint

---

**[Syntax]**

```
tcp session limit limit
no tcp session limit [limit]
```

**[Setting and Initial value]**

- *limit* : Limit
- [Setting] :

Setting	Description
32 to 65535	The number of sessions
none	No limit

- [Initial value] :
  - 1000

**[Description]**

Sets the number of TCP sessions of which the router is an endpoint.

When none is selected, the number of sessions is not limited.

**[Note]**

This limit is not applied to the case where direct connection with the router is not executed.

**[Models]**

RTX810, RTX5000

### 6.1.21 Set Whether to Log Changes in the IPv4 Route Information

---

**[Syntax]**

```
ip route change log log
no ip route change log [log]
```

**[Setting and Initial value]**

- *log*
- [Setting] :

Setting	Description
on	Log changes in the IPv4 route.
off	Not log changes in the IPv4 route.

- [Initial value] : off

**[Description]**

Sets whether to log changes in the IPv4 route information.

The log is recorded at the INFO level.

**[Models]**

RTX810, RTX5000

### 6.1.22 Set the Security by Filtering

---

**[Syntax]**

```
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 and Initial value]**

- *interface*
  - [Setting] : LAN interface name, WAN interface name, loopback interface name, or null interface name
  - [Initial value] : -
- *direction*

- [Setting] :

Setting	Description
in	Filtering of received packets
out	Filtering of packets to be transmitted

- [Initial value] : -
- *filter\_list*
  - [Setting] : Ordering of white-space separated file numbers (The total number of static and active filters is up to 300 for RTX5000. It is up to 128 for all other models.)
  - [Initial value] : -
- *set\_name*
  - [Setting] : Text string indicating the filter set name
  - [Initial value] : -
- *dynamic* : Specify the dynamic filter number immediately after the keyword
  - [Initial value] : -

### [Description]

Limits the type of packets that pass the interface by combining packet filters specified by the **ip filter** command.

In the syntax that specifies a direction, the filter sequence applied to each direction is specified by filter numbers. The specified filters are applied in order, and when a filter that matches the packet is found, that filter determines whether the packet is passed or discarded. Subsequent filters are not applied. Packets that do not meet any of the filters are discarded.

In the syntax that specifies the filter set name, the specified filter set is applied. The order in which the filters are applied complies with the method used by the syntax that specifies a direction. If an undefined filter set name is specified, the router operates as if the filter is not set.

### [Note]

The filter list is scanned. When a match is found, the relevant filter determines whether the packet is passed or 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 source IP address is 192.168.0.1 are not checked by filter 2, because filter 1 determines that the packet is to be passed. Therefore, filter 2 carries no meaning.

Packets that do not match any of the filters in the filter list are discarded.

If RADIUS authentication is used in PP anonymous and the Access-Response sent from the RADIUS server contains the 'Filter-Id' attribute, the filter set specified by the value is applied, and the settings of the **ip pp secure filter** command are ignored.

If the 'Filter-Id' attribute does not exist, the settings of the **ip pp secure filter** command are used as the filter.

Dynamic filtering cannot be used with a loopback or null interface.

You cannot set *direction* to 'in' for a null interface.

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

RTX5000 does not support WAN interface for *interface* parameter.

### [Models]

RTX810, RTX5000

## 6.1.23 Set Whether to Rewrite the DF Bit of the IP Packet That Matches the Rule with 0

### [Syntax]

```
ip fragment remove df-bit rule
no ip fragment remove df-bit [rule]
```

### [Setting and Initial value]

- *rule*
  - [Setting] :

Setting	Description
filter <i>filter_num</i>	<i>filter_num</i> is a filter number registered by the <b>ip filter</b> command

- [Initial value] : -

**[Description]**

Of the IP packets that are forwarded, the DF bit of the packets that match the *rule* are set to 0.

**[Note]**

The DF bit is used in the path MTU discovery algorithm. However, if a firewall that filters ICMP packets exists in the path, the algorithm may not work correctly and may cause problems such as not being able to communicate with a certain peer. This type of phenomenon is called a Path MTU Discovery Blackhole. If a Path MTU Discovery Blackhole exists, the DF bit can be set to 0 in the communication with such peer using this command. If you do, the path MTU discovery will no longer work correctly, but communication will be possible.

**[Models]**

RTX810, RTX5000

### 6.1.24 Set the TOS Field Overwriting of the IP Packet

---

**[Syntax]**

```
ip tos supersede id tos [precedence=precedence]filter_num [filter_num_list]  
no ip tos supersede id [tos]
```

**[Setting and Initial value]**

- *id*
  - [Setting] : ID number (1..65535)
  - [Initial value] : -
- *tos*
  - [Setting] :
    - Overwriting TOS value (0..15)
    - The following mnemonics can be used.

Mnemonic	TOS value
normal	0
min-monetary-cost	1
max-reliability	2
max-throughput	4
min-delay	8

- [Initial value] : -
- *precedence*
  - [Setting] :
    - precedence value (0..7)
    - If precedence is omitted, the PRECEDENCE value is not changed.
  - [Initial value] : -
- *filter\_num*
  - [Setting] : Static filter number (1..21474836)
  - [Initial value] : -
- *filter\_num\_list*
  - [Setting] : List of statistic filter numbers (1..21474836)
  - [Initial value] : -

**[Description]**

Overwrites the TOS field with the specified value when the IP packet is relayed.

The list is checked in the order of ID numbers, and the filters of the *filter\_num* list are applied in order. If the IP filter that matches first is pass, pass-log, pass-nolog, restrict, restrict-log, or restrict-nolog, the TOS field is overwritten. If the IP filter is reject, reject-log, or reject-nolog, the procedure ends without overwriting the TOS field.

**[Models]**

RTX810, RTX5000

### 6.1.25 Set the Proxy ARP

---

**[Syntax]**

```
ip interface proxyarp proxyarp  
ip interface proxyarp vrrp vrid
```

**no ip interface proxyarp** [*proxyarp*]

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN or Bridge interface name
  - [Initial value] : -
- *proxyarp*
  - [Setting] :

Setting	Description
on	Enable Proxy ARP
off	Disable Proxy ARP

- [Initial value] : off
- *vrld*
  - [Setting] : VRRP group ID (1..255)
  - [Initial value] : -

**[Description]**

Enables/Disables proxy ARP operation. If on is specified, the proxy ARP operation is enabled. The MAC address that is used in this case is the true MAC address of the LAN interface. When the bridge interface is specified, enables/disables proxy ARP operation on physical LAN interface which is assigned to bridge interface. In this case, the MAC address of physical LAN interface which received the ARP is used.

If the second syntax is used, proxy ARP operation is carried out only when the VRRP state of the specified VRID is master. The MAC address that is used is the virtual MAC address of the specified VRID.

**[Note]**

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

### 6.1.26 Set the ARP Entry Lifetime

---

**[Syntax]**

**ip arp timer** *timer* [*retry*]  
**no ip arp timer** [*timer* [*retry*]]

**[Setting and Initial value]**

- *timer*
  - [Setting] : ARP entry lifetime in seconds (30..32767)
  - [Initial value] : 1200
- *retry*
  - [Setting] : ARP request retry count (4..100)
  - [Initial value] : 4

**[Description]**

Sets the ARP entry lifetime. The IP address - MAC address pair obtained by the ARP procedure is stored as an ARP entry. This entry is cleared when the time set by this command has elapsed. Before the entry is erased, an ARP procedure is performed again, and if there is no response to the ARP, the entry is erased. The retry count of the ARP request can be set using the *retry* parameter. As for the interval at which the ARP requests are resent, the first retry is set to two seconds, and then one second subsequently. Normally, it is not necessary to change the *retry* parameter from the initial value.

**[Models]**

RTX810, RTX5000

### 6.1.27 Set a Static ARP Entry

---

**[Syntax]**

**ip interface arp static** *ip\_address mac\_address* [*mtu=mtu*]  
**no ip interface arp static** *ip\_address*[...]

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name

- [Initial value] : -
- *ip\_address*
  - [Setting] : IP address
  - [Initial value] : -
- *mac\_address*
  - [Setting] : MAC address
  - [Initial value] : -
- *mtu*
  - [Setting] :

Setting	Description
interface	Use interface MTU value
discovery	Set value using MTU search function
64..9578 (RTX5000)	MTU value
64..1500 (for all cases except the above)	

- [Initial value] : -

#### [Description]

Sets an ARP entry statically. An ARP entry set with this command will show its TTL as 'permanent' (using the **show arp** command), and will always be valid. Moreover, the entry will not be cleared even if the **clear arp** command is executed.

If the *mtu* option is set to discovery, the MTU discovery function will operate using ARP.

When the *mtu* option is omitted, the interface MTU is used as set.

#### [Note]

The *mtu* option can be specified on the RTX5000.

If the *mtu* option is set to discovery, because communication must be possible with the target host while discovery is being performed, if the target host cannot be communicated with because it is not connected, etc., the MTU discovery will fail, the MTU will be used at the default value of 1500 bytes.

#### [Models]

RTX810, RTX5000

### 6.1.28 Limit the Number of Transmission Packets That Are Held until ARP Is Resolved

---

#### [Syntax]

**ip interface arp queue length len**

**no ip interfacearp arp queue length [len]**

#### [Setting and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *len*
  - [Setting] : Queue length (0..10000)
  - [Initial value] :
    - 200

#### [Description]

Sets the maximum number of transmission packets that can be held for each interface until the ARP is resolved or until a timeout occurs confirming that the ARP cannot be resolved, when an attempt is made to send a packet to a host whose ARP is not resolved.

If 0 is specified, no packets are held. Therefore, for example, if you ping a peer whose ARP is not resolved, the first packet will always fail.

#### [Models]

RTX810, RTX5000

### 6.1.29 Set Whether to Log ARP Entry Changes

---

#### [Syntax]

**ip interface arp log switch**

**no ip interface arp log** [*switch*]

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	Log
off	Not log

- [Initial value] : off

**[Description]**

Sets whether to log ARP entry changes.

**[Note]**

When executing `show log | grep ARP:`, you can confirm the past ARP entry history.

**[Models]**

RTX810, RTX5000

### 6.1.30 Set the Level of Preference of Implicit Routes

---

**[Syntax]**

**ip implicit-route preference** *preference*  
**no ip implicit-route preference** [*preference*]

**[Setting and Initial value]**

- *preference*
- [Setting] : Level of preference of implicit routes (1..2147483647)
- [Initial value] : 10000

**[Description]**

Sets the level of preference of implicit routes.

The level of preference is expressed by a value greater than or equal to 1. The larger the value, the higher is the level of preference.

When an implicit route conflicts with a route obtained through a dynamic routing protocol or with a static route specified by the **ip route** command, the route with the higher level of preference is used. When the level of preference of the implicit route is the same as that of the static route, the static route is used.

When the level of preference of the implicit route is the same as that of the route obtained through a dynamic routing protocol, the route that was used first is used. Even if you change the level of preference of implicit routes using the **ip implicit-route preference** command, the level of preference of the implicit routes that are already registered in the routing table does not change.

**[Note]**

An implicit route is a route that passes through an interface with a specified IP address that is registered implicitly while it is active. For example, when a link is established with a LAN interface that has a specified IP address, the netmask address that is obtained by combining the specified IP address and netmask is registered as the implicit route that passes through that LAN interface.

**[Models]**

RTX810, RTX5000

### 6.1.31 Set the Lifetime of Each Flow Table Entry

---

**[Syntax]**

**ip flow timer** *protocol time*  
**no ip flow timer** *protocol [time]*

**[Setting and Initial value]**

- *protocol* : The protocol whose lifetime you want to set
- [Setting] :

Setting	Description
tcp	TCP packet



Setting	Description
udp	UDP packet
icmp	ICMP packet
slow	TCP with FIN/RST bit set

- [Initial value] :
  - tcp = 900
  - udp = 30
  - icmp = 30
  - slow = 30
- *time*
  - [Setting] : Number of seconds (1-21474836)
  - [Initial value] : -

**[Description]**

Set the lifetime of each flow table entry.

'slow' applies to entries that pass through FIN/RST.

When you are using NAT or dynamic filtering, the lifetimes of those entries are applied.

**[Models]**

RTX810, RTX5000

### 6.1.32 Configure the number of entries in the flow table

---

**[Syntax]**

**ip flow limit** *limit*

**no ip flow limit** [*limit*]

**[Setting and Initial value]**

- *limit*
  - [Setting] : Limit value (10-131072)
  - [Initial value] : 131072

**[Description]**

Configures the number of flow table entries that can be used for the IPv4 fast path and the IPv6 fast path. When using the fast path function, flow over this limit value will be processed using the normal path.

**[Models]**

RTX5000

## 6.2 Setting the Remote PP Interface

---

### 6.2.1 Set the IP Address on the Remote PP Interface

---

**[Syntax]**

**ip pp remote address** *ip\_address*

**ip pp remote address** dhcpc [*interface*]

**no ip pp remote address** [*ip\_address*]

**[Setting and Initial value]**

- *ip\_address*
  - [Setting] :

Setting	Description
IP address	xxx.xxx.xxx.xxx where xxx is a decimal number
dhcp	Keyword indicating that DHCP client is to be used

- [Initial value] : -
- dhcpc : Keyword indicating that DHCP client is to be used
  - [Initial value] : -
- *interface*
  - [Setting] :

- Name of the interface operating as a DHCP client
- The interface name is lan1 when omitted.
- [Initial value] : -

**[Description]**

Sets the IP address of the remote PP interface of the selected peer.

If dhcp is specified, the router itself must be operating as a DHCP server. The router assigns an IP address within the DHCP scope that it is managing.

If dhcpc is specified, the LAN interface specified by *interface* obtains an IP address as a DHCP client, and that address is assigned to the remote PP interface. If an IP address cannot be obtained, 0.0.0.0 is assigned.

**[Example]**

If router A specifies

```
no ip pp remote address
ppp ipcp ipaddress on
```

and the connected router B specifies

```
ip pp remote address yyy.yyy.yyy.yyy
```

the actual IP address on the remote PP interface of router A is set to “yyy.yyy.yyy.yyy”.

**[Models]**

RTX810, RTX5000

## 6.2.2 Set the Remote IP Address Pool

---

**[Syntax]**

```
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 dhcpc [interface]
no ip pp remote address pool
```

**[Setting and Initial value]**

- *ip\_address*
  - [Setting] : IP address pooled for anonymous
  - [Initial value] : -
- *ip\_address-ip\_address*
  - [Setting] : IP address range
  - [Initial value] : -
- dhcp : Keyword indicating that its own DHCP server function is to be used
  - [Initial value] : -
- dhcpc : Keyword indicating that DHCP client is to be used
  - [Initial value] : -
- *interface*
  - [Setting] :
    - Name of the interface operating as a DHCP client
    - The interface name is lan1 when omitted.
  - [Initial value] : -

**[Description]**

Sets the IP address pool to be assigned to the peer using anonymous. This command is valid only when the PP is set to anonymous.

If dhcp is specified, the router itself must be operating as a DHCP server. The router assigns an IP address within the DHCP scope that it is managing.

If dhcpc is specified, the LAN *interface* specified by interface obtains only the IP address as a DHCP client, and that address is assigned. If an IP address cannot be obtained, 0.0.0.0 is assigned.

**[Note]**

The number of ip addresses that can be set as ip\_address is as follows:

Model	Maximum allowed
RTX5000	3104
RTX810	18

**[Models]**

RTX810, RTX5000

**6.2.3 Set the Time Interval of Keepalive via the PP****[Syntax]**

```
pp keepalive interval interval [retry-interval=retry-interval] [count=count] [time=time]
no pp keepalive interval [interval [count]]
```

**[Setting and Initial value]**

- *interval*
  - [Setting] : Time interval for sending keepalive packets [seconds] (1..65535)
  - [Initial value] : 30
- *retry-interval*
  - [Setting] : The transmission interval after the confirmation of the keepalive packet fails once. The unit is seconds. If the keepalive packet is confirmed, the transmission interval returns to the value specified by *interval*
  - [Initial value] : 1
- *count*
  - [Setting] : If no response is received consecutively for the specified number of counts, the remote router is considered to have gone down (3..100)
  - [Initial value] : 6
- *time*
  - [Setting] : Time from when the keepalive packet confirmation failed to when the line is considered to be disconnected. The unit is seconds. This cannot be specified simultaneously with the *count* parameter.
  - [Initial value] : -

**[Description]**

Sets the transmission interval of keepalive packets on the PP interface and the number of retransmissions or time until the line is considered to be disconnected.

The keepalive packet is sent at the interval specified by *interval* while a response is returned for the transmitted keepalive packets. If a response is not confirmed, the transmission interval is changed to the value specified by the *retry-interval* parameter. If no response is confirmed consecutively for the number of times specified by the *count* parameter, the line is considered to be disconnected.

If the time for determining the line disconnection is specified by the time parameter, the line is considered to be disconnected if there is no response continuously for at least the specified *time*.

**[Note]**

If the *time* parameter is specified, the value is recalculated by the keepalive interval and the retry count. Therefore, a value different from the specified value may be displayed by the **show config** command.

**[Models]**

RTX810, RTX5000

**6.2.4 Set Whether to Use Keepalive via the PP****[Syntax]**

```
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
```

**[Setting and Initial value]**

- lcp-echo : Use LCP Echo Request/Reply
  - [Initial value] : -
- icmp-echo : Use ICMP Echo/Reply
  - [Initial value] : -
- *dest\_ip*
  - [Setting] : IP address of the keepalive confirmation destination

- [Initial value] : -
- *Sequence of option = value*
- [Setting] :

<i>option</i>	<i>value</i>	Description
upwait	Milliseconds	Wait time for up detection (1..10000)
downwait	Milliseconds	Wait time for down detection (1..10000)
disconnect	Seconds	No response disconnect time (1..21474836)
length	Bytes	Length of the ICMP Echo packet (64-1500)

- [Initial value] : -

**[Initial value]**

pp keepalive use off

**[Description]**

Sets the keepalive operation for the connection to the selected destination.

If lcp-echo is specified, LCP Echo Request/Reply is used. If icmp-echo is also specified, ICMP Echo/Reply is also used simultaneously. You must set the IP address to use icmp-echo.

**[Note]**

If the **pp always-on** command is set to on, keepalive using LCP Echo is carried out even if this command is not set.

The path to the IP address to be confirmed with icmp-echo must be set so that the configured PP interface is set to be the transmission destination.

Even if the response time is limited by the downwait parameter, if the value specified by the **pp keepalive interval** command is smaller, the value specified by the **pp keepalive interval** command takes precedence. If only one of the parameters downwait and upwait is set, the router operates as if the other value is set to the same value.

The disconnect parameter is used when reconnection is necessary at the PPPoE level when using PPPoE. If the disconnect parameter is specified and there is no response to icmp-echo within the specified time, the connection is cut at the PPPoE level. Therefore, reconnection can be carried out by using this command in combination with the **pp always-on** command.

If the disconnect parameter is set around 70 seconds when other parameters are set to default, the disconnection operation is definitely carried out after the down detection.

The length parameter is used to specify the length of the ICMP data section, not the total length of the IP packet.

**[Models]**

RTX810, RTX5000

## 6.2.5 Set Whether to Log Keepalive via the PP

---

**[Syntax]**

**pp keepalive log** *log*  
**no pp keepalive log** [*log*]

**[Setting and Initial value]**

- *log*
- [Setting] :

Setting	Description
on	Keep a log
off	Not keep a log

- [Initial value] : off

**[Description]**

Sets whether to log keepalive via the PP.

**[Note]**

This setting applies to all PPs.

**[Models]**

RTX810, RTX5000

## 6.2.6 Set the Action when a Leased Line Down is Detected

---

### [Syntax]

**leased keepalive down** *action*  
**no leased keepalive down** [*action*]

### [Setting and Initial value]

- *action*
  - [Setting] :

Setting	Description
silent	Do nothing
reset	Restart router

- [Initial value] : silent

### [Description]

Sets the action taken by the router when the keep alive detects that a leased line has gone down.

### [Models]

RTX5000

## 6.2.7 Set Permanent Connection

---

### [Syntax]

**pp always-on** *switch* [*time*]  
**no pp always-on**

### [Setting and Initial value]

- *switch*
  - [Setting] :

Setting	Description
on	Enable permanent connection
off	Disable permanent connection

- [Initial value] : off
- *time*
  - [Setting] : Number of seconds until a reconnection is requested (60..21474836)
  - [Initial value] : -

### [Description]

Sets whether to connect permanently to the selected destination. Also, specifies the time interval for requesting a reconnection when the permanent connection is terminated.

When permanent connection is specified, connection is started at startup and reconnection is started when the communication is terminated. The keepalive function is used to detect whether the connected peer is down. If the connection fails or the communication terminates abnormally, a reconnection request is made after waiting the time interval specified by *time*. If the communication terminates normally, a reconnection request is made immediately. If *switch* is set to on, the *time* setting is activated. If *time* is not specified, *time* is set to 60.

### [Note]

This command can be used on each PP interface.

When an exclusive line is used as PP, or anonymous is selected, this command is invalid.

### [Models]

RTX810, RTX5000

## 6.3 RIP Configuration

---

### 6.3.1 Set Whether to Use RIP

---

#### [Syntax]

**rip use** *use*  
**no rip use** [*use*]

**[Setting and Initial value]**

- *use*
  - [Setting] :

Setting	Description
on	Enable RIP
off	Disable RIP

- [Initial value] : off

**[Description]**

Sets whether to use RIP. When this function is turned OFF, the router no longer sends RIP packets to any of the interfaces and discards received RIP packets.

**[Models]**

RTX810, RTX5000

**6.3.2 Set the RIP Trusted Gateway****[Syntax]**

```
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 and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *gateway*
  - [Setting] : IP addresses
  - [Initial value] : -

**[Description]**

Sets RIP trusted gateway or untrusted gateway.

If the *except* keyword is not specified, the list of gateways is considered to be trusted gateways, and the router receives RIP only from those gateways.

If the *except* keyword is specified, the list of gateways is considered to be untrusted gateways, and the router only receives RIP from other gateways.

*gateway*

**[Note]**

Trusted and untrusted gateways are not set, and RIP from all hosts are handled as if it can be trusted.

**[Models]**

RTX810, RTX5000

**6.3.3 Set the RIP Routing Preference****[Syntax]**

```
rip preference preference [invalid-route-reactivate=switch]
no rip preference [preference [invalid-route-reactivate=switch]]
```

**[Setting and Initial value]**

- *preference*
  - [Setting] : A value greater than or equal to 1
  - [Initial value] : 1000
- *switch*
  - [Setting] :

Setting	Description
on	Invalid routes from RIP are not deleted

Setting	Description
off	Invalid routes from RIP are deleted

- [Initial value] : off

#### [Description]

Sets the level of preference of the route obtained by RIP. The level of preference of a route is expressed by a value greater than or equal to 1. The larger the value, the higher is the level of preference. If the routes obtained from multiple protocols such as static and RIP are in conflict, the one with the higher level of preference is used. If the level of preference is equal, the route adopted earlier in time is activated.

When a route is received from another router via RIP, if the same route is received from a routing protocol that has been assigned a higher priority than RIP (such as static or OSPF), although the route received from RIP would normally be invalidated and deleted, if the `invalid-route-reactivate` option has been set to `on`, when the higher priority route expires, the RIP route that had been invalidated becomes valid again.

#### [Note]

The level of preference of static routes is fixed to 10000.

When the `invalid-route-reactivate` option is set to `on`, because the RIP sender will not notify for the re-validated route, the affected route will continue to remain in the routing table, so it is preferable to set the `invalid-route-reactivate` option to `off`. In addition, the routes remaining in the routing table above can be deleted by stopping the use of RIP.

#### [Models]

RTX810, RTX5000

### 6.3.4 Set the RIP Packet Transmission

#### [Syntax]

**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...*]

#### [Setting and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *send*
  - [Setting] :

Setting	Description
on	Send RIP packets
off	Not send RIP packets

- [Initial value] :
  - off (off (for the tunnel interface))
  - on (for other interfaces)
- *version*
  - [Setting] : Version of the RIP to be sent(1,2)
  - [Initial value] : 1(case of interface other than tunnel interface)
- *broadcast*
  - [Setting] : Broadcast IP address specified by the **ip interface address** command
  - [Initial value] : -

#### [Description]

Sets whether to send RIP packets to the specified interface.

The version of the RIP to be sent can be specified using “`version version`”.

#### [Models]

RTX810, RTX5000

### 6.3.5 Set the RIP Packet Reception

---

#### [Syntax]

```
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 and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *receive*
  - [Setting] :

Setting	Description
on	Receive RIP packets
off	Not receive RIP packets

- [Initial value] :
  - off (for the tunnel interface)
  - on (for other interfaces)
- *version*
  - [Setting] : Version of the RIP to be sent (1,2)
  - [Initial value] : 1 2 (for the tunnel interface)

#### [Description]

Sets whether to receive RIP packets at the specified interface.

The version of the RIP to be received can be specified using “version *version*”. If not specified, both RIP1 and RIP2 are received.

#### [Models]

RTX810, RTX5000

### 6.3.6 Set the RIP Filtering

---

#### [Syntax]

```
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 and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *direction*
  - [Setting] :

Setting	Description
in	Filtering of received RIP
out	Filtering of RIP to be transmitted

- [Initial value] : -
- *filter\_list*
  - [Setting] : Series of static filter numbers delimited by spaces (up to 100)
  - [Initial value] : -



**[Description]**

Sets the filtering of the RIP that passes the interface.

If the source IP address of the filter specified by the **ip filter** command matches the routing information of the RIP to be exchanged, the information is processed if the filter is set to pass. If the filter is set to reject, only that routing information is discarded.

**[Models]**

RTX810, RTX5000

**6.3.7 Set the Number of Hops to Be Added for RIP****[Syntax]**

```
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
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *direction*
  - [Setting] :

Setting	Description
in	Add to the received RIP
out	Add to the RIP to be sent

- [Initial value] : -
- *hop*
  - [Setting] : The value to be added (0..15)
  - [Initial value] : 0

**[Description]**

Sets the number of hops to be added to the RIP exchanged through the interface.

**[Models]**

RTX810, RTX5000

**6.3.8 Set the RIP2 Authentication****[Syntax]**

```
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]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *type*
  - [Setting] :

Setting	Description
text	Carry out text type authentication

- [Initial value] : -

**[Description]**

Sets the authentication at the interface when using RIP2. If text is specified, a text type authentication is carried out.

**[Models]**

RTX810, RTX5000

**6.3.9 Set the RIP2 Authentication Key**

---

**[Syntax]**

```

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 and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *hex\_key*
  - [Setting] : Authentication key expressed as an array of hexadecimal numbers
  - [Initial value] : -
- *text\_key*
  - [Setting] : Authentication expressed as a text string
  - [Initial value] : -

**[Description]**

Sets the authentication key of the interface when using RIP2.

**[Example]**

```

# ip lan1 rip auth key text testing123
# ip pp rip auth key text "hello world"
# ip lan2 rip auth key 01 02 ff 35 8e 49 a8 3a 5e 9d

```

**[Models]**

RTX810, RTX5000

**6.3.10 Set the Route Hold When the Line Is Disconnected**

---

**[Syntax]**

```

ip pp rip hold routing rip_hold
no ip pp rip hold routing [rip_hold]

```

**[Setting and Initial value]**

- *rip\_hold*
  - [Setting] :

Setting	Description
on	Hold the routing information by RIP even when the line is disconnected
off	Discard the routing information by RIP when the line is disconnected

- [Initial value] : off

**[Description]**

Sets whether to hold the routing information obtained by RIP through the PP interface when the line is disconnected.

**[Models]**

RTX810, RTX5000

### 6.3.11 Set the RIP Operation on the Remote PP Interface When the Line Is Connected

#### [Syntax]

```
ip pp rip connect send rip_action
no ip pp rip connect send [rip_action]
```

#### [Setting and Initial value]

- *rip\_action*
- [Setting] :

Setting	Description
interval	Send RIP at the time interval specified by the <b>ip pp rip connect interval</b> command.
update	Send RIP only when the routing information changes
none	Not send RIP

- [Initial value] : update

#### [Description]

Sets the conditions for sending the RIP to the selected peer when the line is connected.

#### [Example]

```
# ip pp rip connect interval 60
# ip pp rip connect send interval
```

#### [Models]

RTX810, RTX5000

### 6.3.12 Set the RIP Transmission Interval on Remote PP Interface When the Line Is Connected

#### [Syntax]

```
ip pp rip connect interval time
no ip pp rip connect interval [time]
```

#### [Setting and Initial value]

- *time*
- [Setting] : Number of seconds (30..21474836)
- [Initial value] : 30

#### [Description]

Sets the time interval for sending the RIP to the selected peer when the line is connected.

This command is valid when the **ip pp rip send** and **ip pp rip receive** commands are on and the **ip pp rip connect send** command is set to interval.

#### [Example]

```
# ip pp rip connect interval 60
# ip pp rip connect send interval
```

#### [Models]

RTX810, RTX5000

### 6.3.13 Set the RIP Operation on the Remote PP Interface When the Line Is Disconnected

#### [Syntax]

```
ip pp rip disconnect send rip_action
no ip pp rip disconnect send [rip_action]
```

#### [Setting and Initial value]

- *rip\_action*
- [Setting] :

Setting	Description
none	Not send RIP when the line is disconnected

Setting	Description
interval	Send RIP at the time interval specified by the <b>ip pp rip disconnect interval</b> command.
update	Send RIP only when the routing information changes

- [Initial value] : none

**[Description]**

Sets the conditions for sending the RIP to the selected peer when the line is disconnected.

**[Example]**

```
# ip pp rip disconnect interval 1800
# ip pp rip disconnect send interval
```

**[Models]**

RTX810, RTX5000

### 6.3.14 Set the RIP Transmission Interval on the Remote PP Interface When the Line Is Disconnected

**[Syntax]**

```
ip pp rip disconnect interval time
no ip pp rip disconnect interval [time]
```

**[Setting and Initial value]**

- *time*
  - [Setting] : Number of seconds (30..21474836)
  - [Initial value] : 3600

**[Description]**

Sets the time interval for sending the RIP to the selected peer when the line is disconnected.

This command 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 set to interval.

**[Example]**

```
# ip pp rip disconnect interval 1800
# ip pp rip disconnect send interval
```

**[Models]**

RTX810, RTX5000

### 6.3.15 Set Whether to Switch the RIP Source Interface during Backup

**[Syntax]**

```
ip pp rip backup interface switch
no ip pp rip backup interface
```

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Switch
off	Not switch

- [Initial value] : off

**[Description]**

Sets whether to switch the RIP source interface during backup. The RIP source interface is a backup source interface when set to off and a backup destination interface when set to on.

**[Note]**

The difference between the two appears as a difference in the source IP address. When set to off, the backup source interface address is selected. When set to on, the backup destination interface address is selected. In either case, RIP is sent via the backup line.

**[Models]**

RTX810, RTX5000

**6.3.16 Force RIP Route Advertisement**

---

**[Syntax]**

```

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 and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *ip-address/netmask*
  - [Setting] : The network address and netmask length of the route that you want to force the advertisement of, or 'default'.
  - [Initial value] : -
- *metric*
  - [Setting] : The metric value to use for advertisement (1 to 15)
  - [Initial value] : 1

**[Description]**

Uses RIP on the specified interface to force the advertisement even when the specified route does not exist in the routing table. When you set the route to 'default', the default route is advertised.

**[Example]**

Only advertise a portion of the LAN2 host to LAN1.

```

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

```

**[Models]**

RTX810, RTX5000

**6.3.17 Method of Comparison for the RIP2 Filter**

---

**[Syntax]**

```

rip filter rule rule
no rip filter rule [rule]

```

**[Setting and Initial value]**

- *rule*
  - [Setting] :

Setting	Description
address-only	Only the network addresses are compared.

Setting	Description
with-netmask	When RIP2 is being used, the network addresses and net masks are compared.

- [Initial value] : address-only

**[Description]**

Sets how the RIP filter compares the specified filter values and RIP entries.

rip filter rule command	Protocol	Method of Comparison
address-only	RIP1	Netmask filters are treated as range specifications, and the router determines whether the address section of the RIP entry falls within the specified filter range.
	RIP2	
with-netmask	RIP1	The router compares the netmask filter address, netmask, RIP entry address, and netmask to determine whether they match.
	RIP2	

**[Models]**

RTX810, RTX5000

### 6.3.18 Adjust the RIP Timer

---

**[Syntax]**

```
rip timer update [invalid [holddown]]
no rip timer [update]
```

**[Setting and Initial value]**

- *update*
  - [Setting] : Regular advertisement transmission interval (10 to 60 s)
  - [Initial value] : 30 s
- *invalid*
  - [Setting] : Time after the router is unable to receive advertisements until the route is deleted (30 to 360 s)
  - [Initial value] : update × 6 (180 s)
- *holddown*
  - [Setting] : Duration for which a deleted route is advertised through the use of a metric value of 16 (20 to 240 s)
  - [Initial value] : update × 4 (120 s)

**[Description]**

Sets the RIP timer values.

The *update*, *invalid*, and *holddown* values must maintain the following relationships.

$$\begin{aligned} update \times 3 &\leq invalid \leq update \times 6 \\ update \times 2 &\leq holddown \leq update \times 4 \end{aligned}$$
**[Note]**

When you use the **ip pp rip connect/disconnect interval** command on the PP interface, that command takes precedence over the **rip timer** command. However, while the **ip pp rip connect/disconnect interval** command affects the *update* and *invalid* timers, it does not affect the *holddown* timer. Given the value of the **ip pp rip connect/disconnect interval** T, the timer values are as follows:

<i>update</i>	T
<i>invalid</i>	T × 6
<i>holddown</i>	the value set by the <b>rip timer</b> command (the default value is 120 s)

There are no applicable commands for interfaces other than the PP interface, so the timer values for these interfaces are always those set by the **rip timer** command.

**[Models]**  
RTX810, RTX5000

## 6.4 VRRP Configuration

### 6.4.1 Set the VRRP for Each Interface

#### [Syntax]

```
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 and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *vrid*
  - [Setting] : VRRP group ID (1..255)
  - [Initial value] : -
- *ip\_address*
  - [Setting] : IP address of the virtual router
  - [Initial value] : -
- *priority*
  - [Setting] : Priority (1..254)
  - [Initial value] : 100
- *preempt* : Preempt mode
  - [Setting] :

Setting	Description
on	Use
off	Not use

- [Initial value] : on
- *auth*
  - [Setting] : Text authentication text string (up to 8 characters)
  - [Initial value] : -
- *time1*
  - [Setting] : VRRP advertisement interval (seconds)
  - [Initial value] : 1
- *time2*
  - [Setting] : Time to determine that the master is down (seconds)
  - [Initial value] : 3

#### [Description]

Sets the router to use the specified VRRP group.

The VRID and the IP address of the virtual router must match among the routers belonging to the same VRRP group. If they do not match, the operation cannot be predicted.

If the *auth* parameter is not specified, the router operates with no authentication.

Set the interval at which the master sends the VRRP advertisements with the *time1* parameter. Set the time for the backup router to monitor the advertisement and determine that the master is down with the *time2* parameter. On a network with high traffic, the operation may stabilize if these values are set longer than the default values. These values must match among all the VRRP routers.

#### [Note]

The settings of the *priority* and *preempt* parameters are discarded, if the IP address of the virtual router is set to the address allocated to its own LAN interface. In this case, the priority is set to the maximum value of 255, and the router operates in preempt mode at all times.

**[Models]**  
RTX810, RTX5000

## 6.4.2 Set the Shutdown Trigger

### [Syntax]

```
ip interface vrrp shutdown trigger vrid interface
ip interface vrrp shutdown trigger vrid pp peer_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 route network
```

### [Setting and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *vrid*
  - [Setting] : VRRP group ID (1..255)
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Peer number
  - [Initial value] : -
- *network*
  - [Setting] :
    - Network address
    - IP address/mask length
    - default
  - [Initial value] : -
- *nexthop*
  - [Setting] :
    - Interface Name
    - IP address
  - [Initial value] : -

### [Description]

Sets the router to shutdown according to the specified conditions when operating as a master router in the specified VRRP group.

Type	Description
LAN interface type	Shut down when the link of the specified LAN interface is deactivated, or after a down detection by <b>lan keepalive</b> .
pp type	Shut down when communication is no longer possible on the line corresponding to the specified peer number. “Communication is no longer possible” refers to the case when layer 1 is deactivated such as when the cable is disconnected as well as the cases indicated below. <ul style="list-style-type: none"> <li>• When the router decides by the LCP keepalive function that the peer goes down if the line is an exclusive line</li> <li>• When the router detects that the peer is down through the <b>pp keepalive use</b> setting.</li> </ul>
route type	Shuts down if the specified route does not exist in the routing table or the route is not directed at the interface specified by <i>nexthop</i> or the gateways specified by an IP address. If <i>nexthop</i> is omitted, the router does not shut down as long as the route exists regardless of where it is directed.

### [Models]

RTX810, RTX5000

## 6.5 Backup Configuration



### 6.5.1 Set the Destination for PP Backup When the Provider Connection Goes Down

#### [Syntax]

```
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 and Initial value]

- none : Not carry out the backup operation
  - [Initial value] : none
- peer\_num
  - [Setting] : Peer number when using the PP as the backup destination
  - [Initial value] : -
- action : Whether to carry out SA reestablishment immediately after recovering from backup
  - [Setting] :

Setting	Description
on	Reconfigure
off	Not reconfigure

- [Initial value] : off
- interface
  - [Setting] : LAN interface used as the backup destination
  - [Initial value] : -
- ip\_address
  - [Setting] : Gateway IP address
  - [Initial value] : -
- tunnel\_num
  - [Setting] : Tunnel interface number
  - [Initial value] : -

#### [Description]

Specifies the interface to be backed up when the PP interface is disconnected.

If the backup destination interface is PP, the ipsec-fast-recovery option can be specified. When this option is turned on, the IPsec SA is reconfigured immediately after recovering from backup. Therefore, the time it takes for the IPsec communication to become possible is shortened.

#### [Note]

This command can be set for each PP interface.

The **pp always-on** command must be set to on to detect the PP interface disconnection. When the line is an exclusive line, use the **pp keepalive uselep-echo** command, instead of **pp always-on** command.

#### [Models]

RTX810, RTX5000

### 6.5.2 Set the Recovery Time from Backup

#### [Syntax]

```
pp backup recovery time time
no pp backup recovery time [time]
```

#### [Setting and Initial value]

- time
  - [Setting] :

Setting	Description
1..21474836	Number of seconds
off	Recover immediately

- [Initial value] : off

**[Description]**

Specifies whether to recover immediately or recover after waiting the specified time when recovering from backup.

**[Note]**

This setting applies to all PPs.

**[Models]**

RTX810, RTX5000

### 6.5.3 Set the Destination for Backup When the Provider Connection via the LAN Goes Down

---

**[Syntax]**

```
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
```

**[Setting and Initial value]**

- none : Not carry out the backup operation
  - [Initial value] : none
- interface
  - [Setting] : Name of the LAN interface to which backup is to be performed
  - [Initial value] : -
- peer\_num
  - [Setting] : Peer number when using pp for backup
  - [Initial value] : -
- backup\_interface
  - [Setting] : LAN interface used for the backup
  - [Initial value] : -
- ip\_address
  - [Setting] : Gateway IP address
  - [Initial value] : -
- tunnel\_num
  - [Setting] : Tunnel interface number
  - [Initial value] : -

**[Description]**

Sets the interface information for backup that is used if the provider connection via the specified LAN interface goes down.

**[Note]**

The setting using the **lan keepalive use** command is also needed to detect the down condition of the connection via the LAN for the backup operation to work.

**[Models]**

RTX810, RTX5000

### 6.5.4 Set the Recovery Time from Backup

---

**[Syntax]**

```
lan backup recovery time interface time
no lan backup recovery time interface [time]
```

**[Setting and Initial value]**

- interface
  - [Setting] : Name of the LAN interface to which backup is to be performed
  - [Initial value] : -
- time
  - [Setting] :
    - Number of seconds (1..21474836)
    - off
  - [Initial value] : off

**[Description]**

Specifies whether to recover immediately or recover after waiting the specified time when recovering from backup for the specified LAN interface.

**[Models]**

RTX810, RTX5000

**6.5.5 Set Whether to Use Keepalive via the LAN****[Syntax]**

**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 and Initial value]**

- *interface*
  - [Setting] : Name of the LAN interface to which backup is to be performed
  - [Initial value] : -
- *dest\_ip*
  - [Setting] : IP address of the keepalive confirmation destination
  - [Initial value] : -
- *Sequence of option = value*
  - [Setting] :

<i>option</i>	<i>value</i>	<b>Description</b>
upwait	Milliseconds	Wait time for up detection (1..10000)
downwait	Milliseconds	Wait time for down detection (1..10000)
length	Bytes	Length of the ICMP Echo packet (64-1500)

- [Initial value] : -

**[Description]**

Sets whether to carry out keepalive operation on the specified LAN interface. If icmp-echo is specified, ICMP Echo/Reply is used. If arp is specified, ARP Request/Reply is used. The two can also be used together.

**[Note]**

The route of the IP address confirmed with icmp-echo must be directed at the LAN interface to which backup is to be carried out.

Even if the response time is limited by the downwait parameter, if the value specified by the **lan keepalive interval** command is smaller, the value specified by the **lan keepalive interval** command takes precedence. If only one of the parameters downwait and upwait is set, the router operates as if the other value is set to the same value.

The length parameter is used to specify the length of the ICMP data section, not the total length of the IP packet.

**[Models]**

RTX810, RTX5000

**6.5.6 Set the Time Interval of Keepalive via the LAN****[Syntax]**

**lan keepalive interval interface interval [count]**

**no lan keepalive interval interface**

**[Setting and Initial value]**

- *interface*
  - [Setting] : Name of the LAN interface to which backup is to be performed
  - [Initial value] : -
- *interval*
  - [Setting] : Time interval for sending keepalive packets (1..65535)
  - [Initial value] : 30

- *count*
  - [Setting] : Count for determining down detection (3..100)
  - [Initial value] : 6

**[Description]**

Sets the transmission interval of keepalive packets and the count for determining the down detection on the specified LAN interface. If the response packet is not detected consecutively for the number of times specified by *count*, the router determines that the connection is down.

Once a response is not detected, the transmission interval of subsequent packets is shortened to 1 second. Therefore, the time needed to detect the down condition even when using the default setting is approximately 35 seconds.

**[Models]**

RTX810, RTX5000

**6.5.7 Set Whether to Log Keepalive via the LAN**

---

**[Syntax]**

**lan keepalive log** *interface log*

**no lan keepalive log** *interface*

**[Setting and Initial value]**

- *interface*
  - [Setting] : Name of the LAN interface to which backup is to be performed
  - [Initial value] : -
- *log*
  - [Setting] :

Setting	Description
on	Keep a log
off	Not keep a log

- [Initial value] : off

**[Description]**

Sets whether to log keepalive packets.

**[Models]**

RTX810, RTX5000

**6.5.8 Set the Network Monitor Function**

---

**[Syntax]**

**ip keepalive** *num kind interval count gateway* [*gateway ...*] [*option=value ...*]

**no ip keepalive** *num*

**[Setting and Initial value]**

- *num*
  - [Setting] : ID number of this command (1..100; RTX5000 is 1...3000)
  - [Initial value] : -
- *kind* : Monitor type
  - [Setting] :

Setting	Description
icmp-echo	Use ICMP Echo

- [Initial value] : -
- *interval*
  - [Setting] : Transmission interval of keepalive in seconds (1..65535)
  - [Initial value] : -
- *count*
  - [Setting] : Number of transmissions until the router determines that there is no reachability (3..100)
  - [Initial value] : -
- *gateway* : Up to 10 can be specified
  - [Setting] :
    - IP address
      - xxx.xxx.xxx.xxx where xxx is a decimal number

- *dhcp interface*

Setting	Description
interface	Name of the LAN interface and WAN interface operating as DHCP client when using the default gateway provided by DHCP

- [Initial value] : -
- *Sequence of option = value*
- [Setting] :

option	value	Description
log	on	Output SYSLOG
	off	Not output SYSLOG
upwait	Number of seconds	Wait time until the router determines that there is reachability (1..1000000)
downwait	Number of seconds	Wait time in seconds until the router determines that there is no reachability (1..1000000)
length	Bytes	Length of the ICMP Echo packet (64-1500)
local-address	IP address	Source IP address
ipsec-refresh	Security Gateway ID	Forces the SAs of the specified security gateway to be updated when the status changes from DOWNUP or UPDOWN (you can specify multiple gateways by delimiting them with commas).
ipsec-refresh-up	Security Gateway ID	Only forces the SAs of the specified security gateway to be updated when the status changes from DOWNUP (you can specify multiple gateways by delimiting them with commas).
ipsec-refresh-down	Security Gateway ID	Only forces the SAs of the specified security gateway to be updated when the status changes from UPDOWN (you can specify multiple gateways by delimiting them with commas).
gateway-selection-rule	head	Always sends to the gateway that was specified first when sending an ICMP Echo packet to a route with multiple gateways.
	normal	Follows the standard guidelines to select the gateway to send to when sending an ICMP Echo packet to a route with multiple gateways.

- [Initial value] :
  - log=off
  - upwait=5
  - downwait=5
  - length=64
  - gateway-selection-rule=head

#### [Description]

Sends ICMP Echo to the specified gateway and determines whether the response can be received.

#### [Note]

The length parameter is used to specify the length of the ICMP data section, not the total length of the IP packet.

When you switch the main and backup lines using the network backup function, you can use the `ipsec-refresh`, `ipsec-refresh-up`, and `ipsec-refresh-down` parameters to reduce the recovery time for IPsec transmissions.

RTX5000 does not support WAN interface for `interface` parameter.

#### [Example]

When the network backup function is used to switch from backup line `pp11` to main line `pp10`, the router forcefully updates the SAs that belongs to the security gateway that is being used by the IPsec connection and whose ID number is 3.

```
# 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
```

When IP `keepalive1` goes down, route `172.16.224.0/24` is activated through the use of the network backup function.

```
# 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
```

#### [Models]

RTX810, RTX5000

## 6.6 PIM-SM Configuration

### 6.7 Setting of the received packet statistics

#### 6.7.1 Set Whether to Record Statistical Information for Received Packets

##### [Syntax]

**ip interface traffic list** *sw*

**ip pp traffic list** *sw*

**ip tunnel traffic list** *sw*

**no ip interface traffic list** [*sw*]

**no ip pp traffic list** [*sw*]

**no ip tunnel traffic list** [*sw*]

##### [Setting and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *switch*
  - [Setting] :

Setting	Description
on	Records the statistical information for received packets on the specified interface
off	Statistical information for received packets on the specified interface is not recorded

- [Initial value] : off

##### [Description]

Sets whether to record statistical information for received packets. For packets where the combination of the source IP address and the receiving IP address are the same, the packet numbers and octet numbers for each one will be recorded as the statistical information. The statistical information for a maximum of 3 interfaces can be recorded simultaneously.

##### [Note]

Statistical information will not be recorded for packets processed through fast pass. When set to off, the statistical information is cleared and recording is stopped. When set to on, all statistical information up to that point is cleared, and a new record is started. For the IP address displayed when an interface with NAT settings is operated, if the NAT is translatable, the IP address after NAT translation is displayed, if the NAT is not translatable, the IP address of the NAT before translation is displayed. Communication that is cancelled by a receipt filter is not recorded.

#### [Models]

RTX5000

### 6.7.2 Clear statistical information for received packets

---

#### [Syntax]

```
clear ip traffic list [interface]
clear ip traffic list pp [peer_num]
clear ip traffic list tunnel [tunnel_num]
```

#### [Setting and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Peer number, when omitted, selected peer number
  - [Initial value] : -
- *tunnel\_num*
  - [Setting] : Tunnel number, when omitted, selected tunnel number
  - [Initial value] : -

#### [Description]

Clears the statistical information for received packets. If *interface* is omitted, the statistical information for all interfaces is cleared.

#### [Models]

RTX5000

### 6.7.3 Showing statistical information for received packets

---

#### [Syntax]

```
show ip traffic list [interface]
show ip traffic list pp [peer_num]
show ip traffic list tunnel [tunnel_num]
```

#### [Setting and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Peer number; when omitted, the selected peer number
  - [Initial value] : -
- *tunnel\_num*
  - [Setting] : Tunnel number; when omitted, the selected tunnel number
  - [Initial value] : -

#### [Description]

Shows the statistical information for received packets. If *interface* is omitted, the statistical information for all interfaces is shown.

#### [Example]

```
# show ip traffic list lan1
Source IP      Destination IP  Packets  Octets
-----
192.168.200.2  133.176.200.1  1411449  1326237183
133.176.200.3  133.176.200.226  12080    2115561
192.168.200.1  192.168.100.1   802      97211
192.168.200.2  133.176.200.3   17       17348
```

#### [Models]

RTX5000

### 6.7.4 Set the Number of Classifications for Statistical Information Recorded for Received Packets

---

#### [Syntax]

```
ip interface traffic list threshold value
```

```

ip pp traffic list threshold value
ip tunnel traffic list threshold value
no ip interface traffic list threshold [value]
no ip pp traffic list threshold [value]
no ip tunnel traffic list threshold [value]

```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *value*
  - [Setting] : Maximum number of classifications for statistical information recorded for packets (64..5000)
  - [Initial value] : 64

**[Description]**

For the specified interface, specifies the number of classifications for statistical information recorded for received packets.

**[Note]**

Classifies packets based on the combination of the originating IP address and receiving IP address. If the maximum value for the number of classifications for statistical information recorded for packets is exceeded, the information for received packets that would be given a new classification is not recorded. When this command is configured, previous statistical information is cleared.

**[Models]**

RTX5000

## 6.8 Set Packet Transfer Filters

---

### 6.8.1 Define a Packet Transfer Filter

---

**[Syntax]**

```

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 and Initial value]**

- *id*
    - [Setting] : Packet transfer filter (1..255)
    - [Initial value] : -
  - *order*
    - [Setting] : Order of analysis (1..255)
    - [Initial value] : -
  - *gateway*
    - [Setting] :
- | Setting       | Description  |
|---------------|--|
| IP address    | IP address of gateway to which packets are transferred |
| wan1          | WAN interface  |
| pp number     | PP interface   |
| tunnel number | TUNNEL interface                                       |
- [Initial value] : -
  - *filter\_id*
    - [Setting] : **ip filter** command ID
    - [Initial value] : -
  - *keepalive\_id*
    - [Setting] : **ip keepalive** コマンドの識別子
    - [Initial value] : -

**[Description]**

Defines a packet transfer filter.

You can use the *id* parameter to group multiple packet transfer filters.

If you want to use multiple packet transfer filters on the same interface, you must specify the same number for all of them.



The *order* parameter indicates the order of analysis, filters with lower numbers are given preference.

Use the *filter\_id* parameter to specify up to 16 **ip filter** command IDs.

When you specify multiple IDs, IDs that are specified earlier are analyzed first.

The **ip filter** commands are examined in order, and **ip filter** commands that match the content of the packet are used.

If the **ip filter** command action is set to reject, the packet is discarded without being sent, otherwise, the packet is transferred to the gateway specified by the *gateway* parameter.

Use the *keepalive\_id* parameter to specify the **ip keepalive** command ID.

If the result of the IP keepalive specified here is down, this gateway is not used.

In other words, even if there is an appropriate **ip filter** command, it is ignored.

To actually use this command, you must also set the **ip interface forward filter** command.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 6.8.2 Applying a Packet Transfer Filter to an Interface

---

**[Syntax]**

**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 and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *id*
  - [Setting] : A packet transfer filter ID specified by the **ip forward filter** command (1..255)
  - [Initial value] : -

**[Description]**

Applies a packet transfer filter to an interface.

The router compares the packets received by the specified interface with the specified packet transfer filter to determine the gateway to transfer the packets to.

Use the **ip local forward filter** command to make the router filter the packets that it sends.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## Chapter 7

### Ethernet Filter Configuration

#### 7.1 Define a Filter

##### [Syntax]

**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 and Initial value]

- *num*
  - [Setting] : Static filter number (1-100)
  - [Initial value] : -

- *kind*
  - [Setting] :

Setting	Description
pass-log	Pass if matched (record in the log)
pass-nolog	Pass if matched (not record in the log)
reject-log	Discard if matched (record in the log)
reject-nolog	Discard if matched (not record in the log)

- [Initial value] : -
- *src\_mac*
  - [Setting] :
    - Source MAC address
    - XX:XX:XX:XX:XX:XX (where XX is a hexadecimal number or \*)
    - \* (Applied to all MAC addresses)
  - [Initial value] : -
- *dst\_mac*
  - [Setting] :
    - Destination MAC address
    - Same format as the source MAC address *src\_mac*
    - Same as a single \* when omitted.
  - [Initial value] : -
- *type*
  - [Setting] :

Setting	Description
dhcp-bind	Apply to hosts reserved by the specified DHCP scope
dhcp-not-bind	Apply to hosts not reserved by the specified DHCP scope

- [Initial value] : -
- *scope*
  - [Setting] :
    - DHCP scope
    - Integer, 1..65535
    - The IP addresses included in the lease range of the DHCP scope
  - [Initial value] : -
- *offset*
  - [Setting] : Decimal value representing the offset (the byte immediately after the source MAC address of the Ethernet frame is assumed to be zero)
  - [Initial value] : -
- *byte\_list*
  - [Setting] :

- Byte list
- Series of XX (two-digit hexadecimal) and \* (represents all bytes) separated by commas (up to 16 items)
- [Initial value] : -

**[Description]**

Sets an Ethernet frame filter. The filters set by this command are used by the **ethernet lan filter** command.

Normal filters are applied to the source MAC address, destination MAC address, etc., of sent and received Ethernet frames. dhcp-bind filters are applied to the Ethernet frames listed below. Frames that the filter does not apply to are filtered out.

- For IPv4 packets that meet one of the following requirements:
  - The Ethernet type is IPv4 (0x0800).
  - In a PPPoE environment, the Ethernet type is PPoE data frame (0x8864), and the protocol ID is IPv4 (0x0800).
  - In a 802.1Q tag VLAN environment, the TPID is 802.1Q tag (0x8100), and the Ethernet type is IPv4 (0x0800).

If the source MAC address and source IP address of an Ethernet frame are reserved in the specified DHCP scope, the frame passes through the filter.

- For the following Ethernet types:
  - ARP(0x0806)
  - RARP(0x8035)
  - PPPoE discovery packet (0x8863)
  - MAC layer control packet (0x8808)

Ethernet frames whose source MAC address is reserved in the specified DHCP scope pass through the filter.

dhcp-not-bind filters are applied to the Ethernet frames listed below. Frames that the filter does not apply to are filtered out.

- When the Ethernet type is IPv4 (0x0800)

If the source IP address of the Ethernet frame is within the leased range of the target DHCP scope, and if the source MAC Address is not reserved in the DHCP scope in the dhcp-not-bind type filter, then it is deemed to match the filter.

Use the *scope* parameter to specify the DHCP scope to use in dhcp-bind and dhcp-not-bind filters.

You can specify the *scope* parameter by entering a DHCP scope number or by entering the IP address of a subnet with a defined DHCP scope. If you specify an IP address with multiple scopes, the scope with the longest netmask is selected.

If you omit the *scope* parameter, the scope is selected from all the scopes in the specified interface.

When a dhcp-bind or dhcp-not-bind filter is specified on a router that is functioning as a DHCP relay agent, the DHCP scope and its client reservation information are obtained from the DHCP server and referred to when the filter is applied. The router obtains the DHCP scope and reservation information from the DHCP server during the relay of DHCP messages. The reservation information is written in the options field of the DHCP messages.

**[Note]**

When you are using the LAN division function, you need to be careful to specify filtering. Since the router internally uses 0x8100 to 0x810f for the Ethernet type, if you specify filtering of such an Ethernet frame to disable sending and receiving data, ports using the LAN division function cannot communicate.

Because dhcp-bind and dhcp-not-bind filters use the Ethernet frame's source MAC address and source IP address for filtering, you can normally only specify the "in" direction with the **ethernet lan filter** command when you use these filters.

If you specify the "out" direction, the source MAC address becomes the address of the router itself, and it will not match with the DHCP reservation information or leased address.

Because the dhcp-bind filter only allows reserved clients to pass, it is typically used with pass filters. On the other hand, because the dhcp-not-bind filter discards clients that are not reserved, it is typically used with reject filters.

**[Models]**

RTX810, RTX5000

## 7.2 Set the Application to the Interface

---

**[Syntax]**

```
ethernet interface filter dir list
no ethernet interface filter dir [list]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *dir*
  - [Setting] :

Setting	Description
in	Filtering of packets coming in from the LAN interface
out	Filtering of packets output to the LAN interface

- [Initial value] : -
- *list*
  - [Setting] : Series of static filter numbers delimited by spaces (up to 100)
  - [Initial value] : -

**[Description]**

Limits the types of packets to pass the LAN interface by combining with the packet filter specified by the **ethernetat filter** command.

**[Note]**

You can specify a physical LAN interface and an interface used for the LAN division function for the LAN interface name. you can specify the VLAN interface for the interface used for the LAN division function.

**[Models]**

RTX810, RTX5000

## 7.3 Show the Ethernet Filter Status

---

**[Syntax]**

**show status ethernet filter** *type* [*scope*]

**[Setting and Initial value]**

- *type*
  - [Setting] :

Setting	Description
dhcp-bind	Hosts reserved by the specified DHCP scope
dhcp-leased	Hosts of which address is leased by the specified DHCP scope

- [Initial value] : -
- *scope*
  - [Setting] : Scope number (1-65535)
  - [Initial value] : -

**[Description]**

Shows the Ethernet filter status.

**[Models]**

RTX810, RTX5000

# Chapter 8

## URL Filter Configuration

### 8.1 Define a Filter

#### [Syntax]

```
url filter id kind keyword [src_addr[/mask]]
```

```
no url filter id
```

#### [Setting and Initial value]

- *id*
  - [Setting] : Filter number (1..65535)
  - [Initial value] : -

- *kind*

- [Setting] :

Setting	Description
pass, pass-nolog	Pass if matched (not record in the log)
pass-log	Pass if matched (record in the log)
reject, reject-log	Discard if matched (record in the log)
reject-nolog	Discard if matched (not record in the log)

- [Initial value] : -

- *keyword*

- [Setting] :

Setting	Description
Arbitrary string	All or part of the URL to be filtered (up to 255 characters)
*	Apply to all URLs

- [Initial value] : -

- *src\_addr* : Source IP address of the IP packet

- [Setting] :

Setting	Description
Arbitrary IPv4 address	A single IPv4 address
Rrange designation	A range specified by two IP addresses separated by a hyphen or one IP address preceded or followed by a hyphen
*	Apply to all IP addresses
Omitted	Same as * when omitted.

- [Initial value] : -

- *mask*

- [Setting] : Netmask length (can be specified only when *src\_addr* is a network address)

- [Initial value] : -

#### [Description]

Sets a URL filter. The filters set by this command are used by the **url interface filter** command.

If the specified keyword contains uppercase characters, they are converted to lowercase characters before the data is saved.

#### [Models]

RTX810, RTX5000

### 8.2 Apply a URL Filter to an Interface

#### [Syntax]

```
url interface filter dir list
```

**url pp filter** *dir list*  
**url tunnel filter** *dir list*  
**no url interface filter**  
**no url pp filter**  
**no url tunnel filter**

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *dir*
  - [Setting] :

Setting	Description
in	Filter the HTTP input
out	Filter the HTTP output

- [Initial value] : -
- *list*
  - [Setting] : Series of URL filter numbers delimited by spaces (up to 512 items for RTX5000, up to 128 items for all other models)
  - [Initial value] : -

**[Description]**

Limits the HTTP packets that pass the interface by combining packet filters specified by the **url filter** command to reject specified URLs.

The number of settable filters is up to 512 on the RTX5000 models, and up to 128 on all other models. The command line character string length is up to 4095 characters.

Packets that do not meet any of the specified filters are discarded.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

### 8.3 Set the HTTP Port Numbers to Apply the URL Filter To

---

**[Syntax]**

**url filter port** *list*  
**no url filter port**

**[Setting and Initial value]**

- *list*
  - [Setting] : Series of port numbers delimited by spaces (up to 4)
  - [Initial value] : 80

**[Description]**

Sets the HTTP port numbers to apply the URL filter to.

**[Models]**

RTX810, RTX5000

### 8.4 Set Whether to Use the URL Filter

---

**[Syntax]**

**url filter use** *switch*  
**no url filter use**

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Use the URL filter.
off	Do not use the URL filter.

- [Initial value] : on

#### [Description]

Sets whether to use the URL filter.

#### [Models]

RTX810, RTX5000

## 8.5 Set the HTTP Response to the Source of a Packet Discarded by the URL Filter

---

#### [Syntax]

```
url filter reject redirect
url filter reject redirect url
url filter reject off
no url filter reject [action]
```

#### [Setting and Initial value]

- **redirect** : Return the HTTP redirect HTTP response and transfer it to the blocked item display
  - [Initial value] : redirect (for all models except RTX5000)
- **off** : Do not return an HTTP response. Use TCP RST to close the TCP session
  - [Initial value] : off (for RTX5000)
- *url*
  - [Setting] : The URL to redirect to (up to 255 characters starting with “http://” or “https://”)
  - [Initial value] : -
- *action*
  - [Setting] :
    - redirect
    - off
  - [Initial value] : -

#### [Description]

Sets the HTTP response to the source of a packet discarded by the URL filter.

In the blocked item display, the filtered keyword and the reason that access was denied appear.

If a *url* was specified, when the URL is actually redirected, a question mark appears after the specified *url*, and a query of the following type is appended.

- The URL whose access was denied
- The keyword setting of the applicable filter

You must set the *url* to a string that starts with “http://” or “https://”.

#### [Note]

On models that support the HTTP server function, to set redirect and show the blocked item display on a Web browser, you must set **httpd service** on.

#### [Models]

RTX810, RTX5000

## 8.6 Set Whether to Log Filter Matches

---

#### [Syntax]

```
url filter log switch
no url filter log
```

#### [Setting and Initial value]

- *switch*
  - [Setting] :

Setting	Description
on	Log filter matches
off	Do not log filter matches

- [Initial value] : on

**[Description]**

Sets whether to log filter matches.

**[Note]**

Even if you select on, logging does not take place for packets that match filters whose *kind* parameter has been set to pass, p pass-nolog, or reject-nolog by the **url filter** command.

**[Models]**

RTX810, RTX5000



## Chapter 9

### PPP Configuration

#### 9.1 Set the Peer Name and Password

##### [Syntax]

```
pp auth username username password [myname myname mypass] [ip_address] [ip6_prefix]
```

```
no pp auth username username [password...]
```

##### [Setting and Initial value]

- *username*
  - [Setting] : Name (up to 64 characters)
  - [Initial value] : -
- *password*
  - [Setting] : Password (up to 64 characters)
  - [Initial value] : -
- *myname* : Keyword for entering the settings on local side
  - [Initial value] : -
- *myname*
  - [Setting] : User name on local side
  - [Initial value] : -
- *mypass*
  - [Setting] : Password on local side
  - [Initial value] : -
- *ip\_address*
  - [Setting] : IP address to be assigned to the peer
  - [Initial value] : -
- *ip6\_prefix*
  - [Setting] : Prefix assigned to the user
  - [Initial value] : -

##### [Description]

Sets the peer name and passwords. Multiple settings are possible.  
The settings on the local side can be entered as an option.

When carrying out authentication in both directions, a process for authenticating itself to the peer starts after the peer user name is confirmed.

If these parameters are not set, the settings of the **pp auth myname** command are viewed.

If the name is set to \*, it is handled as a wildcard. These settings are used for a peer that does not match with other names.

##### [Models]

RTX810, RTX5000

#### 9.2 Set the Type of Authentication to Accept

##### [Syntax]

```
pp auth accept accept [accept]
```

```
no pp auth accept [accept]
```

##### [Setting and Initial value]

- *accept*
  - [Setting] :

Setting	Description
pap	Accept PAP authentication
chap	Accept CHAP authentication
mschap	Accept MSCHAP authentication

Setting	Description
mschap-v2	Accept MSCHAP Version 2 authentication

- [Initial value] : Not accept authentication

#### [Description]

Sets whether to accept PPP authentication requests from the peer. This setting is always applied when making a call. For calls received that is not anonymous, a PP interface is selected through the originating number before this setting is applied. For calls received that is anonymous, this setting is applied when the PP selection through the originating number fails.

Even if the router is set to accept authentication by this command, if its own name and password are not set by the **pp auth myname** command, authentication is rejected.

This command can be used on each PP interface.

#### [Models]

RTX810, RTX5000

## 9.3 Set the Authentication Type to Be Requested

#### [Syntax]

```
pp auth request auth [arrive-only]
no pp auth request [auth[arrive-only]]
```

#### [Setting and Initial value]

- *auth*
- [Setting] :

Setting	Description
pap	Request PAP authentication
chap	Request CHAP authentication
mschap	Request MSCHAP authentication
mschap-v2	Request MSCHAP Version 2 authentication
chap-pap	Request CHAP or PAP authentication

- [Initial value] : -

#### [Description]

Sets whether to request PAP and CHAP authentication to the selected peer. This setting is always applied when making a call. For calls received that is not anonymous, a PP interface is selected through the originating number before this setting is applied. For calls received that is anonymous, this setting is applied when the PP selection through the originating number fails.

If the chap-pap keyword is specified, CHAP is requested first. If it is rejected by the peer, PAP is then requested. This simplifies the connection even if the peer supports only PAP or only CHAP.

If the arrive-only keyword is specified, PPP authentication is requested when a call is received but not when making a call.

#### [Models]

RTX810, RTX5000

## 9.4 Set Its Own Name and Password

#### [Syntax]

```
pp auth myname myname password
no pp auth myname [myname password]
```

#### [Setting and Initial value]

- *myname*
  - [Setting] : Name (up to 64 characters)
  - [Initial value] : -
- *password*
  - [Setting] : Password (up to 64 characters)
  - [Initial value] : -

**[Description]**

Sets its own name and password that are sent to the peer for PAP or CHAP.  
This command can be used on each PP interface.

**[Models]**

RTX810, RTX5000

## 9.5 Set Whether to Prohibit Multiple Connections from a Peer with the Same Username

---

**[Syntax]**

```
pp auth multi connect prohibit prohibit
no pp auth multi connect prohibit [prohibit]
```

**[Setting and Initial value]**

- *prohibit*
- [Setting] :

Setting	Description
on	Prohibit
off	Not prohibit

- [Initial value] : off

**[Description]**

Sets whether to prohibit multiple connections from a peer with the same *username* that was registered by the **pp auth username** command.

**[Note]**

This function is convenient when operating a fixed charge provider. If the users are managed using RADIUS, prohibiting of multiple connections must be handled on the RADIUS server.  
This command is valid only when anonymous is selected.

**[Models]**

RTX810, RTX5000

## 9.6 LCP Configuration

---

### 9.6.1 Set the Address and Control Field Compression Option

---

**[Syntax]**

```
ppp lcp acfc acfc
no ppp lcp acfc [acfc]
```

**[Setting and Initial value]**

- *acfc*
- [Setting] :

Setting	Description
on	Use
off	Not use

- [Initial value] : off

**[Description]**

Sets whether to use the Address and Control Field Compression option of [PPP, LCP] for the selected peer.

**[Note]**

Even if on is specified, the option is not used if it is rejected by the peer.

**[Models]**

RTX810, RTX5000

### 9.6.2 Set the Magic Number Option

---

**[Syntax]**

```
ppp lcp magicnumber magicnumber
```

**no ppp lcp magicnumber** [*magicnumber*]

**[Setting and Initial value]**

- *magicnumber*
- [Setting] :

Setting	Description
on	Use
off	Not use

- [Initial value] : on

**[Description]**

Sets whether to use the Magic Number option of [PPP, LCP] for the selected peer.

**[Note]**

Even if on is specified, the option is not used if it is rejected by the peer.

**[Models]**

RTX810, RTX5000

### 9.6.3 Set the Maximum Receive Unit Option

---

**[Syntax]**

**ppp lcp mru** *mru* [*length*]

**no ppp lcp mru** [*mru* [*length*]]

**[Setting and Initial value]**

- *mru*
- [Setting] :

Setting	Description
on	Use
off	Not use

- [Initial value] : on
- *length* : MRU value
- [Setting] :
  - 1280..1792
- [Initial value] : 1792

**[Description]**

Sets whether to use the Maximum Receive Unit option of [PPP, LCP] for the selected peer and sets the MRU value.

**[Note]**

Even if on is specified, the option is not used if it is rejected by the peer. In general, this option is set to on. However when connecting to a router that cannot connect when this option is specified, select off.

If data compression is used, the *length* parameter value is always 1792.

**[Models]**

RTX810, RTX5000

### 9.6.4 Set the Protocol Field Compression Option

---

**[Syntax]**

**ppp lcp pfc** *pfc*

**no ppp lcp pfc** [*pfc*]

**[Setting and Initial value]**

- *pfc*
- [Setting] :

Setting	Description
on	Use
off	Not use

- [Initial value] : off

**[Description]**

Sets whether to use the Protocol Field Compression option of [PPP, LCP] for the selected peer.

**[Note]**

Even if on is specified, the option is not used if it is rejected by the peer.

**[Models]**

RTX810, RTX5000

**9.6.5 Set the lcp-restart Parameter**

---

**[Syntax]**

```
ppp lcp restart time
no ppp lcp restart [time]
```

**[Setting and Initial value]**

- *time*
  - [Setting] : Milliseconds (20..10000)
  - [Initial value] : 3000

**[Description]**

Sets the retransmission time of configure-request and terminate-request of [PPP, LCP] for the selected peer.

**[Models]**

RTX810, RTX5000

**9.6.6 Set the lcp-max-terminate Parameter**

---

**[Syntax]**

```
ppp lcp maxterminate count
no ppp lcp maxterminate [count]
```

**[Setting and Initial value]**

- *count*
  - [Setting] : Count (1..10)
  - [Initial value] : 2

**[Description]**

Sets the transmission count of terminate-request of [PPP, LCP] for the selected peer.

**[Models]**

RTX810, RTX5000

**9.6.7 Set the lcp-max-configure Parameter**

---

**[Syntax]**

```
ppp lcp maxconfigure count
no ppp lcp maxconfigure [count]
```

**[Setting and Initial value]**

- *count*
  - [Setting] : Count (1..10)
  - [Initial value] : 10

**[Description]**

Sets the transmission count of configure-request of [PPP, LCP] for the selected peer.

**[Models]**

RTX810, RTX5000

**9.6.8 Set the lcp-max-failure Parameter**

---

**[Syntax]**

```
ppp lcp maxfailure count
no ppp lcp maxfailure [count]
```

**[Setting and Initial value]**

- *count*
  - [Setting] : Count (1..10)
  - [Initial value] : 10

**[Description]**

Sets the transmission count of configure-nak of [PPP, LCP] for the selected peer.

**[Models]**

RTX810, RTX5000

## 9.6.9 Set Whether to Send Configure-Request Immediately

---

**[Syntax]**

```
ppp lcp silent switch
no ppp lcp silent [switch]
```

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	For PPP/LCP, delay the transmission of Configure-Request immediately after the line is connected until Configure-Request is received from the peer.
off	For PPP/LCP, send Configure-Request immediately after the line is connected.

- [Initial value] : off

**[Description]**

For PPP/LCP, sets whether to send Configure-Request immediately after the line is connected or delay the transmission until Configure-Request is received from the peer. Normally, it is okay to send Configure-Request immediately after the line is connected. However, on some peers, it may be better to delay the transmission.

**[Models]**

RTX810, RTX5000

## 9.7 PAP Configuration

---

### 9.7.1 Set the pap-restart Parameter

---

**[Syntax]**

```
ppp pap restart time
no ppp pap restart [time]
```

**[Setting and Initial value]**

- *time*
- [Setting] : Milliseconds (20..10000)
- [Initial value] : 3000

**[Description]**

Sets the retransmission time of authenticate-request of [PPP, PAP] for the selected peer.

**[Models]**

RTX810, RTX5000

### 9.7.2 Set the pap-max-authreq Parameter

---

**[Syntax]**

```
ppp pap maxauthreq count
no ppp pap maxauthreq [count]
```

**[Setting and Initial value]**

- *count*
- [Setting] : Count (1..10)
- [Initial value] : 10

**[Description]**

Sets the transmission count of authenticate-request of [PPP, PAP] for the selected peer.

**[Models]**

RTX810, RTX5000

## 9.8 CHAP Configuration

---

### 9.8.1 Set the chap-restart Parameter

---

**[Syntax]**

**ppp chap restart** *time*  
**no ppp chap restart** [*time*]

**[Setting and Initial value]**

- *time*
  - [Setting] : Milliseconds (20..10000)
  - [Initial value] : 3000

**[Description]**

Sets the retransmission time of challenge of [PPP, CHAP] for the selected peer.

**[Models]**

RTX810, RTX5000

### 9.8.2 Set the chap-max-challenge Parameter

---

**[Syntax]**

**ppp chap maxchallenge** *count*  
**no ppp chap maxchallenge** [*count*]

**[Setting and Initial value]**

- *count*
  - [Setting] : Count (1..10)
  - [Initial value] : 10

**[Description]**

Sets the transmission count of challenge of [PPP, CHAP] for the selected peer.

**[Models]**

RTX810, RTX5000

## 9.9 IPCP Configuration

---

### 9.9.1 Set the Van Jacobson Compressed TCP/IP

---

**[Syntax]**

**ppp ipcp vjc** *compression*  
**no ppp ipcp vjc** [*compression*]

**[Setting and Initial value]**

- *compression*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : off

**[Description]**

Sets whether to use Van Jacobson Compressed TCP/IP of [PPP, IPCP] for the selected peer.

**[Note]**

Even if on is specified, the option is not used if it is rejected by the peer.

**[Models]**

RTX810, RTX5000

### 9.9.2 Set the IP Address Negotiation with the Remote PP Interface

---

**[Syntax]**

**ppp ipcp ipaddress** *negotiation*  
**no ppp ipcp ipaddress** [*negotiation*]

**[Setting and Initial value]**

- *negotiation*
  - [Setting] :

Setting	Description
on	Negotiate
off	Not negotiate

- [Initial value] : off

**[Description]**

Sets whether to negotiate the IP address with the remote PP interface for the selected peer.

**[Models]**

RTX810, RTX5000

### 9.9.3 Set the ipcp-restart Parameter

---

**[Syntax]**

```
ppp ipcp restart time
no ppp ipcp restart [time]
```

**[Setting and Initial value]**

- *time*
  - [Setting] : Milliseconds (20..10000)
  - [Initial value] : 3000

**[Description]**

Sets the retransmission time of configure-request and terminate-request of [PPP, IPCP] for the selected peer.

**[Models]**

RTX810, RTX5000

### 9.9.4 Set the ipcp-max-terminate Parameter

---

**[Syntax]**

```
ppp ipcp maxterminate count
no ppp ipcp maxterminate [count]
```

**[Setting and Initial value]**

- *count*
  - [Setting] : Count (1..10)
  - [Initial value] : 2

**[Description]**

Sets the transmission count of terminate-request of [PPP, IPCP] for the selected peer.

**[Models]**

RTX810, RTX5000

### 9.9.5 Set the ipcp-max-configure Parameter

---

**[Syntax]**

```
ppp ipcp maxconfigure count
no ppp ipcp maxconfigure [count]
```

**[Setting and Initial value]**

- *count*
  - [Setting] : Count (1..10)
  - [Initial value] : 10

**[Description]**

Sets the transmission count of configure-request of [PPP, IPCP] for the selected peer.

**[Models]**

RTX810, RTX5000



### 9.9.6 Set the ipcp-max-failure Parameter

---

#### [Syntax]

```
ppp ipcp maxfailure count
no ppp ipcp maxfailure [count]
```

#### [Setting and Initial value]

- *count*
  - [Setting] : Count (1..10)
  - [Initial value] : 10

#### [Description]

Sets the transmission count of configure-nak of [PPP, IPCP] for the selected peer.

#### [Models]

RTX810, RTX5000

### 9.9.7 Set the IP Address of the WINS Server

---

#### [Syntax]

```
wins server server1 [server2]
no wins server [server1 [server2]]
```

#### [Setting and Initial value]

- *server1, server2*
  - [Setting] : IP address (xxx.xxx.xxx.xxx where xxx is a decimal number)
  - [Initial value] : -

#### [Description]

Sets the IP address of the WINS (Windows Internet Name Service).

#### [Note]

Sets the IPCP MS extension option and the IP address of the WINS server to be passed to the client through DHCP. The router does not carry out any operations as a WINS client to this server.

#### [Models]

RTX810, RTX5000

### 9.9.8 Set Whether to Use the IPCP MS Extension Option

---

#### [Syntax]

```
ppp ipcp msex msex
no ppp ipcp msex [msex]
```

#### [Setting and Initial value]

- *msex*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : off

#### [Description]

Sets whether to use the MS extension option of [PPP, IPCP] for the selected peer.

When the IPCP Microsoft extension is enabled, the DNS server IP address and the WINS (Windows Internet Name Service) server IP address can be passed to the Windows PC of the connected peer. The IP addresses of the DNS server and WINS server to be passed are set using the **dns server** and **wins server** commands, respectively

If off is specified, the router does not accept the IP address of the DNS server or WINS server even if it is passed.

#### [Models]

RTX810, RTX5000

### 9.9.9 Set Whether to Accept a Peer IP Address That Has a Host Route

---

#### [Syntax]

```
ppp ipcp remote address check sw
```

**no ppp ipcp remote address check** [*sw*]

**[Setting and Initial value]**

- *sw*
- [Setting] :

Setting	Description
on	Reject PP interface peer address notifications
off	Accept PP interface peer address notifications

- [Initial value] : on

**[Description]**

Sets whether to accept the peer IP address that is received during the establishment of a PP connection when that IP address already has a host route through another PP connection.

**[Models]**

RTX810, RTX5000

## 9.10 MSCBCP Configuration

---

### 9.10.1 Set the mscbcpr-restart Parameter

---

**[Syntax]**

**ppp mscbcpr restart** *time*  
**no ppp mscbcpr restart** [*time*]

**[Setting and Initial value]**

- *time*
  - [Setting] : Milliseconds (20..10000)
  - [Initial value] : 1000

**[Description]**

Sets the retransmission time of request/Response of [PPP, MSCBCP] for the selected peer.

**[Models]**

RTX810, RTX5000

### 9.10.2 Set the mscbcpr-maxretry Parameter

---

**[Syntax]**

**ppp mscbcpr maxretry** *count*  
**no ppp mscbcpr maxretry** [*count*]

**[Setting and Initial value]**

- *count*
  - [Setting] : Count (1..30)
  - [Initial value] : 30

**[Description]**

Sets the transmission count of request/Response of [PPP, MSCBCP] for the selected peer.

**[Models]**

RTX810, RTX5000

## 9.11 CCP Configuration

---

### 9.11.1 Set the Compression Type of All Packets

---

**[Syntax]**

**ppp ccp type** *type*  
**no ppp ccp type** [*type*]

**[Setting and Initial value]**

- *type*
  - [Setting] :

Setting	Description
stac0	Compress using Stac LZS
stac	Compress using Stac LZS
cstac	Compress using Stac LZS (when the peer is a Cisco router)
mppe-40	Encrypt using 40-bit MPPE
mppe-128	Encrypt using 128-bit MPPE
mppe-any	Encrypt using 40-bit or 128-bit MPPE
none	Not Compress

- [Initial value] :
  - stac

**[Description]**

Selects the [PPP, CCP] compression type for the selected peer.

**[Note]**

This can be used in combination with Van Jacobson Compressed TCP/IP.

If *type* is set to stac and packet loss occurs frequently such as due to a poor line condition or large load, communication may not be performed correctly. If this happens, the compression is automatically set to none. No compression continues until the next time the router is started. If such conditions cannot be improved, you should specify stac0. However, the destination must also support stac0. The compression rate is lower for stac0 than stac.

Sometimes communication is not possible when the destination is a Cisco router when stac is applied. If this happens, communication may be possible by changing the setting to cstac.

For mppe-40, mppe-128, mppe-any, a key is exchanged for each packet. MPPE stands for Microsoft Point-To-Point Encryption (Protocol). This extends CCP and uses RC4 as its encryption algorithm. The key length is 40 bits or 128 bits. This is set for generating encryption keys along with the authentication protocol MS-CHAP or MS-CHAPv2.

**[Models]**

RTX810, RTX5000

### 9.11.2 Set the ccp-restart Parameter

---

**[Syntax]**

```
ppp ccp restart time
no ppp ccp restart [time]
```

**[Setting and Initial value]**

- *time*
  - [Setting] : Milliseconds (20..10000)
  - [Initial value] : 3000

**[Description]**

Sets the retransmission time of configure-request and terminate-request of [PPP, CCP] for the selected peer.

**[Models]**

RTX810, RTX5000

### 9.11.3 Set the ccp-max-terminate Parameter

---

**[Syntax]**

```
ppp ccp maxterminate count
no ppp ccp maxterminate [count]
```

**[Setting and Initial value]**

- *count*
  - [Setting] : Count (1..10)
  - [Initial value] : 2

**[Description]**

Sets the transmission count of terminate-request of [PPP, CCP] for the selected peer.

**[Models]**

RTX810, RTX5000

**9.11.4 Set the ccp-max-configure Parameter**

---

**[Syntax]**

```
ppp ccp maxconfigure count
no ppp ccp maxconfigure [count]
```

**[Setting and Initial value]**

- *count*
  - [Setting] : Count (1..10)
  - [Initial value] : 10

**[Description]**

Sets the transmission count of configure-request of [PPP, CCP] for the selected peer.

**[Models]**

RTX810, RTX5000

**9.11.5 Set the ccp-max-failure Parameter**

---

**[Syntax]**

```
ppp ccp maxfailure count
no ppp ccp maxfailure [count]
```

**[Setting and Initial value]**

- *count*
  - [Setting] : Count (1..10)
  - [Initial value] : 10

**[Description]**

Sets the transmission count of configure-nak of [PPP, CCP] for the selected peer.

**[Models]**

RTX810, RTX5000

**9.12 IPV6CP Configuration**

---

**9.12.1 Set Whether to Use IPV6CP**

---

**[Syntax]**

```
ppp ipv6cp use use
no ppp ipv6cp use [use]
```

**[Setting and Initial value]**

- *use*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : on

**[Description]**

Sets whether to use IPV6CP for the selected peer.

**[Models]**

RTX810, RTX5000

**9.13 PPPoE Configuration**

---

**9.13.1 Specify the LAN Interface Used by PPPoE**

---

**[Syntax]**

```
pppoe use interface
no pppoe use
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -

**[Description]**

Specifies the LAN interface used by PPPoE for the selected peer. If it is not specified, PPPoE is not used.

**[Models]**

RTX810, RTX5000

**9.13.2 Set the Access Concentrator Name**

---

**[Syntax]**

**pppoe access concentrator** *name*  
**no pppoe access concentrator**

**[Setting and Initial value]**

- *name*
  - [Setting] : Text string representing the access concentrator name (7-bit US-ASCII)
  - [Initial value] : -

**[Description]**

Sets the name of the access concentrator that is connected using PPPoE for the selected peer. This command is used to specify the access concentrator to be connected when there are multiple access concentrators that can be connected.

**[Models]**

RTX810, RTX5000

**9.13.3 Set the Session Auto Connection**

---

**[Syntax]**

**pppoe auto connect** *switch*  
**no pppoe auto connect**

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Enable auto connection
off	Disable auto connection

- [Initial value] : on

**[Description]**

Sets whether to automatically connect PPPoE sessions for the selected peer.

**[Models]**

RTX810, RTX5000

**9.13.4 Set the Session Auto Disconnection**

---

**[Syntax]**

**pppoe auto disconnect** *switch*  
**no pppoe auto disconnect**

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Enable auto disconnection
off	Disable auto disconnection

- [Initial value] : on

**[Description]**

Sets whether to automatically disconnect PPPoE sessions for the selected peer.

**[Models]**

RTX810, RTX5000

**9.13.5 Set the Maximum Retry Count of PADI Packets**

---

**[Syntax]**

**pppoe padi maxretry** *times*  
**no pppoe padi maxretry**

**[Setting and Initial value]**

- *times*
  - [Setting] : Count (1..10)
  - [Initial value] : 5

**[Description]**

Sets the maximum retry count of PADI packets in the PPPoE protocol.

**[Models]**

RTX810, RTX5000

**9.13.6 Set the Retransmission Time of PADI Packets**

---

**[Syntax]**

**pppoe padi restart** *time*  
**no pppoe padi restart**

**[Setting and Initial value]**

- *time*
  - [Setting] : Milliseconds (20..10000)
  - [Initial value] : 3000

**[Description]**

Sets the retransmission time of PADI packets in the PPPoE protocol.

**[Models]**

RTX810, RTX5000

**9.13.7 Set the Maximum Retry Count of PADR Packets**

---

**[Syntax]**

**pppoe padr maxretry** *times*  
**no pppoe padr maxretry**

**[Setting and Initial value]**

- *times*
  - [Setting] : Count (1..10)
  - [Initial value] : 5

**[Description]**

Sets the maximum retry count of PADR packets in the PPPoE protocol.

**[Models]**

RTX810, RTX5000

**9.13.8 Set the Retransmission Time of PADR Packets**

---

**[Syntax]**

**pppoe padr restart** *time*  
**no pppoe padr restart**

**[Setting and Initial value]**

- *time*
  - [Setting] : Milliseconds (20..10000)
  - [Initial value] : 3000

**[Description]**

Sets the retransmission time of PADR packets in the PPPoE protocol.

**[Models]**

RTX810, RTX5000

### 9.13.9 Set the Disconnection Timer of PPPoE Sessions

---

#### [Syntax]

**pppoe disconnect time** *time*  
**no pppoe disconnect time**

#### [Setting and Initial value]

- *time*
- [Setting] :

Setting	Description
1..21474836	Number of seconds
off	Disable the timer

- [Initial value] : off

#### [Description]

Sets the timeout value for automatically disconnecting PPPoE sessions for the selected peer.

#### [Note]

LCP and NCP packets are not monitored.

#### [Models]

RTX810, RTX5000

### 9.13.10 Set the Service Name

---

#### [Syntax]

**pppoe service-name** *name*  
**no pppoe service-name**

#### [Setting and Initial value]

- *name*
- [Setting] : Text string representing the service name (7-bit US-ASCII, up to 255 characters)
- [Initial value] : -

#### [Description]

Sets the name of the service that is requested using PPPoE for the selected peer.

This command is used to select the access concentrator that can provide the requested service when there are multiple access concentrators that can be connected.

#### [Models]

RTX810, RTX5000

### 9.13.11 Turn ON/OFF the MSS Limit of TCP Packets and the Size

---

#### [Syntax]

**pppoe tcp mss limit** *length*  
**no pppoe tcp mss limit**

#### [Setting and Initial value]

- *length*
- [Setting] :

Setting	Description
1240..1452	Data length
auto	Limit the MSS according to the MTU value
off	Not limit MSS.

- [Initial value] : auto

#### [Description]

Sets whether to limit the MSS (Maximum Segment Size) of TCP packets on a PPPoE session.

#### [Note]

If this command and the **ip interface tcp mss limit** command are both valid, the MSS is limited to the smaller of the two values.

**[Models]**

RTX810, RTX5000

**9.13.12 Set Whether to Forcefully Disconnect PPPoE Sessions That Do Not Exist on the Router**

---

**[Syntax]****pppoe invalid-session forced close** *sw***no pppoe invalid-session forced close****[Setting and Initial value]**

- *sw*

- [Setting] :

Setting	Description
on	Forcefully disconnect PPPoE sessions that do not exist on the router
off	Do not forcefully disconnect PPPoE sessions that do not exist on the router

- [Initial value] : on

**[Description]**

Sets whether to forcefully disconnect PPPoE sessions that do not exist on the router.

**[Models]**

RTX810, RTX5000



# Chapter 10

## DHCP Configuration

DHCP(\*1) server function, DHCP relay agent function, and DHCP client function are implemented as DHCP functions on the router. Auto configuration of the basic network environment is achieved through the use of the DHCP function.

The DHCP client function is implemented on operating systems such as Windows. By combining this with the DHCP server function and DHCP relay agent function of the router, auto configuration of the basic network environment is achieved.

The **dhcp service** command is used to make the router function as a DHCP server, a DHCP relay agent, or neither of the functions. The current setting can be inquired using the **show status dhcp** command.

The DHCP server function assigns (leases) an IP address and provides netmask and DNS server information in response to a configuration request from a DHCP client.

The **dhcp scope** command sets the range and lease period of the IP addresses that are to be assigned.

Multiple IP address ranges can be specified. Each range is managed by a DHCP scope number. When a configuration request is received from a DHCP client, the DHCP server automatically sends a notification indicating an unassigned IP address within the DHCP scope. To lease a certain IP address to a certain DHCP client, the **dhcscope bind** command is used to reserve the IP address by using the scope number that was defined by the **dhcp scope** command. The **no dhcp scope bind** command is used to release the reservation. The lease period of IP addresses can be set to a specific time or infinity. These are set using the **expire** and **maxexpire** keyword parameters of the **dhcp scope** command.

The lease status can be inquired using the **show status dhcp** command. The DNS server IP address information that is sent to the DHCP client is the information that is specified by the **dns server** command.

The DHCP relay agent function transfers a request from a DHCP client in the local segment to a DHCP server at a remote network segment specified in advance. The **dhcp relay server** command is used to set the DHCP server in the remote segment. If multiple DHCP servers are available, you can specify the selection method using the **dhcp relay select** command.

In addition, the DHCP client function can be used to obtain information about the interface, such as the IP address and default routing information, from an external DHCP server. Whether the router functions as a DHCP client is determined by the settings of the **ip interface address**, **ip interface secondary address**, **ip pp remote address**, and **ip pp remote address pool** commands. The current settings can be inquired using the **show status dhcp** command.

(\*1)Dynamic Host Configuration Protocol; RFC1541 , RFC2131

URL reference: <http://rfc.netvolante.jp/rfc/rfc1541.txt> ([rfc2131.txt](http://rfc.netvolante.jp/rfc/rfc2131.txt))

### 10.1 DHCP Server and Relay Agent Function

#### 10.1.1 Set the DHCP Operation

##### [Syntax]

```
dhcp service type
no dhcp service [type]
```

##### [Setting and Initial value]

- *type*
- [Setting] :

Setting	Description
server	Operate the router as a DHCP server
relay	Operate the router as a DHCP relay agent

- [Initial value] : -

##### [Description]

Sets DHCP functions.

The NAT function cannot be used while the DHCP relay agent function is being used.

##### [Note]

For the default settings of this command when it is shipped from the factory and when the **cold start** command is executed, see "1.7 About the Factory Default Settings".

##### [Models]

RTX810, RTX5000

## 10.1.2 Set the RFC2131 Compliant Operation

### [Syntax]

```
dhcp server rfc2131 compliant comp
dhcp server rfc2131 compliant [except] function [function...]
no dhcp server rfc2131 compliant
```

### [Setting and Initial value]

- *comp*

- [Setting] :

Setting	Description
on	Comply with RFC2131
off	Comply with RFC1541

- [Initial value] : on
- *except* : Keyword indicating that the functions other than those specified are RFC2131 compliant

- [Initial value] : -

- *function*

- [Setting] :

Setting	Description
broadcast-nak	Send DHCPNAK by broadcast
none-domain-null	Not add the NULL character at the end of the domain name
remain-silent	Discard DHCPREQUESTs from clients that do not have lease information
reply-ack	Return DHCPACK containing the tolerance value in place of DHCPNAK
use-clientid	Prioritize the Client-Identifier option in the client identification

- [Initial value] : -

### [Description]

Specifies the DHCP server operation. If on is specified, the operation is RFC2131 compliant. If off is specified, the operation is RFC1541 compliant.

If individual functions of RFC2131 are to be supported with RFC1541 as the base, use the parameters below.

Multiple parameters can be specified by delimiting each parameter with a space. If the *except* keyword is specified, functions other than the specified parameter become RFC2131 compliant.

broadcast-nak	Send DHCPNAK to clients on the same subnet as broadcast. If DHCPREQUEST is received from a client in the INIT-REBOOT state, bit B is set if it addressed to giaddr.
none-domain-null	Not add the NULL character at the end of this domain name. RFC1541 did not indicate whether a NULL character is to be added to the end of the domain name. It was prohibited in RFC2131. The DHCP server on Windows NT and Windows 2000 add the NULL character. Therefore, many DHCP clients running Windows expect the NULL character to be present. If the NULL character is not present, problems may occur such as the display being disrupted when winipcfg.exe is run.
remain-silent	When a DHCPREQUEST is received from a client and the router does not have the lease information of the client, DHCPNAK is not sent.
reply-ack	When an option value that is not allowed such as the lease period (excluding the request IP address) is requested from a client, the router returns a DHCPACK containing an allowed value instead of returning DHCPNAK.

use-clientid	Prioritize the use of the Client-Identifier option over the chaddr field in the identification of the client.
--------------	---

**[Note]**

For the default settings of this command when it is shipped from the factory and when the **cold start** command is executed, see “1.7 About the Factory Default Settings”.

**[Models]**

RTX810, RTX5000

### 10.1.3 Set Whether to Check Duplications in the Leased IP Address

---

**[Syntax]**

**dhcp duplicate check** *check1 check2*

**no dhcp duplicate check**

**[Setting and Initial value]**

- *check1* : Wait time for performing a check within the LAN

- [Setting] :

Setting	Description
1..1000	Milliseconds
off	Not perform the check within the LAN

- [Initial value] : 100

- *check2* : Wait time for performing a check outside the LAN (via the DHCP relay agent)

- [Setting] :

Setting	Description
1..3000	Milliseconds
off	Not perform the check outside the LAN (via the DHCP relay agent)

- [Initial value] : 500

**[Description]**

Sets whether to check that the IP address is not used by another host before leasing the IP address to the DHCP client when the router is operating as a DHCP server.

**[Note]**

The check is performed using ARP for scope within the LAN and PING for scope via the DHCP relay agent.

**[Models]**

RTX810, RTX5000

### 10.1.4 Define the DHCP Scope

---

**[Syntax]**

**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 and Initial value]**

- *scope\_num*

- [Setting] : Scope number (1..65535)

- [Initial value] : -

- *ip\_address-ip\_address*

- [Setting] : Range of IP addresses to be assigned in the target subnet

- [Initial value] : -

- *netmask*

- [Setting] :

- xxx.xxx.xxx.xxx where xxx is a decimal number
- Hexadecimal number following 0x
- Number of mask bits

- [Initial value] : -

- *ex\_ip*

- [Setting] : IP addresses to exclude within the specified range of IP addresses (multiple addresses can be specified by delimiting each address with a space or a range can be specified using a hyphen)
- [Initial value] : -
- *gw\_ip*
  - [Setting] : IP address of the gateway of the target IP address network
  - [Initial value] : -
- *time* : Time
  - [Setting] :

Setting	Description
1..2147483647	Minutes
xx:xx	Hour:minutes
infinity	Infinite lease

- [Initial value] :
  - expire time=72:00
  - maxexpire time=72:00

### [Description]

Sets the scope of the IP addresses that the DHCP server is to assign.

Multiple IP addresses to be excluded. The lease period can be set to infinity or an allowable maximum lease period when a request is received from the DHCP client.

### [Note]

Multiple DHCP scopes cannot be set on a single network. Multiple DHCP scopes cannot include the same IP address. If the IP address range includes a network address or broadcast address, it is excluded from the addresses that can be assigned.

If the configuration parameter that uses the gateway keyword is omitted, the IP address of the router itself is sent to DHCP clients that do not traverse a DHCP relay agent.

If a DHCP scope is overwritten, the previous lease information and reserve information are cleared. The expire parameter must be set to a lower value than the maxexpire parameter.

For the default settings of this command when it is shipped from the factory and when the **cold start** command is executed, see “1.7 About the Factory Default Settings”.

### [Models]

RTX810, RTX5000

## 10.1.5 Set the Reserved DHCP Address

### [Syntax]

```

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
no dhcp scope bind scope_num ip_address

```

### [Setting and Initial value]

- *scope\_num*
  - [Setting] : Scope number (1..65535)
  - [Initial value] : -
- *ip\_address*
  - [Setting] :

Setting	Description
xxx.xxx.xxx.xxx	IP address to be reserved (xxx is a decimal number)
*	Do not specify an IP address

- [Initial value] : -
- *type* : Determine the *type* field of the Client-Identifier option
  - [Setting] :

Setting	Description
text	0x00

Setting	Description
ethernet	0x01

- [Initial value] : -
- *id*
- [Setting] :

Setting	Description
When <i>type</i> is ethernet	MAC Address
When <i>type</i> is text	Text string
When <i>type</i> is omitted	Two-digit hexadecimal sequence, the head of which is the type field.

- [Initial value] : -
- *mac\_address*
  - [Setting] : xx:xx:xx:xx:xx:xx (xx is a hexadecimal number) MAC address of the reserved DHCP client
  - [Initial value] : -
- *ipcp* : Keyword indicating that the address is provided to the remote end through IPCP
  - [Initial value] : -

### [Description]

Fixes the DHCP client to which the IP address is to be assigned.

you can specify a client only without fixing the IP address. When deleting this format, you cannot omit the client identifier.

### [Note]

The IP address must be within the DHCP scope range specified by the *scope\_num* parameter. Multiple IP addresses within a DHCP scope cannot be assigned to a single MAC address. If an IP address that is being leased to another DHCP client is reserved, the IP address is assigned after the completion of the current lease.

If the **dhcp scope** command is executed, all related reservations are cleared. The *ipcp* designation is limited by the number of B channels that can connect simultaneously. In addition, the address granted by IPCP is selected from the scope on the LAN side.

To use the first syntax of the command, **dhcp server rfc2131 compliant** on must be specified or the *useclientid* function must be enabled in advance. In addition, when **dhcp server rfc2131 compliant** off is specified or the *use-clientid* function is disabled, all reservations other than those specified by the second syntax of the command are cleared.

The client identifier in the first syntax of the command is set to the value sent by the client as an option. If the *type* parameter is omitted, enter the command including the value of the *type* field. If a keyword is specified in the *type* parameter, the *type* field value is uniquely determined. Thus, enter only the value of the Client-Identifier field.

The MAC address reservation using the second syntax of the command uses the *chaddr* field of the DHCP packet for client identification. The reservation function in this form works only if the RT is set to **dhcp server rfc2131 compliant** off, the *use-clientid* function is disabled, or the DHCP client does not include the Client-Identifier option in the DHCP packet.

If **dhcp server rfc2131 compliant** on or the *use-clientid* parameter is specified, the reservation using the second syntax of the command is invalid when the client uses the Client-Identifier option.

### [Example]

```
A. # dhcp scope bind scope_num ip_address ethernet 00:a0:de:01:23:45
B. # dhcp scope bind scope_num ip_address text client01
C. # dhcp scope bind scope_num ip_address 01 00 a0 de 01 23 45 01 01 01
D. # dhcp scope bind scope_num ip_address 00:a0:de:01:23:45
```

1. When **dhcp server rfc2131 compliant** on is specified or the *use-clientid* function is enabled

- On A. or B. or C. syntax, Client-Identifier is used for identify the client.
- On D. syntax, *chaddr* field of DHCP packet is used, but if Client-Identifier option is included in DHCP packet, this configuration is omitted.

The parameter of Client-Identifier option is used preferentially than the value of *chaddr* field.

It is possible to determine the client is using Client-Identifier option or not by checking client identification using **show status dhcp** command.

- When the MAC address is output as client identification, Client-Identifier option is not used.
  - When the hexadecimal string or string is output as client identification, Client-Identifier option is used. For IP address reservation to the client who use Client-Identifier option, use the displayed hexadecimal string or string.
2. When **dhcp server rfc2131 compliant** off is specified or the *use-clientid* function is disabled
- It can not be configured by A. or B. or C. syntax. Client-Identifier option is omitted.

- On D. syntax, `chaddr` field of DHCP packet is used.

Below are points to keep in mind concerning the mutual operation with the client.

- Using the individual functions independently may cause the client to behave in an unexpected manner. Therefore, we recommend that you use **dhcp server rfc2131 compliant** on or **dhcp server rfc2131 compliant** off.
- As a result, if DHCPDISCOVER that the client sends at the end of the lease period contains the Requested IP Address option, the client can continue to lease the same IP address.

To prevent this from happening, **dhcp server rfc2131 compliant** on (or the remain-silent function) may be effective. In this setting, the Yamaha router does not return DHCPNAK in response to a DHCPREQUEST received from a client that the router does not have the lease information for and instead simply discards the request.

As a result, if DHCPDISCOVER that the client sends at the end of the lease period contains the Requested IP Address option, the client can continue to lease the same IP address.

#### [Models]

RTX810, RTX5000

### 10.1.6 Set the DHCP Address Assignment Operation

#### [Syntax]

**dhcp scope lease type** *scope\_num type* [`fallback=fallback_scope_num`]

**no dhcp scope lease type** *scope\_num* [`type ...`]

#### [Setting and Initial value]

- *scope\_num, fallback\_scope\_num*
  - [Setting] : Scope number (1-65535)
  - [Initial value] : -
- *type* : Assignment type
  - [Setting] :

Setting	Description
bind-priority	Assign by giving priority to the reservation information
bind-only	Assign based only on the reservation information

- [Initial value] : bind-priority

#### [Description]

Control how addresses are assigned within the DHCP scope specified by the *scope\_num* parameter

If *type* is set to bind-priority, clients whose addresses have been reserved by the **dhcp scope bind** command get their reserved addresses assigned to them. Clients that do not have reserved addresses get the remaining unreserved IP addresses within the scope assigned to them.

You cannot specify a fallback option if *type* is set to bind-priority.

If *type* is set to bind-only, the operation varies depending on whether or not a fallback scope is specified as the fallback option.

If no fallback option is specified, clients whose addresses have been reserved by the **dhcp scope bind** command get their reserved addresses assigned to them. Clients without reserved addresses do not get addresses assigned to them even if there are unreserved addresses in the scope.

Described below is the operation for when *type* is set to bind-only and a fallback scope is specified as the fallback option.

1. Clients with reserved IP addresses within the scope get those addresses assigned to them.
2. Clients that do not have reserved IP addresses within the scope but that do have reserved addresses within the fallback scope get their reserved fallback scope addresses assigned to them.
3. For clients that do not have a reserved address within the scope or the fallback scope, the operation varies depending on how the **dhcp scope lease type** command is set.
  - a. If the **dhcp scope lease type** command for the fallback scope is set to bind-priority, the client gets an address from the fallback scope assigned to it as long as an address is available.
  - b. If the **dhcp scope lease type** command for the fallback scope is set to bind-only, the client does not get an IP address assigned to it.

For both cases, the lease period is determined by the DHCP scope definition.

#### [Models]

RTX810, RTX5000

## 10.1.7 Generate Reserved Settings Based on the DHCP Assignment Information

### [Syntax]

**dhcp convert lease to bind** *scope\_n* [except] [*idx* [...]]

### [Setting and Initial value]

- *scope\_n*
  - [Setting] : Scope number (1-65535)
  - [Initial value] : -
- *idx*
  - [Setting] :

Setting	Description
Number	Index numbers shown by the <b>show status dhcp summary</b> command (up to 100 numbers)
all	All information that is assigned
Omitted	all if omitted.

- [Initial value] : -

### [Description]

Generates reserved settings based on the current assignment information. If the **except** keyword is specified, information other than the specified number is applied to the reserved settings.

### [Note]

The IP address assignment information is converted to reserved settings according to the following rules.

Client ID type of the IP address assignment information (name show status dhcp)	Client ID Information Example	Reserved Setting Information Example
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** compliant on or **use-clientid** is specified, the display of the IP address assignment information is highly likely to be the result of the ARP check. Because the client ID option is normally used in the assignment, this format is used to specify the reserved settings. However, if there are hosts that use client IDs that differ from the MAC addresses, the reservation through this automatic conversion does not work effectively. If such hosts exist, the reserved settings must be specified manually.

\*2: If **rfc2131** compliant off or **use-clientid** is specified, use the **chaddr** field.

Generates reserved settings based on the assignment information at the time the command is executed. If time has passed since the summary was displayed until this conversion command was executed, you should check that the reservation of intended pairs has been created using **show config** after executing this command.

### [Models]

RTX810, RTX5000

## 10.1.8 Set the DHCP Options

### [Syntax]

**dhcp scope option** *scope\_num* *option=value*  
**no dhcp scope option** *scope\_num* [*option=value*]

### [Setting and Initial value]

- *scope\_num*
  - [Setting] : Scope number (1..65535)
  - [Initial value] : -
- *option*
  - [Setting] :
    - Option number

- 1..49,62..254
- Mnemonic
- Main mnemonics

router	3
dns	6
hostname	12
domain	15
wins_server	44

- [Initial value] : -
- *value* : Option value
- [Setting] :
  - The types of values that are available are listed below. The option number determines which values can be used. For example, 'router', 'dns' and , 'wins server' are an array of IP addresses, and 'hostname' and 'domain' are text strings.

1-octet integer	0..255
2-octet integer	0..65535
Array of 2-octet integers	Series of 2-octet integers delimited by commas
4-octet integer	0..2147483647
IP address	IP address
Array of IP addresses	IP addresses delimited by commas
Text string	Text string
Switches	"on", "off", "1", or "0"
Binary	Series of 2-digit hexadecimals delimited by commas

- [Initial value] : -

#### [Description]

Sets the DHCP option to be sent for the scope. DHCP options are implicitly sent by **dns server**, **wins server**, and other commands. But, this command can be used to specify them explicitly. In addition, the option values cannot be changed at the scope level in implicit DHCP options, but this command makes it possible.

#### [Note]

If the scope is deleted with the **no dhcp scope** command, all option settings are also cleared.

#### [Models]

RTX810, RTX5000

### 10.1.9 Manually Add DHCP Lease Information

#### [Syntax]

```
dhcp manual lease ip_address [type] id
dhcp manual lease ip_address mac_address
dhcp manual lease ip_address ipcp
```

#### [Setting and Initial value]

- *ip\_address*
  - [Setting] : IP address to be leased
  - [Initial value] : -
- *type* : Determine the type field of the Client-Identifier option
  - [Setting] :

Setting	Description
text	0x00
ethernet	0x01

- [Initial value] : -
- *id*



- [Setting] :

Setting	Description
When <i>type</i> is set to text	Text string
When <i>type</i> is ethernet	MAC Address
When <i>type</i> is omitted	Two-digit hexadecimal sequence, the head of which is the <i>type</i> field.

- [Initial value] : -

- *mac\_address*

- [Setting] : XX:XX:XX:XX:XX:XX (where XX is a hexadecimal) MAC address of the DHCP client

- [Initial value] : -

- *ipcp* : Keyword that indicates that the IP address has been granted to the remote interface through IPCP

- [Initial value] : -

#### [Description]

Manually adds lease information of a specific IP address.

#### [Note]

This command affects the DHCP address distribution that is carried out automatically. It should be used only when you intentionally want to add lease information of a specific IP address.

#### [Models]

RTX810, RTX5000

### 10.1.10 Manually Release DHCP Lease Information

---

#### [Syntax]

**dhcp manual release** *ip\_address*

#### [Setting and Initial value]

- *ip\_address*
  - [Setting] : IP address to be released
  - [Initial value] : -

#### [Description]

Manually releases lease information of a specific IP address.

#### [Note]

This command affects the DHCP address distribution that is carried out automatically. It should be used only when you intentionally want to release lease information of a specific IP address.

#### [Models]

RTX810, RTX5000

### 10.1.11 Set the DHCP Server Designation

---

#### [Syntax]

**dhcp relay server** *host1* [*host2* [*host3* [*host4*]]]

**no dhcp relay server**

#### [Setting and Initial value]

- *host1..host4*
  - [Setting] : IP addresses of DHCP servers
  - [Initial value] : -

#### [Description]

Specifies up to four servers that relay DHCP BOOTREQUEST packets.

The **dhcp relay select** command determines whether the BOOTREQUEST packet is duplicated and relayed to all servers or relayed to a single selected server when multiple servers are specified.

#### [Models]

RTX810, RTX5000

### 10.1.12 Set the DHCP Server Selection Method

---

#### [Syntax]

**dhcp relay select** *type*

**no dhcp relay select** [*type*]

**[Setting and Initial value]**

- *type*
- [Setting] :

Setting	Description
hash	Select a server using the Hash function
all	Select all servers

- [Initial value] : hash

**[Description]**

Sets the handling of multiple servers specified by the **dhcrelay server** command.

If hash is specified, a single server is selected by the Hash function, and the packet is relayed to it. Since this Hash function uses the chaddr field of the DHCP message as a parameter, the same server should be selected at all times for the same DHCP client. If all is specified, the packet is duplicated and relayed to all servers.

**[Models]**

RTX810, RTX5000

### 10.1.13 Set the Relay Reference of the DHCP BOOTREQUEST Packet

---

**[Syntax]**

**dhcp relay threshold** *time*  
**no dhcp relay threshold** [*time*]

**[Setting and Initial value]**

- *time*
- [Setting] : Number of seconds (0..65535)
- [Initial value] : 0

**[Description]**

Compares the secs field of the DHCP BOOTREQUEST packet and the number of seconds specified by this command. DHCP BOOTREQUEST packets whose secs field is smaller than the specified value are not relayed to the server.

This prevents the packet from being relayed to a remote DHCP server even when there is another DHCP server on the same LAN.

**[Models]**

RTX810, RTX5000

## 10.2 DHCP Client Function

---

### 10.2.1 Set the Host Name of the DHCP Client

---

**[Syntax]**

**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 and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name, bridge interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] :
    - Peer number
    - anonymous
  - [Initial value] : -
- *pool\_num*

- [Setting] : The IP address number that is obtained by the **ip pp remote address pool dhcp** command. For example, on models that can obtain two IP addresses using the **ip pp remote address pool dhcp** command, an arbitrary ID can be assigned to each client ID option by setting *pool\_num* to 1 or 2.(1.. Maximum number of IP addresses that can be retrieved using the **ip pp remote address pool dhcp** command)
- [Initial value] : -
- *host*
  - [Setting] : Host name of the DHCP client
  - [Initial value] : -

**[Description]**

Sets the host name of the DHCP client.

**[Note]**

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

When the WAN interface is set, you cannot specify *secondary*.

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 10.2.2 Set the Interface to Obtain the DNS Server Address

---

**[Syntax]**

**dns server dhcp** *interface*

**no dns server dhcp**

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name, bridge interface name
  - [Initial value] : -

**[Description]**

Sets the interface to obtain the DNS server address. If the interface name is specified by this command, when name resolution is carried out through the DNS, a query is made through the specified interface to the DNS server address obtained from the DHCP server. If a DNS server address cannot be obtained from the DHCP server, name resolution is not carried out.

If the DNS server is explicitly specified by the **dns server** command or the DNS server to be queried is specified by the **dns server select** and **dns server pp** commands, the DNS server specified by these commands takes precedence.

**[Note]**

This function requires that the specified interface is operating as a DHCP client.

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 10.2.3 Set the Lease Period of the Requested IP Address

---

**[Syntax]**

**ip interface dhcp lease time** *time*

**no ip interface dhcp lease time** [*time*]

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name, bridge interface name
  - [Initial value] : -
- *time*
  - [Setting] : Minutes (1..21474836)
  - [Initial value] : -

**[Description]**

Sets the lease period of the IP address requested by the DHCP client.

**[Note]**

If the lease period request is not accepted or the lease period is not requested, the lease period from the DHCP server is used.

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.  
RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 10.2.4 Set the Retry Count and Interval of the IP Address Get Request

---

**[Syntax]**

**ip interface dhcp retry** *retry interval*  
**no ip interface dhcp retry** [*retry interval*]

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name, bridge interface name
  - [Initial value] : -
- *retry*
  - [Setting] :

Setting	Description
1..100	Count
infinity	Infinite

- [Initial value] : infinity
- *interval*
  - [Setting] : Number of seconds (1..100)
  - [Initial value] : 5

**[Description]**

Sets the number of retries and the interval when obtaining an IP address fails.

**[Note]**

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.  
RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 10.2.5 Set the DHCP Client ID Option

---

**[Syntax]**

**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 and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name, bridge interface name
  - [Initial value] : -
- *type* : Keyword indicating that the type field value of the ID option is specified
  - [Initial value] : -
- *type*
  - [Setting] : The type field value of the ID option
  - [Initial value] : 1
- *id*
  - [Setting] :
    - ID expressed using an ASCII text string
    - ID expressed using an array of 2-digit hexadecimals
  - [Initial value] : -

- *peer\_num*
  - [Setting] :
    - Peer number
    - anonymous
  - [Initial value] : -
- *pool\_num*
  - [Setting] : The IP address number that is obtained by the **ip pp remote address pool dhcpc** command. For example, on models that can obtain two IP addresses using the **ip pp remote address pool dhcpc** command, an arbitrary ID can be assigned to each client ID option by setting *pool\_num* to 1 or 2.(1.. Maximum number of IP addresses that can be retrieved using the **ip pp remote address pool dhcpc** command)
  - [Initial value] : -

**[Description]**

Sets the type field and ID of the DHCP client ID option.

**[Note]**

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

When the WAN interface is set, you cannot specify *secondary*.

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 10.2.6 Set the Options to Be Stored in the Message That the DHCP Client Sends to the DHCP Server

---

**[Syntax]**

```

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 and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name, bridge interface name
  - [Initial value] : -
- *option*
  - [Setting] : Option number (decimal number)
  - [Initial value] : -
- *value*
  - [Setting] : Option value to be stored (hexadecimal number, multiple values can be specified by delimiting each value with a comma) Note that there is no need to input the option length information.
  - [Initial value] : -
- *peer\_num*
  - [Setting] :
    - Peer number
    - anonymous
  - [Initial value] : -
- *pool\_num*
  - [Setting] : The IP address number that is obtained by the **ip pp remote address pool dhcpc** command. For example, on models that can obtain two IP addresses using the **ip pp remote address pool dhcpc** command, an arbitrary ID can be assigned to each client ID option by setting *pool\_num* to 1 or 2.(1.. Maximum number of IP addresses that can be retrieved using the **ip pp remote address pool dhcpc** command)
  - [Initial value] : -

**[Description]**

Set the options to be stored in the message that the DHCP client sends to the DHCP server.

**[Note]**

Use this command only when it is necessary to resolve compatibility issues in a connection with the server.

The option values are not used inside the router.  
 The WAN interface can be specified for RTX810.  
 When the WAN interface is set, you cannot specify *secondary*.

**[Example]**

1. Request a specific address (192.168.0.128) when obtaining the LAN2 primary address from the DHCP server.

```
# dhcp client option lan2 primary 50=c0,a8,00,80
# ip lan2 address dhcp
(Note: Even in this case, whether the requested address is provided by the server is up to the server.)
```

**[Models]**

RTX810, RTX5000

## 10.2.7 Set Whether to Release the Information When the Link Is Down

---

**[Syntax]**

```
dhcp client release linkdown switch [time]
no dhcp client release linkdown [switch [time]]
```

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Release the information when the interface link is continuously down for <i>time</i> seconds
off	Hold the information even when the interface link is down

- [Initial value] : off
- *time*
  - [Setting] : Number of seconds (0..259200)
  - [Initial value] : 3

**[Description]**

Sets whether to release the information obtained from the DHCP server when the link of the interface as a DHCP client, of which IP address is given by the DHCP server, goes down.

When the link goes down, the timer is activated. The information is released for *time* seconds during the link is continuously down. If *time* has no set value, “3 seconds” is automatically set.

When the information is released, the router tries to obtain the information at the next linkup.

**[Note]**

Setting a large value for the timer prevents impact of the unstable link.

The setting specified by this command is enabled when the link goes down after the command is executed.

If the link is up before the end of the timer setting, the timer is cleared and no information is released.

If the information lease period expires before the end of the timer setting, the timer is cleared and the information is released.

When the following commands are running, the timer being operated is cleared.

**ip interface address, ip pp remote address, ip pp remote address pool, dhcp client linkdown release**

**[Models]**

RTX810, RTX5000

# Chapter 11

## ICMP Configuration

### 11.1 IPv4 Configuration

#### 11.1.1 Set Whether to Send ICMP Echo Reply

**[Syntax]**

```
ip icmp echo-reply send send
no ip icmp echo-reply send [send]
```

**[Setting and Initial value]**

- *send*
- [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : on

**[Description]**

Sets whether to return ICMP Echo Reply when ICMP Echo is received.

**[Models]**

RTX810, RTX5000

#### 11.1.2 Set Whether to Send ICMP Echo Reply When the Link Is Down

**[Syntax]**

```
ip icmp echo-reply send-only-linkup send
no ip icmp echo-reply send-only-linkup [send]
```

**[Setting and Initial value]**

- *send*
- [Setting] :

Setting	Description
on	Return ICMP Echo Reply only when the link is up
off	Return ICMP Echo Reply regardless of the link state

- [Initial value] : off

**[Description]**

Sets whether to return ICMP Echo Reply when ICMP Echo in which the destination IP address is set to the IP address granted to an interface whose link is down. Because the router returns ICMP Echo only when the link is up when on is specified, the link state can be checked using ping. If off is specified, ICMP Echo is returned regardless of the link state.

**[Models]**

RTX810, RTX5000

#### 11.1.3 Set Whether to Send ICMP Mask Reply

**[Syntax]**

```
ip icmp mask-reply send send
no ip icmp mask-reply send [send]
```

**[Setting and Initial value]**

- *send*
- [Setting] :

Setting	Description
on	Send

Setting	Description
off	Not send

- [Initial value] : on

**[Description]**

Sets whether to return ICMP Mask Reply when ICMP Mask Request.

**[Models]**

RTX810, RTX5000

### 11.1.4 Set Whether to Send ICMP Parameter Problem

---

**[Syntax]**

```
ip icmp parameter-problem send send
no ip icmp parameter-problem send [send]
```

**[Setting and Initial value]**

- *send*
- [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : off

**[Description]**

Sets whether to send ICMP Parameter Problem when an error is detected in the IP option in the received IP packet.

**[Models]**

RTX810, RTX5000

### 11.1.5 Set Whether to Send ICMP Redirect

---

**[Syntax]**

```
ip icmp redirect send send
no ip icmp redirect send [send]
```

**[Setting and Initial value]**

- *send*
- [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : on

**[Description]**

Sets whether to send ICMP Redirect to the transmission source, when an IP packet addressed to another gateway is received, and that packet is redirected appropriately to the gateway.

**[Models]**

RTX810, RTX5000

### 11.1.6 Set the Processing When ICMP Redirect Is Received

---

**[Syntax]**

```
ip icmp redirect receive action
no ip icmp redirect receive [action]
```

**[Setting and Initial value]**

- *action*
- [Setting] :



Setting	Description
on	Process
off	Ignore

- [Initial value] : off

**[Description]**

Sets whether to process ICMP Redirect when it is received and update its own route table or ignore it.

**[Models]**

RTX810, RTX5000

### 11.1.7 Set Whether to Send ICMP Time Exceeded

---

**[Syntax]**

```
ip icmp time-exceeded send send [rebound=sw]
no ip icmp time-exceeded send [send rebound=sw]
```

**[Setting and Initial value]**

- *send*
- [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : on

**[Description]**

Sets whether to send ICMP Time Exceeded to the transmission source of the received IP packet when the packet is discarded due to the TTL of the received packet becoming 0. If the rebound option is set to on, the original packet will be transmitted by the receiving interface, regardless of routing.

**[Note]**

RTX810 supports rebound option in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

### 11.1.8 Set Whether to Send ICMP Timestamp Reply

---

**[Syntax]**

```
ip icmp timestamp-reply send send
no ip icmp timestamp-reply send [send]
```

**[Setting and Initial value]**

- *send*
- [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : on

**[Description]**

Sets whether to return ICMP Timestamp Reply when ICMP Timestamp is received.

**[Models]**

RTX810, RTX5000

### 11.1.9 Set Whether to Send ICMP Destination Unreachable

---

**[Syntax]**

```
ip icmp unreachable send send [rebound=sw]
no ip icmp unreachable send [send rebound=sw]
```

**[Setting and Initial value]**

- *send*
- [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : on
- *send*

- [Setting] :

Setting	Description
on	Send from receiving interface
off	Transmit in accordance with routing

- [Initial value] : off

**[Description]**

Sets whether to send ICMP Destination Unreachable to the transmission source of the packet, when the destination is not found in the routing table or when the IP packet is to be discarded due to ARP resolution failure. If the rebound option is set to on, the original packet will be transmitted by the receiving interface, regardless of routing.

**[Note]**

RTX810 supports rebound option in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

**11.1.10 Set Whether to Send ICMP Error for Packets Decoded with IPsec****[Syntax]**

```
ip icmp error-decrypted-ipsec send switch
no ip icmp error-decrypted-ipsec send [switch]
```

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	Send ICMP error for packets decoded with IPsec
off	Not send ICMP error for packets decoded with IPsec

- [Initial value] : on

**[Description]**

Sets whether to send ICMP error for packets decoded with IPsec.

**[Note]**

Because the ICMP error contains the head section of the decoded packet, if IPsec is not used when returning the ICMP error to the transmission source, communication that is supposed to be protected by IPsec may flow through the network without the protection. In particular, caution is necessary when IPsec processing is switched through a protocol using a filter type routing. If the router is configured not to send ICMP errors, phenomenon such as the router not responding to traceroute occurs.

**[Models]**

RTX810, RTX5000

**11.1.11 Set Whether to Log Received ICMP****[Syntax]**

```
ip icmp log log
no ip icmp log [log]
```

**[Setting and Initial value]**

- *log*
- [Setting] :

Setting	Description
on	Record
off	Not record

- [Initial value] : off

#### [Description]

Sets whether to record received ICMP to a debug type log.

#### [Models]

RTX810, RTX5000

### 11.1.12 Set the Stealth Function

#### [Syntax]

```
ip stealth all
ip stealth interface [interface...]
no ip stealth [...]
```

#### [Setting and Initial value]

- all : Carry out stealth operation on packets received from all logical interfaces
  - [Initial value] : -
- interface
  - [Setting] : Carry out stealth operation on packets received from the specified logical interface
  - [Initial value] : -

#### [Description]

When this command is set, the router does not return ICMP and TCP reset that occurs due to packets that is sent to itself from the specified interface.

Normally, if a protocol or IPv6 header not supported by router is received or if a packet is received for a TCP/UDP port that is not opened, the router returns ICMP unreachable or TCP reset. However, this behavior can be prohibited by setting this command. This enables the presence of the router to be hidden when the router is attacked by a port scanner or other device.

#### [Note]

Note that the router also does not respond to PING from the specified interface.

This command cannot control ICMP that occurs due to packets that are not addressed to the router. To prevent such transmissions, the **ip icmp \*** command group must be used.

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

RTX5000 does not support WAN interface for *interface* parameter.

#### [Models]

RTX810, RTX5000

### 11.1.13 Set Whether to Perform MTU Discovery by ARP

#### [Syntax]

```
ip interface arp mtu discovery sw [minimum=min_mtu]
no ip interface arp mtu discovery [sw [minimum=min_mtu]]
```

#### [Setting and Initial value]

- interface
  - [Setting] : LAN interface name
  - [Initial value] : -
- sw
  - [Setting] :

Setting	Description
on	MTU discovery will be carried out by ARP
off	MTU discovery will not be carried out by ARP

- [Initial value] : on
- min\_mtu
  - [Setting] : Minimum MTU for discovery range
  - [Initial value] : 4000

**[Description]**

Sets whether MTU discovery by ARP is performed

When the jumbo frame use condition is set to on for the specified interface via the **lan type** command or the **ip mtu** command, MTU discovery will be carried out by repeatedly sending a large size ARP to the peer as determined by ARP resolution.

**[Models]**

RTX5000

**11.1.14 Set Whether to Send ICMP Destination Unreachable for Truncated Packets****[Syntax]**

```
ip icmp unreachable-for-truncated send send
no ip icmp unreachable-for-truncated send [send]
```

**[Setting and Initial value]**

- *send*
- [Setting] :

Setting	Description
on	Send
off	Do not send

- [Initial value] : on

**[Description]**

Sets whether to send ICMP Destination unreachable (Fragmentation needed) for packets that were sent by the LAN interface, but because the length exceeded the MTU for that interface, the packet was truncated.

**[Note]**

For LANs using jumbo frames, the maximum value of the jumbo frame varies according to the host and switching hub. As a result, if the jumbo frame size for all devices on the LAN are not the same, communication will not be possible.

When a host has been mistakenly configured to send packets that are larger than the router's frame size, the router will normally simply disregard the packets it has received which exceed the MTU for its own interface, but if this command is set to on, an ICMP error will be return for those packets as well. Through this, the route MTU discovery works effectively, and it can be expected that the host will quickly reduce the frame size.

**[Models]**

RTX5000

**11.2 IPv6 Configuration****11.2.1 Set Whether to Send ICMP Echo Reply****[Syntax]**

```
ipv6 icmp echo-reply send send
no ipv6 icmp echo-reply send [send]
```

**[Setting and Initial value]**

- *send*
- [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : on

**[Description]**

Sets whether to send ICMP Echo Reply.

**[Models]**

RTX810, RTX5000

**11.2.2 Set Whether to Send ICMP Echo Reply When the Link Is Down****[Syntax]**

```
ipv6 icmp echo-reply send-only-linkup send
```

**no ipv6 icmp echo-reply send-only-linkup** [*send*]

**[Setting and Initial value]**

- *send*
- [Setting] :

Setting	Description
on	Return ICMP Echo Reply only when the link is up
off	Return ICMP Echo Reply regardless of the link state

- [Initial value] : off

**[Description]**

Sets whether to return ICMP Echo Reply when ICMP Echo in which the destination IP address is set to the IP address granted to an interface whose link is down. Because the router returns ICMP Echo only when the link is up when on is specified, the link state can be checked using ping. If off is specified, ICMP Echo is returned regardless of the link state.

**[Models]**

RTX810, RTX5000

### 11.2.3 Set Whether to Send ICMP Parameter Problem

---

**[Syntax]**

**ipv6 icmp parameter-problem send** *send*  
**no ipv6 icmp parameter-problem send** [*send*]

**[Setting and Initial value]**

- *send*
- [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : off

**[Description]**

Sets whether to send ICMP Parameter Problem.

**[Models]**

RTX810, RTX5000

### 11.2.4 Set Whether to Send ICMP Redirect

---

**[Syntax]**

**ipv6 icmp redirect send** *send*  
**no ipv6 icmp redirect send** [*send*]

**[Setting and Initial value]**

- *send*
- [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : on

**[Description]**

Sets whether to send ICMP Redirect.

**[Models]**

RTX810, RTX5000

### 11.2.5 Set the Processing When ICMP Redirect Is Received

---

**[Syntax]**

**ipv6 icmp redirect receive** *action*  
**no ipv6 icmp redirect receive** [*action*]

**[Setting and Initial value]**

- *action*
  - [Setting] :

Setting	Description
on	Process
off	Ignore

- [Initial value] : off

**[Description]**

Sets whether to process or ignore ICMP Redirect when it is received.

**[Models]**

RTX810, RTX5000

**11.2.6 Set Whether to Send ICMP Time Exceeded**

---

**[Syntax]**

**ipv6 icmp time-exceeded send** *send* [**rebound=sw**]

**no ipv6 icmp time-exceeded send** [*send* **rebound=sw**]

**[Setting and Initial value]**

- *send*
  - [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : on

- *send*
  - [Setting] :

Setting	Description
on	Send from receiving interface
off	Transmit in accordance with routing

- [Initial value] : off

**[Description]**

Sets whether to send ICMP Time Exceeded.

If the rebound option is set to on, the original packet will be transmitted by the receiving interface, regardless of routing.

**[Note]**

RTX810 supports rebound option in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

**11.2.7 Set Whether to Send ICMP Destination Unreachable**

---

**[Syntax]**

**ipv6 icmp unreachable send** *send* [**rebound=sw**]

**no ipv6 icmp unreachable send** [*send* **rebound=sw**]

**[Setting and Initial value]**

- *send*
  - [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : on

- *send*
  - [Setting] :

Setting	Description
on	Send from receiving interface
off	Transmit in accordance with routing

- [Initial value] : off

#### [Description]

Sets whether to send ICMP Destination Unreachable.

If the rebound option is set to on, the original packet will be transmitted by the receiving interface, regardless of routing.

#### [Note]

RTX810 supports rebound option in Rev.11.01.23 or later.

#### [Models]

RTX810, RTX5000

### 11.2.8 Set Whether to Log Received ICMP

---

#### [Syntax]

**ipv6 icmp log** *log*

**no ipv6 icmp log** [*log*]

#### [Setting and Initial value]

- *log*
  - [Setting] :

Setting	Description
on	Record
off	Not record

- [Initial value] : off

#### [Description]

Sets whether to record received ICMP to a debug type log.

#### [Models]

RTX810, RTX5000

### 11.2.9 Set Whether to Send ICMP Packet-Too-Big

---

#### [Syntax]

**ipv6 icmp packet-too-big send** *send*

**no ipv6 icmp packet-too-big send** [*send*]

#### [Setting and Initial value]

- *send*
  - [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : on

#### [Description]

Sets whether to send ICMP Packet-Too-Big.

#### [Models]

RTX810, RTX5000

### 11.2.10 Set Whether to Send ICMP Error for Packets Decoded with IPsec

---

#### [Syntax]

**ipv6 icmp error-decrypted-ipsec send** *switch*

**no ipv6 icmp error-decrypted-ipsec send** [*switch*]

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	Send ICMP error for packets decoded with IPsec
off	Not send ICMP error for packets decoded with IPsec

- [Initial value] : on

**[Description]**

Sets whether to send ICMP error for packets decoded with IPsec.

**[Note]**

Because the ICMP error contains the head section of the decoded packet, if IPsec is not used when returning the ICMP error to the transmission source, communication that is supposed to be protected by IPsec may flow through the network without the protection. In particular, caution is necessary when IPsec processing is switched through a protocol using a filter type routing.

If the router is configured not to send ICMP errors, phenomenon such as the router not responding to traceroute occurs.

**[Models]**

RTX810, RTX5000

### 11.2.11 Set the Stealth Function

---

**[Syntax]**

**ipv6 stealth** all

**ipv6 stealth** *interface* [*interface...*]

**no ipv6 stealth** [...]

**[Setting and Initial value]**

- all : Carry out stealth operation on packets received from all logical interfaces
  - [Initial value] : -
- *interface*
  - [Setting] : Carry out stealth operation on packets received from the specified logical interface
  - [Initial value] : -

**[Description]**

When this command is set, the router does not return ICMP and TCP reset that occurs due to packets that is sent to itself from the specified interface.

Normally, if a protocol or IPv6 header not supported by router is received or if a packet is received for a TCP/UDP port that is not opened, the router returns ICMP unreachable or TCP reset. However, this behavior can be prohibited by setting this command. This enables the presence of the router to be hidden when the router is attacked by a port scanner or other device.

**[Note]**

Note that the router also does not respond to PING from the specified interface.

This command cannot control ICMP that occurs due to packets that are not addressed to the router. To prevent such transmissions, the **ipv6 icmp \*** command group must be used.

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

### 11.2.12 Setting whether to send an ICMP error (Packet Too Big) for truncated frames due to a size error

---

**[Syntax]**

**ipv6 icmp packet-too-big-for-truncated send** *send*

**no ipv6 icmp packet-too-big-for-truncated send** [*send*]

**[Setting and Initial value]**

- *send*
- [Setting] :



Setting	Description
on	Sends error
off	Does not send error

- [Initial value] : on

**[Description]**

Sets whether to send an ICMP error (Packet Too Big) for any frames that were received but were truncated because the length exceeded the interface MTU.

**[Note]**

For LANs using jumbo frames, the maximum value of the jumbo frame varies according to the host and switching hub. As a result, if the jumbo frame size for all devices on the LAN are not the same, communication will not be possible.

When a host has been mistakenly configured to send packets that are larger than the router's frame size, the router will normally simply disregard the packets it has received that exceed the MTU for its own interface, but if this command is set to on, an ICMP error will be returned for those packets as well. The route MTU discovery works effectively with this, and the host can be expected to quickly reduce the frame size.

**[Models]**

RTX5000

## Chapter 12

### Tunneling

#### 12.1 Enable the Tunnel Interface

##### [Syntax]

**tunnel enable** *tunnel\_num*  
**no tunnel enable** *tunnel\_num*

##### [Setting and Initial value]

- *tunnel\_num*
- [Setting] :

Setting	Description
Number	Tunnel interface number
all	All tunnel interfaces

- [Initial value] : -

##### [Description]

Enable the tunnel interface.

All tunnel interfaces are disabled by factory default. To use them, the interface must be enabled using this command.

##### [Models]

RTX810, RTX5000

#### 12.2 Disable the Tunnel Interface

##### [Syntax]

**tunnel disable** *tunnel\_num*

##### [Setting and Initial value]

- *tunnel\_num*
- [Setting] :

Setting	Description
Number	Tunnel interface number
all	All tunnel interfaces

- [Initial value] : -

##### [Description]

Disables the tunnel interface.

It is desirable that the tunnel interface be disabled when setting the tunnel destination.

##### [Models]

RTX810, RTX5000

#### 12.3 Set the Tunnel Interface Type

##### [Syntax]

**tunnel encapsulation** *type*  
**no tunnel encapsulation**

##### [Setting and Initial value]

- *type*
- [Setting] :

Setting	Description
ipsec	IPsec tunnel

Setting	Description
ipip	IPv6 over IPv4 tunnel, IPv4 over IPv6 tunnel, IPv4 over IPv4 tunnel, or IPv6 over IPv6 tunnel
pptp	PPTP tunnel
l2tp	L2TP tunnel
l2tpv3-raw	L2TPv3 tunnel
l2tpv3	L2TPv3/IPsec tunnel
ipudp	IPUDP tunnel

- [Initial value] : ipsec

#### [Description]

Sets the tunnel interface type.

#### [Note]

When using tunneling together with NAT, it is desirable that the destination IP address be set using the **tunnel endpoint address** command.

Models that do not support the PPTP feature cannot use the pptp keyword.

Models that do not support the L2TP/IPsec feature cannot use the l2tp keyword.

Models that do not support the L2TPv3 features cannot use the l2tpv3-raw keyword or the l2tpv3 keyword.

#### [Models]

RTX810, RTX5000

## 12.4 Set the IPv4 Address of the Tunnel Interface

---

#### [Syntax]

**ip tunnel address** *ip\_address*[/*mask*]

**no ip tunnel address** [*ip\_address*[/*mask*]]

#### [Setting and Initial value]

- *ip\_address*
  - [Setting] : IPv4 address
  - [Initial value] : -
- *mask*
  - [Setting] :
    - xxx.xxx.xxx.xxx where xxx is a decimal number
    - Hexadecimal number following 0x
    - Number of mask bits
  - [Initial value] : -

#### [Description]

Sets the IPv4 address and netmask of the tunnel interface.

Setting this command enables BGP connections to be established via the tunnel interface.

#### [Models]

RTX810, RTX5000

## 12.5 Set the Peer IPv4 Address of the Tunnel Interface

---

#### [Syntax]

**ip tunnel remote address** *ip\_address*

**no ip tunnel remote address** [*ip\_address*]

#### [Setting and Initial value]

- *ip\_address*
  - [Setting] : IPv4 address
  - [Initial value] : -

**[Description]**

Sets the IPv4 address and netmask of the tunnel interface.

Setting this command enables BGP connections to be established via the tunnel interface.

**[Models]**

RTX810, RTX5000

## 12.6 Set the End Point IP Address of the Tunnel Interface

---

**[Syntax]**

**tunnel endpoint address** [*local*] *remote*

**no tunnel endpoint address** [[*local*] *remote*]

**[Setting and Initial value]**

- *local*
  - [Setting] : End point IP address of the tunnel interface on the local side
  - [Initial value] : -
- *remote*
  - [Setting] : End point IP address of the tunnel interface on the remote side
  - [Initial value] : -

**[Description]**

Sets the end point IP address of the tunnel interface. The IP address can be of either IPv4 or IPv6. However, the IPv4 or IPv6 type must match between *local* and *remote*. If an IPv4 address is specified as the tunnel interface end point, IPv4 over IPv4 tunnel and IPv6 over IPv4 tunnel can be used. Likewise, if an IPv6 address is specified, IPv4 over IPv6 tunnel and IPv6 over IPv6 tunnel can be used.

If *local* is omitted, the IP address of an appropriate interface is used.

**[Note]**

The IP address set with this command is used only when the **tunnel encapsulation** command is set to *pptp*, *l2tp*, or *ipip*. The tunnel end point for IPsec tunneling is set using the **ipsec ike local address** and **ipsec ike remote address** commands. You do not need to set the end point when using an anonymous connection to a PPTP server or L2TP/IPsec server.

**[Models]**

RTX810, RTX5000

## Chapter 13

### IPsec Configuration

The IPsec function that assures the security of IP communication by encryption is implemented. In IPsec, IKE (Internet Key Exchange) is used. The required key is automatically generated by IKE, but the pre-shared key that is used as the key seed must be registered in advance using the **ipsec ike pre-shared-key** command. This key can be set for each security gateway. Whether the router answers key exchange requests is set using the **ipsec ike remote address** command.

Management information including the key, key life time, encryption, and authentication algorithm are managed by an SA (Security Association). The ID that distinguishes SAs is automatically granted. The SA ID and state can be confirmed using the **show ipsec sa** command. SAs has a life time that matches with the life time of the key. The parameters that the user can specify in the SA attributes are called policies. The number associated with a policy is called a policy ID and is defined by the **ipsec sa policy** command. The life time is set using the **ipsec ike duration ipsec-sa** and **ipsec ike duration isakmp-sa** commands.

SAs are deleted using the **ipsec sa delete** command and initialized using the **ipsec refresh sa** command. The SAs can also be automatically refreshed using the **ipsec auto refresh** command.

Communication using IPsec can be divided into two types, tunnel mode and transport mode.

Tunnel mode is for using VPN (Virtual Private Network) through IPsec. The router acts as a security gateway and exchanges data with the peer security gateway by encrypting IP packet data that flows through the LAN. Because the router carries out all procedures needed for IPsec, the start point and end point hosts on the LAN do not require special configuration.

When using tunnel mode, a virtual interface called tunnel interface is defined. The route is configured so that all IP packets to be processed flow through the tunnel interface. Each tunnel interface is managed by a tunnel interface number. To switch the tunnel number for configuration, use the **tunnel select** command. Whether a tunnel interface is enabled or disabled is set using the **tunnel enable** and **tunnel disable** commands.

Configuration using a peer number		Configuration using a tunnel interface number
<ul style="list-style-type: none"> <li>• <b>pp enable</b></li> <li>• <b>pp disable</b></li> <li>• <b>pp select</b></li> </ul>	<=>	<ul style="list-style-type: none"> <li>• <b>tunnel enable</b></li> <li>• <b>tunnel disable</b></li> <li>• <b>tunnel select</b></li> </ul>

Transport mode is a special mode that assures security of communications in which the router itself becomes a start point or end point. This mode can be used in special cases such as entering a remote router from a router using TELNET. To use transport mode, define the mode using the **ipsec transport** command. To stop using transport mode, delete the definition using the **no ipsec transport** command.

The security gateway ID and tunnel interface number vary depending on the model as shown in the table below.

Model	Security Gateway ID	Tunnel interface number
RTX5000	1-3000	1-3000
RTX810	1-50	1-50

The router supports main mode and aggressive mode. Main mode is used when both of the routers constructing a VPN have fixed global addresses. Aggressive mode is used when only one of the routers has a fixed global address.

To use main mode, you must set the IP addresses of the peer routers using the **ipsec ike remote address** command. To use aggressive mode, the configuration varies depending on whether the router has a fixed global address. For a router that has a fixed global address, set the **ipsec ike remote name** command and set the **ipsec ike remote address** command to any. For a router that does not have a fixed global address, set the **ipsec ike local name** command and set the **ipsec ike remote address** command to set the IP address. In main mode, the **ipsec ike local name** and **ipsec ike remote name** commands cannot be specified. In aggressive mode, the **ipsec ike local name** and **ipsec ike remote name** commands cannot be specified simultaneously. If you do, the router may not operate correctly.

#### 13.1 Set the IPsec Operation

##### [Syntax]

- ipsec use** *use*
- no ipsec use** [*use*]

##### [Setting and Initial value]

- *use*
- [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : on

**[Description]**

Sets whether to enable IPsec.

**[Models]**

RTX810, RTX5000

## 13.2 Set the IKE Version

---

**[Syntax]**

```
ipsec ike version gateway_id version
no ipsec version gateway_id [version]
```

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *version*
  - [Setting] : IKE version to be used
  - [Setting] :

Setting	Description
1	IKE version 1
2	IKE version 2

- [Initial value] : 1

**[Description]**

Sets a version of IKE used for the security gateway.

**[Note]**

Only connection with the versions other than the version specified with *version* is accepted.

**[Models]**

RTX810, RTX5000

## 13.3 Set the IKE Authentication Method

---

**[Syntax]**

```
ipsec ike auth method gateway_id method
no ipsec ike auth method gateway_id [method]
```

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *method*
  - [Setting] :

Setting	Description
auto	Select an authentication method automatically
pre-shared-key	Pre-shared key
certificate	Digital signature
eap-md5	EAP-MD5

- [Initial value] :
  - auto

**[Description]**

Sets the IKE authentication method.

When auto is set for METHOD, an authentication method is determined according to the following conditions:

- Pre-shared key method
  - When the **ipsec ike pre-shared-key** command is specified.
- Digital signature method

When all of the following conditions are met

- A 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 specified.

- EAP-MD5 method

When all of the following conditions are met

- A certificate is stored in the location specified by the **ipsec ike pki file** command.
- The **ipsec ike eap request** command or the **ipsec ike eap myname** command is not specified.

If multiple conditions are met among the conditions to determine the authentication method mentioned above, the priority is as follows:

1. Pre-shared key method
2. Digital signature method
3. EAP-MD5 method

When settings other than auto is specified for *method*, the method specified for *method* is used for authentication, regardless of the conditions to determine the authentication method mentioned above.

**[Note]**

This command can be only used with IKEv2, and do not affect on IKEv1 operation.

**[Models]**

RTX810, RTX5000

## 13.4 Register the Pre-Shared Key

---

**[Syntax]**

```
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 and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *key*
  - [Setting] : Hexadecimal sequence starting with 0x that is to be the key (up to 128 bytes)
  - [Initial value] : -
- *text*
  - [Setting] : Key expressed using ASCII text characters (up to 128 characters)
  - [Initial value] : -

**[Description]**

Registers the pre-shared key that is needed for the key exchange. If this is not specified, the router does not carry out key exchange.

The peer router on which key exchange is to be carried out must have the same pre-shared key set in advance.

**[Example]**

```
ipsec ike pre-shared-key 1 text himitsu
ipsec ike pre-shared-key 8 0xCDEEEDC0CDEDCD
```

**[Models]**

RTX810, RTX5000

## 13.5 Set the PKI Files to Use in IKEv2 Authentication

---

**[Syntax]**

```
ipsec ike pki file gateway_id certificate=cert_id [crl=crl_id]
no ipsec ike pki file gateway_id [...]
```

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *cert\_id*
  - [Setting] :

Setting	Description
1..8	Certificate file identifier

- [Initial value] : -
- *crl\_id*
  - [Setting] :

Setting	Description
1..8	CRL file identifier

- [Initial value] : -

**[Description]**

Sets the PKI files to use in IKEv2 authentication.

When carrying out authentication with the digital certificate method, specify an identifier of the file storing a certificate to be used for *cert\_id*.

When carrying out EAP-MD5 authentication, the initiator specifies an identifier of the file storing its certificate for *cert\_id* in order to evaluate the peer certificate.

**[Note]**

This command can be only used with IKEv2, and do not affect on IKEv1 operation.

**[Models]**

RTX810, RTX5000

## 13.6 Set Its Own Name and Password Used for EAP-MD5 Authentication

---

**[Syntax]**

```
ipsec ike eap myname gateway_id name password
no ipsec ike eap myname gateway_id [...]
```

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *name*
  - [Setting] : Name (up to 256 characters)
  - [Initial value] : -
- *password*
  - [Setting] : Password(up to 64 characters)
  - [Initial value] : -

**[Description]**

Sets the name and password that are used when EAP-MD5 authentication is requested.

**[Note]**

This command can be only used with IKEv2, and do not affect on IKEv1 operation.

**[Models]**

RTX810, RTX5000

## 13.7 Configure EAP-MD5 User Authentication

---



**[Syntax]**

```
ipsec ike eap request gateway_id sw group_id
no ipsec ike eap request gateway_id [...]
```

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *sw*
  - [Setting] :

Setting	Description
on	Make a request
off	Not make a request

- [Initial value] : off
- *group\_id*
  - [Setting] : User Group ID to use in XAUTH authentication
  - [Initial value] : -

**[Description]**

On IKEv2, select whether or not to request EAP-MD5 authentication from the client. If you specify a value for *group\_id*, authentication is requested from the users in the specified user group.

The settings made with this command are only valid when the router operates as a responder. If the IKE AUTH exchange sent from the security gateway at the initiator does not include the AUTH payload, the router performs user authentication using EAP-MD5.

**[Note]**

This command can be only used with IKEv2, and do not affect on IKEv1 operation.

**[Models]**

RTX810, RTX5000

## 13.8 Set Whether to Send the Certificate Request Payload in EAP-MD5 Authentication

---

**[Syntax]**

```
ipsec ike eap send certreq gateway_id switch
no ipsec ike eap send certreq gateway_id [switch]
```

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *switch*
  - [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : off

**[Description]**

When the EAP-MD5 authentication method is used, sets whether to include a certificate request (CERTREQ) in the IKE\_AUTH exchange sent from the security gateway at the initiator.

**[Note]**

This command can be only used with IKEv2, and do not affect on IKEv1 operation.

**[Models]**

RTX810, RTX5000

## 13.9 Set Whether to Start IKE

---

**[Syntax]**

**ipsec auto refresh** [*gateway\_id*] *switch*

**no ipsec auto refresh** [*gateway\_id*]

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *switch*
  - [Setting] :

Setting	Description
on	Start the key exchange
off	Not start the key exchange

- [Initial value] :
  - off (overall operation)
  - on (every *gateway\_id*)

**[Description]**

Sets whether to start IKE. The router accepts key exchanges that other routers start regardless of the setting of this command.

A syntax that does not specify the *gateway\_id* parameter determines the overall operation of the router. If this setting is off, the router does not start the key exchange.

A syntax that specifies the *gateway\_id* parameter is provided to put restraints on the starting of the key exchange for the specified security gateway.

For example in the following setting, the key exchange is started on all security gateways except the first security gateway.

```
ipsec auto refresh on
ipsec auto refresh 1 off
```

**[Note]**

In the **ipsec auto refresh** off setting, the syntax that specifies the *gateway\_id* parameter does not have any effect. For example in the following setting, the key exchange is not started on the first security gateway.

```
ipsec auto refresh off (default setting)
ipsec auto refresh 1 on
```

**[Models]**

RTX810, RTX5000

## 13.10 Set Whether to Reject Key Exchange When the Setting Differs

---

**[Syntax]**

**ipsec ike negotiate-strictly** *gateway\_id* *switch*

**no ipsec ike negotiate-strictly** *gateway\_id*

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *switch*
  - [Setting] :

Setting	Description
on	Reject the key exchange
off	Accept the key exchange

- [Initial value] : off

**[Description]**

Sets whether to reject key exchange in operation as IKEv1 when the setting differs. If off is specified, the operation is the same as with earlier firmware versions. In other words, the key exchange is accepted even when the parameter proposed by the peer is different from the local setting. If on is specified, the proposal from the peer in the same condition is rejected. The parameters to which this command applies and the corresponding commands are as follows:

Parameter	Corresponding Command
Encryption algorithm	<b>ipsec ike encryption</b>
Group	<b>ipsec ike group</b>
Hash algorithm	<b>ipsec ike hash</b>
PFS	<b>ipsec ike pfs</b>
Phase 1 mode	<b>ipsec ike local name etc.</b>

**[Note]**

This command does not affect operation of IKEv2.

**[Models]**

RTX810, RTX5000

## 13.11 Set Whether to Continue Key Exchange When IKE Fails

---

**[Syntax]**

**ipsec ike always-on** *gateway\_id* *switch*

**no ipsec ike always-on**

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *switch*
  - [Setting] :

Setting	Description
on	Continue the key exchange
off	Halt the key exchange

- [Initial value] : off

**[Description]**

This command enables the key exchange to be continued even when IKE fails. If IKE keepalive is used, key exchange always continues even if this command is not set.

**[Models]**

RTX810, RTX5000

## 13.12 Set the Retry Count and Interval of Key Exchange

---

**[Syntax]**

**ipsec ike retry** *count interval* [*max\_session*]

**no ipsec ike retry** [*count interval* [*max\_session*]]

**[Setting and Initial value]**

- *count*
  - [Setting] : Retry count (1..50)
  - [Initial value] : 10
- *interval*
  - [Setting] : Retransmission interval in seconds (1..100)
  - [Initial value] : 5
- *max\_session*
  - [Setting] : Maximum number of phase 1s that operate simultaneously (1..5)
  - [Initial value] : 3

**[Description]**

Sets the retry count and interval that are applied when the key exchange packet does not reach the peer.

In addition, the *max\_session* parameter specifies the maximum number of phase 1s that operate simultaneously in IKEv1. To generate the key quickly, the router sometimes starts a new phase 1 when phase 1 is not established and retransmission is being repeated. This parameter limits the number of phase 1s that operate simultaneously in such conditions. This parameter limits the phase 1 on the initiator and has no effect on the phase 1 on the responder.

**[Note]**

When operating as IKEv2, the *max\_session* parameter has no effect. At maximum, always one key exchange session starts up to the same remote security gateway.

If load on the remote security gateway is very large, change of this command setting may allow success of key exchange.

**[Models]**

RTX810, RTX5000

### 13.13 Set the Remote Security Gateway Name

---

**[Syntax]**

**ipsec ike remote name** *gateway name* [*type*]

**no ipsec ike remote name** *gateway* [*name*]

**[Setting and Initial value]**

- *gateway*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *name*
  - [Setting] : Name (up to 256 characters)
  - [Initial value] : -
- *type* : id type
  - [Setting] :

Setting	Description
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

- [Initial value] : -

**[Description]**

Sets the remote security gateway name and ID.

Other influences and points to notice of this command, which differ according to activated IKE version, are as follows:

- IKEv1
 

These command settings are used for the phase 1 aggressive mode, but not used for the main mode.  
Also the *type* parameter is not taken into consideration when a remote security gateway is determined.
- IKEv2
 

When a remote security gateway is determined, the *name* setting and the *type* setting must match.  
When the *type* parameter is not 'key-id': the router tries to specify an IP address of the remote security gateway with name.  
When the router can specify the IP address, it starts key exchange to that host. In this case, there is not need to configure the **ipsec ike remote address** command.  
However, when the **ipsec ike remote address** command has been configured, a host to be connected at the startup time is determined according to that setting.

**[Models]**

RTX810, RTX5000

### 13.14 Set the IP Address of the Remote Security Gateway

---

**[Syntax]**

**ipsec ike remote address** *gateway\_id* *ip\_address*

**no ipsec ike remote address** *gateway\_id* [*ip\_address*]

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *ip\_address*
  - [Setting] :

Setting	Description
IP address or host name	IP address or host name of the remote security gateway (up to 255 characters)
any	Auto select

- [Initial value] : -

#### [Description]

Sets the IP address or host name of the remote security gateway. If the remote security gateway is specified by host name, the corresponding IP address is searched using DNS at the start of the key exchange.

Other influences and points to notice of this command, which differ according to activated IKE version, are as follows:

- IKEv1

When the router is a responder, the host specified with this command is used for determining a remote security gateway. If 'any' is specified, key exchange from an arbitrary host is accepted as a remote security gateway. However, key exchange cannot be started from the local side. This keyword is used in aggressive mode on the router that has the fixed global address.

- IKEv2

A host specified with this command is used only as a destination at the time of startup of key exchange. The keyword 'any' shows explicitly that it does not startup key exchange.

When the router is a responder, a remote security gateway with this command setting is determined by configuration of the **ipsec ike remote name** or other commands.

#### [Note]

When specifying a host name, be sure to specify the DNS server with the **dns server** or other commands.

#### [Models]

RTX810, RTX5000

## 13.15 Set the Remote ID

#### [Syntax]

```
ipsec ike remote id gateway_id ip_address[/mask]
no ipsec ike remote id gateway_id [ip_address[/mask]]
```

#### [Setting and Initial value]

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *ip\_address*
  - [Setting] : IP address
  - [Initial value] : -
- *mask*
  - [Setting] : Netmask
  - [Initial value] : -

#### [Description]

Sets the remote ID that is used in IKEv1 phase 2.

If this command is not specified, the router does not send the ID in the phase 2.

If the *mask* parameter is omitted, the router sends a type 1 ID. If the *mask* parameter is specified, the router sends a type 4 ID.

#### [Note]

This command does not affect operation of IKEv2.

#### [Models]

RTX810, RTX5000

## 13.16 Set the Local Security Gateway Name

#### [Syntax]

```
ipsec ike local name gateway_id name [type]
no ipsec ike local name gateway_id [name]
```

#### [Setting and Initial value]

- *gateway\_id*

- [Setting] : Security Gateway ID
- [Initial value] : -
- *name*
  - [Setting] : Name (up to 256 characters)
  - [Initial value] : -
- *type* : id type
  - [Setting] :

Setting	Description
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

- [Initial value] : -

#### [Description]

Sets the local security gateway name and ID.

Note that at the time of operation as IKEv1, when the *type* parameter is set to be 'ipv4-addr', 'ipv6-addr', the router operation is similar to the case where 'key-id' is specified.

#### [Models]

RTX810, RTX5000

## 13.17 Set the IP Address of the Local Security Gateway

#### [Syntax]

```

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 pp_num
no ipsec ike local address gateway_id [ip_address]

```

#### [Setting and Initial value]

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *ip\_address*
  - [Setting] : IP address of the local security gateway
  - [Initial value] : -
- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *vrid*
  - [Setting] : VRRP group ID (1..255)
  - [Initial value] : -
- *prefix*
  - [Setting] : Prefix
  - [Initial value] : -
- *pp\_num*
  - [Setting] : PP interface number
  - [Initial value] : -

#### [Description]

Sets the IP address of the local security gateway.

In the second syntax that specifies the *vrrp* keyword, the virtual IP address of the specified LAN interface/VRRP group ID is used as the local security gateway address only when the router is operating as a VRRP master. Key exchange is not carried out if the router is not a VRRP master.

In the third syntax, which contains the *ipv6* keyword, specify the IPv6 dynamic address.

In the fourth syntax, which contains the `ipcp` keyword, specify the PP interface to acquire the IPCP address from.

**[Note]**

If this command is not specified, IKE is started using an IP address of an interface close to the remote security gateway.

**[Models]**

RTX810, RTX5000

## 13.18 Set the Local ID

---

**[Syntax]**

```
ipsec ike local id gateway_id ip_address[/mask]
no ipsec ike local id gateway_id [ip_address[/mask]]
```

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *ip\_address*
  - [Setting] : IP address
  - [Initial value] : -
- *mask*
  - [Setting] : Netmask
  - [Initial value] : -

**[Description]**

Sets the local ID that is used in IKEv1 phase 2.

If this command is not specified, the router does not send the ID in the phase 2.

If the *mask* parameter is omitted, the router sends a type 1 ID. If the *mask* parameter is specified, the router sends a type 4 ID.

**[Note]**

This command does not affect operation of IKEv2.

**[Models]**

RTX810, RTX5000

## 13.19 Set the IKE Keepalive Function

---

**[Syntax]**

```
ipsec ike keepalive use gateway_id switch [down=disconnect]
ipsec ike keepalive use gateway_id switch heartbeat [interval count [upwait]] [down=disconnect]
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 and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *switch* : Keepalive operation
  - [Setting] :

Setting	Description
on	Use keepalive
off	Do not use keepalive
auto	Only send a keepalive packet when a keepalive is received from the peer router(only valid for heartbeat and rfc4306)

- [Initial value] : auto
- *ip\_address*
  - [Setting] : IP address (IPv4/IPv6) to ping
  - [Initial value] : -

- *length*
  - [Setting] : Length of the data area when TYPE is set to icmp-echo (64..1500)
  - [Initial value] : 64
- *interval*
  - [Setting] : Transmission interval of keepalive packets in seconds (1..600)
  - [Initial value] : 10
- *count*
  - [Setting] : Number of times the router tries to resend an unsent keepalive packet before deciding that there has been a failure (1..50)
  - [Initial value] : 6
- *upwait*
  - [Setting] : Time from when IPsec SA is generated until the tunnel interface is actually activated (0..1000000)
  - [Initial value] : 0

**[Description]**

Sets the IKE keepalive operation.

This command operates differently according to activated IKE version as follows:

- IKEv1

You can set the keepalive method to heartbeat, ICMP Echo, or DPD (RFC3706). The first syntax is automatically the heartbeat syntax.

To set the heartbeat syntax, use the first and second syntax. When the *switch* parameter is auto, the router only sends a heartbeat packet after first receiving one from a peer. Therefore, if both routers are set to auto, IKE keepalive will not function.

To set ICMP Echo, use the third syntax and specify a destination IP address. You have the option to specify the length of the ICMP Echo data area. In this case, the router operation is similar to the case where the *switch* parameter is on even when the parameter setting is auto.

To set DPD, use the fourth syntax. In this case, the router operation is similar to the case where the *switch* parameter is on even when the parameter setting is auto.

If a method (syntax) that IKEv1 does not support is set, the router operates alternatively with the heartbeat syntax. In this case, the settings of *switch*, *count*, *interval*, and *upwait* parameters are applied.

- IKEv2

You can set the keepalive method to RFC4306 (IKEv2 standard) or ICMP Echo. The first syntax is automatically the RFC4306 method.

To set the RFC4306 method, use the first or fifth syntax. In this case, when a related SA generates another communication and a remote security gateway's heartbeat is clear, sending of keepalive packets is restricted. When the *switch* parameter is auto, the router sends response packets only when it receives keepalive packets based on the RFC4306 method. Note that the router operates similarly even when the *switch* parameter is auto or off because IKEv2 requires the router to respond any keepalive packets based on the RFC4306 method.

To set ICMP Echo, use the third syntax, and set a destination IP address. You have the option to specify the length of the ICMP Echo data area. In this case, the router operation is similar to the case where the *switch* parameter is on even when the parameter setting is auto.

If a method (syntax) that IKEv2 does not support is set, the router operates alternatively with RFC4306. In this case, the settings of *switch*, *count*, *interval*, and *upwait* parameters are applied.

**[Note]**

If there is a PP interface between the router and the peer router, you can specify the down option.

When you specify the down option, you can disconnect the PP interface when a linkdown is detected by keepalive or when the IKE resend count is reached.

You can use this option when network conditions warrant actions such as improving tunnel conditions by reconnecting to the PP interface.

The *length* parameter is used to specify the length of the ICMP data section, not the total length of the IP packet.

You cannot use multiple keepalive methods with the same peer.

**[Models]**

RTX810, RTX5000

## 13.20 Set Whether to Output SYSLOG Related to IKE Keepalive

---



**[Syntax]**

```
ipsec ike keepalive log gateway_id log
no ipsec ike keepalive log gateway_id [log]
```

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *log*
  - [Setting] :

Setting	Description
on	Output
off	Not output

- [Initial value] : on

**[Description]**

Sets whether to output SYSLOG related to IKE keepalive. This SYSLOG is a DEBUG level output.

**[Models]**

RTX810, RTX5000

## 13.21 Set the Encryption Algorithm That IKE Uses

---

**[Syntax]**

```
ipsec ike encryption gateway_id algorithm
no ipsec ike encryption gateway_id [algorithm]
```

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *algorithm*
  - [Setting] :

Setting	Description
3des-cbc	3DES-CBC
des-cbc	DES-CBC
aes-cbc	AES-CBC
aes256-cbc	AES256-CBC

- [Initial value] :
  - 3des-cbc

**[Description]**

Sets the encryption algorithm used for phase 1 of the IKEv1 operation.

If the router works as an initiator, the router proposes the algorithm specified by this command. If the router works as a responder, supported arbitrary algorithms can be used regardless of the setting of this command.

However, when the **ipsec ike negotiate-strictly** command is on, the router can use only a set algorithm even when it is a responder.

**[Note]**

In IKEv2, when the **ipsec ike proposal-limitation** command is set to "on", the encryption algorithm which is configured by this command will be proposed for negotiation. When the **ipsec ike proposal-limitation** command is set to "off", All supported algorithms will be proposed simultaneously, and let a remote security gateway select one. Also if it works as a responder, it selects the safest algorithm among the proposed ones.

In case of the router works as a responder in IKEv2, the priority of the encryption algorithm is following.

- AES256-CBC > AES192-CBC > AES128-CBC > 3DES-CBC > DES-CBC
- ## AES192-CBC is supported in only IKEv2, and it cannot be selected by command.

**[Example]**

```
# ipsec ike encryption 1 aes-cbc
```

**[Models]**

RTX810, RTX5000

## 13.22 Set the Length of the Queue That Stores the Received IKE Packets

---

**[Syntax]**

```
ipsec ike queue length length
no ipsec ike queue length [length]
```

**[Setting and Initial value]**

- *length* : Queue length
  - [Setting] :

Setting	Model
3000...12000	RTX5000
6...12	RTX810

- [Initial value] :
  - 6000 (RTX5000)
  - 12 (RTX810)

**[Description]**

Sets the length of the queue that stores the received IKE packets. This setting determines the router behavior when a high volume of IKE packets is received in a short time. The larger the specified value, the larger the number of IKE packets that the router can process without dropouts. However, because the length of time that the IKE packets are held in the router is increased, the keepalive response is delayed, and the possibility of detecting tunnel failure by mistake increases. In normal operation, this setting does not need to be changed. However, if numerous tunnels are configured and condition in which numerous SAs need to be cleared simultaneously exists, it is better to set this value to a large value.

**[Note]**

By increasing the length of the queue, the number of IKE packets that can be received and processed at once is increased. However, if the length is increased too much, the processing of the IKE packets that are accumulated inside the router is delayed, and the peer router may time out. Therefore, changing the setting of this command must be carried out carefully.

In normal operation, this setting does not need to be changed.

**[Models]**

RTX810, RTX5000

## 13.23 Set the Group That IKE Uses

---

**[Syntax]**

```
ipsec ike group gateway_id group [group]
no ipsec ike group gateway_id [group [group]]
```

**[Setting and Initial value]**

- *gateway\_id* : Security Gateway ID
  - [Initial value] : -
- *group* : Group ID
  - [Setting] :
    - modp768
    - modp1024
    - modp1536
    - modp2048
  - [Initial value] :
    - modp1024

**[Description]**

Sets the group that IKE uses.

If the router is to function as an initiator, the router proposes a group specified by this command. If the router is to function as a responder, supportable arbitrary groups can be used regardless of the setting of this command.

Other influences and points to notice of this command, which differ according to activated IKE version, are as follows:

- IKEv1

If two types of groups are specified, the first group is proposed in phase 1, and the second group is proposed in phase 2. If only one type of group is specified, the specified group is proposed in both phase 1 and phase 2.

However, when the **ipsec ike negotiate-security** command is on, the router can use only a set group even when it is a responder.

- IKEv2

Always only a first set group is used. A second set group is ignored.

Also when a peer rejects a group the router proposes as an initiator and requests another group, it proposes that group again (when the requested group is supportable). Then, until the IPsec setting is changed or restarted, the re-proposed group is preferentially used against the same remote security gateway.

**[Models]**

RTX810, RTX5000

## 13.24 Set the Hash Algorithm That IKE Uses

**[Syntax]**

**ipsec ike hash** *gateway\_id* *algorithm*

**no ipsec ike hash** *gateway\_id* [*algorithm*]

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *algorithm*
  - [Setting] :

Setting	Description
md5	MD5
sha	SHA-1
sha256	SHA-256

- [Initial value] :
  - sha

**[Description]**

Sets the hash algorithm for phase 1 of the IKEv1 operation.

If the router works as an initiator, the router proposes the algorithm specified by this command. If the router works as a responder, supported arbitrary algorithms can be used regardless of the setting of this command.

However, when the **ipsec ike negotiate-strictly** command is on, the router can use only a set algorithm even when it is a responder.

**[Note]**

IKEv2 has two negotiation parameters corresponding to the IKEv1 hash algorithm, Integrity Algorithm and PRF (Pseudo-Random Function). In IKEv2, when the **ipsec ike proposal-limitation** command is set to "on", the encryption algorithm which is configured by this command will be proposed. When the **ipsec ike proposal-limitation** command is set to "off", All supported algorithms will be proposed simultaneously, and let a remote security gateway select one. Also if it works as a responder, it selects the safest algorithm among the proposed ones.

The integrity algorithms that IKEv2 can support and the priority of selection at the time of response are as follows:

- HMAC-SHA2-256-128 > HMAC-SHA-1-96 > HMAC-MD5-96

Also, the PRF that IKEv2 can support, and the priority at the time of response selection are as follows:

- HMAC-SHA2-256 > HMAC-SHA-1 > HMAC-MD5

**[Models]**

RTX810, RTX5000

## 13.25 Set Whether to Output to the Log When the SPI Value of the Received Packet Is Invalid

**[Syntax]**

**ipsec log illegal-spi** *switch*

**no ipsec log illegal-spi**

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	Output to the log
off	Not output to the log

- [Initial value] : off

**[Description]**

Sets whether to log the event when the SPI value of the received packet is invalid in IPsec. The SPI value and the remote IP address are logged.

To reduce the possibility of a DoS attack in which large volumes of packets with invalid SPI values are received, a maximum of 10 types of packets are logged per second. The actual number of received packets cannot be found out.

**[Note]**

During the key exchange, this log may be output temporarily due to a difference in the key generation speed. In other words, even when one peer starts using a new key, the other peer may not be able to use the key causing the log to be output.

**[Models]**

RTX810, RTX5000

## 13.26 Set the IKE Payload Type

---

**[Syntax]**

```
ipsec ike payload type gateway_id type1 [type2]
no ipsec ike payload type gateway_id [type1 ...]
```

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security gateway identifier
  - [Initial value] : -
- *type1* : IKEv1 message format
  - [Setting] :

Setting	Description
1	Maintain compatibility Yamaha router release 2
2	Adapt to Yamaha router release 3
3	Adapt the generation method of the initial vector (IV) to some of the implementations.

- [Initial value] : 2
- *type2* : IKEv2 message format
  - [Setting] :

Setting	Description
1	Maintain compatibility Yamaha router IKEv2 release 1
2	Adapt the method of the key exchange and key usage to some of the implementations.

- [Initial value] : 2

**[Description]**

Sets the payload type for IKEv1 and IKEv2.

**[Models]**

RTX810, RTX5000

## 13.27 Setting the IKEv1 key exchange type

---

**[Syntax]**

```
ipsec ike backward-compatibility gateway_id type
```

**no ipsec ike backward-compatibility** *gateway\_id* [*type*]

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security gateway identifier
  - [Initial value] : -
- *type* : Key exchange type used in IKEv1
  - [Setting] :

Setting	Description
1	Preserves compatibility with Yamaha router Release 1 (previous release)
2	Conforms to Yamaha router Release 2 (new release)

- [Initial value] : 1

**[Description]**

Sets the key exchange type used in IKEv1. If connecting to a Yamaha router with the old revision using IKEv1, the *type* parameter must be set to 1.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

## 13.28 Set Whether to Send the IKE Information Payload

---

**[Syntax]**

**ipsec ike send info** *gateway\_id* *info*

**no ipsec ike send info** *gateway\_id* [*info*]

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *info*
  - [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : on

**[Description]**

Sets whether to send the information payload at the time of IKEv1 operation. For reception, all information payloads are parsed regardless of this setting.

**[Note]**

This command is used for special purposes such as in the verification of the connectivity. In steady-state operation, this command needs to be set to on.

This command does not affect operation of IKEv2. In IKEv2, the information payload is always sent and received if necessary.

**[Models]**

RTX810, RTX5000

## 13.29 Set Whether to Use PFS

---

**[Syntax]**

**ipsec ike pfs** *gateway\_id* *pfs*

**no ipsec ike pfs** *gateway\_id* [*pfs*]

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID

- [Initial value] : -
- *pfs*
- [Setting] :

Setting	Description
on	Use
off	Not use

- [Initial value] : off

**[Description]**

Sets whether to use PFS (Perfect Forward Secrecy) when the router is to function as an IKE initiator. When it is to function as a responder, it operates according to availability of PFS of the remote security gateway, regardless of this command configuration.

However, when the router operates as IKEv1 and also the **ipsec ike negotiate-strictly** command is on, this command configuration and PFS availability of the remote security gateway must match.

**[Models]**

RTX810, RTX5000

### 13.30 Set XAUTH

---

**[Syntax]**

```
ipsec ike xauth myname gateway_id name password
no ipsec ike xauth myname gateway_id
```

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *name*
  - [Setting] : Name to notify using XAUTH (up to 32 characters)
  - [Initial value] : -
- *password*
  - [Setting] : Password to notify using XAUTH (up to 32 characters)
  - [Initial value] : -

**[Description]**

Sets the name and password that are notified when XAUTH authentication is requested.

**[Models]**

RTX810, RTX5000

### 13.31 Set the User ID to Use in XAUTH Authentication or EAP-MD5 Authentication

---

**[Syntax]**

```
auth user userid username password
no auth user userid [username ...]
```

**[Setting and Initial value]**

- *userid*
  - [Setting] :
    - User ID number

Setting	Model
1..3000	RTX5000
1..1000	RTX810

- [Initial value] : -
- *username*
  - [Setting] :
    - User name

Setting	Model
Up to 256 characters	RTX5000, RTX810

\* More than or equal to 3 characters.

- [Initial value] : -
- *password*
- [Setting] :
  - Password

Setting	Model
Up to 64 characters	RTX5000, RTX810

\* More than or equal to 3 characters.

- [Initial value] : -

#### [Description]

Sets the user ID to use in IKEv1 XAUTH authentication or IKEv2 EAP-MD5 authentication.

#### [Models]

RTX810, RTX5000

## 13.32 Set the Attributes of the User ID to Use in XAUTH Authentication or EAP-MD5 Authentication

#### [Syntax]

**auth user attribute** *userid attribute=value* [*attribute=value ...*]

**no auth user attribute** *userid* [*attribute=value ...*]

#### [Setting and Initial value]

- *userid*
- [Setting] :
  - User ID number

Setting	Model
1..3000	RTX5000
1..1000	RTX810

- [Initial value] : -
- *attribute=value*
  - [Setting] : User attribute
  - [Initial value] : *xauth=off*

#### [Description]

Sets the attribute of an IKEv1 XAUTH authentication or IKEv2 EAP-MD5 authentication user ID.

The attributes that you can set are listed below.

<i>attribute</i>	<i>value</i>	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 addresses allowed)	Report this address as the internal IP address when an IPsec connection is made.
xauth-dns	IP address(IPv6 addresses allowed)	Report this address as the DNS server address when an IPsec connection is made.

<i>attribute</i>	<i>value</i>	Description
xauth-wins	IP address(IPv6 addresses allowed)	Report this address as the WINS server address when an IPsec connection is made.
xauth-filter	Text string indicating the filter set name	Apply this filter when an IPsec connection is made.
eap-md5	on	Use this ID for IKEv2 EAP-MD5 authentication
	off	Do not use this ID for IKEv2 EAP-MD5 authentication

If one attribute is repeatedly specified, a command error occurs.

**[Note]**

Attributes that are set explicitly by this command have priority over attributes that are set for the user group that the user ID belongs to by the **auth user group attribute** command.

**[Models]**

RTX810, RTX5000

### 13.33 Set the User Group to Use in XAUTH Authentication or EAP-MD5 Authentication

**[Syntax]**

**auth user group** *groupid* *userid* [*userid* ...]

**no auth user group** *groupid*

**[Setting and Initial value]**

- *groupid*
  - [Setting] :
    - User group ID number

Setting	Model
1..3000	RTX5000
1..1000	RTX810

- [Initial value] : -
- *userid*
  - [Setting] : User ID number or range of user ID numbers (You can specify multiple numbers and ranges)
  - [Initial value] : -

**[Description]**

Sets the user group to use in IKEv1 XAUTH authentication or IKEv2 EAP-MD5 authentication.

**[Example]**

```
# auth user group 1 100 101 102
# auth user group 1 200-300
# auth user group 1 100 103 105 107-110 113
```

**[Models]**

RTX810, RTX5000

### 13.34 Set the Attribute to Use in XAUTH Authentication or EAP-MD5 Authentication

**[Syntax]**

**auth user group attribute** *groupid* *attribute=value* [*attribute=value* ...]

**no auth user group attribute** *groupid* [*attribute=value* ...]

**[Setting and Initial value]**

- *groupid*
  - [Setting] :
    - User group ID number



Setting	Model
1..3000	RTX5000
1..1000	RTX810

- [Initial value] : -
- *attribute=value*
  - [Setting] : User group attribute
  - [Initial value] : xauth=off

**[Description]**

Sets the attribute of an IKEv1 XAUTH authentication or IKEv2 EAP-MD5 authentication. The attributes that you can set are listed below.

<i>attribute</i>	<i>value</i>	<b>Description</b>
xauth	on	Use the user IDs in this group for IPsec XAUTH authentication.
	off	Do not use the user IDs in this group for IPsec XAUTH authentication.
xauth-addresspool	IP address range (IPv6 addresses allowed)	Select an address from this address pool and report it as the internal IP address when an IPsec connection is made.
xauth-dns	IP address(IPv6 addresses allowed)	Report this address as the DNS server address when an IPsec connection is made.
xauth-wins	IP address(IPv6 addresses allowed)	Report this address as the WINS server address when an IPsec connection is made.
xauth-filter	Text string indicating the filter set name	Apply this filter when an IPsec connection is made.
eap-md5	on	Use this ID for IKEv2 EAP-MD5 authentication
	off	Do not use this ID for IKEv2 EAP-MD5 authentication

You can set the range of addresses for the xauth-address-pool attribute in one of the following ways:

- IP address[/netmask]
- IP address-IP address[/netmask]

If one attribute is repeatedly specified, a command error occurs.

**[Note]**

The attributes set using this command apply to all the users in the specified user group.

**[Models]**

RTX810, RTX5000

## 13.35 Configure XAUTH User Authentication

---

**[Syntax]**

```
ipsec ike xauth request gateway_id auth [group_id]
no ipsec ike xauth request gateway_id [auth ...]
```

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security gateway ID
  - [Initial value] : -
- *group\_id*
  - [Setting] : User Group ID to use in XAUTH authentication
  - [Initial value] : -
- *auth*

- [Setting] :

Setting	Description
on	Make a request
off	Not make a request

- [Initial value] : off

#### [Description]

Select whether or not to request XAUTH user authentication from the client after Phase1 of IPsec authentication finishes.

If you specify a value for *group\_id*, authentication is requested from the users in the specified user group.

If RADIUS server settings have been configured and you do not specify a value for *group\_id* or the users in the specified user group could not be authenticated, the router will attempt to use a RADIUS server for authentication.

#### [Note]

The settings made with this command are only valid when the router operates as a passive device. If the isakmp SA parameter sent from the security gateway of the initiator contains XAUTHInitPreShared (65001) as an authentication method, the router accepts the isakmp SA parameter and performs user authentication using XAUTH.

#### [Models]

RTX810, RTX5000

## 13.36 Set an Internal IP Address Pool

---

#### [Syntax]

```
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 and Initial value]

- *pool\_id*
  - [Setting] : Address pool ID (1..65535)
  - [Initial value] : -
- *ip\_address*
  - [Setting] : IP address (IPv6 addresses allowed)
  - [Initial value] : -
- *ip\_address-ip\_address*
  - [Setting] : IP address range (IPv6 addresses allowed)
  - [Initial value] : -
- *mask*
  - [Setting] : Netmask (prefix length for IPv6 addresses)
  - [Initial value] : -

#### [Description]

Sets an internal IP address pool for assigning to an IPsec client.

Address pools set using this command are used by the **ipsec ike mode-cfg address gateway\_id ...** command.

#### [Models]

RTX810, RTX5000

## 13.37 Set the IKE XAUTH Mode-Cfg Method

---

#### [Syntax]

```
ipsec ike mode-cfg method gateway_id method [option]
no ipsec ike mode-cfg method gateway_id [method...]
```

#### [Setting and Initial value]

- *gateway\_id*
  - [Setting] : Security gateway ID
  - [Initial value] : -
- *method*
  - [Setting] :

Setting	Description
set	SET method

- [Initial value] : set
- *option*

- [Setting] :

Setting	Description
openswan	Openswan conversion method

- [Initial value] : -

#### [Description]

Set the address assignment method for IKE XAUTH Mode-Cfg. You can only specify the SET method.

If you set *option* to 'openswan,' Openswan conversion mode is enabled, and you can connect to Openswan.

#### [Models]

RTX810, RTX5000

## 13.38 Set the Internal IP Address Pool That Is Assigned to the IPsec Client

#### [Syntax]

```
ipsec ike mode-cfg address gateway_id pool_id
no ipsec ike mode-cfg address gateway_id [pool_id]
```

#### [Setting and Initial value]

- *gateway\_id*
  - [Setting] : Security gateway ID
  - [Initial value] : -
- *pool\_id*
  - [Setting] : Address pool ID
  - [Initial value] : -

#### [Description]

Set the internal IP address pool that the router refers to when assigning an internal IP address to an IPsec client.

Because the IPsec client receives the internal IP address through the Config-Mode used by XAUTH authentication, the client will not receive an IP address when XAUTH authentication is not used.

If an internal IP address is set for each authenticated user through one of the methods listed below, the client will receive a uniquely set address instead of an address from the address pool.

- Registration by a RADIUS server
- One of the following commands:
  - **auth user attribute** *userid* xauth-address=*address[/mask]*
  - **auth user group attribute** *groupid* xauth-address-pool=*address-address[/mask]*

If all of the addresses in the address pool have been used, address assignment will not take place.

#### [Models]

RTX810, RTX5000

## 13.39 Registering the VPN client simultaneous connection control license

#### [Syntax]

```
ipsec ike license-key license_id key
no ipsec ike license-key license_id [...]
```

#### [Setting and Initial value]

- *license\_id*
  - [Setting] : Router key ID (1..500)
  - [Initial value] : -
- *key*
  - [Setting] : Router key (up to 64 characters)
  - [Initial value] : -

#### [Description]

Sets the router key (license key) in order to accept VPN connections from the VPN client (simultaneous connection version).

Each router key is assigned a unique simultaneous connection number. By registering multiple different router keys, the total maximum number of simultaneous connections for each router key can be secured. At this point, the VPN client software can use any of the client keys that correspond to the router keys registered by this command. Regardless of the client key used by the VPN client software, the connection limit is provided based on the maximum number of simultaneous connections from all the registered router keys

**[Example]**

```
[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 msextn on
# 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
```

**[Models]**

RTX5000

## 13.40 Application of the VPN client simultaneous connection control license

**[Syntax]**

```
ipsec ike license-key use gateway_id sw
no ipsec ike license-key use gateway_id [...]
```

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security gateway identifier
  - [Initial value] : -
- *sw*
  - [Setting] :

Setting	Description
on	Allows application of the router key
off	Does not allow application of the router key

- [Initial value] : off

**[Description]**

Sets whether the router key (license key) used to accept VPN connections from the VPN client (simultaneous connection version) is applied or not.

Gateways that are allowed to apply the router key can connect to VPN client software that has the corresponding client key.

**[Models]**

RTX5000

## 13.41 Set the IKE Log Type

### [Syntax]

```
ipsec ike log gateway_id type [type]
no ipsec ike log gateway_id [type]
```

### [Setting and Initial value]

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *type*
  - [Setting] :

Setting	Description
message-info	IKE message information
payload-info	Payload processing information
key-info	Processing information of key calculation

- [Initial value] : -

### [Description]

Sets the type of log to be output. All logs are output as debug level SYSLOGs.

When the router is to function as a responder, and if a security gateway cannot be identified, the configuration without the *gateway\_id* parameter is applied to communication.

### [Note]

If this command is not set, only the minimum amount of logs is output. Multiple *type* parameters can also be specified.

### [Models]

RTX810, RTX5000

## 13.42 Set Whether to Exchange ESP by Encapsulating It in UDP

### [Syntax]

```
ipsec ike esp-encapsulation gateway_id encap
no ipsec ike esp-encapsulation gateway_id
```

### [Setting and Initial value]

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *encap*
  - [Setting] :

Setting	Description
on	Encapsulate ESP in UDP and send it
off	Not encapsulate ESP in UDP and send it

- [Initial value] : off

### [Description]

In environments in which ESP cannot pass such as due to the effect of NAT, this command enables ESP to be transmitted/received by encapsulating ESP in UDP in order to establish an IPsec communication. The settings of this command must be the same between peer routers.

### [Note]

This command does not affect IPsec communication along with SA established by IKEv2.

### [Models]

RTX810, RTX5000

## 13.43 Set Whether to Restrict or not the Negotiation Parameter

### [Syntax]

```
ipsec ike proposal-limitation gateway_id switch
```

**no ipsec ike proposal-limitation** *gateway\_id* [*switch*]

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security gateway ID
  - [Initial value] : -
- *switch*
  - [Setting] :

Setting	Description
on	Restrict the negotiation parameter.
off	Do not restrict the negotiation parameter.

- [Initial value] : off

**[Description]**

Set whether to propose the negotiation parameter for constructing SAs as limited to particular command settings or not when the key exchange for IKEv2 is initiated.

When this command is disabled, the router proposes all supported negotiation parameters. The commands applied this command settings are as follow.

Parameter	Command
Encryption algorithm	<b>ipsec ike encryption for phase 1</b>
Group	<b>ipsec ike group for phase 1</b>
Hash algorithm	<b>ipsec ike hash for phase 1</b>
Encryption and hash algorithm for phase 2	<b>ipsec sa policy</b>

**[Note]**

This command is for only IKEv2. It does not affect the IKEv1.  
RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810

## 13.44 Set the Management of IKE Message ID

**[Syntax]**

**ipsec ike message-id-control** *gateway\_id* *switch*

**no ipsec ike message-id-control** *gateway\_id* [*switch*]

**[Setting and Initial value]**

- *gateway\_id*
  - [Setting] : Security gateway ID
  - [Initial value] : -
- *switch*
  - [Setting] :

Setting	Description
on	Manage the sending of the request message by message ID
off	Do not manage the sending of the request message by message ID

- [Initial value] : off

**[Description]**

Set the management method of message ID for sending the request message of IKEv2.

When this command is enabled and all response packet of IKE message sent by using a IKE SA is not received, the new IKE message does not send.

**[Note]**

This command is for only IKEv2. It does not affect the IKEv1.  
RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810

## 13.45 SA Configuration

---

Keep in mind that all SAs are cleared when the router is restarted.

### 13.45.1 Set the SA Life Time

---

**[Syntax]**

```
ipsec ike duration sa gateway_id second [kbytes] [rekey rekey]
no ipsec ike duration sa gateway_id [second [kbytes] [rekey rekey]]
```

**[Setting and Initial value]**

- *sa*

- [Setting] :

Setting	Description
ipsec-sa (or child-sa)	IPsec SA
isakmp-sa (or ike-sa)	ISAKMP SA

- [Initial value] : -

- *gateway\_id*

- [Setting] : Security Gateway ID
- [Initial value] : -

- *second*

- [Setting] : Number of seconds (300..691200)
- [Initial value] : 28800 seconds

- *kbytes*

- [Setting] : Number of bytes in KB (100..100000)
- [Initial value] : -

- *rekey* : SA update timing

- [Setting] :

Setting	Description
70%-90%	Percentage
off	No updating (Can only be specified when the <i>sa</i> parameter is set to isakmp-sa)

- [Initial value] : 75%

**[Description]**

Sets the lifetime of each SA.

When the *kbytes* parameter is specified, the SA is cleared after the amount of time specified by the *second* parameter elapses or after the specified amount of data is processed. *kbytes* is only valid when the SA parameter is set to ipsec-sa (child-sa). SA is updated when 75% of the bytes set for the *kbytes* parameter are processed.

The *rekey* parameter determines the timing at which the SA is updated. For example, if you set the *second* parameter to 20000 and the *rekey* parameter to 75%, a new SA is created 15000 seconds after the previous SA was created. The *rekey* parameter indicates a percentage of the *second* parameter. It is unrelated to the *kbytes* parameter.

You can only set the *rekey* parameter to 'off' if the *sa* parameter is set to isakmp-sa(ike-sa). In this case, ISAKMP SA (IKE SA) updating does not take place unless an IPsec SA (CHILD SA) must be created, so the creation of ISAKMP SAs (IKE SA) is kept to as low a level as possible.

Other influences and points to notice of this command, which differ according to activated IKE version, are as follows:

- IKEv1

If the router is to function as an initiator, a lifetime value specified with this command is proposed. If it is to function as a responder, the lifetime value proposed by the peer is used regardless of this command configuration.

Also then the *rekey* parameter to ISAKMP SA is set to off, to achieve this result, you must configure the settings in the following way:

1. Make the life time of ISAKMP SA shorter than that of IPsec SA.
  2. Enable dangling SAs. In other words, set the **ipsec ike restrict-dangling-sa** command to off.
- IKEv2

IKEv2 does not negotiate SA lifetime values, and each security gateway independently manages it. Therefore, established SA always has a lifetime value specified with this command. However, if a remote security gateway updates SA earlier, SA is updated earlier correspondingly.

IF the ISAKMP SA (IKE SA) lifetime expires earlier than the IPsec SA (CHILD SA) lifetime, match the ISAKMP SA (IKE SA) lifetime value to the IPsec SA (CHILD SA) lifetime value.

When you execute this command, the life times of SAs that already exist do not change. The life time setting only applies to the life times of newly created SAs.

#### [Models]

RTX810, RTX5000

### 13.45.2 Define the SA Policy

#### [Syntax]

```
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]
```

#### [Setting and Initial value]

- *policy\_id*
  - [Setting] : Policy ID(1..2147483647)
  - [Initial value] : -
- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *ah* : Keyword indicating the authentication header
  - [Initial value] : -
- *esp* : Keyword indicating the encapsulating security payload
  - [Initial value] : -
- *ah\_algorithm* : Integrity algorithm
  - [Setting] :

Setting	Description
md5-hmac	HMAC-MD5
sha-hmac	HMAC-SHA-1
sha256-hmac	HMAC-SHA2-256

- [Initial value] :
  - sha-hmac (for use of AH protocol)
  - - (for use of ESP protocol)
- *esp\_algorithm* : Encryption algorithm
  - [Setting] :

Setting	Description
3des-cbc	3DES-CBC
des-cbc	DES-CBC
aes-cbc	AES128-CBC
aes256-cbc	AES256-CBC

- [Initial value] :
  - aes-cbc
- *local-id*
  - [Setting] : Local private network
  - [Initial value] : -
- *remote-id*
  - [Setting] : Remote private network
  - [Initial value] : -



- *check*
  - [Setting] :

Setting	Description
on	Perform a sequence number check
off	Not perform a sequence number check

- [Initial value] : on

#### [Description]

Defines the SA policy. This definition is needed in the configuration of tunnel mode and transport mode. This definition can be used in multiple tunnel modes and transport modes.

In *local-id* and *remote-id*, describe a range of the source and destination addresses of the packet you want to encapsulate with a network address. In this way, the router can create multiple IPsec SAs to one security gateway, and use SA according to IP packet content.

When *check=on*, redundancy and order of the sequence number are checked for each received packet. Packets with an error are discarded. When a packet is discarded, the following information is logged at the debug level.

```
[IPSEC] sequence difference
[IPSEC] sequence number is wrong
```

If the remote side is performing priority and bandwidth control on the tunnel interface, packets may be received with sequence numbers that are out of order. In this case, the log above may be displayed and the packet may be discarded even though it is not actually an error. If this happens, it is better to specify off.

In IKEv2, when the **ipsec ike proposal-limitation** command is set to "on", the encryption algorithm which is configured by this command will be proposed for negotiation. When the **ipsec ike proposal-limitation** command is set to "off", All supported algorithms will be proposed simultaneously, and let a remote security gateway select one. Also if it works as a responder, it selects the safest algorithm among the proposed ones.

Also if it works as a responder, it selects an algorithm among the proposed ones according to the following priority:

- Integrity algorithm  
HMAC-SHA2-256 > HMAC-SHA-1 > HMAC-MD5
- Encryption algorithm  
AES256-CBC > AES192-CBC > AES128-CBC > 3DES-CBC > DES-CBC  
## AES192-CBC is supported in only IKEv2, and it cannot be selected by command.

In IKEv2, it has no effect on the *local-id* and the *remote-id* parameters.

#### [Note]

The *local-id* and *remote-id* set on both peers must match.

#### [Example]

```
# ipsec sa policy 101 1 esp aes-cbc sha-hmac
```

[Models]  
RTX810, RTX5000

### 13.45.3 Manually Refresh the SA

#### [Syntax]

```
ipsec refresh sa
```

#### [Description]

Manually refreshes the SA.

#### [Note]

Deletes all SAs being managed and initializes the IKE state.

Because this command does not notify the peer of the SA deletion, it is better to use the **ipsec sa delete all** command in normal operation.

[Models]  
RTX810, RTX5000

### 13.45.4 Set the Dangling SA Operation

#### [Syntax]

```
ipsec ike restrict-dangling-sa gateway_id action
no ipsec ike restrict-dangling-sa gateway_id [action]
```

#### [Setting and Initial value]

- *gateway\_id*
  - [Setting] : Security Gateway ID
  - [Initial value] : -
- *action*
  - [Setting] :

Setting	Description
auto	Synchronize IKE SA and IPsec SA only on the initiator of aggressive mode
off	Not synchronize IKE SA and IPsec SA.

- [Initial value] : auto

#### [Description]

This command places limitations on the operation of IKEv1 dangling SAs.

Dangling SA refers to the condition in which the corresponding IPsec SA is not deleted when the IKE SA is deleted. The RT series is basically designed to allow dangling SAs. IKE SA and IPsec SA are deleted at independent times.

If auto is specified, the router eliminates dangling SAs on the initiator of aggressive mode and deletes IKE SA and IPsec SA in sync. This operation is required for IKE keepalive to work correctly.

If off is specified, the router allows dangling SAs. IKE SA and IPsec SA are deleted at independent times.

If the router is not the client side of a dialup VPN, the router always manages IKE SA and IPsec SA independently regardless of the setting of this command. The delete timing is not necessarily synchronized.

#### [Note]

Even if a dangling SA is forcibly deleted, communication is not interrupted, because usually a new IPsec SA based on a new IKE SA exists.

The client side of a dialup VPN can use this command to change operation. Otherwise, it continues communication without doing anything even when a dangling SA occurs.

Not allowing dangling SAs on the client side of a dialup VPN is a requirement for the proper operation of IKE keepalive.

IKE keepalive carries out keepalive based on the IKE SA. If A dangling SA occurs, keepalive operation is not possible because the IKE SA that carries out keepalive does not exist. Therefore, in order to run IKE keepalive effectively, A dangling SA when it occurs must be forcibly deleted, and communication must be performed using an IPsec SA whose corresponding IKE SA exists.

This command does not affect operation of IKEv2. The IKEv2 specification prohibits existence of dangling SAs.

#### [Models]

RTX810, RTX5000

### 13.45.5 Configure Settings for IPsec NAT Traversal

#### [Syntax]

```
ipsec ike nat-traversal gateway switch [keepalive=interval] [force=force_switch]
no ipsec ike nat-traversal gateway [switch ...]
```

#### [Setting and Initial value]

- *gateway*
  - [Setting] : Security gateway ID
  - [Initial value] : -
- *switch* : Operation on/off setting
  - [Setting] :

Setting	Description
on	Enable NAT traversal operations

Setting	Description
off	Disable NAT traversal operations

- [Initial value] : off
- *interval* : NAT keepalive transmission interval
- [Setting] :

Setting	Description
off	Not send
30-100000	Time [seconds]

- [Initial value] : 300
- *force\_switch*
- [Setting] :

Setting	Description
on	Even if there is no NAT on the communication route, NAT traversal is used.
off	If there is no NAT on the communication route, NAT traversal is not used.

- [Initial value] : off

#### [Description]

Sets NAT traversal operations. When NAT traversal is enabled, NAT traversal negotiation is performed through IKE. If the peer does not support NAT traversal or there is no NAT processing on the communication route, the router communicates with ESP packets and does not use NAT traversal. NAT traversal settings must be configured on the peer router or terminal. If NAT traversal settings are only configured on one device, NAT traversal will not be used, and the router will communicate with ESP packets instead.

In IKEv2, the *switch* parameter affects only when the router is to function as an initiator. This option is used for the case where the router connects to a target device that needs NAT traversal operation even when there is no NAT process on the communication route. It is desirable that the parameter is 'off' normally.

#### [Note]

You cannot use this command with the **ipsec ike esp-encapsulation** command.  
 You cannot use this command with a tunnel interface that has been set to use IPComp.  
 In IKEv1, you can only use this command with an ESP tunnel in aggressive mode. You cannot use this command in main mode, with AH packets, or in transport mode.  
 In IKEv2, you can use this command only when an ESP tunnel is established. You cannot use it with AH, or in transport mode.

#### [Models]

RTX810, RTX5000

### 13.45.6 Deleting SAs

#### [Syntax]

**ipsec sa delete *id***

#### [Setting and Initial value]

- *id*
- [Setting] :

Setting	Description
Number	SA ID
all	All SAs

- [Initial value] : -

#### [Description]

Deletes the specified SA.  
 The SA ID is automatically granted and can be confirmed using the **show ipsec sa** command.

**[Models]**

RTX810, RTX5000

## 13.46 Tunnel Interface Configuration

---

### 13.46.1 Set the Fragmentation of IPv4 Packets Outside of IPsec Tunnel

---

**[Syntax]**

```
ipsec tunnel fastpath-fragment-function follow df-bit switch
no ipsec tunnel fastpath-fragment-function follow df-bit [switch]
```

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	If fragmentation of an ESP packet is necessary, determine whether or not to fragment according to the ESP packet's DF bit.
off	If fragmentation of an ESP packet is necessary, then fragment it, regardless of the ESP packet's DF bit.

- [Initial value] : off

**[Description]**

If fragmentation of an ESP packet is necessary, determine whether or not to fragment according to the DF bit. Even if the DF bit was set for an ESP packet using the ipsec tunnel outer df-bit command, if this command is set to off, it will be fragmented. This command is set for the tunnel interface, and only applicable to ESP packets processed by fastpath processing.

**[Models]**

RTX810, RTX5000

### 13.46.2 Set the DF Bit Control of the IPv4 Packet on the Outside of the IPsec Tunnel

---

**[Syntax]**

```
ipsec tunnel outer df-bit mode
no ipsec tunnel outer df-bit [mode]
```

**[Setting and Initial value]**

- *mode*
- [Setting] :

Setting	Description
copy	Copy the DF bit of the internal IPv4 packet to the outside
set	Always 1.
clear	Always 0.

- [Initial value] : copy

**[Description]**

Controls how to set the DF bit on the IPv4 packet outside the IPsec tunnel.

If copy is specified, the DF bit of the internal IPv4 packet is copied as-is to the outside.

If set or clear is specified, the DF bit of the outer IPv4 packet is set to 1 or 0 regardless of the DF bit of internal IPv4 packet.

This command is used for each tunnel interface.

**[Note]**

If the IPsec packet must be fragmented due to the magnitude relationship between the tunnel interface MTU and the MTU value of the actual interface, the DF bit is set to 0 regardless of the setting of this command.

**[Models]**

RTX810, RTX5000

### 13.46.3 Set the SA Policy to Be Used

---

#### [Syntax]

```
ipsec tunnel policy_id
no ipsec tunnel [policy_id]
```

#### [Setting and Initial value]

- *policy\_id*
  - [Setting] : Integer (1..2147483647)
  - [Initial value] : -

#### [Description]

Sets the SA policy to be used on the selected tunnel interface.

#### [Models]

RTX810, RTX5000

### 13.46.4 Set Data Compression Using IPComp

---

#### [Syntax]

```
ipsec ipcomp type type
no ipsec ipcomp type [type]
```

#### [Setting and Initial value]

- *type*
  - [Setting] :

Setting	Description
deflate	Compress the data using deflate compression
none	Disable data compression

- [Initial value] : none

#### [Description]

Sets whether to perform data compression using IPComp. The only supported algorithm is deflate.

No special setting is needed to decompress received IPComp packets. If an IPComp packet that has been compressed with a supported algorithm is received, the router decompresses the packet regardless of the setting of this command.

It is not always necessary to set this command to both peers of the security gateway. If this command is set on one peer, only the IP packets sent from that security gateway is compressed.

When using transport mode only, IPComp cannot be used.

#### [Note]

Data compression is also accomplished through the CCP used by PPP, and FRF.9 used by frame relay. The compression algorithm deflate used by IPComp and Stac-LZS used by CCP/FRF.9 are basically the same. However, CCP/FRF.9 data compression is carried out after the IPsec encryption. Therefore, there is hardly any effect, because the data is random after the encryption. On the other hand, IPComp compresses the data before the IPsec encryption and produces a given effect. In addition, unlike CCP/FRF.9, compressed data traverses all routes to the peer security gateway. Thus, one can expect the effects of the data compression even when the router output interface is LAN, for example.

#### [Models]

RTX810, RTX5000

### 13.46.5 Set the Tunnel Backup

---

#### [Syntax]

```
tunnel backup none
tunnel backup interface ip_address
tunnel backup pp peer_num [switch-router=switch1]
tunnel backup tunnel tunnel_num [switch-interface=switch2]
no tunnel backup
```

#### [Setting and Initial value]

- none : Do not use the tunnel backup
  - [Initial value] : none
- *interface*
  - [Setting] : LAN interface name

- [Initial value] : -
- *ip\_address*
  - [Setting] : IP address of the backup destination gateway
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Peer number of the backup destination
  - [Initial value] : -
- *tunnel\_num*
  - [Setting] : Tunnel interface number
  - [Initial value] : -
- *switch1* : Whether to divide the router receiving the backup to two units
  - [Setting] :

Setting	Description
on	Divide
off	Not divide

- [Initial value] : off
- *switch2* : Whether to recreate the tunnel according to the backup of the LAN/PP interface
  - [Setting] :

Setting	Description
on	Recreate
off	Not recreate

- [Initial value] : on

#### [Description]

Specifies the interface to be used as backup when a failure occurs on the tunnel interface.

Set the switch-router option to on when the following two conditions are met.

- There are two routers on the backup receiving end. One is connected to the backup source line, and the other is connected to the backup destination line.
- The firmware revision of the router connected to the backup destination line is older than this revision.

#### [Models]

RTX810, RTX5000

### 13.46.6 Set a Tunnel Template

#### [Syntax]

**tunnel template** *tunnel* [*tunnel* ...]

**no tunnel template**

#### [Setting and Initial value]

- *tunnel*
  - [Setting] : Tunnel interface number, or a range of tunnel interface numbers specified using a hyphen (-) in between.
  - [Initial value] : -

#### [Description]

Using the tunnel interface which was selected by the **tunnel select** command as the source, this command specifies the target tunnel interfaces to apply the command settings from the source tunnel interface.

The following commands, when set for the source tunnel interface, will also be applied to the target tunnel interfaces: For the commands with an asterisk (\*), see [Note]

- **ipsec tunnel**
- **ipsec sa policy**
- Of the commands that begin with **ipsec ike**, those that have a security gateway identifier as a parameter.
- **ipsec auto refresh** (only if a security gateway identifier is specified as an argument)
- **tunnel encapsulation**
- Commands that start with **l2tp** (\*)
- **tunnel enable**

Of the above commands, the following commands are applied only if the values of specific parameters matches the source tunnel interface number. In such case, the value of such parameter is replaced by the target tunnel interface number.

Command	Parameter
<b>ipsec tunnel</b>	Policy ID
<b>ipsec sa policy</b>	Policy ID
Commands that begin with <b>ipsec ike</b>	Security gateway identifier
<b>ipsec auto refresh</b>	Security gateway identifier
<b>tunnel enable</b>	Tunnel interface number

In the **ipsec sa policy** command, the security gateway identifier is replaced by the target tunnel interface number.

In the **ipsec ike remote name** command, the target tunnel interface number is appended to the name of the security gateway on the peer side.

If the command that was set for the source tunnel interface is already set for the target tunnel interface, priority is given to the command set for the target tunnel interface.

After a command has been applied, you can check the settings referenced during router operation, by specifying the keyword **expand** in the **show config tunnel** command.

#### [Note]

This can be used only when the tunnel interface is selected.

Of the applicable commands, the commands with (\*) are supported in the following models and revisions.

Model	Revision
RTX5000	All revisions
RTX810	Rev.11.01.23 or later

#### [Example]

For the target tunnel interface, you can write the specification both by number and by range, simultaneously.

```
tunnel select 1
tunnel template 8 10-20
tunnel select 2
tunnel template 100 200-300 400
```

The following two examples indicate the same settings.

```
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 esp aes-cbc sha-hmac
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
```

**[Models]**

RTX810, RTX5000

## 13.47 Transport Mode Configuration

---

### 13.47.1 Define the Transport Mode

---

**[Syntax]**

```
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 and Initial value]**

- *id*
  - [Setting] : Transport ID (1..2147483647)
  - [Initial value] : -
- *policy\_id*
  - [Setting] : Policy ID(1..2147483647)
  - [Initial value] : -
- *proto*
  - [Setting] : Protocol
  - [Initial value] : -
- *src\_port\_list* : UDP and TCP source port number sequence
  - [Setting] :
    - A decimal number representing the port number
    - Mnemonic representing the port number
    - \* (all ports)
  - [Initial value] : -
- *dst\_port\_list* : UDP and TCP source port number sequence
  - [Setting] :
    - A decimal number representing the port number
    - Mnemonic representing the port number
    - \* (all ports)
  - [Initial value] : -

**[Description]**

Sets the transport mode

After the transport mode is defined, communication in transport mode starts on IP packets that conform to the *proto*, *src\_port\_list*, and *dst\_port\_list* parameters.

**[Example]**

- Communicate the TELNET data to the router at 192.168.112.25 in transport mode

```
# ipsec sa policy 102 192.168.112.25 esp des-cbc sha-hmac
# ipsec transport 1 102 tcp * telnet
```

**[Models]**

RTX810, RTX5000

### 13.47.2 Setting the transport mode template

---

**[Syntax]**

```
ipsec transport template id1 id2 [id2 ...]
no ipsec transport id1 [id2 ...]
```

**[Setting and Initial value]**

- *id1*
  - [Setting] : Source transport ID
  - [Initial value] : -
- *id2*



- [Setting] : Target transport ID, or a range of transport IDs specified with a hyphen (-) in between them
- [Initial value] : -

**[Description]**

Sets the transport ID, which is the target of the specified ipsec transport command setting. The policy ID for the target is set to be identical to the source transport ID.

If a setting already exists for the source transport ID, the setting for the source is given precedence.

This command can expand the ipsec transport command setting up to the number of VPN zones. It cannot expand beyond the range of the number of VPN zones.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Example]**

The transport ID for the source setting and the range of transport IDs can be simultaneously specified.

```
ipsec transport 1 1 udp 1701 * ipsec transport template 1 10 20-30
```

The following two examples show the same settings.

```
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 *
```

**[Models]**

RTX810, RTX5000

## 13.48 PKI Configuration

---

### 13.48.1 Set the Certification File

---

**[Syntax]**

```
pki certificate file cert_id file type [password]
no pki certificate file cert_id [file ...]
```

**[Setting and Initial value]**

- *cert\_id*
  - [Setting] :

Setting	Description
1..8	Certificate file identifier

- [Initial value] : -
- *file*

- [Setting] :

Setting	Description
Specify the absolute or relative path of the external memory and file in the RTFS area	Certificate file name

- [Initial value] : -
- *type* : File format

- [Setting] :

Setting	Description
pkcs12	PKCS#12 format file
x509-pem	X.509 PEM format file

- [Initial value] : -
- *password*
  - [Setting] : Password to decrypt the file(up to 64 characters)

- [Initial value] : -

### [Description]

Sets the certificate file.

Note that models that store PKI files in the dedicated area of the internal flash ROM and models that store them in the external memory or the RTFS area have different formats to specify *file*.

For models that store PKI files in the dedicated area of the internal flash ROM, you can check a certificate file number with the **show file list internal** command.

When specifying a relative path in the *file* parameter for a model that allows using of the external memory or the RTFS area, specify the relative path from the directory specified with the environment variable of the **set** command, *pwd*.

If specifying pkcs12 for *type*, you must specify *password* to decrypt files.

### [Models]

RTX810, RTX5000

## 13.48.2 Set the CRL File

---

### [Syntax]

**pki crl file** *crl\_id file*

**no pki crl file** *crl\_id [file]*

### [Setting and Initial value]

- *crl\_id*
  - [Setting] :

Setting	Description
1..8	CRL file identifier

- [Initial value] : -
- *file*

- [Setting] :

Setting	Description
Specify the absolute or relative path of the external memory and file in the RTFS area	CRL file name

- [Initial value] : -

### [Description]

Sets the CRL file.

Note that models that store PKI files in the dedicated area of the internal flash ROM and models that store them in the external memory or the RTFS area have different formats to specify *file*.

For models that store PKI files in the dedicated area of the internal flash ROM, you can check a CRL file number with the **show file list internal** command.

When specifying a relative path in the *file* parameter for a model that allows using of the external memory or the RTFS area, specify the relative path from the directory specified with the environment variable of the **set** command, *pwd*.

### [Models]

RTX810, RTX5000

# Chapter 14

## Set the L2TP Function

### L2TP/IPsec function

L2TP (Layer Two Tunneling Protocol) is a tunneling protocol that allows VPN (Virtual Private Network) connection between networks. Although L2TP itself has no decryption system, the combination use of L2TP and IPsec (L2TP/IPsec), which provides VPN connection allowing data security and integrity, is available. The Yamaha router operates as a remote access VPN server with the use of L2TP/IPsec. It allows secure communication from a L2TP client loaded on smartphones to a terminal in the private network under the Yamaha router over the Internet.

L2TP/IPsec that the Yamaha router supports has the following restrictions:

- L2TP functions are not provided. Only L2TP/IPsec is supported.
- The Yamaha router operates as a remote access VPN server. It does not operate as a client.
- VPN connection between LANs is not supported.
- To listen to a L2TP packet at the first time, the UDP port number 1701 is used. You cannot change it.
- Only IKEv1 is supported. IKEv2 is not available.

### L2TPv3 function

L2TPv3 (Layer 2 Tunneling Protocol version 3) is a tunneling protocol that allows a VPN connection (L2 Virtual Private Network) using data link layers (L2). Through encapsulation of the L2 frame as an IP packet, L2 frame transmission is possible between routers, and the network can be constructed using multiple points of the same segment. Because L2TPv3 itself does not incorporate encryption, by using it together with IPsec, it is possible to create L2TPv3/IPsec, a VPN connection in which data confidentiality and safety is maintained. Yamaha routers can create an L2VPN using L2TPv3 or an L2VPN using L2TPv3/IPsec.

The L2TPv3 supported by the Yamaha router has the following restrictions:

- Only the UDP packet encapsulation method (L2TPv3 over UDP) is supported for L2 frame encapsulation. Does not support IP packet encapsulation using IP protocol number 115 (L2TPv3 over IP).
- UDP port 1701 is used to receive L2TPv3 packets. This cannot be changed.
- The only L2 frames that can tunnel under L2TPv3 are Ether frames.
- L2TPv3/IPsec only supports the IKEv1 transport mode.

## 14.1 Set Whether to Run L2TP

### [Syntax]

```
l2tp service service [version [version]]
no l2tp service [service [version [version]]]
```

### [Setting and Initial value]

- *service*
  - [Setting] :

Setting	Description
on	L2TP is activated.
off	L2TP is not activated.

- [Initial value] : off
- *version*
  - [Setting] :

Setting	Description
l2tp	L2TP/IPsec is activated
l2tpv3	L2TPv3, L2TPv3/IPsec is activated

- [Initial value] : -

### [Description]

Sets whether to run L2TP.

The version can be used to specify the L2TP version that will be run. If no version is specified, both L2TPv2 and L2TPv3 will be run.

When L2TP is valid, opens the UDP port number 1701 and waits for L2TP connection.

When L2TP is invalid, closes the UDP port number 1701 and disconnects all activated L2TP connections.

**[Note]**

The version can only be specified on models that support L2TPv3 functionality.

**[Models]**

RTX810, RTX5000

## 14.2 L2TP Tunnel Authentication Configuration

---

**[Syntax]**

**l2tp tunnel auth** *switch* [*password*]

**no l2tp tunnel auth** [*switch ...*]

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	Carry out L2TP tunnel authentication
off	Not carry out L2TP tunnel authentication

- [Initial value] : off
- *password*
  - [Setting] : Password used for the L2TP tunnel authentication(up to 32 characters)
  - [Initial value] : -

**[Description]**

Sets whether to carry out the L2TP tunnel authentication. If the password is omitted, the model name is used as the password. For example, for RTX810, the password is "RTX810".Please note the password is case sensitive.

**[Models]**

RTX810, RTX5000

## 14.3 Set the Disconnection Timer of L2TP Tunnel

---

**[Syntax]**

**l2tp tunnel disconnect time** *time*

**no l2tp tunnel disconnect time** [*time*]

**[Setting and Initial value]**

- *time*
- [Setting] :

Setting	Description
1..21474836	Number of seconds
off	Disable the timer

- [Initial value] : 60

**[Description]**

Sets the disconnection timer of the L2TP tunnel.

Sets the duration of data packet inactivity (no reception or transmission) after which the connection with the selected L2TP tunnel is disconnected.

Since all except L2TP control messages are data packets, disconnection of the L2TP tunnel by the disconnection timer may not be carried out in such a case where the PPP keepalive is used.

It is settable only for tunnel interfaces.

**[Models]**

RTX810, RTX5000

## 14.4 Set the L2TP Keepalive

---

**[Syntax]**

**l2tp keepalive use** *switch* [*interval* [*count*]]

**no l2tp keepalive use** [*switch ...*]

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Enable L2TP keepalive
off	Disable L2TP keepalive

- [Initial value] : on
- *interval*
  - [Setting] : Time interval for sending keepalive packets[seconds] (1..600)
  - [Initial value] : 10
- *count*
  - [Setting] : Count for determining down detection (1..50)
  - [Initial value] : 6

**[Description]**

Sets whether to use L2TP keepalive.

When keepalive is carried out, it is activated by the L2TP Hello message according to the *interval* and *count* values. It is settable only for tunnel interfaces.

**[Models]**

RTX810, RTX5000

## 14.5 Set L2TP Keepalive Logging

---

**[Syntax]**

**l2tp keepalive log** *log*  
**no l2tp keepalive log** [*log*]

**[Setting and Initial value]**

- *log*
  - [Setting] :

Setting	Description
on	Output L2TP keepalive to the log
off	Not output L2TP keepalive to the log

- [Initial value] : off

**[Description]**

Sets whether to output L2TP keepalive logs. All logs are output into the debug level SYSLOG. It is settable only for tunnel interfaces.

**[Models]**

RTX810, RTX5000

## 14.6 Set Whether to Output L2TP Connection Control to the Syslog

---

**[Syntax]**

**l2tp syslog** *syslog*  
**no l2tp syslog** [*syslog*]

**[Setting and Initial value]**

- *syslog*
  - [Setting] :

Setting	Description
on	Output the logs about L2TP connection control to the SYSLOG
off	Not output the logs about L2TP connection control to the SYSLOG

- [Initial value] : off

**[Description]**

Sets whether to output logs about L2TP connection control to the SYSLOG.  
 Logs about L2TP keepalive are not output.  
 All logs are output into the debug level SYSLOG.  
 It is settable only for tunnel interfaces.

**[Models]**

RTX810, RTX5000

## 14.7 Setting a permanent L2TPv3 connection

---

**[Syntax]**

**l2tp always-on** *sw*  
**no l2tp always-on** [*sw*]

**[Setting and Initial value]**

- *sw*
- [Setting] :

Setting	Description
on	Enable permanent connection
off	Disable permanent connection

- [Initial value] : on

**[Description]**

Configures whether to set the L2TPv3 connection as permanent or not. It is possible to set only the tunnel interface.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX5000

## 14.8 Setting the L2TP tunnel host name

---

**[Syntax]**

**l2tp hostname** *hostname*  
**no l2tp hostname** [*name*]

**[Setting and Initial value]**

- *name*
- [Setting] : Host name (up to 32 characters)
- [Initial value] : Model name

**[Description]**

Sets the host name to be notified to the connection peer. Shows the L2TP tunnel information output by the show status l2tp command. The model name will be used as the host name if nothing is set using this command. It is possible to set only the tunnel interface.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX5000

## 14.9 Setting the L2TPv3 local Router ID

---

**[Syntax]**

**l2tp local router-id** *ipv4\_address*  
**no l2tp local router-id** [*ipv4\_address*]

**[Setting and Initial value]**

- *ipv4\_address*

- [Setting] : IPv4 address
- [Initial value] : 0.0.0.0

**[Description]**

Sets the Router ID notified to the L2TPv3 connection peer. Sets the connection peer Remote Router ID as the same IPv4 address. The IPv4 address assigned to the router does not have to be used. It is possible to set only the tunnel interface.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX5000

## 14.10 Setting the L2TPv3 Remote Router ID

---

**[Syntax]**

```
l2tp remote router-id ipv4_address
no l2tp remote router-id [ipv4_address]
```

**[Setting and Initial value]**

- *ipv4\_address*
  - [Setting] : IPv4 address
  - [Initial value] : 0.0.0.0

**[Description]**

Sets the Router ID for the L2TPv3 connection peer. Sets the connection peer Local Router ID as the same IPv4 address. The IPv4 address assigned to the router does not have to be used. It is possible to set only the tunnel interface.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX5000

## 14.11 Setting the L2TPv3 Remote End ID

---

**[Syntax]**

```
l2tp remote end-id end-id
no l2tp remote end-id [end-id]
```

**[Setting and Initial value]**

- *end-id*
  - [Setting] : Arbitrary character string (up to 32 characters)
  - [Initial value] : None

**[Description]**

Sets the L2TPv3 Remote End ID. Sets the connection peer Remote End ID as the same character string. It is possible to set only the tunnel interface.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX5000

## Chapter 15

### PPTP Configuration

You can only use PPTP to connect to a PC if the PC has the Microsoft Windows VPN.

#### 15.1 Common Configuration

Refer also to the **tunnel encapsulation**, **tunnel endpoint address**, and **ppp ccp type** commands.

##### 15.1.1 Set Whether to Operate as a PPTP Server

###### [Syntax]

```
pptp service service
no ptp service [service]
```

###### [Setting and Initial value]

- service*
- [Setting] :

Setting	Description
on	Operate as a PPTP server
off	Do not operate as a PPTP server

- [Initial value] : off

###### [Description]

Sets whether to operate as a PPTP server.

###### [Note]

When off is set, TCP port 1723, which is used by the PPTP server, is closed. The default setting is off, so if you want the router to operate as a PPTP server, set **pptp service** to on.

###### [Models]

RTX810

##### 15.1.2 Set the Tunnel Interfaces That Are Bound to the Peer Information Number

###### [Syntax]

```
pp bind interface [interface ...]
no pp bind [interface]
```

###### [Setting and Initial value]

- interface*
- [Setting] :

Setting	Description
tunnelN	TUNNEL interface name
tunnelN-tunnelM	Range of TUNNEL interfaces

- [Initial value] : -

###### [Description]

Specify the tunnel interfaces that are bound to the selected peer information number.

First and second syntax can both be specified for the anonymous interface, and although it is possible to specify them simultaneously together, if anything other than an anonymous interface has been selected, specifying multiple tunneling interfaces will cause an error.

###### [Note]

Set PPTP or L2TP for every PP.

You can make PPTP communication possible by using the **tunnel encapsulation** command to bind the tunnel interfaces that have been set to pptp.

You can make L2TP communication possible by using the **tunnel encapsulation** command to bind the tunnel interfaces that have been set to l2tp.



**[Models]**  
RTX810, RTX5000

### 15.1.3 Set the PPTP Operation Type

---

**[Syntax]**

**pptp service type** *type*  
**no pptp service type** [*type*]

**[Setting and Initial value]**

- *type*
  - [Setting] :

Setting	Description
server	Operate as a server
client	Operate as a client

- [Initial value] : server

**[Description]**

Choose whether to operate as a server or as a client.

**[Note]**

PPTP is a server-client connection method. When it is used to connect two routers, one router must be the server, and one must be the client.

**[Models]**  
RTX810

### 15.1.4 Set the PPTP Host Name

---

**[Syntax]**

**pptp hostname** *name*  
**no pptp hostname** [*name*]

**[Setting and Initial value]**

- *name*
  - [Setting] : Host name (64 bytes or less)
  - [Initial value] : Model name

**[Description]**

Sets the PPTP host name.

**[Note]**

The user-defined name set by the command is reported to the peer. If no name is specified, the model name is reported. On the peer, the name appears next to “Access Concentrator:” when the **show status pp** command is executed.

**[Models]**  
RTX810

### 15.1.5 Set the PPTP Packet Window Size

---

**[Syntax]**

**pptp window size** *size*  
**no pptp window size** [*size*]

**[Setting and Initial value]**

- *size*
  - [Setting] : Number of packets (1..128)
  - [Initial value] : 32

**[Description]**

Set the maximum number of unanswered received packets that can be put into the buffer.

**[Models]**  
RTX810

### 15.1.6 Set the Authentication Method to Request for Creating PPTP Encryption Keys

---

**[Syntax]**

```
pp auth request auth [arrive-only]
no pp auth request [auth]
```

**[Setting and Initial value]**

- *auth*
  - [Setting] :

Setting	Description
pap	PAP
chap	CHAP
mschap	MSCHAP
mschap-v2	MSCHAP-Version2
chap-pap	CHAP and PAP

- [Initial value] : -

**[Description]**

Sets the authentication method to request.

**[Note]**

To generate PPTP encryption keys, set the authentication protocol to MS-CHAP or MS-CHAPv2. This setting is normally configured on the server side.

**[Models]**

RTX810

### 15.1.7 Set the Acceptable Authentication Methods for Creating PPTP Encryption Keys

---

**[Syntax]**

```
pp auth accept auth [auth]
no pp auth accept [auth auth]
```

**[Setting and Initial value]**

- *auth*
  - [Setting] :

Setting	Description
pap	PAP
chap	CHAP
mschap	MSCHAP
mschap-v2	MSCHAP-Version2

- [Initial value] : -

**[Description]**

Sets the acceptable authentication methods.

**[Note]**

To generate PPTP encryption keys, set the authentication protocol to MS-CHAP or MS-CHAPv2. This setting is normally configured on the client side.

When using MacOS 10.2 and later, Windows Vista, or Windows 7 as a client, use mschap-v2.

**[Models]**

RTX810

### 15.1.8 Set Whether to Output PPTP Connection Control to the Syslog

---

**[Syntax]**

```
pptp syslog syslog
no pptp syslog [syslog]
```

**[Setting and Initial value]**

- *syslog*
  - [Setting] :

Setting	Description
on	Output
off	Not output

- [Initial value] : off

**[Description]**

Sets whether to output PPTP connection control to the syslog.  
Keepalive echo requests and replies are not output.

**[Models]**

RTX810

## 15.2 Remote Access VPN Function

---

### 15.2.1 Set the PPTP Tunnel Disconnection Timer

---

**[Syntax]**

```
pptp tunnel disconnect time time
no pptp tunnel disconnect time [time]
```

**[Setting and Initial value]**

- *time*
  - [Setting] :

Setting	Description
1..21474836	Number of seconds
off	Disable the timer

- [Initial value] : 60

**[Description]**

Sets the duration of data packet inactivity (no reception or transmission) after which the connection with the selected PPTP tunnel is disconnected.

**[Models]**

RTX810

### 15.2.2 Set the Tunnel Endpoint Name

---

**[Syntax]**

```
tunnel endpoint name [local_name] remote_name
no tunnel endpoint name [local_name remote_name]
```

**[Setting and Initial value]**

- *local\_name*
  - [Setting] : Local name
  - [Initial value] : -
- *remote\_name*
  - [Setting] : Remote name
  - [Initial value] : -

**[Description]**

Sets the tunnel endpoint name.

**[Note]**

The **tunnel endpoint address** command has priority over this command.  
For PPTP tunnels, the name specifies the domain name (FQDN).

**[Models]**

RTX810, RTX5000

### 15.2.3 Set the PPTP Keepalive

---

#### [Syntax]

**pptp keepalive use** *use*  
**no pptp keepalive use** [*use*]

#### [Setting and Initial value]

- *use*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : on

#### [Description]

Sets whether to use tunnel keepalive.

#### [Note]

The router sends a PPTP control connection confirmation request (Echo-Request) to the PPTP tunnel endpoint and determines whether or not there is a reply (Echo-Reply). If there is no reply, the router disconnects from the tunnel as configured to by the **pptp keepalive interval** command.

#### [Models]

RTX810

### 15.2.4 Set PPTP Keepalive Logging

---

#### [Syntax]

**pptp keepalive log** *log*  
**no pptp keepalive log** [*log*]

#### [Setting and Initial value]

- *log*
  - [Setting] :

Setting	Description
on	Log
off	Do not log

- [Initial value] : off

#### [Description]

Select whether or not to log tunnel keepalive activity.

#### [Models]

RTX810

### 15.2.5 Set the PPTP Keepalive Interval and Count

---

#### [Syntax]

**pptp keepalive interval** *interval* [*count*]  
**no pptp keepalive interval** [*interval count*]

#### [Setting and Initial value]

- *interval*
  - [Setting] : Interval (1..65535)
  - [Initial value] : 30
- *count*
  - [Setting] : Count (3..100)
  - [Initial value] : 6

#### [Description]

Set the interval at which to send out tunnel keepalive packets and the count to use for downlink detection.

**[Note]**

After the router determines that a reply to a PPTP control connection confirmation request (Echo-Request) has not been received, it shortens the detection timer to 1 second.

**[Models]**

RTX810

### 15.2.6 Set Whether to Allow Connection According to the Encryption of the PPTP Connection

---

**[Syntax]**

**ppp ccp no-encryption** *mode*

**no ppp ccp no-encryption** [*mode*]

**[Setting and Initial value]**

- *mode*

- [Setting] :

Setting	Description
reject	Reject unencrypted connections
accept	Accept unencrypted connections

- [Initial value] : accept

**[Description]**

Set the operation to perform when MPPE (Microsoft Point-to-Point Encryption) has not been negotiated.

**[Models]**

RTX810

# Chapter 16

## Set the SIP Function

### 16.1 Common Configuration

#### 16.1.1 Set Whether to Use SIP

**[Syntax]**

**sip use** *use*

**no sip use**

**[Setting and Initial value]**

- *use*
- [Setting] :

Setting	Description
off	Disable
on	Enable

- [Initial value] : off

**[Description]**

Sets whether to use the SIP protocol.

**[Note]**

Change of setting from on to off becomes valid after re-startup.

**[Models]**

RTX810, RTX5000

#### 16.1.2 Set the Timer Value of the SIP Session-Timer Function

**[Syntax]**

**sip session timer** *time* [update=*update*] [refresher=*refresher*]

**no sip session timer**

**[Setting and Initial value]**

- *time*
- [Setting] :

Setting	Description
Number of seconds (60..540)	
0	Do not use the session-timer function

- [Initial value] : 0

- *update*

- [Setting] :

Setting	Description
on	Use the UPDATE method
off	Do not use the UPDATE method

- [Initial value] : -

- *refresher*

- [Setting] :

Setting	Description
none	Do not set the parameter refresher
uac	Set uac for the parameter refresher.

Setting	Description
uas	Set uas for the parameter refresher.

- [Initial value] : -

**[Description]**

Sets the timer value of the SIP session-timer function. If a peer suddenly drops during an SIP call due to a power outage etc., the call is disconnected automatically by the timer. If *update* is set to "on", the UPDATE method will become available in session-timer function at the time of sending. If *refresher* was set to none, the parameter refresher is not set, however, if uac/uas was set, it will send using the respective parameter value.

**[Models]**

RTX810, RTX5000

### 16.1.3 Select the IP Protocol to Use at the Time of Sending Calls Using SIP

---

**[Syntax]**

**sip ip protocol** *protocol*

**no sip ip protocol**

**[Setting and Initial value]**

- *protocol*
- [Setting] :

Setting	Description
udp	Use UDP
tcp	Use TCP

- [Initial value] : udp

**[Description]**

Selects the IP protocol to use for call control when sending calls using SIP.

**[Models]**

RTX810, RTX5000

### 16.1.4 Set Whether to Support 100rel when Sending Calls Using SIP

---

**[Syntax]**

**sip 100rel** *switch*

**no sip 100rel**

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	Support 100rel
off	Do not support 100rel

- [Initial value] : off

**[Description]**

Sets whether or not to support 100rel when sending calls using SIP.

**[Models]**

RTX810, RTX5000

### 16.1.5 Set the Additional User-Agent Header to SIP Packet to Be Sent

---

**[Syntax]**

**sip user agent** *sw* [*user-agent*]

**no sip user agent**

**[Setting and Initial value]**

- *sw*
- [Setting] :

Setting	Description
on	Add
off	Not add

- [Initial value] : off
- *user-agent*
  - [Setting] : Text string described in the header
  - [Initial value] : -

**[Description]**

You can add the User-Agent header in a SIP packet to be sent.  
A text string can be specified in the *user-agent* parameter, with up to 64 ASCII characters.

**[Models]**

RTX810, RTX5000

### 16.1.6 Setting When refresher Is Not Specified in INVITE at the Time of Call Reception Using SIP

---

**[Syntax]**

**sip arrive session timer refresher** *refresher*  
**no sip arrive session timer refresher**

**[Setting and Initial value]**

- *refresher*
  - [Setting] :

Setting	Description
uac	Specify refresher=uac
uas	Specify refresher=uas

- [Initial value] : uac

**[Description]**

Enables to specify UAC/UAS when INVITE at the time of call reception by SIP does not specify refresher.

**[Models]**

RTX810, RTX5000

### 16.1.7 Set Whether to Support P-N-UAType Header at the Time of Call Reception Using SIP

---

**[Syntax]**

**sip arrive ringing p-n-uatype** *switch*  
**no sip arrive ringing p-n-uatype**

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Add P-N-UAType header
off	Do not add P-N-UAType header

- [Initial value] : off

**[Description]**

Sets whether or not to add a P-N-UAType header to the Ringing response sent at the time of call reception using SIP.

**[Models]**

RTX810, RTX5000

### 16.1.8 Set Session Timer Request at the Time of Call Reception Using SIP

---

**[Syntax]**

**sip arrive session timer method** *method*  
**no sip arrive session timer method** [*method*]



**[Setting and Initial value]**

- *method*
- [Setting] :

Setting	Description
auto	Determine automatically
invite	Use INVITE only

- [Initial value] : auto

**[Description]**

Sets a request used in the session timer function at the time of call reception by SIP.

When auto is set, both UPDATE and INVITE are available. If a caller or server supports UPDATE, UPDATE is used.

When invite is set, the router operates without using UPDATE even though a caller or server supports UPDATE.

The setting to use UPDATE only is not available.

Also, since this setting cannot be set for every server, it is valid for all call receptions.

In case of originating calls, use the *update* option of the **sip server session timer** or **sip session timer** command to set it.

**[Models]**

RTX810, RTX5000

**16.1.9 Set Whether to Verify the User Name at the Time of SIP Reception****[Syntax]**

**sip arrive address check** *switch*

**no sip arrive address check**

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	Verify a user name
off	Not verify a user name

- [Initial value] : on

**[Description]**

Sets whether to verify consistency of the Request-URI at the time of reception and the Contact header of the sent REGISTER when a SIP server is set.

In the VoIP function using SIP, when using the setting to use the SIP server and the setting to use in Peer to Peer simultaneously, set off.

Also, when using RTV01 for the SIP server, set off.

**[Note]**

This verification is valid when the **sip server** setting is available.

**[Models]**

RTX810, RTX5000

**16.1.10 Set an SIP Response Code to Be Returned When No Port to Receive Calls Is Available****[Syntax]**

**sip response code busy** *code*

**no sip response code busy**

**[Setting and Initial value]**

- *code* : Response code
- [Setting] :

Setting	Description
486	Return 486
503	Return 503

- [Initial value] : 486

**[Description]**

Sets a response code to be returned when the router cannot receive any call due to busy state at the time of SIP reception.

**[Models]**

RTX810, RTX5000

**16.1.11 Set the IP Address Used by SIP**

---

**[Syntax]**

**sip outer address** *ipaddress*  
**no sip outer address**

**[Setting and Initial value]**

- *ipaddress*
  - [Setting] :

Setting	Description
auto	Automatic configuration
IP address	IP address

- [Initial value] : auto

**[Description]**

Sets the IP address to use for SIP. This value is also used for RTP/RTCP.

**[Note]**

It is recommended that you keep the initial setting.

**[Models]**

RTX810, RTX5000

**16.1.12 Set Whether to Log SIP Messages**

---

**[Syntax]**

**sip log** *switch*  
**no sip log**

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Log SIP messages
off	Not log SIP messages

- [Initial value] : off

**[Description]**

Set whether to log SIP messages at DEBUG level.

**[Models]**

RTX810, RTX5000

## Chapter 17

### SNMP Configuration

By configuring SNMP (Simple Network Management Protocol as defined in RFC1157), an SNMP management application can monitor and change the network management information. In this case, the Yamaha router functions as an SNMP agent.

The Yamaha router supports communication using SNMPv1, SNMPv2c, and SNMPv3. It also supports RFC1213 (MIB-II) and private MIB for the MIB (Management Information Base). Detail of the private MIB is available in the following URL:

- Yamaha private MIB: <http://www.yamaha.com/products/en/network//RT/docs/mib/>

In SNMPv1 and SNMPv2c, a caller notifies a name of the group called community to a peer, and communicates between hosts belonging to the same community only. In this case, you can specify a community name individually for two access modes, read-only and read-write.

In this way, a community name performs as a sort of password. On the other hand, since such a community name is always a plain text on networks, its security is vulnerable. If you need more secure communication, it is recommended to use SNMPv3.

SNMPv3 supports authentication and encryption of communication contents. SNMPv3 discards the community concept, and newly creates a security model called USM (User-based Security Model) to establish a higher security level.

SNMP messages that report the status of a Yamaha router are called traps. The Yamaha router sends a unique trap to report a special event for some functions in some cases, in addition to the SNMP standard traps. These unique traps are defined as private MIB.

You can specify multiple hosts to receive traps for each SNMP version.

The initial value of the read-only and transmission trap community name which are used in SNMPv1 and SNMPv2c is "public". The community name of the SNMP management application is also often "public". Therefore, change the community name if considering security for communication with the relative version. However as previously mentioned, since the form of community names is a plain text on the networks, be sure not use the community name for the login password or administrator password.

By factory default, no access is allowed in each SNMP version. In addition, no host to receive traps is set. Thus, the router does not send traps to any destination.

#### 17.1 Set the Host to Allow Access Using SNMPv1

##### [Syntax]

```
snmp host host [ro_community [rw_community]]
```

```
no snmp host [host]
```

##### [Setting and Initial value]

- *host* : Host to allow access using SNMPv1
  - [Setting] :

Setting	Description
<i>ip_address</i>	The IP address can be a single address, two IP addresses with a hyphen in between them (range designation)
lanN	Allow access from a specified LAN interface
bridgeN	Allow access from a specified bridge interface
any	Allow access from all hosts
none	Prohibit access from all hosts

- [Initial value] : none
- *ro\_community*
  - [Setting] : Read-only community name (up to 16 characters)
  - [Initial value] : -
- *rw\_community*
  - [Setting] : Read-write community name (up to 16 characters)
  - [Initial value] : -

##### [Description]

Sets the host to allow access using SNMPv1.

If any is specified, access from any host using SNMPv1 is allowed.

If the host is specified by the IP address, lanN or bridgeN, the community name can also be specified. If the *rw\_community* parameter is omitted, access in the read-write mode is prohibited. If the *ro\_community* parameter is also omitted, the setting values of the **snmp community read-only** command and **snmp community read-write** command are used.

**[Note]**

RTX810 supports IP address range, lanN, bridgeN as *HOST* parameter in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

## 17.2 Set the SNMPv1 Read-Only Community Name

---

**[Syntax]**

**snmp community read-only** *name*

**no snmp community read-only**

**[Setting and Initial value]**

- *name*
  - [Setting] : Community name (up to 16 characters)
  - [Initial value] : public

**[Description]**

Sets the name of the community whose SNMPv1 access mode is read-only.

**[Models]**

RTX810, RTX5000

## 17.3 Set the SNMPv1 Read-Write Community Name

---

**[Syntax]**

**snmp community read-write** *name*

**no snmp community read-write**

**[Setting and Initial value]**

- *name*
  - [Setting] : Community name (up to 16 characters)
  - [Initial value] : -

**[Description]**

Sets the name of the community whose SNMPv1 access mode is read-write.

**[Models]**

RTX810, RTX5000

## 17.4 Set the SNMPv1 Trap Transmission Destination

---

**[Syntax]**

**snmp trap host** *host* [*community*]

**no snmp trap host** *host*

**[Setting and Initial value]**

- *host*
  - [Setting] : IP address of the host to receive SNMPv1 traps (IPv4/IPv6)
  - [Initial value] : -
- *community*
  - [Setting] : Community name (up to 16 characters)
  - [Initial value] : -

**[Description]**

Specifies the host to which the router sends SNMPv1 traps. Multiple hosts can be specified simultaneously by setting this command multiple times. The setting of the *community* parameter of this command is used for the community name when sending traps. However, if omitted, the setting of the **snmp trap community** command is used.

**[Models]**

RTX810, RTX5000

## 17.5 Set the SNMPv1 Trap Community Name

---

**[Syntax]**

**snmp trap community** *name*

**no snmp trap community**

**[Setting and Initial value]**

- *name*
  - [Setting] : Community name (up to 16 characters)
  - [Initial value] : public

**[Description]**

Sets the community name for sending SNMPv1 traps.

**[Models]**

RTX810, RTX5000

## 17.6 Set the Hosts to Allow Access Using SNMPv2c

---

**[Syntax]**

```
snmpv2c host host [ro_community [rw_community]]
no snmpv2c host [host]
```

**[Setting and Initial value]**

- *host* : Host to allow access using SNMPv2c
  - [Setting] :

Setting	Description
<i>ip_address</i>	The IP address can be a single address, two IP addresses with a hyphen in between them (range designation)
lanN	Allow access from a specified LAN interface
bridgeN	Allow access from a specified bridge interface
any	Allow access from all hosts
none	Prohibit access from all hosts

- [Initial value] : none
- *ro\_community*
  - [Setting] : Read-only community name (up to 16 characters)
  - [Initial value] : -
- *rw\_community*
  - [Setting] : Read-write community name (up to 16 characters)
  - [Initial value] : -

**[Description]**

Sets the host to allow access using SNMPv2c.

If 'any' is specified, access from any host using SNMPv2c is allowed.

If the host is specified by the IP address, lanN or bridgeN, the community name can also be specified. If the *rw\_community* parameter is omitted, access in the read-write mode is prohibited. If the *ro\_community* parameter is also omitted, the setting values of the **snmpv2c community read-only** command and **snmpv2c community read-write** command are used.

**[Note]**

RTX810 supports IP address range, lanN, bridgeN as *HOST* parameter in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

## 17.7 Set the SNMPv2c Read-Only Community Name

---

**[Syntax]**

```
snmpv2c community read-only name
no snmpv2c community read-only
```

**[Setting and Initial value]**

- *name*
  - [Setting] : Community name (up to 16 characters)
  - [Initial value] : public

**[Description]**

Sets the name of the community whose SNMPv2c access mode is read-only.

**[Models]**

RTX810, RTX5000

## 17.8 Set the SNMPv2c Read-Write Community Name

---

**[Syntax]****snmpv2c community read-write** *name***no snmpv2c community read-write****[Setting and Initial value]**

- *name*
  - [Setting] : Community name (up to 16 characters)
  - [Initial value] : -

**[Description]**

Sets the name of the community whose SNMPv2c access mode is read-write.

**[Models]**

RTX810, RTX5000

## 17.9 Set the SNMPv2c Trap Transmission Destination

---

**[Syntax]****snmpv2c trap host** *host* [*type* [*community*]]**no snmpv2c trap host** *host***[Setting and Initial value]**

- *host*
  - [Setting] : IP address of the host to receive SNMPv2c traps (IPv4/IPv6)
  - [Initial value] : -
- *type* : Message type
  - [Setting] :

Setting	Description
trap	Send the trap
inform	Send the Inform request

- [Initial value] : trap
- *community*
  - [Setting] : Community name (up to 16 characters)
  - [Initial value] : -

**[Description]**Specifies the host to which the router sends SNMPv2c traps. Multiple hosts can be specified simultaneously by setting this command multiple times. The setting of the *community* parameter of this command is used for the community name when sending traps. However, if omitted, the setting of the **snmpv2c trap community** command is used.If 'inform' is specified for the *type* parameter, a request is sent up to three times at 5-second interval until the destination returns response.**[Models]**

RTX810, RTX5000

## 17.10 Set the SNMPv2c Trap Community Name

---

**[Syntax]****snmpv2c trap community** *name***no snmpv2c trap community****[Setting and Initial value]**

- *name*
  - [Setting] : Community name (up to 16 characters)
  - [Initial value] : public

**[Description]**

Sets the community name for sending SNMPv2c traps.

**[Models]**

RTX810, RTX5000

**17.11 Set the SNMPv3 Engine ID**

---

**[Syntax]**

```
snmpv3 engine id engine_id
no snmpv3 engine id
```

**[Setting and Initial value]**

- *engine\_id*
  - [Setting] : SNMP engine ID(up to 27 characters)
  - [Initial value] : LAN1 MAC address (00a0deXXXXXX)

**[Description]**

Specifies a unique ID to identify the SNMP engine. The SNMP engine ID is reported to the destination via SNMPv3 communication.

**[Models]**

RTX810, RTX5000

**17.12 Set the SNMPv3 Context Name**

---

**[Syntax]**

```
snmpv3 context name name
no snmpv3 context name
```

**[Setting and Initial value]**

- *name*
  - [Setting] : SNMP context name (up to 16 characters)
  - [Initial value] : -

**[Description]**

Specifies a name to identify an SNMP context. The SNMP context name is reported to the peer with SNMPv3 communication.

**[Models]**

RTX810, RTX5000

**17.13 Set the User Managed with SNMPv3 USM**

---

**[Syntax]**

```
snmpv3 usm user user_id name [group group_id] [auth auth_pass [priv priv_pass]]
no snmpv3 usm user user_id
```

**[Setting and Initial value]**

- *user\_id*
  - [Setting] : User number (1..65535)
  - [Initial value] : -
- *name*
  - [Setting] : User name (up to 32 characters)
  - [Initial value] : -
- *group\_id*
  - [Setting] : User group number (1..65535)
  - [Initial value] : -
- *auth* : Integrity algorithm
  - [Setting] :

Setting	Description
md5	HMAC-MD5-96
sha	HMAC-SHA1-96

- [Initial value] : -
- *auth\_pass*
  - [Setting] : Authentication password (between 8 and 32 characters in length)
  - [Initial value] : -
- *priv* : Encryption algorithm

- [Setting] :

Setting	Description
des-cbc	DES-CBC
aes128-cfb	AES128-CFB

- [Initial value] : -
- *priv\_pass*
  - [Setting] : Encryption password (between 8 and 32 characters in length)
  - [Initial value] : -

#### [Description]

Sets information of users who can access using SNMPv3.

When a user group number is specified, it becomes a target of VACM access control. Otherwise, a specified user can access all MIB objects.

SNMPv3 allows authentication and encryption of communication contents. To use these functions, specify a user name, and algorithm and password at the same time. Note that the encryption operation is not available without authentication.

Availability of authentication and encryption, algorithm, and password must match the user settings at the peer SNMP manager.

#### [Models]

RTX810, RTX5000

## 17.14 Set the Host to Allow Access Using SNMPv3

#### [Syntax]

**snmpv3 host** *host* user *user\_id* ...

**snmpv3 host** none

**no snmpv3 host** [*host*]

#### [Setting and Initial value]

- *host* : Host to allow access using SNMPv3
  - [Setting] :

Setting	Description
<i>ip_address</i>	The IP address can be a single address, two IP addresses with a hyphen in between them (range designation)
lanN	Allow access from a specified LAN interface
bridgeN	Allow access from a specified bridge interface
any	Allow access from all hosts

- [Initial value] : -
- none : Prohibit access from all hosts
  - [Initial value] : none
- *user\_id* : User number
  - [Setting] :
    - A number, two numbers with a hyphen in between them (range designation), or a list of numbers and ranges (up to 128)
  - [Initial value] : -

#### [Description]

Sets the host to allow access using SNMPv3.

If 'any' is specified for the *host* parameter, access from any host using SNMPv3 is allowed. Note that no access is allowed unless a user matches the user specified with the *user\_id* parameter even if the accessed host matches the *host* parameter.

#### [Note]

RTX810 supports IP address range, lanN, bridgeN as *HOST* parameter in Rev.11.01.23 or later.

#### [Models]

RTX810, RTX5000

## 17.15 Set the MIB View Family Managed with SNMPv3 VACM

#### [Syntax]

**snmpv3 vacm view** *view\_id* *type* *oid* [*type oid* ...]



**no snmpv3 vacm view** *view\_id*

**[Setting and Initial value]**

- *view\_id*
  - [Setting] : View number (1..65535)
  - [Initial value] : -
- *type*
  - [Setting] :

Setting	Description
include	Include the specified object ID in the management target
exclude	Exclude the specified object ID from the management target

- [Initial value] : -
- *oid*
  - [Setting] : MIB object ID (the number of sub IDs: between 2 and 128 characters in length)
  - [Initial value] : -

**[Description]**

Sets an MIP view family for management using VACM. The MIB view family is a group of variable to be specified when the access right is allowed.

A pair of the *type* parameter and the *oid* parameter means whether to include MIB sub trees under the specified object ID in the management target. Also, when specifying multiple pairs, for object IDs among individually specified ones, which have inclusive relation, the *type* parameter corresponding to the object ID specifying a lower layer is given priority. You can specify up to 128 pairs.

**[Example]**

- The internet sub-tree (1.3.6.1) and later are to be managed. However, the enterprises sub-tree (1.3.6.1.4.1) and later are excluded.

```
# snmpv3 vacm view 1 include 1.3.6.1 exclude 1.3.6.1.4.1
```

**[Models]**

RTX810, RTX5000

## 17.16 Set the Access Policy Managed with SNMPv3 VACM

**[Syntax]**

**snmpv3 vacm access** *group\_id* **read** *read\_view* **write** *write\_view*

**no snmpv3 vacm access** *group\_id*

**[Setting and Initial value]**

- *group\_id*
  - [Setting] : Group number (1..65535)
  - [Initial value] : -
- *read\_view*
  - [Setting] :

Setting	Description
<i>view_id</i>	View number to set readable access right
none	Not set a readable view

- [Initial value] : -
- *write\_view*
  - [Setting] :

Setting	Description
<i>view_id</i>	View number to set writable access right
none	Not set a writable view

- [Initial value] : -

**[Description]**

Sets an accessible MIB view family for a user group. Access to MIB variable that are not included in the MIB view family specified with this command is prohibited.

**[Models]**

RTX810, RTX5000

**17.17 Set the SNMPv3 Trap Transmission Destination**

---

**[Syntax]****snmpv3 trap host** *host* [*type*] user *user\_id***no snmpv3 trap host** *host***[Setting and Initial value]**

- *host*
  - [Setting] : IP address of the host to which SNMPv3 traps are to be sent (IPv4/IPv6)
  - [Initial value] : -
- *type* : Message type
  - [Setting] :

Setting	Description
trap	Send the trap
inform	Send the Inform request

- [Initial value] : trap
- *user\_id*
  - [Setting] : User number
  - [Initial value] : -

**[Description]**

Specifies the host to which the router sends SNMPv3 traps. Multiple hosts can be specified simultaneously by setting this command multiple times. A user setting specified with the **snmpv3 usm user** command is used for trap transmission.

If 'inform' is specified for the *type* parameter, a request is sent up to three times at 5-second interval until the destination returns response.

**[Models]**

RTX810, RTX5000

**17.18 Set the Source Address of the SNMP Transmission Packet**

---

**[Syntax]****snmp local address** *ip\_address***no snmp local address****[Setting and Initial value]**

- *ip\_address*
  - [Setting] : IP address (IPv4/IPv6)
  - [Initial value] : Automatically select from the IP addresses set to the various interfaces

**[Description]**

Sets the source IP address of the SNMP transmission packet.

**[Models]**

RTX810, RTX5000

**17.19 Set sysContact**

---

**[Syntax]****snmp syscontact** *name***no snmp syscontact****[Setting and Initial value]**

- *name*
  - [Setting] : Name to be registered as sysContact (text string of up to 255 characters)
  - [Initial value] : -

**[Description]**

Sets the MIB variable sysContact. To include spaces, enclose the entire parameter in double quotation marks or single quotation marks.

An administrator name or contact information is usually stored in sysContact.

**[Example]**

```
# snmp syscontact "RT administrator"
```

**[Models]**

RTX810, RTX5000

## 17.20 Set sysLocation

---

**[Syntax]**

**snmp syslocation** *name*

**no snmp syslocation**

**[Setting and Initial value]**

- *name*
  - [Setting] : Name to be registered as sysLocation (text string of up to 255 characters)
  - [Initial value] : -

**[Description]**

Sets the MIB variable sysLocation. To include spaces, enclose the entire parameter in double quotation marks or single quotation marks.

The installation location of the equipment is usually stored in sysLocation.

**[Example]**

```
# snmp syslocation "RT room"
```

**[Models]**

RTX810, RTX5000

## 17.21 Set sysName

---

**[Syntax]**

**snmp sysname** *name*

**no snmp sysname**

**[Setting and Initial value]**

- *name*
  - [Setting] : Name to be registered as sysName (text string of up to 255 characters)
  - [Initial value] : -

**[Description]**

Sets the MIB variable sysName. To include spaces, enclose the entire parameter in double quotation marks or single quotation marks.

The equipment name is usually stored in sysName.

**[Example]**

```
# snmp sysname "RTX810"
```

**[Models]**

RTX810, RTX5000

## 17.22 Set Whether to Send the SNMP Standard Traps

---

**[Syntax]**

**snmp trap enable snmp** *trap* [*trap...*]

**snmp trap enable snmp** all

**no snmp trap enable snmp**

**[Setting and Initial value]**

- *trap* : Standard trap type
  - [Setting] :

Setting	Description
coldstart	When all settings are initialized
warmstart	When the router is restarted
linkdown	When the link is down
linkup	When the link is up
authenticationfailure	When authentication fails

- [Initial value] : -
- all : All the standard traps are sent
  - [Initial value] : -

**[Initial value]**

snmp trap enable snmp all

**[Description]**

Sets whether to send the SNMP standard trap.

If all is specified, the router sends all the standard traps. If an individual trap is specified, the router sends only the specified trap.

**[Note]**

This command controls whether the router sends the authenticationFailure trap.

The coldStart trap is sent after startup at the time of power-on or retry of power-on, and after re-startup at the update of firmware revision.

The linkDown traps can be controlled for each interface using the **snmp trap send linkdown** command. The linkDown traps are sent on an interface only when the transmission is permitted by the **snmp trap send linkdown** command and by this command.

**[Models]**

RTX810, RTX5000

## 17.23 Set the Transmission Control of SNMP LinkDown Traps

**[Syntax]**

```
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 and Initial value]**

- *interface*
  - [Setting] :
    - LAN interface name
    - WAN interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Peer number
  - [Initial value] : -
- *tunnel\_num*
  - [Setting] : Tunnel interface number
  - [Initial value] : -
- *switch*
  - [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : on

**[Description]**

Sets whether to send linkDown traps of the specified interface.

**[Models]**

RTX810, RTX5000

## 17.24 Set Whether to Display the PP Interface Information in the MIB2 Range

---

**[Syntax]**

```
snmp yrifppdisplayatmib2 switch
no snmp yrifppdisplayatmib2
```

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	Set the MIB variable yrIfPpDisplayAtMib2 to enabled (1).
off	Set the MIB variable yrIfPpDisplayAtMib2 to enabled (2).

- [Initial value] : off

**[Description]**

Sets the value of the MIB variable yrIfPpDisplayAtMib2. This MIB variable determines whether the PP interface is displayed in the MIB2 range.

**[Models]**

RTX810, RTX5000

## 17.25 Set Whether to Display the Tunnel Interface Information in the MIB2 Range

---

**[Syntax]**

```
snmp yriftunneldisplayatmib2 switch
no snmp yriftunneldisplayatmib2
```

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	Set the MIB variable yrIfTunnelDisplayAtMib2 to enabled (1).
off	Set the MIB variable yrIfTunnelDisplayAtMib2 to enabled (2).

- [Initial value] : off

**[Description]**

Sets the value of the MIB variable yrIfTunnelDisplayAtMib2. This MIB variable determines whether the tunnel interface is displayed in the MIB2 range.

**[Models]**

RTX810, RTX5000

## 17.26 Set Whether to Display the Switch Interface Information in the MIB2 Range

---

**[Syntax]**

```
snmp yrifswitchdisplayatmib2 switch
no snmp yrifswitchdisplayatmib2
```

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	Set the MIB variable yrIfSwitchDisplayAtMib2 to enabled (1).
off	Set the MIB variable yrIfSwitchDisplayAtMib2 to enabled (2).

- [Initial value] : off

**[Description]**

Sets the value of the MIB variable `yrIfSwitchDisplayAtMib2`. This MIB variable determines whether the tunnel interface is displayed in the MIB2 range.

**[Models]**

RTX810

## 17.27 Set the Forced Display of the PP Interface Address

---

**[Syntax]**

**snmp display ipcp force** *switch*

**no snmp display ipcp force**

**[Setting and Initial value]**

- *switch*

- [Setting] :

Setting	Description
on	Always display the PP interface address as the IP address granted using IPCP
off	Not necessarily display the PP interface address as the IP address granted by IPCP

- [Initial value] : off

**[Description]**

When NAT is not used or when a fixed IP address is specified for the external NAT address, the IP address obtained using IPCP is used as the PP interface address. In this case, the normal procedure used to check the interface IP address in SNMP can be used to check the address obtained using IPCP.

However, if the external NAT address is set to `ipcp`, the IP address obtained using IPCP is used as the external NAT address and is not granted to the interface. Therefore, even if the IP address of the interface is checked using SNMP, the actual address obtained using IPCP cannot be found out.

Even when the IP address obtained using IPCP is used as the external NAT address, that address is displayed as the interface address using SNMP if this command is set to `on`. Because the address is not actually granted to the interface, it is never used as a source IP address.

**[Models]**

RTX810, RTX5000

## 17.28 Set Whether to Send a Trap When the Link of Each Port of the LAN Interface Goes Up or Down

---

**[Syntax]**

**snmp trap link-updown separate-l2switch-port** *interface switch*

**no snmp trap link-updown separate-l2switch-port** *interface*

**[Setting and Initial value]**

- *interface* : Interface (only 'lan1' is currently available)

- [Setting] :

- lan1

- [Initial value] : -

- *switch*

- [Setting] :

Setting	Description
on	Send the trap
off	Not set the trap

- [Initial value] : off

**[Description]**

Sets whether to send a trap when the link of each port goes up or down.

**[Models]**

RTX810, RTX5000

## 17.29 Set Whether to Send the Signal Strength Trap

### [Syntax]

```
snmp trap mobile signal-strength switch [level]
no snmp trap mobile signal-strength [switch [level]]
```

### [Setting and Initial value]

- *switch*
- [Setting] :

Setting	Description
on	Send the trap
off	Not set the trap

- [Initial value] : off
- *level* : Threshold for the number of antennas
- [Setting] :

Setting	Description
0..3	The number of antennas
Omitted	When omitted, outside of the range

- [Initial value] : -

### [Description]

Sets whether to send the signal strength trap of the mobile terminal. Regardless of auto/manual, trap transmission is allowed when the router obtains the signal strength. When the number of antennas for the signal strength is equal or lower than the threshold, the trap is sent.

### [Note]

The trap `yrIfMobileStatusTrap` is sent.

### [Models]

RTX810

## 17.30 Set the Interface Number Statically Added to the Switch

### [Syntax]

```
snmp ifindex switch static index index switch
no snmp ifindex switch static index index [switch]
```

### [Setting and Initial value]

- *index*
  - [Setting] : Object ID index (100000000 .. 199999999)
  - [Initial value] : -
- *switch* : Pair of MAC address or port number
  - [Initial value] : -

### [Description]

Specifies statically the top of an object ID index showing the switch interface.

### [Note]

The operation is not guaranteed when an object ID is specified repeatedly.

When the top of an object ID index is statically specified, the object ID index showing the switch interface is not allocated dynamically.

When the `snmp yrswindex switch static index` command is specified, only the switch specified with the command is allocated to the index.

### [Models]

RTX810

## 17.31 Set the Switch Number Statically Added to the Switch

### [Syntax]

```
snmp yrswindex switch static index index switch
```

**no snmp yrswindex switch static index** *index* [*switch*]

**[Setting and Initial value]**

- *index*
  - [Setting] : Object ID index (1 .. 2147483647)
  - [Initial value] : -
- *switch* : Pair of MAC address or port number
  - [Initial value] : -

**[Description]**

Specifies statically an object ID index of the switch.

**[Note]**

When specifying an object ID index statically, the object ID index of the switch is not allocated dynamically.

**[Models]**

RTX810

## 17.32 Set the Conditions of SNMP Trap According to Switch Status

---

**[Syntax]**

**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 and Initial value]**

- *switch* : default, Pair of MAC address or port number
  - [Initial value] : default
- *trap* : Trap type
  - [Setting] :

Setting	Description
linkup	When the link is up
linkdown	When the link is down
fanlock	When the fan has a failure
loopdetect	When a loop is detected

- [Initial value] : -
- all : Send all traps
  - [Initial value] : -
- none : Send no trap
  - [Initial value] : -

**[Initial value]**

snmp trap enable switch all

**[Description]**

Sets the conditions for sending traps according to monitoring status of the selected switch. When default is specified for setting, determines operation in the case where there is no SNMP trap condition for individual switch.

When all is specified, sends all traps. When none is specified, sends no trap. When specifying a trap individually, sends only the specified trap.

The linkup and linkdown traps are standard MIB traps. To send them, allow trap transmission also with the **snmp trap enable snmp** command.

To send the loopdetect trap, the **switch control function set loopdetect-linkdown linkdown** command or **switch control function set loopdetect-linkdown linkdown-recovery** command must be set at the switch side.

**[Models]**

RTX810

## 17.33 Set Conditions of Common SNMP Trap for Switches

---

**[Syntax]**

**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 and Initial value]**

- *trap* : Trap type
- [Setting] :

Setting	Description
find-switch	When monitoring of the switch starts
linkdown	When monitoring of the switch stops

- [Initial value] : -
- all : Send all traps
- [Initial value] : -
- none : Send no trap
- [Initial value] : -

**[Initial value]**

snmp trap enable switch common all

**[Description]**

Sets the conditions to send traps according to monitoring status of the switch.

**[Models]**

RTX810

## Chapter 18

### RADIUS Configuration

A RADIUS server can be used to manage the authentication and account for ISDN connections. Authentication and account management for PPTP connections is not supported.

#### 18.1 Set Whether to Use RADIUS Authentication

##### [Syntax]

```
radius auth auth
no radius auth [auth]
```

##### [Setting and Initial value]

- auth*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : off

##### [Description]

Sets whether to query the RADIUS server when the router is configured to request some kind of authentication for anonymous and the user name received from the peer (UserID if PAP and NAME if CHAP) is not included in the user name held locally (specified by the **pp auth username** command).

##### [Note]

The RADIUS authentication and RADIUS account can be used independently.  
For supported attributes, refer to the document <<http://www.yamaha.com/products/en/network/>> in our WWW site.

##### [Models]

RTX810, RTX5000

#### 18.2 Set Whether to Use RADIUS Account

##### [Syntax]

```
radius account account
no radius account [account]
```

##### [Setting and Initial value]

- account*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : off

##### [Description]

Sets whether to use the RADIUS account.

##### [Note]

The RADIUS authentication and RADIUS account can be used independently.  
For supported attributes, refer to the document <<http://www.yamaha.com/products/en/network/>> in our WWW site.

##### [Models]

RTX810, RTX5000

#### 18.3 Set the RADIUS Server

**[Syntax]**

```
radius server ip1 [ip2]
no radius server [ip1 [ip2]]
```

**[Setting and Initial value]**

- *ip1*
  - [Setting] : IP address of the RADIUS server (primary) (IPv6 addresses allowed)
  - [Initial value] : -
- *ip2*
  - [Setting] : IP address of the RADIUS server (secondary) (IPv6 addresses allowed)
  - [Initial value] : -

**[Description]**

Sets the RADIUS server. Up to two servers can be specified. If a response cannot be received from the primary server, the router queries the secondary server.

**[Note]**

There are two functions in RADIUS, authentication and account. Each server can be set independently using the **radius auth server** and **radius account server** commands. The setting by the **radius server** command is valid when the individual settings are not specified and is used for both authentication and account.

**[Models]**

RTX810, RTX5000

## 18.4 Set the RADIUS Authentication Server

---

**[Syntax]**

```
radius auth server ip1 [ip2]
no radius auth server [ip1 [ip2]]
```

**[Setting and Initial value]**

- *ip1*
  - [Setting] : IP address of the RADIUS authentication server (primary) (IPv6 addresses allowed)
  - [Initial value] : -
- *ip2*
  - [Setting] : IP address of the RADIUS authentication server (secondary) (IPv6 addresses allowed)
  - [Initial value] : -

**[Description]**

Sets the RADIUS authentication server. Up to two servers can be specified. If a response cannot be received from the primary server, the router queries the secondary server.

**[Note]**

If the IP address of the RADIUS authentication server is not specified by this command, the IP address specified by the **radius server** command is used as the authentication server.

**[Models]**

RTX810, RTX5000

## 18.5 Set the RADIUS Account Server

---

**[Syntax]**

```
radius account server ip1 [ip2]
no radius account server [ip1 [ip2]]
```

**[Setting and Initial value]**

- *ip1*
  - [Setting] : IP address of the RADIUS account server (primary) (IPv6 addresses allowed)
  - [Initial value] : -
- *ip2*
  - [Setting] : IP address of the RADIUS account server (secondary) (IPv6 addresses allowed)
  - [Initial value] : -

**[Description]**

Sets the RADIUS account server. Up to two servers can be specified. If a response cannot be received from the primary server, the router queries the secondary server.

**[Note]**

If the IP address of the RADIUS account server is not specified by this command, the IP address specified by the **radius server** command is used as the account server.

**[Models]**

RTX810, RTX5000

## 18.6 Set the UDP Port of the RADIUS Authentication Server

---

**[Syntax]**

```
radius auth port port_num
no radius auth port [port_num]
```

**[Setting and Initial value]**

- *port\_num*
  - [Setting] : UDP port number
  - [Initial value] : 1645

**[Description]**

Sets the UDP port number of the RADIUS authentication server.

**[Note]**

RFC2138 specifies that 1812 is used for the port number. [Initial

**[Models]**

RTX810, RTX5000

## 18.7 Set the UDP Port of the RADIUS Account Server

---

**[Syntax]**

```
radius account port port_num
no radius account port [port_num]
```

**[Setting and Initial value]**

- *port\_num*
  - [Setting] : UDP port number
  - [Initial value] : 1646

**[Description]**

Sets the UDP port number of the RADIUS account server.

**[Note]**

RFC2138 specifies that 1813 is used for the port number.

**[Models]**

RTX810, RTX5000

## 18.8 Set the RADIUS Secret Key

---

**[Syntax]**

```
radius secret secret
no radius secret [secret]
```

**[Setting and Initial value]**

- *secret*
  - [Setting] : Secret text string (up to 16 characters)
  - [Initial value] : -

**[Description]**

Sets the RADIUS secret key.

**[Models]**

RTX810, RTX5000

## 18.9 Set the RADIUS Retry Parameter

---

**[Syntax]**

```
radius retry count time
no radius retry [count time]
```

**[Setting and Initial value]**

- *count*
  - [Setting] : Retry count (1..10)
  - [Initial value] : 4
- *time*
  - [Setting] : Milliseconds (20..10000)
  - [Initial value] : 3000

**[Description]**

Sets the retry count and the time interval of RADIUS packets.

**[Models]**

RTX810, RTX5000

## Chapter 19

### NAT Function

The NAT function enables IP networks of different address systems to connect by converting the source and destination IP addresses or the TCP/UDP port number of IP packets that the router transfers.

The NAT function enables data to be transferred between a private address space and the global address space or assign multiple hosts to a single global IP address.

On Yamaha router, NAT refers to the conversion of only the source and destination IP addresses. Those that entail conversion of TCP/UDP port numbers are called IP masquerade.

A description that expresses the address conversion rules is called a NAT descriptor. Each NAT descriptor defines the target address space in which addresses are to be converted. The **nat descriptor address inner** and **nat descriptor address outer** commands are used for the address space description. The former defines the inner address space of the NAT process, and the latter defines the outer address space of the NAT process. By setting these two commands in pairs, the mapping of the address before the conversion to the address after the conversion is essentially defined.

The NAT descriptor is applied to an interface. The inner address space of the NAT process is from the interface to which the NAT descriptor is applied to the external network connected to another interface via the router.

A NAT descriptor has an operation type property. When using functions such as IP masquerade and dynamic address assignment, the corresponding operation type must be selected.

#### 19.1 Apply the NAT Descriptor to the Interface

##### [Syntax]

```
ip interface nat descriptor nat_descriptor_list [reverse nat_descriptor_list]
ip pp nat descriptor nat_descriptor_list [reverse nat_descriptor_list]
ip tunnel 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 tunnel nat descriptor [nat_descriptor_list [reverse nat_descriptor_list]]
```

##### [Setting and Initial value]

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *nat\_descriptor\_list*
  - [Setting] : Sequence of NAT descriptor numbers (1..2147483647) delimited by spaces (up to 16 numbers)
  - [Initial value] : -

##### [Description]

Carries out the NAT conversions as defined by the NAT descriptors in the order specified in the list for packets that pass the interface to which this command is applied.

NAT conversion is performed on the IP address and port number that are opposite to those that are normally processed for the NAT descriptor written after reverse.

##### [Note]

For LAN addresses outside of the NAT descriptor, the router returns an ARP response to an ARP request coming from the same LAN.

RTX5000 does not support WAN interface for *interface* parameter.

##### [Models]

RTX810, RTX5000

#### 19.2 Set the Operation Type of the NAT Descriptor

##### [Syntax]

```
nat descriptor type nat_descriptor type
no nat descriptor type nat_descriptor [type]
```

##### [Setting and Initial value]

- *nat\_descriptor*
  - [Setting] : NAT descriptor number (1..2147483647)

- [Initial value] : -
- *type*
- [Setting] :

Setting	Description
none	Not use the NAT conversion function
nat	Use dynamic NAT conversion and static NAT conversion
masquerade	Use static NAT conversion and IP masquerade conversion
nat-masquerade	Use dynamic NAT conversion, static NAT conversion, and IP masquerade conversion

- [Initial value] : none

#### [Description]

Specifies the operation type of NAT conversion.

#### [Note]

If nat-masquerade is specified, the router rescues packets that could not be converted through dynamic NAT conversion using the IP masquerade conversion. For example, if 16 outer addresses are available, the first 15 is converted through NAT conversion, and the rest is converted through IP masquerade conversion.

#### [Models]

RTX810, RTX5000

## 19.3 Set the Outer IP Address of the NAT Process

#### [Syntax]

```
nat descriptor address outer nat_descriptor outer_ipaddress_list
no nat descriptor address outer nat_descriptor [outer_ipaddress_list]
```

#### [Setting and Initial value]

- *nat\_descriptor*
  - [Setting] : NAT descriptor number (1..2147483647)
  - [Initial value] : -
- *outer\_ipaddress\_list* : List of outer NAT IP address ranges or mnemonic
  - [Setting] :

Setting	Description
IP address	An IP address, two IP addresses with a hyphen in between them (range designation), or a list containing these addresses
ipcp	IP address that is notified from the connected peer by the IP-Address option of IPCP of PPP.
primary	IP address specified by the <b>ip interface address</b> command
secondary	IP address specified by the <b>ip interface secondary address</b> command

- [Initial value] : ipcp

#### [Description]

Specifies the range of outer IP addresses to which the dynamic NAT process applies. In IP masquerade, the first outer IP address is used.

#### [Note]

A mnemonic cannot be placed in a list.

The parameters that can be used vary depending on the applied interface.

Applied Interface	LAN	PP	Tunnel
ipcp	×	○	×
primary	○	×	×
secondary	○	×	×
IP address	○	○	○

**[Models]**

RTX810, RTX5000

## 19.4 Set the Inner IP Address of the NAT Process

---

**[Syntax]**

```

nat descriptor address inner nat_descriptor inner_ipaddress_list
no nat descriptor address inner nat_descriptor [inner_ipaddress_list]

```

**[Setting and Initial value]**

- *nat\_descriptor*
  - [Setting] : NAT descriptor number (1..2147483647)
  - [Initial value] : -
- *inner\_ipaddress\_list* : listList of inner NAT IP address ranges or mnemonic
  - [Setting] :

Setting	Description
IP address	An IP address, two IP addresses with a hyphen in between them (range designation), or a list containing these addresses
auto	All

- [Initial value] : auto

**[Description]**

Specifies the range of inner IP addresses to which the NAT and IP masquerade processes apply.

**[Models]**

RTX810, RTX5000

## 19.5 Set a Static NAT Entry

---

**[Syntax]**

```

nat descriptor static nat_descriptor id outer_ip=inner_ip [count]
no nat descriptor static nat_descriptor id [outer_ip=inner_ip [count]]

```

**[Setting and Initial value]**

- *nat\_descriptor*
  - [Setting] : NAT descriptor number (1..2147483647)
  - [Initial value] : -
- *id*
  - [Setting] : Static NAT entry ID (1..2147483647)
  - [Initial value] : -
- *outer\_ip*
  - [Setting] : Outer IP address (1 address)
  - [Initial value] : -
- *inner\_ip*
  - [Setting] : Inner IP address (1 address)
  - [Initial value] : -
- *count*
  - [Setting] :
    - Number of consecutive addresses to be specified
    - 1 when omitted
  - [Initial value] : -
- *netmask*
  - [Setting] :
    - xxx.xxx.xxx.xxx where xxx is a decimal number
    - Hexadecimal number following 0x
    - Number of mask bits (16..32)
  - [Initial value] : -

**[Description]**

Specifies the combinations of IP addresses to be statically assigned by the NAT conversion. If the count is specified, this command is applied to a range of consecutive IP addresses from the specified address.



**[Note]**

Specifies the combinations of IP addresses to be statically assigned by the NAT conversion. If the count is specified, this command is applied to a range of consecutive IP addresses from the specified address.

The outer address does not have to be an address that is specified as an address to which the NAT process is to be applied.

If you are only using static NAT, you must pay attention to the settings of the **nat descriptor address outer** and **nat descriptor address inner** commands. The initial values for these commands are ipcp and auto, respectively. Therefore, for example, you can specify some IP address as a dummy to prevent the NAT from operating dynamically.

**[Models]**

RTX810, RTX5000

## 19.6 Set Whether to Use rlogin, rcp, and ssh When Using IP Masquerade

**[Syntax]**

```
nat descriptor masquerade rlogin nat_descriptor use
no nat descriptor masquerade rlogin nat_descriptor [use]
```

**[Setting and Initial value]**

- *nat\_descriptor*
  - [Setting] : NAT descriptor number (1..2147483647)
  - [Initial value] : -
- *use*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : off

**[Description]**

Sets whether to allow the use of rlogin, rcp, and ssh when using IP masquerade.

**[Note]**

If on is specified, the port number is not converted for the rlogin, rcp, and ssh traffic. In addition, rsh cannot be used if on is specified.

**[Models]**

RTX810, RTX5000

## 19.7 Set the Static IP Masquerade Entry

**[Syntax]**

```
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 and Initial value]**

- *nat\_descriptor*
  - [Setting] : NAT descriptor number (1..2147483647)
  - [Initial value] : -
- *id*
  - [Setting] : Static IP masquerade entry ID (a value greater than equal to 1)
  - [Initial value] : -
- *inner\_ip*
  - [Setting] : Inner IP address (1 address)
  - [Initial value] : -
- *protocol*
  - [Setting] :

Setting	Description
esp	ESP

Setting	Description
tcp	TCP protocol
udp	UDP protocol
icmp	ICMP protocol
Protocol number	Protocol numbers assigned by IANA

- [Initial value] : -
- *outer\_port*
  - [Setting] : Outer port number to fix (mnemonic)
  - [Initial value] : -
- *inner\_port*
  - [Setting] : Inner port number to fix (mnemonic)
  - [Initial value] : -

**[Description]**

Fix the port so that the port number is not converted in communications using IP masquerade.

**[Note]**

If the *outer\_port* and *inner\_port* are specified, the port number of packets from the outside of the interface to the inside is converted from *outer\_port* to *inner\_port* when the IP masquerade is applied. Likewise, the port number of packets from the inside of the port to the outside is converted from *inner\_port* to *outer\_port*.

If only the *inner\_port* parameter is specified, the port number is not converted.

**[Models]**

RTX810, RTX5000

## 19.8 Set the Timer for Clearing the NAT IP Address Map

---

**[Syntax]**

```

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 and Initial value]**

- *nat\_descriptor*
  - [Setting] : NAT descriptor number (1..2147483647)
  - [Initial value] : -
- *time*
  - [Setting] : Timeout value in seconds (30..21474836)
  - [Initial value] : 900
- *time2*
  - [Setting] : Timeout value in seconds after passing through TCP/FIN (1-21474836)
  - [Initial value] : 60
- *protocol*
  - [Setting] : Protocol
  - [Initial value] : -
- *port\_range*
  - [Setting] : Range of port numbers. Valid only when the protocol is TCP or UDP
  - [Initial value] : -

**[Description]**

Sets the NAT timer for holding the session information of NAT or IP masquerade. For IP masquerade, NAT timers can also be set for each protocol or port number. For protocols that are not specified, the NAT timer value specified in the first syntax is used.

For IP masquerade, NAT timers can be set for sessions that pass through TCP/FIN. Sessions that pass through TCP/FIN will be terminated, so you can use TCP/FIN timeout timers to reduce the size of NAT tables.

**[Models]**

RTX810, RTX5000

## 19.9 Set the Action Taken When a Conversion Table Corresponding to the Packet Received from the Outside Does Not Exist

**[Syntax]**

```
nat descriptor masquerade incoming nat_descriptor action [ip_address]
no nat descriptor masquerade incoming nat_descriptor
```

**[Setting and Initial value]**

- *nat\_descriptor*
  - [Setting] : NAT descriptor number (1..2147483647)
  - [Initial value] : -
- *action*
  - [Setting] :

Setting	Description
through	Pass the packet without conversion
reject	Discard and return RST in the case of TCP
discard	Discard and return nothing
forward	Forward the packet to the specified host

- [Initial value] : reject
- *ip\_address*
  - [Setting] : Forward destination IP address
  - [Initial value] : -

**[Description]**

Sets the action that the router takes when a conversion table corresponding to the packet received from the outside does not exist in IP masquerade. If *action* is set to forward, you must set the *ip\_address*.

**[Models]**

RTX810, RTX5000

## 19.10 Set the Range of Ports Used for IP Masquerade

**[Syntax]**

```
nat descriptor masquerade port range nat_descriptor port_range1 [port_range2]
no nat descriptor masquerade port range nat_descriptor [port_range1 [port_range2]]
```

**[Setting and Initial value]**

- *nat\_descriptor*
  - [Setting] : NAT descriptor number (1..2147483647)
  - [Initial value] : -
- *port\_range1, port\_range2*
  - [Setting] : Range of port numbers indicated by two port numbers with a hyphen between them
  - [Initial value] :

According to the maximum number of usable port for IP masquerade, the range of port is as follows:

- 4096 : port\_range1=60000-64095
- 10000 : port\_range1=60000-64095, port\_range2=54095-59999
- 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

**[Description]**

Sets the range of port numbers used for IP masquerade.

Port numbers in the *port\_range1* range are used first. When all the port numbers in *port\_range1* have been used, the port numbers in the *port\_range2* range start to be used. By starting with *port\_range1* and using up to *port\_rangeN*, port numbers are used from the range with smallest number to the largest.

For models that can handle 65534 simultaneous NAT sessions, the initial setting allows for 64511 ports to be used (with the exception of the well-known ports). To use 65534 ports, the following commands must be used to expand the port range.

**[Note]**

Maximum number of usable port for IP masquerade and number of usable port ranges is shown below for each model.

Model	Maximum number of usable port for IP masquerade	Number of port ranges
RTX5000	65534	4
RTX810	10000	2

**[Models]**

RTX810, RTX5000

## 19.11 Set the Port Number Identified as FTP

---

**[Syntax]**

```
nat descriptor ftp port nat_descriptor port [port...]
no nat descriptor ftp port nat_descriptor [port...]
```

**[Setting and Initial value]**

- *nat\_descriptor*
  - [Setting] : NAT descriptor number (1..2147483647)
  - [Initial value] : -
- *port*
  - [Setting] : Port number (1..65535)
  - [Initial value] : 21

**[Description]**

The router processes the NAT by assuming that the port number specified by this command corresponds to communications on the FTP control channel for all TCP packets that the router processes.

**[Models]**

RTX810, RTX5000

## 19.12 Set the Range of Ports Not Converted by IP Masquerade

---

**[Syntax]**

```
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 and Initial value]**

- *nat\_descriptor*
  - [Setting] : NAT descriptor number (1..2147483647)
  - [Initial value] : -
- *protocol*
  - [Setting] :

Setting	Description
tcp	TCP
udp	UDP

- [Initial value] : -
- *port*
  - [Setting] : Range of port numbers
  - [Initial value] : -

**[Description]**

Sets the range of port numbers that are not converted by IP masquerade.

If if-possible is specified and the port number to be processed is not used by another communication, the value is used as-is without conversion.

**[Models]**

RTX810, RTX5000

## 19.13 Set Whether to Log NAT Address Assignments

### [Syntax]

```
nat descriptor log switch
no nat descriptor log
```

### [Setting and Initial value]

- *switch*
  - [Setting] :

Setting	Description
on	Log
off	Not log

- [Initial value] : off

### [Description]

Sets whether to log NAT address assignments.

### [Models]

RTX810, RTX5000

## 19.14 Set Whether to Overwrite the IP Address Included in SIP Messages

### [Syntax]

```
nat descriptor sip nat_descriptor sip
no nat descriptor sip nat_descriptor
```

### [Setting and Initial value]

- *nat\_descriptor*
  - [Setting] : NAT descriptor number (1..2147483647)
  - [Initial value] : -
- *sip*
  - [Setting] :

Setting	Description
on	Convert
off	Not convert
auto	Determined by the <b>sip use</b> command setting value

- [Initial value] :
  - auto

### [Description]

Sets whether to overwrite the IP address included in SIP messages using static NAT or static IP masquerade.

### [Models]

RTX810, RTX5000

## 19.15 Set Whether to Remove the DF Bit during IP Masquerade Conversion

### [Syntax]

```
nat descriptor masquerade remove df-bit remove
no nat descriptor masquerade remove df-bit [remove]
```

### [Setting and Initial value]

- *remove*
  - [Setting] :

Setting	Description
on	Remove the DF bit during IP masquerade conversion
off	Not remove the DF bit during IP masquerade conversion

- [Initial value] : on

**[Description]**

Sets whether to remove the DF bit during IP masquerade conversion.

The DF bit is used for path MTU recovery, but to do so ICMP error in response to packets that are too long must be returned correctly to the sender. However, because the IP masquerade overwrites the IP address and related information, ICMP errors may to be returned correctly to the sender. If this happens, the packet cannot be sent indefinitely. A condition in which the ICMP error for path MTU discovery does not reach the sender such as in this case is called a path MTU discovery black hole.

This path MTU discovery black hole can be avoided if the DF bit is removed during IP masquerade conversion. In return, however, because path MTU discovery is not carried out, communication efficiency may degrade.

**[Note]**

The fast path procedure saves the information of a packet that is passed once using the normal path procedure and transfers the same type of packets at high speeds. For example, if the **ping** command is executed the first time, normal path procedure is used. For subsequent commands, fast path procedure is used. This resulted in the DF bit being deleted the first time and not for the subsequent times.

**[Models]**

RTX810, RTX5000

## 19.16 Set the Number of Sessions for every Host Converted by IP Masquerade

---

**[Syntax]**

```
nat descriptor masquerade session limit nat_descriptor id limit
no nat descriptor masquerade session limit nat_descriptor id
```

**[Setting and Initial value]**

- *nat\_descriptor*
  - [Setting] : NAT descriptor number (1..2147483647)
  - [Initial value] : -
- *id*
  - [Setting] : ID for session number configuration (1)
  - [Initial value] : -
- *limit*
  - [Setting] :
    - Limit (1..65534)(RTX5000)
    - Limit (1..10000)(RTX810)
  - [Initial value] :
    - 65534(RTX5000)
    - 10000(RTX810)

**[Description]**

Sets the maximum number of sessions to convert with IP masquerade for a specific host.

The host is identified by the source IP address of the packet. The number of times the specified host can be registered in the conversion table is limited to the value specified for *limit*.

**[Models]**

RTX810, RTX5000

## Chapter 20

### DNS Configuration

The router DNS (Domain Name Service) functions are name resolution, the recursive server function, the upper DNS server selection function, and the simple DNS server function (static DNS record registration).

The name resolution function enables the name to be specified in place of the IP address parameter in commands such as **ping**, **traceroute**, **rdate**, **ntpdate**, and **telnet** and resolves IP addresses to names in display functions such as SYSLOG.

The recursive server function relays DNS packets by residing between the DNS server and the client. The DNS query packet that the router receives from the client is relayed to the DNS server specified by commands such as the **dns server** command. The response from the DNS server is received by the router, and the router transfers it back to the client. The router has a cache for the number of entries specified by the **dns cache max entry** command (initial value=256). For data in the cache, the router returns the response without querying the DNS server, thereby reducing the DNS traffic. The cache is held only for the time specified in the data when it is received from the DNS server.

To use the DNS function, the **dns server** command must be specified. This setting is also applied to the configuration information sent to the DHCP client by the DHCP server function.

#### 20.1 Set Whether to Use the DNS

##### [Syntax]

```
dns service service
no dns service [service]
```

##### [Setting and Initial value]

- service*
- [Setting] :

Setting	Description
recursive	Operate as a DNS recursive server
off	Stop the services

- [Initial value] : recursive

##### [Description]

Sets whether the router operates as a DNS recursive server. If off is specified, all DNS functions are disabled. In addition, port 53/udp is also closed.

##### [Models]

RTX810, RTX5000

#### 20.2 Set the IP Address of the DNS Server

##### [Syntax]

```
dns server ip_address [ip_address...]
no dns server [ip_address...]
```

##### [Setting and Initial value]

- ip\_address*
- [Setting] : IP address of the DNS server (up to four locations can be specified, delimiting each location with a space)
- [Initial value] : -

##### [Description]

Specifies the IP address of the DNS server.

This IP address is also used when the router operating as a DHCP server reports the IP address to the DHCP client and when the router reports the IP address to the peer using the MS extension option of IPCP.

If other commands have configured the DNS server, the configuration from the command with the highest priority will be used. For the priority of the commands that can configure the DNS server, refer to the explanation at the beginning of this chapter.

##### [Models]

RTX810, RTX5000

#### 20.3 Set the DNS Domain Name

**[Syntax]**

**dns domain** *domain\_name*  
**no dns domain** [*domain\_name*]

**[Setting and Initial value]**

- *domain\_name*
  - [Setting] : Text string representing the DNS domain
  - [Initial value] : -

**[Description]**

Sets the DNS domain to which the router belongs.

If name resolution fails when the host functions of the router (ping and traceroute) are used, resolution is attempted again through the complementing of this domain name. If the router is to function as a DHCP server, the specified domain name is also used to notify the DHCP client. The domain is reported to the DHCP clients in the same network as the router and its sub networks.

To specify an empty text string, enter the command as **dns domain**.

**[Models]**

RTX810, RTX5000

## 20.4 Set the Peer Number from Which the DNS Server Is to Be Notified

---

**[Syntax]**

**dns server pp** *peer\_num*  
**no dns server pp** [*peer\_num*]

**[Setting and Initial value]**

- *peer\_num*
  - [Setting] : Peer number from which the DNS server is to be notified
  - [Initial value] : -

**[Description]**

Sets the peer number from which the DNS server is to be notified. If a peer number is specified by this command, the router first calls this peer before carrying out DNS name resolution, and queries the DNS server that is notified by the IPCP MS extension function of PPP.

If the router cannot connect to the peer or if the DNS server is not notified even when the connection is successful, name resolution is not carried out.

If other commands have configured the DNS server, the configuration from the command with the highest priority will be used. For the priority of the commands that can configure the DNS server, refer to the explanation at the beginning of this chapter.

**[Note]**

To use this function, the **ppp ipcp msextn** on setting is required in the peer information specified by the **dns server pp** command.

**[Example]**

```
# pp select 2
pp2# ppp ipcp msextn on
pp2# dns server pp 2
```

**[Models]**

RTX810, RTX5000

## 20.5 Set the Order in Which the DNS Servers Are Notified in the DHCP/IPCP MS Extension

---

**[Syntax]**

**dns notice order** *protocol server* [*server*]  
**no dns notice order** *protocol* [*server* [*server*]]

**[Setting and Initial value]**

- *protocol*
  - [Setting] :



Setting	Description
dhcp	Notification using DHCP
msex	Notification using IPCP MS extension

- [Initial value] : dhcp and msex
- *server*
- [Setting] :

Setting	Description
none	Never notified
me	The router itself
server	Group of servers specified by the <b>dns server</b> command

- [Initial value] : me server

#### [Description]

Multiple DNS servers can be notified in the DHCP and IPCP MS extension. This command specifies the order in which the DNS servers are notified.

If none is specified, the router does not notify the DNS server regardless of the other settings. The me keyword notifies the router's own IP address indicating that the router's DNS recursive server function is to be used. If *server* is specified, the group of servers specified by the **dns server** command is notified. In IPCP MS extension, the maximum number of servers that can be notified is limited to two. Therefore, if the me keyword is appended, the first DNS server and the router itself are notified. If *server* is specified by itself, the first two DNS servers are notified.

#### [Models]

RTX810, RTX5000

## 20.6 Set Whether to Process Queries Directed at a Private Address

#### [Syntax]

```
dns private address spoof spoof
no dns private address spoof [spoof]
```

#### [Setting and Initial value]

- *spoof*
- [Setting] :

Setting	Description
on	Process
off	Not process

- [Initial value] : off

#### [Description]

If on is specified, the router DNS server function does not transfer the queries for PTR records of private addresses to the upper server. Instead, the function returns an “NXDomain” error indicating that no such record exists.

#### [Models]

RTX810, RTX5000

## 20.7 Set Whether to Resolve Names Using DNS on the SYSLOG Display

#### [Syntax]

```
dns syslog resolv resolv
no dns syslog resolv [resolv]
```

#### [Setting and Initial value]

- *resolv*
- [Setting] :

Setting	Description
on	Resolve

Setting	Description
off	Not resolve

- [Initial value] : off

#### [Description]

Sets whether to resolve names using DNS on the SYSLOG display.

#### [Models]

RTX810, RTX5000

## 20.8 Select the DNS Server According to the Contents of the DNS Query

#### [Syntax]

**dns server select** *id server* [*server2*] [*type*] *query* [*original-sender*] [*restrict pp connection-pp*]

**dns server select** *id pp peer\_num* [*default-server*] [*type*] *query* [*original-sender*] [*restrict pp connection-pp*]

**dns server select** *id dhcp interface* [*default-server*] [*type*] *query* [*original-sender*] [*restrict pp connection-pp*]

**dns server select** *id reject* [*type*] *query* [*original-sender*]

**no dns server select** *id*

#### [Setting and Initial value]

- *id*
  - [Setting] : DNS server selection table number
  - [Initial value] : -
- *server*
  - [Setting] : Primary DNS server IP address
  - [Initial value] : -
- *server2*
  - [Setting] : Secondary DNS server IP address
  - [Initial value] : -
- *type* : DNS record type
  - [Setting] :

Setting	Description
a	Host IP address
aaaa	Host IPv6 address
ptr	Reverse IP address lookup pointer
mx	Mail server
ns	Name server
cname	Alias
any	Matches all types
Omitted	a when omitted

- [Initial value] : -
- *query* : Contents of the DNS query
  - [Setting] :

Setting	Description
When the <i>type</i> is a, aaaa, mx, ns, or cname	The <i>query</i> parameter represents the domain name and used for backward match. For example, if “yamaha.co.jp” is specified, rtp.yamaha.co.jp is a match. If “.” is specified, all domain names match.
When <i>type</i> is ptr	The <i>query</i> parameter represents the IP address ( <i>ip_address[/masklen]</i> ). If <i>masklen</i> is omitted, only the IP address is matched. If <i>masklen</i> is specified, all IP addresses included in the network address are matched. The FQDN written in the .in-addr.arpa domain that is included in the DNS query is converted to an IP address and then compared. There is no setting that matches with all IP addresses.

Setting	Description
When the reject keyword is specified	The <i>query</i> parameter represents a perfect match. You can use an asterisk to search for addresses that match a string at the beginning or end. In other words, if you search for matches at the beginning by specifying “NetVolante.*”, the query will return NetVolante.jp, NetVolante.rtrpro.yamaha.co.jp, etc., as matches. You can also search for matches at the end by specifying “*yamaha.co.jp”.

- [Initial value] : -
- *original-sender*
  - [Setting] : IP address range of the sender of the DNS query
  - [Initial value] : -
- *connection-pp*
  - [Setting] : Connection peer number for checking the connection status when selecting a DNS server
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Connection peer number when using the DNS server notified from the peer using IPCP
  - [Initial value] : -
- *interface*
  - [Setting] : LAN interface name when using the DNS server obtained by the DHCP server
  - [Initial value] : -
- *default-server*
  - [Setting] : IP address of the DNS server that is used when the DNS server cannot be obtained from the connection peer specified by the *peer\_num* parameter.
  - [Initial value] : -

#### [Description]

If other commands have configured the DNS server, the configuration from the command with the highest priority will be used. For the priority of the commands that can configure the DNS server, refer to the explanation at the beginning of this chapter.

If the syntax using the reject keyword is specified and *query* matches, that DNS query packet is discarded, and the DNS query is not resolved.

If the restrict pp section is specified, whether the peer specified by *connection-pp* is up is added to the conditions for selecting the server. If the peer is down, it is not selected. If the peer is up and other conditions match, the specified server is selected.

#### [Note]

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

RTX5000 does not support WAN interface for *interface* parameter.

#### [Models]

RTX810, RTX5000

## 20.9 Register the Static DNS Record

#### [Syntax]

**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 and Initial value]

- *type* : Name type
- [Setting] :

Setting	Description
a	IPv4 address of the host
aaaa	IPv6 address of the host
ptr	Reverse IP address lookup pointer
mx	Mail server
ns	Name server

Setting	Description
cname	Alias

- [Initial value] : -
- *name, value*
- [Setting] :

The meaning varies depending on the *type* parameter as follows:

<i>type</i> parameter	<i>name</i>	<i>value</i>
a	FQDN	IPv4 address
aaaa	FQDN	IPv6 address
ptr	IPv4 address	FQDN
mx	FQDN	FQDN
ns	FQDN	FQDN
cname	FQDN	FQDN

- [Initial value] : -
- *fqdn*
  - [Setting] : Host name including the domain name
  - [Initial value] : -
- *ttl*
  - [Setting] : Number of seconds (1 to 4294967295)
  - [Initial value] : -

#### [Description]

Defines a static DNS record.

The **ip host** command is a simplified version of the **dns static** command that requires both a and ptr to be specified.

#### [Note]

The DNS record that is returned in response to the query has the following characteristics.

- The TTL field is set to the value specified for the *ttl* parameter. When the *ttl* parameter is omitted, the TTL field is set to 1.
- Only one DNS record (the answer) is set in the Answer section, and the DNS record is not set in the Authority/Additional section.
- The preference field of the MX record is set to 0.

#### [Example]

```
# ip host pc1.rupro.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
```

#### [Models]

RTX810, RTX5000

## 20.10 Set the Source Port Number of the DNS Query Packet

#### [Syntax]

```
dns srcport port[port]
no dns srcport [port-port]
```

#### [Setting and Initial value]

- *port*
  - [Setting] : Port number (1..65535)
  - [Initial value] :
    - 10000-10999

#### [Description]

Sets the source port number of the DNS query packet that the router sends.

If only one port number is set, the specified port is used as the source port.

If a range of ports is set, the router randomly selects a port from within the range when it sends a DNS query packet.

**[Note]**

When handling DNS query packets with a filter, it is necessary to keep in mind that the source port number will change randomly.

**[Models]**

RTX810, RTX5000

## 20.11 Set the IP Address of the Host Allowed to Access the DNS Server

---

**[Syntax]**

```
dns host ip_range [ip_range [...]]
no dns host
```

**[Setting and Initial value]**

- *ip\_range* : The setting is applied to subsequent DNS connections after the change.
  - [Setting] :

Setting	Description
IP address	An IP address, two IP addresses with a hyphen in between them (range designation), or a list containing these addresses
any	Allow access from all hosts
lan	Allow hosts in all the networks of the LAN port
lanN	Allow hosts in a specific network of the LAN port (N is the interface number)
none	Prohibit access from all hosts

- [Initial value] : any

**[Description]**

Sets the hosts to allow access to the DNS server.

**[Note]**

If the LAN interface is specified by this command, access from IP addresses excluding the network address and limited broadcast address are allowed. If neither the primary or secondary address is set on the specified LAN interface, access is not allowed.

**[Models]**

RTX810, RTX5000

## 20.12 Set Whether to Use DNS Cache

---

**[Syntax]**

```
dns cache use switch
no dns cache use [switch]
```

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Use DNS cache
off	Do not use DNS cache

- [Initial value] : on

**[Description]**

Sets whether to use the DNS cache.

Set *switch* to on to use the DNS cache. After sending a DNS query packet, the router stores the response from the upper DNS server in internal memory, and the next time it has the same query, it uses the stored response instead of querying the server again.

If the response from the upper DNS server contains multiple RR records, the length of time for which these records are stored in the cache is determined by the length of the shortest TTL. If there are no RR records in the response, the response is stored in the cache for 60 seconds.

The number of DNS entries that can be stored in the router is determined by the **dns cache max entry** command.

If you set `switch` to off, the DNS cache is not used. The router does not store responses to DNS query packets from the upper DNS server in internal memory. Even if the router has the same query, it will always query the DNS server.

**[Models]**

RTX810, RTX5000

## 20.13 Set the Maximum Number of DNS Cache Entries

---

**[Syntax]**

**dns cache max entry** *num*

**no dns cache max entry** [*num*]

**[Setting and Initial value]**

- *num*
  - [Setting] : Maximum number of entries (1...1024)
  - [Initial value] : 256

**[Description]**

Sets the maximum number of DNS cache entries.

This setting determines the number of responses from the upper DNS server that can be stored in the router's internal DNS cache. If the specified number of responses is exceeded, older responses are discarded in the order that they were received. If the response from the upper DNS server contains multiple RR records, the length of time for which these records are stored in the cache is determined by the length of the shortest TTL. If there are no RR records in the response, the response is stored in the cache for 60 seconds. When the time from when a response was received to the present exceeds the storage time, the entry for the response is deleted from the DNS cache.

**[Models]**

RTX810, RTX5000

## 20.14 Set Whether to Unify the DNS Fallback Operations of the Router

---

**[Syntax]**

**dns service fallback** *switch*

**no dns service fallback** [*switch*]

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Unify the DNS fallback operations to give preference to IPv6
off	The DNS fallback operations vary according to model

- [Initial value] : off

**[Description]**

Sets whether to unify the DNS fallback operations of all functions of the router.

To change a host name to an IP address, the router asks which one to take, IPv4 or IPv6, to the DNS server in advance, and if it cannot solve the address, it asks another address. This operation is called DNS fallback. Previously, when the router itself made a query, IPv4 was selected first for some functions, and IPv6 was selected first for other functions. In precise, the following functions prefer IPv6 for the DNS fallback operations, and the other functions prefer IPv4:

- HTTP revision update function
- HTTP upload function

When setting this command on, all functions of the router prefer IPv6.

**[Note]**

As a DNS recursive server, when the router transfers queries from PCs in the LAN to the upper DNS server, it transfers the queries from the PCs directly to the upper server. Therefore, actually equipped functions on the PCs are directly applied to the DNS fallback operations, and this command setting is not affected.

**[Models]**

RTX810, RTX5000

## Chapter 21

### Priority Control and Bandwidth Control

The priority control and bandwidth control functions reorder the packets input through the interface and output them to another interface. If these functions are not used, the packets are processed in the order that they are received.

The priority control assigns priorities to the classified queues, outputs the queue of the highest priority first, and then outputs the packets in the next priority queue when the first queue becomes empty.

The bandwidth control monitors the classified queues using the round robin method. The bandwidth for each queue is differentiated by putting different weights on the monitor frequency.

Classes group packets using definitions similar to packet filtering with the **queue class filter** command. On the RTX5000 classes are identified by a number between 1 and 100, and they are identified by a number between 1 and 16 for all other models. The classes that can be used in priority control and bandwidth control are as follows:

Model	Classes That Can Be Used in Priority Control	Classes That Can Be Used in Bandwidth Control
RTX5000	1-16	1-100
RTX810	1 to 4	1 to 16

The higher the class number the higher is the priority.

The packet processing algorithm is selected from priority control, bandwidth control, and simple FIFO using the **queue interface type** command. The algorithm can be selected for each interface.

For the RTX5000, RTX3500 and RTX3000, the class structure is arranged in a hierarchy, and the second hierarchy layer can contain prioritized classes. In other words, the first hierarchy layer can be specified for bandwidth control and priority control, and the second hierarchy layer can be specified for priority control.

#### 21.1 Set the Interface Speed

##### [Syntax]

```
speed interface speed
speed pp speed
no speed interface [speed]
no speed pp [speed]
```

##### [Setting and Initial value]

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *speed*
  - [Setting] : Interface speed (bit/s)
  - [Initial value] : 0 (for a PP interface)

##### [Description]

Sets the interface speed for the specified interface. When CBQ is used for bandwidth control, it is desirable that this speed matches the physical speed since it is used in the parameter calculation. In this case, if the line speed fluctuates dynamically through MP, set the lowest speed.

##### [Note]

If 'k' or 'M' is appended to the *speed* parameter, the speed is handled as kbits/s or Mbits/s.

RTX810 cannot use the **speed pp** command.

RTX5000 does not support WAN interface for *interface* parameter.

##### [Models]

RTX810, RTX5000

#### 21.2 Set the Filter for Classification

##### [Syntax]

```
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]]]]
```

**no queue class filter** *num* [*class1...*]

**[Setting and Initial value]**

- *num*
  - [Setting] : Class filter ID number
  - [Initial value] : -
- *class1*
  - [Setting] :

Setting	Description
1..100 (RTX5000)	Class
1..16 (RTX810)	
precedence	Classify (into class 1-8) according to the precedence (0-7) of the TOS field of the packet to be forwarded and carry out priority control or bandwidth control through shaping, Dynamic Traffic Control, or CBQ
dscp	Classify (into class 1-9) according to the PHB, defined by the DSCP value of the DS field of the packet to be forwarded, and carry out priority control or bandwidth control through shaping, Dynamic Traffic Control, or CBQ (can be specified only on RTX5000)

- [Initial value] : -
- *class2*
  - [Setting] : Secondary class (1..4)
  - [Initial value] : -
- *cos*
  - [Setting] :

Setting	Description
0-7	CoS value
precedence	Convert the precedence (0-7) of the ToS of the packet to CoS and store the result in the COS value

- [Initial value] : -
- *src\_addr*
  - [Setting] :
    - IP Destination IP address of the IP packet
    - Same as one \* when omitted
  - [Initial value] : -
- *dest\_addr*
  - [Setting] :
    - Destination IP address of the IP packet
    - Same as one \* when omitted
  - [Initial value] : -
- *protocol* : Type of packets to be filtered
  - [Setting] :
    - Decimal value indicating the protocol
    - Mnemonic indicating the protocol

icmp	1
tcp	6
udp	17

- Series of above items delimited by commas (up to 5 items)
- \* (All protocols)
- established
- Same as \* when omitted.
- [Initial value] : -
- *src\_port* : UDP and TCP source port number



- [Setting] :
  - A decimal number representing the port number
  - Mnemonic representing the port number (a section)

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
ntp	123
nntp	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540
submission	587

- Two of the above items with a minus sign in between them, an above item with a minus sign in front, and an above item with a minus sign in the back indicate a range.
- Series of above items delimited by commas (up to 10 items)
- \* (all ports)
- Same as \* when omitted.
- [Initial value] : -
- *dest\_port* : UDP and TCP destination port number
  - [Initial value] : -

### [Description]

Sets the filter for classification.

If *class1* is set to precedence, packets that match the filter are classified according to the precedence value of the IP header of that packet.

If *cos = cos* is specified, the specified CoS value is stored in the *user\_priority* field of the IEEE802.1 Q tag that is attached to the packet matching the filter. If precedence is specified for *cos*, the value corresponding to the precedence value in the IP header of that packet is stored in the *user\_priority* field.

Packets that match the packet filter are grouped into the specified class. Whether the filter specified command is used or the order in which the filter is applied is set using the **queue interface class filter list** command for each interface.

*class1* and *class2* can be specified concatenated with a slash (/) .*class2* can be specified on the RTX5000.

### [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
```

**[Models]**

RTX810, RTX5000

## 21.3 Select the Queuing Algorithm Type

---

**[Syntax]****queue** *interface type type***queue pp type** *type***no queue** *interface type* [*type*]**no queue pp type** [*type*]**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *type*
  - [Setting] :

Setting	Description
fifo	First In, First Out type of queuing
priority	Priority control queuing
cbq	Bandwidth control queuing
wfq	Weighted Fair Queue type queuing
shaping	Bandwidth control

- [Initial value] : fifo

**[Description]**

Selects the queuing algorithm type for the specified interface.

fifo is the most basic queue. If fifo is specified, the packets are always sent in the order that the router received them. The packet order never changes. If the number of packets in the fifo queue exceeds the value specified by the **queue interface length** command, the packet at the very end of the queue (the very last packet that arrived) is discarded.

If priority is specified, the router carries out priority control. Packets are classified using the **queue class filter** and **queue interface class filter list** commands, and the router sends the packet in the class with the highest priority among the packets waiting to be sent.

If shaping is specified, the router carries out bandwidth control on the LAN interface. It can be specified only for the LAN interface.

**[Note]**

RTX810	<i>type</i> can be specified in fifo, priority and shaping.
Models not listed above	<i>type</i> can be specified in fifo, priority, cbq, wfq and shaping.

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 21.4 Apply the Classification Filter

---

**[Syntax]****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 and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -

- *filter\_list*
  - [Setting] : Series of class filters delimited by spaces
  - [Initial value] : -

**[Description]**

Sets the order in which the filters specified by the **queue class filter** command are applied to the specified LAN interface, WAN interface, PP, or tunnel. Packets that do not match the filters are classified into the default class specified by the **queue interface default class** command.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 21.5 Set the Queue Length for Each Class

---

**[Syntax]**

```
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 and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *len1..lenN*
  - [Setting] :
    - Queue length for Class 1 to Class 16 (1..10000)
    - Queue length for RTX5000 Class 1 to Class 100 (1..10000)
  - [Initial value] :
    - 200
- *len1..len16*
  - [Setting] : Queue length from class 1 to class 16 (1..10000)
  - [Initial value] : 20

**[Description]**

Specifies the number of packets that can fit in the queue of the specified class for the interface. For classes of which the queue length is not specified, the queue length specified last is applied.

**[Note]**

*dthreshold-mid* and *dthreshold-high* parameters can be specified on the RTX5000.

RTX5000 does not support WAN interface for *interface* parameter.

If the secondary class queue length is specified on the RTX5000 using the **queue interface length secondary** command, the queue length specified by the **queue interface length secondary** command will take priority.

**[Models]**

RTX810, RTX5000

## 21.6 Setting the secondary class queue length

---

**[Syntax]**

```
queue interface length secondary [primary=primary_class] len1 [len2 ...len4]
no queue interface length secondary [primary=primary_class...]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *primary\_class*
  - [Setting] :
    - Primary class (1..100)

- When omitted, sets the queue length for the secondary class, which is subordinate to the primary class, to the same value.
- [Initial value] : -
- *len1...len4*
  - [Setting] : Class 1 to Class 4 queue length (1..10000)
  - [Initial value] : 200

**[Description]**

Specifies the number of packets that can fit in the queue of the specified secondary class, which is subordinate to the primary class, for the interface. For classes with no setting, the queue length specified last is applied.

**[Models]**

RTX5000

## 21.7 Set the Default Class

---

**[Syntax]**

**queue** *interface* **default class** *class*

**queue pp default class** *class*

**no queue** *interface* **default class** [*class*]

**no queue pp default class** [*class*]

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *class*
  - [Setting] : Class (RTX810:1..16, RTX5000:1..100)
  - [Initial value] : 2

**[Description]**

Specifies the class in which the packets that do not match the filters are grouped for the interface.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 21.8 Setting the secondary default class

---

**[Syntax]**

**queue** *interface* **default class secondary** [*primary=primary\_class*] *class*

**no queue** *interface* **default class secondary** [*primary=primary\_class...*]

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *primary\_class*
  - [Setting] :
    - Primary class (1..100)
    - When omitted, sets the default class for the secondary class, which is subordinate to the primary class, to the same value.
  - [Initial value] : -
- *class*
  - [Setting] : Class (1..4)
  - [Initial value] : 2

**[Description]**

Specifies the class in which the packets that do not match the filters are grouped for the secondary class, which is subordinate to the specified primary class.

**[Models]**

RTX5000

## 21.9 Set the Class Property

---

### [Syntax]

```

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...]

```

### [Setting and Initial value]

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *class*
  - [Setting] : Class (RTX810:1..16, RTX5000:1..100)
  - [Initial value] : -
- *bandwidth*
  - [Setting] :
    - Bandwidth allotted to the class (bit/s)
    - If 'k' or 'M' is appended to the value, it is handled as kbit/s or Mbit/s. If '%' is appended to the value, it is handled as a percentage of the entire line bandwidth.
  - [Initial value] : -

### [Description]

Sets the properties of the specified class.

### [Note]

The total bandwidth allotted to each class using the *bandwidth* parameter cannot exceed the bandwidth of the entire line. The bandwidth of the entire line is set using the **speed** command. If bandwidth control by cbq is used, the bandwidth allotted to each class must be less than or equal to that of the parent class.

If shaping is specified by the **queue interface type** command, bandwidth can be controlled through Dynamic Traffic Control. To perform Dynamic Traffic Control, the assured bandwidth and the upper limit bandwidth are set by specifying two speeds delimited by a comma in the bandwidth parameter. The smaller of the two values is always the assured bandwidth regardless of the order in which they are specified. The total assured bandwidth must not exceed the bandwidth of the entire line.

The type parameter is only valid when shaping is specified using the **queue interface type** command. Even when speed distribution is being carried out via bandwidth control in the interface, because a priority is assigned to the *type* parameter, that class will become a priority control class, and packet transfer will be performed at a higher priority than the bandwidth control class. If there are multiple classes that have been assigned a priority with the *type* parameter, the priority will be higher the higher the class numbers. The *type* parameter can be specified on the RTX5000 model.

Classes that do not have this command set are always allotted 100% of the bandwidth. Therefore, this command must be set on at least the target class and the default class, if bandwidth control is to be specified. Because 100% of the bandwidth is allotted to the default class if the default class is not specified, the target class ends up being allotted a bandwidth that is narrower than the default bandwidth.

RTX5000 does not support WAN interface for *interface* parameter.

### [Models]

RTX810, RTX5000

## 21.10 Set Dynamic Class Control

---

### [Syntax]

```

queue interface class control class [except ip_address ...] [option=value ...]
no queue interface class control class [except ip_address...]

```

### [Setting and Initial value]

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *class*
  - [Setting] : Class to enable DCC for (RTX810:1..16, RTX5000:1..100)
  - [Initial value] : -

- *ip\_address*
- [Setting] :

Setting	Description
IP address	Set the host IP addresses of servers and other devices that you do not want to monitor. (You can specify multiple addresses by delimiting them with spaces, and you can specify a range by using a hyphen.)

- [Initial value] : -
- *Sequence of option = value*
- [Setting] :

option	value	Description
forwarding	reject, 1..16	Classes that excess traffic is forwarded to
watch	source	Monitor bandwidth by source IP address
	destination	Monitor bandwidth by destination IP address
threshold	Bandwidth use, seconds	Set the bandwidth use threshold and the time threshold, delimited by a comma, for determining excess traffic (bandwidth use: 1%..100%; seconds: 10..86400).
time	infinity	The amount of time for which excessive traffic is cut off or for which a different class is used (in seconds).
	10..604800	
mode	forced	Set the mode to forced control mode
	adaptive	Set the mode to adaptive control mode
trigger	winny	Start control when Winny is detected
	share	Start control when Share is detected
	masquerade-session	Start control when the IP masquerade conversion session limit is reached
notice	on	Indicate that control is taking place
	off	Do not indicate that control is taking place

- [Initial value] :
  - watch=source
  - threshold=70%,30
  - time=600
  - mode=forced
  - notice=on

### [Description]

Monitors the specified interface to make sure that a single host is not using an excessive amount of bandwidth for sending and receiving.

When the QoS type on the monitored interface is shaping, the percentage of the class bandwidth specified by the **queue interface class property** command (when a guaranteed value and an upper limit are specified, the percentage of the guaranteed value is used) that is being used is monitored. When the QoS type is priority, the percentage of the interface bandwidth that is being used is monitored. During monitoring, the router checks the bandwidth usage every 10 seconds and determines that the threshold has been exceeded when the percentage of bandwidth usage exceeds the specified percentage for the specified amount of time.

For example, if threshold=70%,30, when the percentage of bandwidth usage exceeds 70% for 10 seconds three times in a row, the router determines that the threshold has been exceeded.

When the router detects that a host is sending (watch = source) or receiving (watch = destination) excessive traffic, that traffic is forwarded to the class specified by the *forwarding* parameter, and packets are sent according to the settings of the class that

receives the forwarded traffic. If you set the *forwarding* parameter to reject, the excess traffic is cut off. Also, you can omit the *forwarding* command. When you do so, no forwarding control takes place, but you can see what host is exceeding the threshold by using the **show status qos** command.

The *time* parameter indicates the amount of time for which forwarding control is performed. If you set the parameter to infinity, the excessive traffic is cut off or a different class is used indefinitely.

The *mode* parameter specifies the operation mode. If you set the parameter to forced, the specified flow control is performed immediately after the time specified by the threshold parameter. Also, after the control time specified by time passes, the flow control stops. If you set the mode to adaptive, even if the time specified by threshold passes, the router postpones flow control until the bandwidth being used by the class is 90% or more of the guaranteed bandwidth. Also, even if the control time specified by the time parameter passes, the router will postpone stopping flow control until the amount of bandwidth used by the class falls below 90% of the guaranteed bandwidth.

Hosts whose control is postponed are not shown by the **show status qos** command. If the bandwidth usage of the host whose control is postponed goes below the threshold, the host is released immediately.

The *trigger* parameter specifies the internal router event that triggers the start of control. You can specify multiple triggers delimited by commas.

The *notice* parameter specifies whether the router notifies the host that it is using Dynamic Class Control. If you specify on, after control is used on a host, a notification appears on the host's browser when it accesses an http server (port number: 80) through the Web.

The *notice* parameter can be used with models which incorporate the Web GUI function.

#### **[Note]**

Traffic forwarding can only be performed once. If this command has been specified for the class that the traffic is forwarded to, the setting for the second forwarding will be disabled so that the traffic is not forwarded twice.

RTX5000 does not support WAN interface for *interface* parameter.

#### **[Models]**

RTX810, RTX5000

## Chapter 22

### Cooperation Function

#### 22.1 Set Whether to Use the Cooperation Function

##### [Syntax]

**cooperation** *type role sw*

**no cooperation** *type role [sw]*

##### [Setting and Initial value]

- *type* : Cooperation type
  - [Setting] :

Setting	Description
bandwidth-measuring	Line bandwidth detection
load-watch	Load watch notification

- [Initial value] : -
- *role* : Cooperation role
  - [Setting] :

Setting	Description
server	Server operation
client	Client operation

- [Initial value] : -
- *sw*

- [Setting] :

Setting	Description
on	Enable the function
off	Disable the function

- [Initial value] : All operation functions set to off

##### [Description]

Sets the operation of each cooperation function.

##### [Models]

RTX810, RTX5000

#### 22.2 Set the Port Number to Be Used by the Cooperation Function

##### [Syntax]

**cooperation port** *port*

**no cooperation port** [*port*]

##### [Setting and Initial value]

- *port*
  - [Setting] : Port Number
  - [Initial value] : 59410

##### [Description]

Sets the UDP port number to be used by the cooperation function. This number is used as the source port number of packets send by the cooperation function. When packets with this destination port number is received, they are handled as packets of the cooperation function.

##### [Models]

RTX810, RTX5000

#### 22.3 Set the Operation of Each Peer That Is to Cooperate in the Bandwidth Measurement



**[Syntax]**

**cooperation bandwidth-measuring remote** *id role address [option=value]*

**no cooperation bandwidth-measuring remote** *id [role address [option=value]]*

**[Setting and Initial value]**

- *id*
  - [Setting] : Peer ID number (1..100)
  - [Initial value] : -
- *role* : Role of the peer in the cooperation
  - [Setting] :

Setting	Description
server	The peer performs server operation
client	The peer performs client operation

- [Initial value] : -
- *address*
  - [Setting] : Peer IP address of the cooperation, FQDN, or 'any'
  - [Initial value] : -
- *option* : Option
  - [Setting] :

Setting	Description
apply	Whether the measured result is applied to the speed setting of the LAN interface or WAN interface ('on' or 'off')
port	UDP port number that the peer uses (1-65535)
initial-speed	Measurement start value (64000-100000000)[bit/s]
interval	Watch interval (60..2147483647)[sec]or'off'
retry-interval	Interval between the end of an error and the next attempt (60..2147483647)[sec]
sensitivity	Measurement sensitivity (high, middle or low)
syslog	Whether to log the operation (on or off)
interface	LAN interface or WAN interface that the measurement results are applied to
class	Class that the measurement results are applied to
limit-rate	Maximum percentage of change in the set value (1-10000)[%]
number	Number of packets to use in measurement (5..100)
local-address	Source IP address of the sent packets

- [Initial value] :
  - apply=on
  - port=59410
  - initial-speed=10000000
  - interval=3600
  - retry-interval=3600
  - sensitivity=high
  - syslog=off
  - number=30

**[Description]**

Sets the operation of each peer that is to cooperate in the bandwidth measurement.

**[Note]**

If you set the *role* parameter to client, only port and syslog can be specified for the options. If you specify server, all options can be used.

You can only specify any as the peer to cooperate with when the *role* parameter is set to client.

When the apply option is 'on', the bandwidth measurement result is overwritten to the setting of the **speed lan** command of the LAN interface or **speed wan1** command of the WAN interface, directed at the peer. When the value is specified for the class

option, the measured results affect the *bandwidth* parameter of the **queue lan class property**, or the *bandwidth* parameter of the **queue wan1 class property** command of the specified class.

The initial-speed option can be used to set the speed at which the measurement is started. If 'k' or 'M' is appended to the parameter, it is handled as kbit/s or Mbit/s.

The retry-interval option sets the time until the next retry after the bandwidth measurement fails because of a failure to receive a response from the peer, an overly large measured value, or some other reason. However, if the measurement is failing, retrying at short intervals is unadvisable, because it will increase the load on the network. The highest priority should be given to avoiding the cause of the measurement problem.

You can use the number option to specify the number of packets to use in measurement. In an environment where the interval between packets varies widely, you can achieve more stable results by specifying a large number for this option. However, because the number of measurement packets increases, the packets are likely to have a larger influence on other data transmission.

You can use the sensitivity option to change the measurement sensitivity. In an environment where the interval between packets varies widely or there is packet loss, you can restrain frequent setting changes and reduce the amount of time until measurement is completed by reducing the measurement sensitivity.

When a LAN interface is specified for the interface option, the measured results affect that interface's **speed lan** command. When a value is specified for the class option, the measured results affect the *bandwidth* parameter of the **queue lan class property** command of the specified class. When a WAN interface is specified, the measured results affect that interface's **speed wan1** command. When a value is specified for the class option, the measured results affect the *bandwidth* parameter of the **queue wan1 class property** command of the specified class.

The class option can only be used on models with bandwidth control.

Use the limit-rate option when you want to limit sharp changes in the specified value to a certain percentage. If there is a large difference between the previous measured result and the current measured result, the router will set the current value according to the limit-rate setting instead of using the current measured result.

You can use the local-address option to set the source IP address of the sent packets. If you do not set this option, the IP address of the interface is used.

RTX5000 does not support WAN interface for *interface* parameter.

#### [Models]

RTX810, RTX5000

## 22.4 Set the Operation of Each Peer That Is to Cooperate in the Load Watch Notification

### [Syntax]

**cooperation load-watch remote** *id* *role* *address* [*option=value*]

**no cooperation load-watch remote** *id* [*role* *address* [*option=value*]]

### [Setting and Initial value]

- *id*
  - [Setting] : Peer ID number (1..100)
  - [Initial value] : -
- *role* : Role of the peer in the cooperation
  - [Setting] :

Setting	Description
server	The peer performs server operation
client	The peer performs client operation

- [Initial value] : -
- *address*
  - [Setting] : Peer IP address of the cooperation, FQDN, or 'any'
  - [Initial value] : -
- *option* : Option
  - [Setting] :

Setting	Description
trigger	Trigger definition number (1-65535) corresponding to the condition used to notify the client when the local side is operating as a server. Multiple numbers can be specified by separating each number with a comma. Can be specified only when the peer operation is set to client.

Setting	Description
control	Control operation definition number (1-65535) when a notification is received from the server when the local side is operating as a client. Can be specified only when the peer operation is set to server.
port	UDP port number that the peer uses (1-65535)
syslog	Whether to log the operation (on or off)
apply	Whether to apply the result of the load watch notification to the operation (on or off)
register	Whether to send registration packets to the server (on or off)
register-interval	Interval at which registration packets are sent from the client to the server (1..2147483647)[sec]
register-time	The amount of time for which client registration information is stored on the server (1..2147483647)[sec]
name	Name for identifying the peer (up to 16 characters)
local-address	Source IP address of the sent packets

- [Initial value] :
  - port=59410
  - syslog=off
  - apply=on
  - register=off
  - register-interval=1200
  - register-time=3600

#### [Description]

Sets the operation of each peer that is to cooperate in the load watch notification.

#### [Note]

The trigger option can be used when the *role* parameter is set to client, and the trigger option must be set when the *role* parameter is set to client. The control option can be used when the *role* parameter is set to server, and the control option must be set when the *role* parameter is set to server.

If any is specified on the server side, on the client side, register must be set to on so that the server can be notified of the client's existence.

When the name option is specified, the setting only functions when the same name is set on both the server and the client.

You can use the local-address option to set the source IP address of the sent packets. If you do not set this option, the IP address of the interface is used.

If multiple triggers are specified, the transmission timing of the suppression request is detected individually by each trigger. If the transmission timing of the trigger differs, the suppression request is sent at the individual timing. If the timing matches, a single suppression request is sent.

If a suppression release is sent to the peer, no more suppression release is sent until a suppression request is sent.

Suppression release notification is not sent even if the trigger condition meets the suppression release condition if the suppression request has not been sent.

If the peer information is deleted while performing suppression control, the speed of the controlled interface maintains the setting at that point.

#### [Models]

RTX810, RTX5000

## 22.5 Set the Operation Trigger for the Load Watch Server

#### [Syntax]

```
cooperation load-watch trigger id point high=high [, count] low=low [, count] [option=value]
no cooperation load-watch trigger id [point high=high [, count] low=low [, count] [option=value]]
```

#### [Setting and Initial value]

- *id*
  - [Setting] : Peer ID number (1-100)
  - [Initial value] : -
- *point* : Load watch point

- [Setting] :
  - `cpu load`
    - Specify the value for monitoring the CPU load at a given unit time interval as a percentage.
  - `interface receive`
    - Monitor the amount of reception per unit time on the interface. Specify the value as a number of bits per second.

<code>interface</code>	Interface name (LAN,TUNNEL)
------------------------	-----------------------------

- `interface overflow`
  - Monitor the increasing number of reception overflows and receive buffer errors per unit time on the LAN interface. Specify the value as a count.

<code>interface</code>	LAN interface name
------------------------	--------------------

- `interface [class] transmit`
  - Monitor the amount of transmission per unit time on the interface. Specify the value as a number of bits per second.

<code>interface</code>	Interface name (LAN,TUNNEL)
<code>class</code>	Class number (for a LAN interface)

- [Initial value] : -
- `high`
  - [Initial value] : High load detection threshold
- `low`
  - [Setting] : Load decrease detection threshold
  - [Initial value] : -
- `count`
  - [Setting] : Number of detections at which the notification is to be sent (1-100). 3 if omitted.
  - [Initial value] : -
- `option` : Option
  - [Setting] :

Setting	Description
<code>interval</code>	Watch interval (1-65535)[sec]. 10[sec] if omitted.
<code>syslog</code>	Whether to log the operation (on or off). off if omitted.

- [Initial value] : -

### [Description]

Sets the conditions for detecting the router load and sending traffic suppression requests to the peer. The load at the watch point is monitored at a unit time interval. When the threshold specified by `high` is exceeded the number of times specified by `count`, a suppression request is sent. As long as the high load condition in which the threshold value is exceeded persists, the suppression request is sent continuously at the `count` interval.

Likewise, if the traffic is less than the threshold value specified by `low` the number of times specified by `count`, a suppression release is sent. The suppression release is not sent to the same peer continuously.

The class option can only be used on models with bandwidth control functions.

### [Note]

To determine the threshold values, information that is shown by `show environment` and `show status lan` as well as the value shown in the log through the `syslog` option can be used as reference.

### [Example]

```
# cooperation load-watch trigger 1 cpu load high=80 low=30
```

Monitor the CPU load at a constant interval. If the load is greater than or equal to 80% for three consecutive measurements, send a suppression request. Then, if the load is less than or equal to 30% for three consecutive measurements, send a suppression release.

```
# cooperation load-watch trigger 2 lan2 receive high=80m,5 low=50m,1
```

Determine the reception speed from the number of received bytes from LAN2 within the unit time. If the value is greater than 80 [Mbit/s] for five consecutive measurements, send a suppression request. Then, if the value is less than or equal to 50 [Mbits/s] at least once, send a suppression release.

```
# cooperation load-watch trigger 3 lan2 overflow high=2,1 low=0,5
```

Watch the increase in the number of reception overflows at LAN2 within a unit time. If an overflow is detected twice, send a suppression request. If an overflow is not detected five consecutive times, send a suppression release.

**[Models]**

RTX810, RTX5000

## 22.6 Set the Operation Trigger for the Load Watch Client

**[Syntax]**

```
cooperation load-watch control id high=high [raise=raise] low=low [lower=lower] [interval=interval]  
no cooperation load-watch control id [high=high [raise=raise] low=low [lower=lower] [interval=interval]]
```

**[Setting and Initial value]**

- *id*
  - [Setting] : Peer ID number (1-100)
  - [Initial value] : -
- *high*
  - [Setting] : bit/sec. Upper bandwidth limit.
  - [Initial value] : -
- *raise*
  - [Setting] :
    - Percentage. The bandwidth is increased by this percentage at a constant interval while the upper bandwidth limit is not reached.
    - 5% if omitted.
  - [Initial value] : -
- *low*
  - [Setting] : bit/sec. Lower bandwidth limit.
  - [Initial value] : -
- *lower*
  - [Setting] :
    - Decrease the transmission bandwidth by this percentage when a suppression request is received until the lower bandwidth limit is reached.
    - 30% if omitted.
  - [Initial value] : -
- *option* : Option
  - [Setting] :

Setting	Description
interval	Interval at which the bandwidth is increased (1-65535) [sec]. 10[sec] if omitted.
interface	LAN interface for which bandwidth is increased
class	Class for which bandwidth is increased

- [Initial value] : -

**[Description]**

Sets the operation for the case when a traffic suppression request is received. The bandwidth is controlled between the bandwidth specified by *high* and the bandwidth specified by *low*.

If a suppression request is received, the transmission bandwidth is decreased by the percentage of the operating bandwidth specified by *lower*. If the bandwidth is less than *high*, the operating bandwidth increases according to the *raise* value.

If a traffic suppression release is received, the bandwidth increases to the bandwidth specified by *high*.

Class can be specified in options only on units which have bandwidth control functionality enabled.

**[Models]**

RTX810, RTX5000

## 22.7 Manually Execute the Cooperation Function

**[Syntax]**

```
cooperation bandwidth-measuring go id  
cooperation load-watch go id type
```

**[Setting and Initial value]**

- bandwidth-measuring : Line bandwidth detection
  - [Initial value] : -
- load-watch : Load watch notification
  - [Initial value] : -
- *id*
  - [Setting] : Peer ID number (1-100)
  - [Initial value] : -
- *type* : Packet type
  - [Setting] :

Setting	Description
lower	Load decrease detection packet
raise	High load detection packet

- [Initial value] : -

**[Description]**

Manually executes the cooperation function.

**[Note]**

When bandwidth-measuring is specified, the measured results appear in the log. If the interface speed is set so that the line bandwidth detection value is used, the result obtained by executing this command is also applied to the setting.

If load-watch is specified, a packet that is same as the packet delivered to the specified peer according to load watch trigger is delivered. It is valid only for peers whose role is set to client.

**[Models]**

RTX810, RTX5000

## Chapter 23

### OSPF

OSPF is a type of interior gateway protocol. It is a dynamic link-state routing protocol based on a graph-theoretic model.

#### 23.1 Apply OSPF

##### [Syntax]

**ospf configure refresh**

##### [Description]

Applies OSPF settings. If you change OSPF settings, you must restart the router or execute this command.

##### [Models]

RTX810, RTX5000

#### 23.2 Enable/Disable OSPF

##### [Syntax]

**ospf use use**

**no ospf use [use]**

##### [Setting and Initial value]

- *use*
- [Setting] :

Setting	Description
on	Enable OSPF
off	Disable OSPF

- [Initial value] : off

##### [Description]

Sets whether to use OSPF.

##### [Note]

The following functions are not supported:

- NSSA (RFC1587)
- OSPF over demand circuit (RFC1793)
- OSPF MIB

##### [Models]

RTX810, RTX5000

#### 23.3 Set the Level of Precedence of the OSPF Routing

##### [Syntax]

**ospf preference preference**

**no ospf preference [preference]**

##### [Setting and Initial value]

- *preference*
- [Setting] : Level of precedence of the OSPF routing (a value greater than or equal to 1)
- [Initial value] : 2000

##### [Description]

Sets the level of precedence of the OSPF routing. The level of preference is expressed by a value greater than or equal to 1. The larger the value, the higher is the level of preference. If the routes obtained from multiple protocols such as OSPF and RIP are in conflict, the one with the higher level of preference is used. If the level of preference is equal, the route adopted earlier in time is activated.

##### [Note]

The level of preference of static routes is fixed to 10000.

##### [Models]

RTX810, RTX5000

## 23.4 Set the OSPF Router ID

---

### [Syntax]

```
ospf router id router-id
no ospf router id [router-id]
```

### [Setting and Initial value]

- *router id*
  - [Setting] : IP address
  - [Initial value] : -

### [Description]

Specifies the OSPF router ID.

### [Note]

If the router ID has not been set by this command, the primary IPv4 address assigned to the interface is searched in the following order, and the first IPv4 address found is used as the router ID.

- LAN interface (from smallest number)
- LOOPBACK interface (from smallest number)

Moreover, if there is no interface with primary IPv4 address, the initial value is not set.

### [Models]

RTX810, RTX5000

## 23.5 Set Whether to Apply the Route Received through OSPF to the Routing Table

---

### [Syntax]

```
ospf export from ospf [filter filter_num...]
no ospf export from ospf [filter filter_num...]
```

### [Setting and Initial value]

- *filter\_num*
  - [Setting] : Filter number of the **ospf export filter** command
  - [Initial value] : All routes are applied to the routing table.

### [Description]

Sets whether to apply the route received through OSPF to the routing table. Only the route that matches the specified filter is applied to the routing table. If this command is not specified, or data after the filter keyword is omitted, all routes are applied to the routing table.

### [Note]

Up to 100 filter numbers can be set.

This command does not affect the link state database of OSPF. In other words, the operation of exchanging information with other routers using OSPF does not change regardless of the setting of this command. This command only specifies whether the route calculated by OSPF is used to actually route packets.

### [Models]

RTX810, RTX5000

## 23.6 Route Import Using External Protocol

---

### [Syntax]

```
ospf import from protocol [filter filter_num...]
no ospf import from protocol [filter filter_num...]
```

### [Setting and Initial value]

- *protocol* : External protocol to be imported in the OSPF routing table
  - [Setting] :

Setting	Description
static	Static route
rip	RIP
bgp	BGP

- [Initial value] : -



- *filter\_num*
  - [Setting] : Filter number
  - [Initial value] : -

**[Description]**

Sets whether to import the route by an external protocol into the OSPF routing table. The imported route is announced as an AS external route to other OSPF routers.

Set *filter\_num* to the filter number defined by the **ospf import filter** command. The route being imported from an external protocol is checked by the specified filter. If the route matches the filter, the route is imported into OSPF. A route that does not match any of the filters is not imported. If the filter number after the filter keyword is omitted, all routes are imported into OSPF.

The metric value, metric type, and tag parameters for announcing the route use the values specified by the **ospf import filter** command that matched the filter check. If the keywords after filter are omitted, the following parameters are used.

- metric=1
- type=2
- tag=1

**[Note]**

The filter number can be set up to 300 for the RTX5000. It can be set up to 100 for all other models.

**[Models]**

RTX810, RTX5000

## 23.7 Set the Filter for Handling the Route Received through OSPF

---

**[Syntax]**

```
ospf export filter filter_num [nr] kind ip_address/mask...  
no ospf export filter filter_num [...]
```

**[Setting and Initial value]**

- *filter\_num*
  - [Setting] : Filter number
  - [Initial value] : -
- *nr* : Filter interpretation method
  - [Setting] :

Setting	Description
not	Import routes that do not match the filter
reject	Not import routes that match the filter
When omitted	Import routes that match the filter

- [Initial value] : -
- *kind* : Filter type
  - [Setting] :

Setting	Description
include	Routes included in the specified network address (including the network address itself)
refines	Routes included in the specified network address (not including the network address itself)
equal	Routes that match the specified network address

- [Initial value] : -
- *ip\_address/mask*
  - [Setting] : IP address and mask length representing the network address
  - [Initial value] : -

**[Description]**

Defines the filter that is applied when importing a route received from another OSPF router into the routing table through OSPF. The filter defined by this command takes effect when it is specified by the filter section of the **ospf export from** command.

Set the network address with the *ip\_address/mask* parameter. This parameter can be specified multiple times, and a check is performed on each network address when checking the route.

If *nr* is omitted, the route is imported when any filter matches.

If *not* is specified, the route is imported when none of the filters match. If *reject* is specified, the route is not imported when any of the filters matches.

The *kind* parameter specifies how the route is checked.

include	Filtering is applied to routes that match the network address and routes included in the network address
refines	Filtering is applied to the routes included in the network address but not the route that matches the network address
equal	Filtering is applied to only the routes that match the network address

#### [Note]

Caution must be exercised when a filter specified by *not* is used multiple times with the **ospf export from** command. Whether a network address that matches a filter specified by *not* is advertised is not determined by that filter, and the address is checked by the next filter. Therefore, for example, setting the filters as shown below results in all routes being imported and is meaningless.

```
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
```

The first filter imports routes other than 192.168.1.0/24, and the second filter imports routes other than 192.168.2.0/24. In other words, the route 192.168.1.0/24 is imported by the second filter, and the route 192.168.2.0/24 is imported by the first filter. This means that there are no routes that are not imported.

If you do not want to import routes 192.168.1.0/24 and 192.168.2.0/24, you must set the filters as shown below.

```
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
```

#### [Models]

RTX810, RTX5000

## 23.8 Define Filters Applied to the Importing of AS External Routes

#### [Syntax]

```
ospf import filter filter_num [nr] kind ip_address/mask... [parameter...].
no ospf import filter filter_num [[not] kind ip_address/mask... [parameter...]]
```

#### [Setting and Initial value]

- *filter\_num*
  - [Setting] : Filter number
  - [Initial value] : -
- *nr* : Filter interpretation method
  - [Setting] :

Setting	Description
not	Announce routes that do not match the filter
reject	Not announce routes that match the filter
When omitted	Announce routes that match the filter

- [Initial value] : -
- *kind*
  - [Setting] :

Setting	Description
include	Routes included in the specified network address (including the network address itself)
refines	Routes included in the specified network address (not including the network address itself)
equal	Routes that match the specified network address

- [Initial value] : -
- *ip\_address/mask*
  - [Setting] : IP address and mask length representing the network address
  - [Initial value] : -
- *parameter* : Parameter for announcing AS external routes
  - [Setting] :

Setting	Description
metric	Metric value (0..16777215)
type	Metric type (1..2)
tag	Tag value (0..4294967295)

- [Initial value] : -

### [Description]

Defines the filter to be applied when importing AS external routes into the OSPF routing table. The filter defined by this command takes effect when it is specified by the filter section of the **ospf import from** command. Set the network address with the *ip\_address/mask* parameter. This parameter can be specified multiple times, and a check is performed on each network address when checking the route. If any of the filters matches, it is applied.

If *nr* is omitted, the route is advertised when any filter matches. If not is specified, the route is advertised when none of the filters match. If reject is specified, the route is not advertised when any of the filters matches.

The *kind* parameter specifies how the route is checked.

include	Filtering is applied to routes that match the network address and routes included in the network address
refines	Filtering is applied to the routes included in the network address but not the route that matches the network address
equal	Filtering is applied to only the routes that match the network address

If the not keyword is placed before the *kind* parameter, the determination of match/mismatch is inverted. For example, in not equal, filtering is applied to routes that do not match the network address.

The *parameter* metric value, metric type, and tag for advertising the matched route as an AS external route of OSPF can be specified by metric, type, and tag. If these keywords are omitted, the following values are used.

- metric=1
- type=2
- tag=1

### [Note]

Caution must be exercised when a filter specified by not is used multiple times with the **ospf import from** command. Whether a network address that matches a filter specified by not is advertised is not determined by that filter, and the address is checked by the next filter. Therefore, for example, setting the filters as shown below results in all routes being advertised and is meaningless.

```
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, 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. This means that there are no routes that are not advertised.

If you do not want to advertise routes 192.168.1.0/24 and 192.168.2.0/24, you must set the filters as shown below.

```
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
```

#### [Models]

RTX810, RTX5000

## 23.9 Set the OSPF Area

### [Syntax]

```
ospf area area [auth=auth] [stub [cost=cost]]
no ospf area area [auth=auth] [stub [cost=cost]]
```

### [Setting and Initial value]

- *area*
- [Setting] :

Setting	Description
backbone	Backbone area
A value greater than or equal to 1	Non backbone area
IP address notation (0.0.0.0 is not allowed)	Non backbone area

- [Initial value] : -
- *auth*

- [Setting] :

Setting	Description
text	Plain text authentication
md5	MD5 authentication

- [Initial value] : No authentication
- *stub* : Specifies that it is a stub area.
  - [Initial value] : Not a stub area
- *cost*
  - [Setting] : A value greater than or equal to 1
  - [Initial value] : -

### [Description]

Sets the OSPF area.

The *cost* parameter is a value greater than or equal to 0. It is used as a cost of the default route that the area border router advertises within the area. If the *cost* parameter is not specified, the default route advertisement is not carried out.

#### [Models]

RTX810, RTX5000

## 23.10 Advertise the Route to an Area

### [Syntax]

```
ospf area network area network/mask [restrict]
no ospf area network area network/mask [restrict]
```

### [Setting and Initial value]

- *area*
- [Setting] :

Setting	Description
backbone	Backbone area

Setting	Description
A value greater than or equal to 1	Non backbone area
IP address notation (0.0.0.0 is not allowed)	Non backbone area

- [Initial value] : -
- *network*
  - [Setting] : IP address
  - [Initial value] : -
- *mask*
  - [Setting] : Net mask length
  - [Initial value] : -

**[Description]**

The routes within the range of the network specified by this command are advertised as a single network route when an area border router advertises the route to another area. If the restrict keyword is specified, routes in the range including aggregate routes not advertised.

**[Models]**

RTX810, RTX5000

## 23.11 Advertise Stub Connections

---

**[Syntax]**

**ospf area stubhost** *area host* [cost *cost*]

**no ospf area stubhost** *area host*

**[Setting and Initial value]**

- *area*
  - [Setting] :

Setting	Description
backbone	Backbone area
A value greater than or equal to 1	Non backbone area
IP address notation (0.0.0.0 is not allowed)	Non backbone area

- [Initial value] : -
- *host*
  - [Setting] : IP address
  - [Initial value] : -
- *cost*
  - [Setting] : A value greater than or equal to 1
  - [Initial value] : -

**[Description]**

Advertises that the specified host is connected as a stub at the specified cost.

**[Models]**

RTX810, RTX5000

## 23.12 Set the Virtual Link

---

**[Syntax]**

**ospf virtual-link** *router\_id area* [*parameters...*]

**no ospf virtual-link** *router\_id* [*area* [*parameters...*]]

**[Setting and Initial value]**

- *router\_id*
  - [Setting] : Router ID of the peer of the virtual link
  - [Initial value] : -
- *area*
  - [Setting] :

Setting	Description
A value greater than or equal to 1	Non backbone area
IP address notation (0.0.0.0 is not allowed)	Non backbone area

- [Initial value] : -
- *parameters*
  - [Setting] : Array of NAME=VALUE
  - [Initial value] :
    - retransmit-interval = 5 seconds
    - transmit-delay = 1 seconds
    - hello-interval = 10 seconds
    - dead-interval = 40 seconds
    - authkey=None
    - md5key=None
    - md5-sequence-mode=second

#### [Description]

Sets the virtual link. A virtual link is established to the router specified by *router\_id* by traversing the area specified by *area*. Parameters of the virtual link can be specified by *parameters*. The parameters are specified in the form NAME=VALUE. The following types are available.

NAME	VALUE	Description
retransmit-interval	Number of seconds	Set the retransmission interval when sending LSAs consecutively.
transmit-delay	Number of seconds	Set the time when the LSA is sent after the link state changes in unit of seconds.
hello-interval	Number of seconds	Set the transmission interval of HELLO packets in unit of seconds.
dead-interval	Number of seconds	Set the time until the router decides that the peer is down when HELLO cannot be received from the peer.
authkey	Text string	Set the text string representing the plain text authentication key. KEY is a text string consisting of up to 8 characters.
md5key	ID, text string	Set the ID representing the MD5 authentication key and the key string. The ID is a decimal number between 0 and 255. KEY is a text string consisting of up to 16 characters. Up to two MD5 authentication keys can be set. If multiple MD5 authentication keys are set, multiple packets with the same content are sent with the authentication data of each key attached. When receiving packets, the key with the matching ID is compared.
md5-sequence-mode	second	Seconds of transmission time
	increment	Monotonic increase

#### [Note]

- Regarding hello-interval/dead-interval  
The hello-interval and dead-interval values must be the same among all neighbor routers with which the interface can directly communicate. If OSPF HELLO packets whose parameter values that differ from the specified values are received, they are discarded.
- Regarding MD5 Authentication Key  
The function that allows multiple MD5 authentication keys to be set is available for smoothly changing the MD5 authentication key.

In normal operation, set only one MD5 authentication key. When changing the MD5 authentication key, set two MD5 authentication keys (new and old) on a single router. Then, change the MD5 authentication key to the new one on neighbor routers. Finally, delete the old key on the router on which the two keys are set last.

#### [Models]

RTX810, RTX5000

## 23.13 Set the OSPF Area of the Specified Interface

### [Syntax]

```
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...]]
```

### [Setting and Initial value]

- *interface*
  - [Setting] : LAN or loopback interface name
  - [Initial value] : -
- *area*
  - [Setting] :

Setting	Description
backbone	Backbone area
A value greater than or equal to 1	Non backbone area
IP address notation (0.0.0.0 is not allowed)	Non backbone area

- [Initial value] : The interface does not belong to an OSPF area.
- *parameters*
  - [Setting] : Array of NAME=VALUE
  - [Initial value] :
    - type=broadcast (when specifying the LAN interface)
    - type=point-to-point (When a PP interface is specified)
    - type=loopback (when a loopback interface is specified)
    - passive=The interface is not passive
    - cost=1 (when a LAN or loopback interface is specified), varies depending on the line speed for PP
    - priority=1
    - retransmit-interval=5 seconds
    - transmit-delay=1 seconds
    - hello-interval=10 seconds (type = when broadcast is specified)
    - hello-interval=10 seconds (When point-to-point is specified)
    - hello-interval=30 seconds (when non-broadcast is specified)
    - hello-interval=30 seconds (When point-to-multipoint is specified)
    - dead-interval=Four times hello-interval
    - poll-interval=120 seconds
    - authkey=None
    - md5key=None
    - md5-sequence-mode=second

### [Description]

Sets the OSPF area to which the specified interface belongs.

The type keyword of the NAME parameter specifies the type of network of the interface.

Set the link parameters in *parameters*. The parameters are specified in the form NAME=VALUE. The following types are available.

NAME	VALUE	Description
type	broadcast	Broadcast

NAME	VALUE	Description
	point-to-point	Point-to-point
	point-to-multipoint	Point-to-multipoint
	non-broadcast	NBMA
passive		Not send OSPF packets to the interface. Specify this parameter when other OSPF routers are not present at the respective interface.
cost	Cost	Set the interface cost. The default value is determined by the interface type and the line speed. The cost is 1 for a LAN interface. For a PP interface, the cost is calculated by the expression shown below with the line speed of the bound lines denoted as S [kbit/s]. For example, the cost is 1562 for 64 kbit/s and 65 for 1.536 Mbit/s. (0 .. 65535) <ul style="list-style-type: none"> <li>COST=100000/S</li> </ul> For a TUNNEL interface, the default value is 1562.
priority	Priority	Set the priority for selecting the designated router. The router with a large PRIORITY value is selected as the designated router. If set to 0, the router is not selected as the designated router. (0..255)
retransmit-interval	Number of seconds	Set the retransmission interval when sending LSAs consecutively.
transmit-delay	Number of seconds	Set the time when the LSA is sent after the link state changes in unit of seconds.
hello-interval	Number of seconds	Set the transmission interval of HELLO packets in unit of seconds.
dead-interval	Number of seconds	Set the time until the router decides that the neighbor is down when HELLO cannot be received from the neighbor.
poll-interval	Number of seconds	Parameter only valid on a non broadcast link. Set the transmission interval of HELLO packets when the neighbor router is down in unit of seconds.
authkey	Text string	Set the text string representing the plain text authentication key. A text string consisting up to 8 characters.
md5key	ID, text string	Set the ID representing the MD5 authentication key and the key string. The ID is a decimal number between 0 and 255. KEY is a text string consisting of up to 16 characters. Up to two MD5 authentication keys can be set. If multiple MD5 authentication keys are set, multiple packets with the same content are sent with the authentication data of each key attached. When receiving packets, the key with the matching ID is compared.
md5-sequence-mode	second	Seconds of transmission time



NAME	VALUE	Description
	increment	Monotonic increase

When you specify a loopback interface, you can specify the interface type with the *type* parameter and the interface *cost* with the *cost* parameter. You can set the loopback interface type to one of the two options listed below.

NAME	VALUE	Advertised Route Types	OSPF Interface Handling	
			Type	Condition
type	loopback	Only the host routes of the loopback interface IP address	point-to-point	Loopback
	loopback-network	Implicit loopback interface network routes	NBMA	DROther

#### [Note]

- Regarding type of the NAME parameter

Only broadcast is allowed for the type keyword of the NAME parameter on a LAN interface. On a PP interface, point-to-point can be specified when PPP is used, and point-to-multipoint or non-broadcast can be specified when frame relay is used.

When non-broadcast (NBMA) is used in frame relay, the status must have a PVC that have been set between all sites in frame relay, and allow each router connected with FR to communicate with other routers directly. In other words, a full mesh network is necessary. Also, since non-broadcast cannot identify neighbor routers automatically, you must set all neighbor routers with the **ip pp ospf neighbor** command.

To use point-to-multipoint, the frame relay PVC does not have to be a full-mesh network. Even a partial mesh without some parts can be used. Since neighbor routers are automatically identified using InArp, InArp is mandatory. You can set whether to use InArp for RT with the **fr inarp** command. By default, InArp has been set for use, and you only have to give a proper IP address to the interface with the **ip pp address** command.

The setting of the **ip pp ospf neighbor** command is discarded on an interface specified as point-to-multipoint.

There are less network limitations and configuration is easier for point-to-multipoint than non-broadcast, but the traffic that flows through the line is greater in return. In non-broadcast, the designated router is selected in the same manner as broadcast, and the OSPF traffic such as HELLO is limited between each router and the designated router. However, because point-to-multipoint assumes that a point-to-point link exists among all router pairs that can communicate, OSPF traffic is exchanged among all router pairs.

- Regarding passive

Specify the passive keyword when there are no other OSPF routers in the network to which the interface is connected. When passive is specified, OSPF packets are not sent from the interface. This suppresses unneeded traffic and also prevents operation errors at the receiving end.

For a LAN interface (interface set to 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 specified. Therefore, for a LAN interface that connects to a network that does not use OSPF, the **ip interface ospf area** command with the passive keyword attached can be specified to advertise the route to the network to other OSPF routers without using OSPF.

If the **ip interface ospf area** command is not specified for a PP interface, the route to the network to which the interface is connected is handled as an AS external route. Because it is an AS external route, the **ospf import** command must be specified to advertise the route to other OSPF routers.

- Regarding hello-interval/dead-interval

The hello-interval and dead-interval values must be the same among all neighbor routers to which the interface can directly communicate. If OSPF HELLO packets whose parameter values that differ from the specified values are received, they are discarded.

- Regarding MD5 Authentication Key

The function that allows multiple MD5 authentication keys to be set is available for smoothly changing the MD5 authentication key.

In normal operation, set only one MD5 authentication key. When changing the MD5 authentication key, set two MD5 authentication keys (new and old) on a single router. Then, change the MD5 authentication key to the new one on neighbor routers. Finally, delete the old key on the router on which the two keys are set last.

**[Models]**

RTX810, RTX5000

**23.14 Specify the OSPF Router Connected to a Non-Broadcast Network**

---

**[Syntax]**

```

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 and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *ip\_address*
  - [Setting] : IP address of the neighbor router
  - [Initial value] : -

**[Description]**

Specifies the OSPF router connected to a non-broadcast network.

The router with the eligible keyword specified indicates that it is eligible of becoming a designated router.

**[Models]**

RTX810, RTX5000

**23.15 Set the Handling of the Network Route When Stubs Are Present**

---

**[Syntax]**

```

ospf merge equal cost stub merge
no ospf merge equal cost stub

```

**[Setting and Initial value]**

- *merge*
  - [Setting] :

Setting	Description
on	Merge stub of equal cost with other routes
off	Not merge stub of equal cost with other routes

- [Initial value] : on

**[Description]**

Sets the handling of stubs of the same cost as other routes.

If on is specified, the route to the stub is merged with another route to create an equal-cost multipath. This is in accordance with the description in the RFC2328.

If off is specified, the route to the stub is ignored.

**[Models]**

RTX810, RTX5000

**23.16 Set Whether to Log OSPF State Transitions and Packet Exchanges**

---

**[Syntax]**

```

ospf log log [log...]
no ospf log [log...]

```

**[Setting and Initial value]**

- *log*
  - [Setting] :

Setting	Description
interface	State transition of the interface
neighbor	State transition of the neighbor router
packet	Packets sent or received

- [Initial value] : Not log OSPF

**[Description]**

Logs the specified type of log at INFO level.

**[Models]**

RTX810, RTX5000

## Chapter 24

### BGP

#### 24.1 Set the BGP Startup

##### [Syntax]

```

bgp use use
no bgp use [use]

```

##### [Setting and Initial value]

- *use*
- [Setting] :

Setting	Description
on	Start
off.	Not start

- [Initial value] : off

##### [Description]

Sets whether to start BGP.

##### [Note]

BGP cannot be used if a secondary address has been assigned to one of the interfaces.

##### [Models]

RTX810, RTX5000

#### 24.2 Set Aggregate Routes

##### [Syntax]

```

bgp aggregate ip_address/mask filter filter_num ...
no bgp aggregate ip_address/mask [filter filter_num... ]

```

##### [Setting and Initial value]

- *ip\_address/mask*
  - [Setting] : IP address/netmask
  - [Initial value] : -
- *filter\_num*
  - [Setting] : Filter number (1..2147483647)
  - [Initial value] : -

##### [Description]

Sets the aggregate routes to advertise using BGP. Specify the number defined by the **bgp aggregate filter** command for the filter number.

##### [Models]

RTX810, RTX5000

#### 24.3 Set the Filter for Route Aggregation

##### [Syntax]

```

bgp aggregate filter filter_num protocol [reject] kind ip_address/mask ...
no bgp aggregate filter filter_num [protocol [reject] kind ip_address/mask ...]

```

##### [Setting and Initial value]

- *filter\_num*
  - [Setting] : Filter number (1..2147483647)
  - [Initial value] : -
- *protocol*
  - [Setting] :

Setting	Description
static	Static route
rip	RIP
ospf	OSPF
bgp	BGP
all	All protocols

- [Initial value] : -
- *kind*
- [Setting] :

Setting	Description
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 that match the specified network

- [Initial value] : -
- *ip\_address/mask*
  - [Setting] : IP address/netmask
  - [Initial value] : -

#### [Description]

Defines the filter for aggregating routes to be advertised with BGP. The filter defined by this command takes effect when it is specified by the filter section of the **bgp aggregate** command.

Set the network address with the *ip\_address/mask* parameter. Multiple network addresses can be specified. The setting with the longest matching network length is used.

If the reject keyword is placed before *kind*, that route is excluded from aggregation.

#### [Models]

RTX810, RTX5000

## 24.4 Set the AS Number

---

#### [Syntax]

```
bgp autonomous-system as
no bgp autonomous-system [as]
```

#### [Setting and Initial value]

- *as*
  - [Setting] : AS number (1..65535)
  - [Initial value] : -

#### [Description]

Sets the AS number of the router.

#### [Note]

The BGP does not work until the AS number is set.

#### [Models]

RTX810, RTX5000

## 24.5 Set the Router ID

---

#### [Syntax]

```
bgp router id ip_address
no bgp router id [ip_address]
```

#### [Setting and Initial value]

- *ip\_address*
  - [Setting] : IP address
  - [Initial value] : Automatically select from the primary address granted to the interface.

**[Description]**

Sets the router ID.

**[Note]**

Normally, this command does not need to be specified.

**[Models]**

RTX810, RTX5000

## 24.6 Set the BGP Route Preference

---

**[Syntax]**

```
bgp preference preference
no bgp preference [preference]
```

**[Setting and Initial value]**

- *preference*
  - [Setting] : Priority (1..2147483647)
  - [Initial value] : 500

**[Description]**

Sets the BGP route preference. The level of preference is expressed by a value greater than or equal to 1. The larger the value, the higher is the level of preference. If the routes obtained from BGP and other protocols are in conflict, the one with the higher level of preference is used. If the level of preference is equal, the route adopted earlier is activated.

**[Note]**

The default values of the level of preference assigned to each protocol are as follows:

Static	10000
RIP	1000
OSPF	2000
BGP	500

**[Models]**

RTX810, RTX5000

## 24.7 Apply the Filter to the Route Received with BGP

---

**[Syntax]**

```
bgp export remote_as filter filter_num ...
bgp export aspath seq "aspath_regex" filter filter_num ...
no bgp export remote_as [filter filter_num ...]
no bgp export aspath seq ["aspath_regex" [filter filter_num ...]]
```

**[Setting and Initial value]**

- *remote\_as*
  - [Setting] : Remote AS number (1..65535)
  - [Initial value] : -
- *seq*
  - [Setting] : Evaluation order for when an AS path is specified (1..65535)
  - [Initial value] : -
- *aspath\_regex*
  - [Setting] : Regular expression
  - [Initial value] : -
- *filter\_num*
  - [Setting] : Filter number (1..2147483647)
  - [Initial value] : -

**[Description]**

Sets the filter for the route received with BGP. When you specify a filter with *remote\_as*, the routes received from the peer that pass through the filter are used in the actual routing table, and other protocols such as RIP and OSPF are also notified. Routes that do not pass through the filter are not used, and other protocols are not notified of them. Specify the number defined by the **bgp export filter** command for the filter number. When you specify a filter with *aspath\_regex*, just as when you specify a

filter with *remote\_as*, the routes whose AS paths match the regular expression and that pass through the filter are used in the routing table. Specify a search pattern for *aspath\_regex* that can be used by the **grep** command.

If you specify multiple filters that use *aspath\_regex*, they are evaluated in order of smallest *seq* value. Also, filters that specify *aspath\_regex* have priority over filters that specify *remote\_as*.

#### [Note]

Examples of Specifying AS Paths with Regular Expressions

- All AS paths

```
# bgp export aspath 10 ".*" filter 1
```

- AS paths that start with a number from 1000 to 1100

```
# bgp export aspath 20 "^1[01]00 .*" filter 1
```

- AS paths that contain the number 2000

```
# bgp export aspath 30 "2000" filter 1
```

- AS paths that are either 3000, 3100, or 3200

```
# bgp export aspath 40 "^3000 3100 3200$" filter 1
```

- AS paths that contain AS\_SET

```
# bgp export aspath 50 "{.*}" filter 1
```

If this command is not specified, all routes received by BGP are discarded.

Up to 100 filter numbers can be set.

#### [Models]

RTX810, RTX5000

## 24.8 Set the Filter to Be Applied to the Routes Received with BGP

#### [Syntax]

```
bgp export filter filter_num [reject] kind ip_address/mask ... [parameter ]
no bgp export filter filter_num [[reject] kind ip_address/mask ... [parameter]]
```

#### [Setting and Initial value]

- *filter\_num*
  - [Setting] : Filter number (1..2147483647)
  - [Initial value] : -
- *kind*
  - [Setting] :

Setting	Description
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 that match the specified network

- [Initial value] : -
- *ip\_address/mask*
  - [Setting] :

Setting	Description
<i>ip_address/mask</i>	IP address/netmask
all	All networks

- [Initial value] : -
- *parameter* : Group of Type=VALUE
  - [Setting] :

TYPE	VALUE	Description
preference	0..255	The level of preference used to select a route when the same route is received from multiple peers.

- [Initial value] : 0

#### [Description]

Defines the filter to be applied to the routes received with BGP. The filter defined by this command takes effect when it is specified by the filter section of the **bgp export** command.

Set the network address with the *ip\_address/mask* parameter. If multiple settings are present, the setting with the longest matching prefix is used.

If the reject keyword is placed before *kind*, that route is rejected.

#### [Note]

The preference setting is used to assign the level of preference among the BGP routes. Set the level of preference of the entire BGP route using the **bgp preference** command.

#### [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
```

#### [Models]

RTX810, RTX5000

## 24.9 Apply the Filter to the Route to Be Imported in BGP

#### [Syntax]

```
bgp import remote_as protocol [from_as] filter filter_num ...
no bgp import remote_as protocol [from_as] [filter filter_num ...]
```

#### [Setting and Initial value]

- *remote\_as*
  - [Setting] : Remote AS number (1..65535)
  - [Initial value] : -
- *protocol*
  - [Setting] :

Setting	Description
static	Static route
rip	RIP
ospf	OSPF
bgp	BGP
aggregate	Aggregate routes

- [Initial value] : -
- *from\_as*
  - [Setting] : AS that received the route to be imported (only when *protocol* is set to bgp) (1..65535)
  - [Initial value] : -
- *filter\_num*
  - [Setting] : Filter number (1..2147483647)
  - [Initial value] : -

#### [Description]

Sets the filter to be applied when importing a route other than BGP such as RIP and OSPF. Only routes that match the filters are imported. Specify the number defined by the **bgp import filter** command for the filter number. To import a BGP route, the AS number that received the route must be specified.

#### [Note]

AS external routes are imported only when this command is specified.

Up to 100 filter numbers can be set.



[Models]  
RTX810, RTX5000

## 24.10 Activate the BGP Configuration

### [Syntax]

**bgp configure refresh**

### [Description]

Activates the BGP configuration. When you change the BGP configuration, you must restart the router or execute this command.

[Models]  
RTX810, RTX5000

## 24.11 Set the Filter to Be Applied to the Routes to Be Imported in BGP

### [Syntax]

**bgp import filter** *filter\_num* [reject] *kind ip\_address/mask ... [parameter]*  
**no bgp import filter** *filter\_num* [[reject] *kind ip\_address/mask ... [parameter]*]

### [Setting and Initial value]

- *filter\_num*
  - [Setting] : Filter number (1..2147483647)
  - [Initial value] : -
- *kind*
  - [Setting] :

Setting	Description
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 that match the specified network

- [Initial value] : -

- *ip\_address/mask*
  - [Setting] :

Setting	Description
<i>ip_address/mask</i>	IP address/netmask
all	All networks

- [Initial value] : -
- *parameter* : Group of Type=VALUE
  - [Setting] :

TYPE	VALUE	Description
metric	1..16777215	Metric value notified with MED (Multi-Exit Discriminator) (MED is sent only when specified)
preference	0..255	This preference is for selecting a single party when the same pathway is received from multiple parties

- [Initial value] :
  - preference=100

### [Description]

Defines the filter to be applied to the routes to be imported in BGP. The filter defined by this command takes effect when it is specified by the filter section of the **bgp import** command.

Set the network address with the *ip\_address/mask* parameter. If multiple settings are present, the setting with the longest

matching prefix is used.

If the reject keyword is placed before *kind*, that route is rejected.

**[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
```

**[Models]**

RTX810, RTX5000

## 24.12 Set the BGP Destination

**[Syntax]**

```
bgp neighbor neighbor_id remote_as remote_address [parameter...]
no bgp neighbor neighbor_id [remote_as remote_address [parameter...]]
```

**[Setting and Initial value]**

- *neighbor\_id*
  - [Setting] : Neighbor router number (1...2147483647)
  - [Initial value] : -
- *remote\_as*
  - [Setting] : Remote AS number (1..65535)
  - [Initial value] : -
- *remote\_address*
  - [Setting] : Remote IP address
  - [Initial value] : -
- *parameter* : Group of Type=VALUE
  - [Setting] :

TYPE	VALUE	Description
hold-time	off or integer greater than or equal to 3 [s]	Keepalive transmission interval
metric	1..21474836	Metric to be notified with MED (Multi-Exit Discriminator)
passive	on or off	Whether to suppress active BGP connection
gateway	IP address/interface	Address of the gateway handling the destination
local-address	IP address	Own address of the BGP connection
ignore-capability	on or off	Whether capability is ignored or not

- [Initial value] :
  - hold-time=180
  - metric is not sent.
  - passive=off
  - gateway not specified.
  - local-address not specified.
  - ignore-capability=off

**[Description]**

Defines the neighbor for establishing a BGP connection.

**[Note]**

The *metric* parameter specifies the default value of all MEDs. If the MED is specified by the **bgp import** command, that value has priority.

The gateway option is used to specify the gateway (next hop) to the destination when the destination is not within the same segment.

you can specify up to 32 routers.

The ignore-capability option can be specified for the following revisions.

- RTX810 : Rev.11.01.23

**[Models]**  
RTX810, RTX5000

## 24.13 Set the BGP Log

---

### [Syntax]

**bgp log** *log* [*log*]  
**no bgp log** [*log* ...]

### [Setting and Initial value]

- *log*
- [Setting] :

Setting	Description
neighbor	State transition for the neighbor router
packet	Packets sent or received

- [Initial value] : Not log.

### [Description]

Logs the specified type of log at INFO level.

**[Models]**  
RTX810, RTX5000

# Chapter 25

## IPv6

### 25.1 Common Configuration

#### 25.1.1 Set Whether to Process IPv6 Packets

**[Syntax]**

```
ipv6 routing routing
no ipv6 routing [routing]
```

**[Setting and Initial value]**

- *routing*
- [Setting] :

Setting	Description
on	Handle
off	Not handle

- [Initial value] : on

**[Description]**

Sets whether to route IPv6 packets. This switch must be turned on to enable IPv6 functions on the remote PP interface. Configuration using TELNET, access using TFTP, PING, and so forth can be used even when IP routing is turned off.

**[Models]**

RTX810, RTX5000

#### 25.1.2 Set the Link MTU of the IPv6 Interface

**[Syntax]**

```
ipv6 interface mtu mtu
ipv6 pp mtu mtu
no ipv6 interface mtu [mtu]
no ipv6 pp mtu [mtu]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *mtu*
  - [Setting] : MTU value (RTX810:1280..1500, RTX5000:1280..9578)
  - [Initial value] : 1500

**[Description]**

Sets the link MTU of the IPv6 interface.

**[Models]**

RTX810, RTX5000

#### 25.1.3 Set the MSS Limit of the TCP Session

**[Syntax]**

```
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 and Initial value]**

- *interface*

- [Setting] : LAN interface name
- [Initial value] : -
- *mss*
- [Setting] :

Setting	Description
536..1440	Maximum length of MSS
auto	Auto setting
off	Not set

- [Initial value] : off

#### [Description]

Limits the MSS of the TCP session passing the interface. The router monitors the TCP packets that pass the interface, and overwrites the MSS option value with the specified value if it exceeds the specified value. If the auto keyword is specified, the MSS value is overwritten with a value calculated from the interface MTU or the MRU if the remote MRU value is known on the PP interface.

#### [Note]

For a PP interface for PPPoE, the **pppoe tcp mss limit** command can also be used to limit the MSS of the TCP session. If this command and the **pppoe tcp mss limit** command are both valid, the MSS is limited to the smaller of the two values.

#### [Models]

RTX810, RTX5000

### 25.1.4 Set Whether to Discard IPv6 Packets with Type 0 Routing Headers

#### [Syntax]

```
ipv6 rh0 discard switch
no ipv6 rh0 discard
```

#### [Setting and Initial value]

- *switch*
- [Setting] :

Setting	Description
on	Discard
off	Do not discard

- [Initial value] : on

#### [Description]

Sets whether to discard IPv6 packets with type 0 routing headers.

#### [Models]

RTX810, RTX5000

### 25.1.5 Set the IPv6 Fast Path Function

#### [Syntax]

```
ipv6 routing process process
no ipv6 routing process
```

#### [Setting and Initial value]

- *process*
- [Setting] :

Setting	Description
fast	Use the fast path function
normal	Do not use the fast path function. Process all IPv6 packets using the normal path.

- [Initial value] : fast

#### [Description]

Sets whether to process the IPv6 packet transfer using the fast path function or normal path function.

**[Note]**

There are no limitations on the functions that can be used with fast path. However, packets may be processed using normal path depending on the type of packets being handled.

when you specify fast, IPv6 multicast packets are also processed using the fast path function.

**[Models]**

RTX810, RTX5000

## 25.2 IPv6 Address Management

---

### 25.2.1 Set the IPv6 Address of the Interface

---

**[Syntax]**

```

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 and Initial value]**

- *interface*
  - [Setting] : LAN or loopback interface name
  - [Initial value] : -
- *ipv6\_addres*
  - [Setting] : IPv6 address section
  - [Initial value] : -
- *prefix\_len*
  - [Setting] : IPv6 prefix length
  - [Initial value] : -
- *address\_type*
  - [Setting] :

Setting	Description
unicast	Unicast
anycast	Anycast

- [Initial value] : unicast
- auto : Keyword indicating that an IPv6 address is created based on a prefix obtained with RA and an interface MAC address
  - [Initial value] : -
- dhcp : Keyword indicating that an IPv6 address is created based on a prefix obtained with DHCPv6 and an interface MAC address

- [Initial value] : -
- *proxy* : Proxy
- [Setting] :
  - *prefix\_type @ prefix\_interface* [ : *interface\_id/prefix\_len* ]
    - *prefix\_type*

Setting	Description
dhcp-prefix	DHCPv6 proxy
ra-prefix	RA proxy

- *prefix\_interface*

Setting	Description
<i>prefix_interface</i>	Interface name of transfer source

- *interface\_id*

Setting	Description
<i>interface_id</i>	Interface ID

- *prefix\_len*

Setting	Description
<i>prefix_len</i>	IPv6 prefix length

- [Initial value] : -

#### [Description]

Grants an IPv6 address to the interface.

#### [Note]

The address granted by this command can be checked using the **show ipv6 address** command.

The auto address configuration function can be used on multiple LAN interfaces. In precise, two functions are available: the function with which an IPv6 address is created based on a prefix obtained with RA and an interface ID, and another function with which an IPv6 address is created based on a prefix obtained with DHCPv6 and an interface ID.

When specifying them, the default route is directed to the interface that completed the auto configuration last.

When a loopback interface is specified, *auto*, *dhcp*, *address\_type*, and *proxy* cannot be specified.

A loopback interface cannot be specified for *prefix\_interface*.

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

#### [Example]

Add ::1 to the prefix of RA received by LAN2 to create an IPv6 address, and grant it to LAN1

```
# ipv6 lan1 address ra-prefix@lan2::1/64
```

#### [Models]

RTX810, RTX5000

## 25.2.2 Set the IPv6 Address Based on the Prefix to the Interface

#### [Syntax]

```
ipv6 interface prefix ipv6_prefix/prefix_len
ipv6 interface prefix proxy
ipv6 pp prefix ipv6_prefix/prefix_len
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 and Initial value]**

- *interface*
  - [Setting] : LAN interface name, bridge interface name
  - [Initial value] : -
- *ipv6\_prefix*
  - [Setting] : IPv6 prefix address section
  - [Initial value] : -
- *prefix\_len*
  - [Setting] : IPv6 prefix length
  - [Initial value] : -
- *proxy* : Proxy
  - [Setting] :
    - *proxy\_type @ proxy\_interface* : *interface\_id/prefix\_len*
      - *proxy\_type*

Setting	Description
dhcp-prefix	DHCPv6 proxy
ra-prefix	RA proxy

- *proxy\_interface*

Setting	Description
<i>proxy_interface</i>	Interface name of transfer source

- *interface\_id*

Setting	Description
<i>interface_id</i>	Interface ID

- *prefix\_len*

Setting	Description
<i>prefix_len</i>	IPv6 prefix length

- [Initial value] : -

**[Description]**

Grants an IPv6 address to the interface. Unlike the **ipv6 interface address** command, this command specifies only the prefix and not the address. The section after the prefix is automatically completed based on the MAC address. The MAC address assigned to the interface that you are trying to configure is used to complete the address. For the PP interface or tunnel interface that does not have the MAC address, the MAC address of the LAN1 interface is used.

A command with a similar name, **ipv6 prefix**, is used to define the prefix that is notified by the router advertisement and does not grant the IPv6 address. However, in normal operation, the prefix of the IPv6 address granted to the interface and the prefix notified by the router advertisement are the same. Therefore, it is often the case that the same prefix is set for both commands.

**[Note]**

The address granted by this command can be checked using the **show ipv6 address** command.

A loopback interface cannot be specified for *proxy\_interface*.

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

**[Example]**

Grant an RA prefix received on LAN2 to LAN1

```
# ipv6 lan1 prefix ra-prefix@lan2::/64
```

**[Models]**

RTX810, RTX5000

**25.2.3 Set Whether to Log Changes to IPv6 Prefix****[Syntax]**

```
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 and Initial value]**

- *interface*
  - [Setting] : LAN interface name, bridge interface name
  - [Initial value] : -
- *log*
  - [Setting] :

Setting	Description
on	Log changes to the IPv6 prefix
off	Do not log changes to the IPv6 prefix

- [Initial value] : off

**[Description]**

When there is a change in the IPv6 prefix, this command sets whether or not to log the change. The log is entered at INFO level.

If multiple addresses are set for the same prefix, the same log will be displayed multiple times.

**[Note]**

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

## 25.2.4 Set the DHCPv6 Operation

---

**[Syntax]**

```

ipv6 interface dhcp service type
ipv6 interface dhcp service client [ir=value]
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 and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *type*
  - [Setting] :

Setting	Description
off	Not use DHCPv6
client	Client
server	Server

- [Initial value] : off
- *value*
  - [Setting] :

Setting	Description
on	When operating as a client, send Inform-Request

Setting	Description
off	When operating as a client, send Solicit

- [Initial value] : off

**[Description]**

Sets the DHCPv6 operation at each interface.

**[Models]**

RTX810, RTX5000

### 25.2.5 Set the DAD (Duplicate Address Detection) Retry Count

---

**[Syntax]**

**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 and Initial value]**

- *interface*
  - [Setting] : LAN interface name, bridge interface name
  - [Initial value] : -
- *count*
  - [Setting] : DAD retry count on the selected interface (0..10)
  - [Initial value] : 1

**[Description]**

Sets the retry count of DAD that is sent to detect duplication in the address when an IPv6 address is set on the interface. However, if 0 is specified, the address is considered to be valid without sending DADs.

**[Note]**

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

### 25.2.6 Set the Maximum Number of Automatically Set IPv6 Addresses

---

**[Syntax]**

**ipv6 max auto address** *max*

**no ipv6 max auto address** [*max*]

**[Setting and Initial value]**

- *max*
  - [Setting] : Maximum number of IPv6 addresses that can be automatically set for a single interface (1 to 256)
  - [Initial value] : 16

**[Description]**

Sets the maximum number of IPv6 addresses per interface that can be set automatically according to RAs.

**[Models]**

RTX810, RTX5000

### 25.2.7 Set the Rule for Determining the Source IPv6 Address

---

**[Syntax]**

**ipv6 source address selection rule** *rule*

**no ipv6 source address selection rule** [*rule*]

**[Setting and Initial value]**

- *rule* : Rule for determining the source IPv6 address
  - [Setting] :

Setting	Description
prefix	Maximum prefix match length

Setting	Description
lifetime	Prioritize longest life time

- [Initial value] : prefix

#### [Description]

Sets the rule for determining the source IPv6 address.

When you select 'prefix', the router compares the destination IPv6 address and the source IPv6 address candidates. From the source address candidates, the router selects the address with the longest matching prefix.

When you select 'lifetime', the router chooses the IPv6 address with the longest life time.

#### [Note]

'prefix' is appropriate for most situations, but when address renumbering occurs, the 'lifetime' setting may be more appropriate.

#### [Models]

RTX810, RTX5000

## 25.3 Neighbor Discovery

### 25.3.1 Define the Prefix Distributed by the Router Advertisement

#### [Syntax]

```
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 and Initial value]

- *prefix\_id*
  - [Setting] : Prefix number
  - [Initial value] : -
- *prefix*
  - [Setting] : Prefix
  - [Initial value] : -
- *prefix\_len*
  - [Setting] : Prefix length
  - [Initial value] : -
- *proxy* : Proxy
  - [Setting] :
    - *proxy\_type @ proxy\_interface* [ : *interface\_id/prefix\_len* ]
      - *proxy\_type*

Setting	Description
dhcp-prefix	DHCPv6 proxy
ra-prefix	RA proxy

- *proxy\_interface*

Setting	Description
<i>proxy_interface</i>	Interface name of transfer source

- *interface\_id*

Setting	Description
<i>interface_id</i>	Interface ID

- *prefix\_len*

Setting	Description
<i>prefix_len</i>	IPv6 prefix length

- [Initial value] : -
- valid\_lifetime : Valid prefix lifetime
  - [Setting] : 0..4294967295

- [Initial value] : 2592000
- `preferred_lifetime` : Preferred prefix lifetime
  - [Setting] : 0..4294967295
  - [Initial value] : 604800
- `time` : Time setting
  - [Setting] :
    - yyyy-mm-dd[,hh:mm[:ss]]

Setting	Description
yyyy	Year (1980..2079)
mm	Month (01..12)
dd	Day (01..31)
hh	Hour (00..23)
mm	Minutes (00..59)
ss	seconds (00..59. 00 when omitted)

- [Initial value] : -
- `l_flag` : on-link flag
  - [Initial value] : on
- `a_flag` : autonomous address configuration flag
  - [Initial value] : on
- `switch`
  - [Setting] :
    - on
    - off
  - [Initial value] : -

**[Description]**

Defines the prefix distributed by the router advertisement. To actually advertise, the `ipv6 interface rtadv send` command must be set.

Set the number of seconds or the `time` when the lifetime elapses in the time parameter. If a value (greater than or equal to 0 and less than or equal to 4294967295) is set in `time`, the number of seconds is advertised as the lifetime. If a time is set in `time`, the lifetime is calculated and advertised. When setting the time, follow the format given above. A valid lifetime is the time until the IP address is invalidated. A preferred lifetime is the time until the address can be used on a new connection. Set the on-link flag to on, when the prefix is fixed to the data link. Set the autonomous address configuration flag to on, when the prefix can be used in the autonomous address configuration.

A loopback interface cannot be specified for `proxy_interface`.

RTX810 supports bridge interface for `interface` parameter in Rev.11.01.23 or later.

**[Note]**

The prefix of the link local cannot be specified.

**[Example]**

Transfer RA received on LAN2 to LAN1

```
# ipv6 prefix 1 ra-prefix@lan2::/64
# ipv6 lan1 rtadv send 1
```

**[Models]**

RTX810, RTX5000

**25.3.2 Control the Router Advertisement Transmission****[Syntax]**

```
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 and Initial value]**

- `interface`

- [Setting] : LAN interface name
- [Initial value] : -
- *prefix\_id*
  - [Setting] : Prefix number
  - [Initial value] : -
- *option=value* : Array of NAME=VALUE
- [Setting] :

NAME	VALUE	Description
m_flag	on, off	Managed address configuration flag. Set whether to allow the host to use auto address configuration by means other than router advertisement typified by DHCP6.
o_flag	on, off	Other stateful configuration flag. Set whether allow the host to automatically obtain option information other than the IPv6 address by means other than router advertisement.
max-rtr-adv-interval	Number of seconds	Maximum interval for sending router advertisements (4-1,800 s)
min-rtr-adv-interval	Number of seconds	Minimum interval for sending router advertisements (3-1,350 s)
adv-default-lifetime	Number of seconds	Active time of the default route of the terminal configured by the router advertisement (0-9,000 s)
adv-reachable-time	Number of Milliseconds	The valid time of reachability confirmed between nodes by the terminal receiving the router advertisement (0-3,600,000 ms)
adv-retrans-time	Number of Milliseconds	Interval for re-sending router advertisements (0-4,294,967,295 ms)
adv-cur-hop-limit	Number of hops	The marginal number of hops of router advertisement (0-255)
mtu	auto, off, number of bytes	Whether to include the MTU option in the router advertisement and the value when included. When set to auto, the interface MTU is used.

- [Initial value] :
  - m\_flag = off
  - o\_flag = off
  - 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

#### [Description]

Controls the router advertisement transmission for each interface. The prefix specified by the **ipv6 prefix** command is sent. The m\_flag and o\_flag options can be used to specify how the managed host interprets auto configuration information other than router advertisements. Options can also be used to set the transmission interval of router advertisements, and the information included in the router advertisements.

#### [Models]

RTX810, RTX5000

## 25.4 Route Control

### 25.4.1 Add IPv6 Routing Information

#### [Syntax]

```
ipv6 route network gateway gateway [parameter] [gateway gateway [parameter]]
no ipv6 route network [gateway...]
```

#### [Setting and Initial value]

- *network*

- [Setting] :

Setting	Description
IPv6 address/prefix length	Destination host
default	Default route

- [Initial value] : -

- *gateway* : Gateway

- [Setting] :

- IP address % scope ID
- pp *peer\_num* : Route to the PP interface.
  - *peer\_num*
    - Peer number
    - anonymous
- pp anonymous name=*name*

Setting	Description
name	Name specified by PAP/CHAP authentication

- *dhcp interface*

Setting	Description
<i>interface</i>	Name of the LAN or bridge interface operating as a DHCP client when using the default gateway provided by DHCP

- tunnel *tunnel\_num* : Route to the tunnel interface
- Loopback interface name, null interface name

- [Initial value] : -

- *parameter* : Multiple parameters below can be specified by delimiting each parameter with a space

- [Setting] :

Setting	Description
metric <i>metric</i>	Specify the metric <ul style="list-style-type: none"> <li>• <i>metric</i> <ul style="list-style-type: none"> <li>• Metric value (1..15)</li> <li>• 1 when omitted.</li> </ul> </li> </ul>
hide	An option that is valid only when the output interface is PP and indicates that the route is valid only when the line is connected.

- [Initial value] : -

#### [Description]

Adds IPv6 routing information. On models with multiple LAN interfaces, the interface must be specified by the scope ID. The **show ipv6 address** command shows the scope ID of the interface.

If the scope ID is omitted on models with a single LAN interface, it is assumed that LAN1 is specified.

#### [Note]

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

[Models]  
RTX810, RTX5000

## 25.5 RIPng

### 25.5.1 Set Whether to Use RIPng

[Syntax]

**ipv6 rip use** *use*  
**no ipv6 rip use**

[Setting and Initial value]

- *use*
- [Setting] :

Setting	Description
on	Use RIPng
off	Not use RIPng

- [Initial value] : off

[Description]

Sets whether to use RIPng.

[Models]  
RTX810, RTX5000

### 25.5.2 Set the Transmission Policy of RIPng on the Interface

[Syntax]

**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 and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *send*
  - [Setting] :

Setting	Description
on	Send RIPng
off	Not send RIPng

- [Initial value] : on

[Description]

Sets the transmission policy of RIPng.

[Models]  
RTX810, RTX5000

### 25.5.3 Set the Reception Policy of RIPng on the Interface

[Syntax]

**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**

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *receive*
  - [Setting] :

Setting	Description
on	Process received RIPng packets
off	Discard received RIPng packets

- [Initial value] : on

**[Description]**

Sets the reception policy of RIPng.

**[Models]**

RTX810, RTX5000

### 25.5.4 Set the Number of Hops to Be Added for RIPng

---

**[Syntax]**

```

ipv6 interface rip hop direction hop
ipv6 pp rip hop direction hop
no ipv6 interface rip hop direction
no ipv6 pp rip hop direction

```

**[Setting and Initial value]**

- *direction*
  - [Setting] :

Setting	Description
in	Add when a RIPng packet is received
out	Add when a RIPng packet is sent

- [Initial value] : -
- *hop*
  - [Setting] : Number of hops to be added (0..15)
  - [Initial value] : 0

**[Description]**

Sets the number of hops to be added to the metric of the RIPng exchanged through the PP interface.

**[Models]**

RTX810, RTX5000

### 25.5.5 Set the Trusted RIPng Gate on the Interface

---

**[Syntax]**

```

ipv6 interface rip trust gateway [except] gateway [gateway...]
ipv6 pp rip trust gateway [except] gateway [gateway...]
no ipv6 interface rip trust gateway
no ipv6 pp rip trust gateway

```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *gateway*
  - [Setting] : IPv6 address
  - [Initial value] : -

**[Description]**

Sets the trusted RIPng gateway.

If the except keyword is not specified, the list of gateways is considered to be trusted gateways, and the router receives RIP



only from those gateways.

If the `except` keyword is specified, the list of gateways is considered to be untrusted gateways, and the router only receives RIP from other gateways.

Up to 10 *gateway* may be specified.

**[Models]**

RTX810, RTX5000

### 25.5.6 Set the Filtering to Be Applied to the Route Exchanging RIPng Packets

**[Syntax]**

**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*

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *direction*
  - [Setting] :

Setting	Description
in	Apply to inward packets
out	Apply to outward packets

- [Initial value] : -
- *filter\_list*
  - [Setting] : Filter number
  - [Initial value] : -

**[Description]**

Sets the filter to be applied to RIPng packets exchanged through the interface.

**[Models]**

RTX810, RTX5000

### 25.5.7 Set the RIPng Operation on the Remote PP Interface When the Line Is Connected

**[Syntax]**

**ipv6 pp rip connect send** *action*

**no ipv6 pp rip connect send**

**[Setting and Initial value]**

- *action*
  - [Setting] :

Setting	Description
none	Not send RIPng
interval	Send RIPng at the time interval specified by the <b>ipv6 pp rip connect interval</b> command.
update	Send RIPng only when the routing information changes

- [Initial value] : update

**[Description]**

Sets the conditions for sending the RIPng to the selected peer when the line is connected.

**[Example]**

```
# ipv6 pp rip connect interval 60
# ipv6 pp rip connect send interval
```

**[Models]**

RTX810, RTX5000

**25.5.8 Set the RIPng Transmission Interval on the Remote PP Interface When the Line Is Connected**

---

**[Syntax]**

```
ipv6 pp rip connect interval time
no ipv6 pp rip connect interval
```

**[Setting and Initial value]**

- *time*
  - [Setting] : Number of seconds (30..21474836)
  - [Initial value] : 30

**[Description]**

Sets the time interval for sending the RIPng to the selected peer when the line is connected.

**[Example]**

```
# ipv6 pp rip connect interval 60
# ipv6 pp rip connect send interval
```

**[Models]**

RTX810, RTX5000

**25.5.9 Set the RIPng Operation on the Remote PP Interface When the Line Is Disconnected**

---

**[Syntax]**

```
ipv6 pp rip disconnect send action
no ipv6 pp rip disconnect send
```

**[Setting and Initial value]**

- *action*
  - [Setting] :

Setting	Description
none	Not send RIPng
interval	Send RIPng at the time interval specified by the <b>ipv6 pp rip connect interval</b> command.
update	Send RIPng only when the routing information changes

- [Initial value] : none

**[Description]**

Sets the conditions for sending the RIPng to the selected peer when the line is disconnected.

**[Example]**

```
# ipv6 pp rip disconnect interval 1800
# ipv6 pp rip disconnect send interval
```

**[Models]**

RTX810, RTX5000

**25.5.10 Set the RIPng Transmission Interval on the Remote PP Interface When the Line Is Disconnected**

---

**[Syntax]**

```
ipv6 pp rip disconnect interval time
no ipv6 pp rip disconnect interval
```

**[Setting and Initial value]**

- *time*
  - [Setting] : Number of seconds (30..21474836)
  - [Initial value] : 3600

**[Description]**

Sets the time interval for sending the RIPng to the selected peer when the line is disconnected.

**[Example]**

```
# ipv6 pp rip disconnect interval 1800
# ipv6 pp rip disconnect send interval
```

**[Models]**

RTX810, RTX5000

**25.5.11 Set Whether to Hold the Route Obtained by RIPng When the Line Is Disconnected**

---

**[Syntax]**

```
ipv6 pp rip hold routing hold
no ipv6 pp rip hold routing
```

**[Setting and Initial value]**

- *hold*
- [Setting] :

Setting	Description
on	Hold
off	Not hold

- [Initial value] : off

**[Description]**

Sets whether to hold the route obtained by RIPng through the PP interface when the line is disconnected.

**[Models]**

RTX810, RTX5000

**25.5.12 Set the RIPng Routing Preference**

---

**[Syntax]**

```
ipv6 rip preference preference
no ipv6 rip preference [preference]
```

**[Setting and Initial value]**

- *preference*
- [Setting] : RIPng routing preference (1-2147483647)
- [Initial value] : 1000

**[Description]**

Sets the RIPng routing preference. The level of preference is expressed by a value greater than or equal to 1. The larger the value, the higher is the level of preference. If the routes obtained from multiple protocols such as OSPFv3 and static are in conflict, the one with the higher level of preference is used. If the level of preference is equal, the route adopted earlier in time is activated. If the level of preference is equal, the route adopted earlier in time is activated.

**[Note]**

The level of preference of static routes is fixed to 10000.

**[Models]**

RTX810, RTX5000

**25.6 Set the VRRPv3**

---

**25.6.1 Set VRRPv3 for Each Interface**

---

**[Syntax]**

```
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 and Initial value]**

- *interface*
- [Setting] : LAN interface name
- [Initial value] : -
- *vrid*

- [Setting] : VRRPv3 Group ID (1..255)
- [Initial value] : -
- *ipv6\_address*
  - [Setting] : IPv6 address of virtual router
  - [Initial value] : -
- *priority*
  - [Setting] : Priority (1..254)
  - [Initial value] : 100
- *preempt* : Preempt mode
  - [Setting] :

Setting	Description
on	Enable the VRRPv3
off	Disable the VRRPv3

- [Initial value] : on
- *auth*
  - [Setting] : Text string for authentication (8 characters or less)
  - [Initial value] : -
- *time1*
  - [Setting] : Interval time of VRRPv3 advertisement (1..60 seconds)
  - [Initial value] : 1
- *time2*
  - [Setting] : The time until detecting the down of master (3..180 seconds)
  - [Initial value] : 3

#### [Description]

Set whether to utilize specified VRRPv3 group or not.

VRID and IPv6 address of virtual router must be matched on the routers belonged to a VRRPv3 group.

When the *auth* parameter is not set, the authentication does not performed.

It is possible to set the interval time of VRRPv3 advertisement from master and the time until detecting the down of master by *time1* and *time2* parameter. VRRPv3 may be stable by setting these command parameters longer than the initial value. These parameters must be matched on routers belonged to same VRRP group.

#### [Note]

When own IPv6 address is set as IPv6 address of virtual router, *priority* and *preempt* parameters are ignored. In this case, *priority* is treated as 255 (top priority) and it works as preempt mode.

RTX810 supports this command in Rev.11.01.23 or later.

#### [Models]

RTX810

## 25.6.2 Set the Shutdown trigger

#### [Syntax]

```

ipv6 interface vrrp shutdown trigger vrid interface
ipv6 interface vrrp shutdown trigger vrid pp peer_num [dlsi=dlci]
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 route network

```

#### [Setting and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *vrid*
  - [Setting] : VRRPv3 Group ID (1..255)
  - [Initial value] : -
- *peer\_num*

- [Setting] : Peer number
- [Initial value] : -
- *dldi*
  - [Setting] : DLCI number
  - [Initial value] : -
- *network*
  - [Setting] :
    - IPv6 prefix/prefix length
    - default
  - [Initial value] : -
- *nextHop*
  - [Setting] :
    - Interface name
    - IPv6 address
  - [Initial value] : -

**[Description]**

Sets the router to shutdown according to the specified conditions when operating as a master router in the specified VRRPv3 group.

Type	Description
LAN interface type	Shut down when the link of the specified LAN interface is deactivated, or after a down detection by <b>lan keepalive</b> .
pp type	Shut down when communication is no longer possible on the line corresponding to the specified peer number. “Communication is no longer possible” refers to the case when layer 1 is deactivated such as when the cable is disconnected as well as the cases indicated below. <ul style="list-style-type: none"> <li>• When the router decides by the LCP keepalive function that the peer goes down if the line is an exclusive line</li> <li>• When the router detects that the peer is down through the <b>pp keepalive use</b> setting.</li> </ul>
route type	Shuts down if the specified route does not exist in the routing table or the route is not directed at the interface specified by <i>nextHop</i> or the gateways specified by an IPv6 address. If <i>nextHop</i> is omitted, the router does not shut down as long as the route exists regardless of where it is directed.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810

## 25.7 Filter Configuration

---

### 25.7.1 Define an IPv6 Filter

---

**[Syntax]**

```

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 and Initial value]**

- *filter\_num*
  - [Setting] : Static filter number (1..21474836)
  - [Initial value] : -
- *pass\_reject*
  - [Setting] : Filter type (conforms to the **ip filter** command)
  - [Initial value] : -
- *src\_addr*
  - [Setting] : Source IP address of the IP packet

- [Initial value] : -
- *prefix\_len*
  - [Setting] : Prefix length
  - [Initial value] : -
- *dest\_addr*
  - [Setting] : Destination IP address of the IP packet (same format as *src\_addr*). Same as one \* when omitted
  - [Initial value] : -
- *protocol* : Type of packets to be filtered (conforms to the **ip filter** command)
  - [Setting] :

icmp-nd	Keyword indicating the designation of packets related to neighbor discovery (ICMPv6 packets whose type is 133, 134, 135, or 136)
icmp4	Keyword indicating the designation of ICMPv4 packets
icmp	Keyword indicating the designation of ICMPv6 packets
icmp6	

- [Initial value] : -
- *src\_port\_list*
  - [Setting] : TCP/UDP source port number or ICMPv6 type (conforms to the **ip filter** command)
  - [Initial value] : -
- *dest\_port\_list*
  - [Setting] : TCP/UDP destination port number or ICMPv6 code
  - [Initial value] : -

**[Description]**

Defines an IPv6 filter.

**[Note]**

Packets related to neighbor discovery refers the following:

- 133: Router Solicitation
- 134: Router Advertisement
- 135: Neighbor Solicitation
- 136: Neighbor Advertisement

**[Example]**

```
Record IPv6 Packet Too Big packets that are sent and received through PP 1
# pp select 1
# ip pp secure filter in 1 100
# ip pp secure filter out 1 100
# ipv6 filter 1 pass-log * * icmp6 2
# ipv6 filter 100 pass * *
```

**[Models]**

RTX810, RTX5000

**25.7.2 Apply the IPv6 Filter****[Syntax]**

```
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 and Initial value]**

- *interface*
  - [Setting] : LAN, loopback, null, or bridge interface name
  - [Initial value] : -
- *direction*
  - [Setting] :

Setting	Description
in	Filtering of received packets
out	Filtering of packets to be transmitted

- [Initial value] : -
- *filter\_list*
  - [Setting] : Series of filter numbers delimited by spaces (total of the number of static filters and dynamic filters: up to 128)
  - [Initial value] : -
- *dynamic* : Specify the dynamic filter number immediately after the keyword
  - [Initial value] : -

**[Description]**

Applies the IPv6 filter to the interface.

**[Note]**

Dynamic filtering cannot be used with a loopback or null interface.

You cannot set *direction* to 'in' for a null interface.

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

### 25.7.3 Define a Dynamic IPv6 Filter

---

**[Syntax]**

**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 and Initial value]**

- *dyn\_filter\_num*
  - [Setting] : Dynamic filter number (1..21474836)
  - [Initial value] : -
- *srcaddr*
  - [Setting] : Source IPv6 address
  - [Initial value] : -
- *prefix\_len*
  - [Setting] : Prefix length
  - [Initial value] : -
- *dstaddr*
  - [Setting] : Destination IPv6 address
  - [Initial value] : -
- *protocol* : Protocol mnemonic
  - [Setting] :
    - 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
  - [Initial value] : -
- *filter\_list*
  - [Setting] : List of filter numbers registered by the **ipv6 filter** command
  - [Initial value] : -
- *option*
  - [Setting] :
    - syslog=*switch*

Setting	Description
on	Keep the communication log of the connection in SYSLOG
off	Not keep the communication log of the connection in SYSLOG

- timeout=*time*

Setting	Description
time	Number of seconds until the connection information is released after the data stops flowing

- [Initial value] :
  - syslog=on
  - timeout=60

### [Description]

Defines a dynamic IPv6 filter. In the first syntax, an application name registered in the router in advance is specified.

In the second syntax, the user specifies the access control rules. Following the keywords filter, in, and out, set a filter number defined by the **ipv6 filter** command.

If a connection (trigger) that corresponds to the filter specified after the filter keyword is detected, subsequent connections that correspond to the filter specified after the in keyword and out keyword are passed. The in keyword controls accesses in the reverse direction to the trigger direction, and the out keyword controls accesses in the same direction as the dynamic filter. The IP address in the **ipv6 filter** command is ignored. The pass/reject parameter is also ignored.

It may be possible to handle applications not listed here by creating definitions using the filter keyword. It is particularly easy to handle protocols of which the port number does not change dynamically such as snmp.

It may be possible to handle applications not listed here by specifying tcp or udp. Protocols of which the port number does not change dynamically as with telnet can be handled by specifying tcp.

### [Models]

RTX810, RTX5000

## 25.8 IPv6 Multicast Packet Forwarding Configuration

The router provides MLDv1, MLDv2, and MLD proxy functions. MLDv1 and MLDv2 are supported on both ends, host end and router end, and the host and router functions can be set separately for each interface. MLDv1 corresponds to RFC2710, and MLDv2 corresponds to draft-vida-mld-v2-07.txt. The MLD proxy is a function that relays listener information on the downstream interface to the upstream interface. It is implemented based on draft-ietf-magma-igmp-proxy-04.txt.

The router duplicates a multicast packet sent by a given terminal and delivers it to multiple terminals. The terminal sending the multicast packet is called a source, and the terminal receiving it is called a listener. In the explanation below, multicast packets are simply written as packets.

As a general rule, packets sent by a source reaches all listeners. However, if you wish to change the packets received by listeners, the listeners can be divided into groups. Terminals belonging to a same group receives the same packets, and terminals belonging to a different group receives different packets. A multicast address is assigned to each group as an identifier.

The destination address of the IP header of the packet stores the multicast address corresponding to a group. The routers in the network look at this multicast address to check the group to which the packet is to be forwarded. Because the routers in the network have a routing table organized by groups, the routers deliver the packet according to this table. The routing table is usually automatically generated through a routing protocol such as PIM-SM, PIM-DM, and DVMRP.

The purpose of the MLD (Multicast Listener Discovery) is for a terminal to notify the multicast network of the group in which the terminal will participate.

The router in the network sends a query message to the terminal. The terminal receiving the message returns a report message back to the router. The multicast address of the group in which the terminal will participate is stored in the report. The router receiving the report applies the information to the routing operation.

In MLDv2, the source receiving the packet can be limited. Filter mode and source list are used to achieve this function. In filter mode, sources that are allowed are listed in INCLUDE and sources that are not allowed are listed in EXCLUDE.

For example, only packets with the source set to 2001:x:x:x::1 and 2001:x:x:x::2 are forwarded in the next case.

- Filter mode: INCLUDE
- Source list: 2001:x:x:x::1, 2001:x:x:x::2



As a general rule, MLD messages cannot pass over routers. Therefore, if a router exists between the terminal and the multicast network, the router must have an MLD proxy function. A router with a MLD proxy function sends a query to the LAN interface and receives a report from it. In addition, the router forwards the information included in the report to the WAN interface.

### 25.8.1 Set the MLD Operation

#### [Syntax]

```
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 and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *type* : MLD operation type
  - [Setting] :

Setting	Description
off	Disable MLD
router	Operate as an MLD router
host	Operate as an MLD host

- [Initial value] : off
- *option* : Option
  - [Setting] :
    - version=*version*
      - MLD version

Setting	Description
1	MLDv1
2	MLDv2
1,2	Support both MLDv1 and MLDv2 (MLDv1 compatible mode)

- *syslog=switch*
  - Whether to output detailed information to syslog

Setting	Description
on	Show
off	Not show

- *robust-variable=VALUE(1..10)*
  - Set the robust variable value specified by MLD.
- [Initial value] :
  - version=1,2
  - syslog=off
  - robust-variable=2

#### [Description]

Sets the MLD operation of the interface.

#### [Models]

RTX810, RTX5000

### 25.8.2 Set Static MLD

#### [Syntax]

```
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 and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *group*
  - [Setting] : Group multicast address
  - [Initial value] : -
- *filter\_mode* : Filter mode
  - [Setting] :

Setting	Description
include	MLD “INCLUDE” mode
exclude	MLD “EXCLUDE” mode

- [Initial value] : -
- *source*
  - [Setting] :

Setting	Description
IPv6 address	Transmission source address of multicast packets
Omitted	When omitted, operate similarly to all transmission source addresses

- [Initial value] : -

**[Description]**

It is assumed that a listener always exists in the specified group. Set this command when there is no listener that supports MLD. *filter\_mode* and *source* are used to limit the transmission source of multicast packets.

If *filter\_mode* is set to include, list the *source* from which to receive multicast packets. When *source* is omitted, no request from any transmission source is received.

If *filter\_mode* is set to exclude, list the *source* from which not to receive multicast packets. When *source* is omitted, requests from all transmission sources are received.

**[Note]**

The listener set by this command is notified to the interface specified by host of the **ipv6 interface mld** command. If this interface uses MLDv1, the *filter\_mode* and *source* values are discarded.

**[Models]**

RTX810, RTX5000

## 25.9 Neighbor Solicitation

---

### 25.9.1 Set Whether to Respond to Address Duplication Checking by Performing Neighbor Solicitation

---

**[Syntax]**

```

ipv6 nd ns-trigger-dad on [option=value]
ipv6 nd ns-trigger-dad off
no ipv6 nd ns-trigger-dad [...]

```

**[Setting and Initial value]**

- on
  - [Setting] : Perform neighbor solicitation
  - [Initial value] : -
- off
  - [Setting] : Do not perform neighbor solicitation
  - [Initial value] : -
- *Sequence of option = value* : MLD operation type
  - [Setting] :

<i>option</i>	<i>value</i>	<b>Description</b>
na-proxy	all	After neighbor solicitation is performed, all neighbor advertisements to the source of the address duplication check are performed through proxy.
	discard-one-time	After neighbor solicitation is performed, the first neighbor advertisement to the source of the address duplication check is discarded, and subsequent advertisements are performed through proxy.

- [Initial value] : na-proxy=all

**[Initial value]**

ipv6 nd ns-trigger-dad off

**[Description]**

Sets whether to send neighbor solicitation upstream, taking the global address of a downstream neighbor solicitation through RA proxy for an address duplication check as the source.

**[Models]**

RTX810, RTX5000

## Chapter 26

### OSPFv3

#### 26.1 Applying OSPFv3

**[Syntax]**

**ipv6 ospf configure refresh**

**[Description]**

Applies OSPFv3 settings. If you change OSPFv3 settings, you must restart the router or execute this command.

**[Note]**

When entering this command, if any of the following are missing, the OSPFv3 settings will not be applied.

- Router ID not configured
- Area not configured
- Does not belong to any interface or area
- The area that the virtual link traverses does not exist
- There are no interfaces that belong to the area the virtual link traverses

If this command is entered when OSPFv3 settings are already applied, the settings will be reinitialized from their default state. As a result, any route information that OSPFv3 has maintained and route information distributed to other protocols will be completely discarded, and operation from the default state will begin.

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

#### 26.2 Enabling/disabling OSPFv3

**[Syntax]**

**ipv6 ospf use use**

**no ipv6 ospf use [use]**

**[Setting and Initial value]**

- *use*
- [Setting] :

Setting	Description
on	Enable OSPFv3
off	Disable OSPFv3

- [Initial value] : off

**[Description]**

Sets whether to use OSPFv3.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

#### 26.3 Setting the OSPFv3 router ID

**[Syntax]**

**ipv6 ospf router id router-id**

**no ipv6 ospf router id [router-id]**

**[Setting and Initial value]**

- *router\_id*
- [Setting] : IPv4 address notation (0.0.0.0 is not allowed)
- [Initial value] : -

**[Description]**

Sets the router ID.

**[Note]**

When the **ipv6 ospf configure refresh** command is entered, if the router ID has not been set by this command, the primary IPv4 address assigned to the interface is searched in the following order, and the first IPv4 address found is used as the router.

- LAN interface (from smallest number)
- LOOPBACK interface (from smallest number)

Moreover, if there is no interface with a primary IPv4 address, the initial value is not set.

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

## 26.4 Setting the OSPFv3 area

---

**[Syntax]**

```
ipv6 ospf area area [stub [cost=cost]]
no ipv6 ospf area area [stub [cost=cost]]
```

**[Setting and Initial value]**

- *area*
  - [Setting] :

Setting	Description
backbone	Backbone area
A value greater than or equal to 1 (1...4294967295)	Non-backbone area
IPv4 address notation (0.0.0.0 is not allowed)	Non-backbone area

- [Initial value] : -
- *cost*
  - [Setting] : Default route cost (0~16777215)
  - [Initial value] : 0

**[Description]**

Sets the OSPFv3 area.

If the stub keyword has been specified, that area will be expressed as a stub area. If *cost* is a value above 0, the area edge routers are used as the advertised route cost inside the area. If *cost* is not specified, the default route is not advertised.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

## 26.5 Advertising the route to an area

---

**[Syntax]**

```
ipv6 ospf area network area ipv6_prefix/prefix_len [restrict]
no ipv6 ospf area network area ipv6_prefix/prefix_len [restrict]
```

**[Setting and Initial value]**

- *area*
  - [Setting] :

Setting	Description
backbone	Backbone area
A value greater than or equal to 1 (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] : IPv6 prefix
- [Initial value] : Subnet range not configured

**[Description]**

The routes within the range of the subnet specified by this command are advertised as a single subnet route when an area border router advertises the route to another area. If the restrict keyword is specified, routes in the range, including aggregate routes, are not advertised.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

## 26.6 Setting the OSPFv3 area of the specified interface

---

**[Syntax]**

**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 and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *area*
  - [Setting] :

Setting	Description
backbone	Backbone area
A value greater than or equal to 1 (1...4294967295)	Non-backbone area
IPv4 address notation (0.0.0.0 is not allowed)	Non-backbone area

- [Initial value] : The interface does not belong to an OSPF area.
- *parameters*
  - [Setting] : Array of NAME=VALUE
  - [Initial value] :
    - type=broadcast (when specifying the LAN interface)
    - type=point-to-point (when a PP interface is specified when tunnel interface is specified)
    - passive=The interface is not passive
    - cost=1 (when a LAN interface is specified), 1562 (when a tunnel is specified), varies depending on the line speed for PP
    - priority=1
    - retransmit-interval=5 seconds
    - transmit-delay=1 second
    - hello-interval=10 seconds
    - dead-interval=40 seconds

**[Description]**

Sets the OSPFv3 area to which the specified interface belongs. The type keyword of the NAME parameter specifies the type of network link of the interface. Set the link parameters in *parameters* . Parameters are specified in the form NAME=VALUE. The following types are available.

NAME	VALUE	Description
type	broadcast	Broadcast
	point-to-point	Point to point

NAME	VALUE	Description
passive		Does not send OSPFv3 packets to the interface. Specify this parameter when there are no other OSPFv3 routers in the interface.
cost	Cost (1...65535)	Set the interface cost. The default value is determined by the interface type and the line speed. The cost is 1 for a LAN interface and 1562 for a tunnel interface. For a PP interface, the cost is calculated by the expression shown below, with the line speed of the bound lines denoted as S [kbit/s]. For example, the cost is 1562 for 64 kbit/s and 65 for 1.536 Mbit/s. cost=100000/S
priority	Priority (0...255)	Set the priority for selecting the designated router. The router with the largest PRIORITY value is selected as the designated router. If set to 0, the router is not selected as the designated router.
retransmit-interval	Number of seconds (1...65535)	Set the retransmission interval when sending LSAs consecutively.
transmit-delay	Number of seconds	Set the time when the LSA is sent after the link state changes in seconds.
hello-interval	Number of seconds (1...65535)	Set the transmission interval of HELLO packets in seconds.
dead-interval	Number of seconds (1...65535)	Set the time until the router decides that the peer (neighboring router) is down when HELLO cannot be received from the peer (neighboring router) in seconds.

**[Note]**

- Regarding the NAME parameter type

For the NAME parameter type, only broadcast can be specified for the LAN interface. When PPP is used for the PP interface or when the tunnel interface is used, only point-to-point can be specified.

- Specify the passive keyword when there are no other OSPFv3 routers in the network to which the interface is connected. When passive is specified, OSPFv3 packets are not sent from the interface. This suppresses unneeded traffic, and also prevents operation errors at the receiving end.

For a LAN interface (interface set to type=broadcast), the route to the network to which the interface is connected is not advertised to other OSPF routers unless the **ipv6 interface ospf area** command is specified. Therefore, for a LAN interface that connects to a network that does not use OSPF, the **ipv6 interface ospf area** command with the passive keyword attached can be specified to advertise the route to the network to other OSPF routers without using OSPF.

If the **ipv6 pp ospf area** command is not specified for a PP interface, the route to the network to which the interface is connected is handled as an AS external route. Because it is an AS external route, the **ipv6 ospf import** command must be specified to advertise the route to other OSPF routers.

- Regarding hello-interval/dead-interval

The hello-interval and dead-interval values must be the same among all neighboring routers with which the interface can directly communicate. If HELLO packets with parameter values that differ from the specified values are received, they are discarded. If the dead-interval is not specified, the value will be set to the hello-interval x 4.

- Regarding instance ID

The instance ID for the main unit is usually 0. When OSPFv3 packets are received, only packets with the same value will be accepted.

RTX810 supports this command in Rev.11.01.23 or later.

[Models]  
RTX5000

## 26.7 Setting the virtual link

### [Syntax]

```
ipv6 ospf virtual-link router_id area [parameters ...]
no ipv6 ospf virtual-link router_id [area [parameters...]]
```

### [Setting and Initial value]

- *router\_id*
  - [Setting] : Router ID of the peer of the virtual link
  - [Initial value] : -
- *area* : Area (which the virtual link traverses)
  - [Setting] :

Setting	Description
A value greater than or equal to 1 (1...4294967295)	Non-backbone area
IPv4 address notation (0.0.0.0 is not allowed)	Non-backbone area

- [Initial value] : -
- *parameters*
  - [Setting] : Array of NAME=VALUE
  - [Initial value] :
    - retransmit-interval=5 seconds
    - transmit-delay=1 second
    - hello-interval=10 seconds
    - dead-interval=40 seconds

### [Description]

Sets the virtual link. A virtual link is established to the router specified by *router\_id* by traversing the area specified by *area*. Parameters of the virtual link can be specified by *parameters*. The parameters are specified in the form NAME=VALUE. The following types are available.

NAME	VALUE	Description
retransmit-interval	Number of seconds (1...65535)	Set the retransmission interval when sending LSAs consecutively.
transmit-delay	Number of seconds (1...65535)	Set the time when the LSA is sent after the link state changes in seconds.
hello-interval	Number of seconds (1...65535)	Set the transmission interval of HELLO packets in seconds.
dead-interval	Number of seconds (1...65535)	Set the time until the router decides that the peer is down when HELLO cannot be received from the peer in seconds.

### [Note]

- Regarding hello-interval/dead-interval  
The hello-interval and dead-interval values must be the same among all neighbor routers with which the interface can directly communicate. If HELLO packets whose parameter values that differ from the specified values are received, they are discarded.
  - Regarding instance ID  
The instance ID for the main unit is usually 0. When OSPFv3 packets are received, only packets with the same value will be accepted.
  - Regarding output interface  
If a virtual link has been configured and the global address for the output interface to the area traversed is not assigned, the virtual link cannot be used.
- RTX810 supports this command in Rev.11.01.23 or later.



**[Models]**  
RTX810, RTX5000

## 26.8 Setting the level of preference of the OSPFv3 routing

---

### [Syntax]

```
ipv6 ospf preference preference
no ipv6 ospf preference [preference]
```

### [Setting and Initial value]

- *preference*
  - [Setting] : Level of preference of the OSPFv3 routing
  - [Initial value] : 2000

### [Description]

Sets the level of preference of the OSPFv3 routing. The level of preference is expressed by a value greater than or equal to 1. The larger the value, the higher is the level of preference. If the routes obtained from multiple protocols such as OSPFv3 and RIPng are in conflict, the one with the higher level of preference is used. If the level of preference is equal, the route adopted earlier in time is activated.

### [Note]

The level of preference of static routes is fixed at 10000.  
RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**  
RTX810, RTX5000

## 26.9 Setting whether to apply the route received through OSPFv3 to the routing table

---

### [Syntax]

```
ipv6 ospf export from ospf filter filter_num ...
no ipv6 ospf export from ospf [filter filter_num...]
```

### [Setting and Initial value]

- *filter\_num*
  - [Setting] : Filter number of the **ipv6 ospf export filter** command (1...2147483647)
  - [Initial value] : All routes are applied to the routing table

### [Description]

Sets whether to apply the route received through OSPFv3 to the routing table. Filters are evaluated in the specified order, and only the first route to match the filter is applied to the routing table. Routes that have been determined to be not for application and routes that do not match a filter are not applied.

If this command is not specified, all routes are applied to the routing table.

### [Note]

This command does not affect the link state database of OSPFv3. In other words, the operation of exchanging information with other routers using OSPFv3 does not change regardless of the setting of this command. This command only specifies whether the route calculated by OSPFv3 is used to actually route packets.

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**  
RTX810, RTX5000

## 26.10 Setting the filter for handling the route received through OSPFv3

---

### [Syntax]

```
ipv6 ospf export filter filter_num [nr] kind ipv6_prefix/prefix_len ...
no ipv6 ospf export filter filter_num[...]
```

### [Setting and Initial value]

- *filter\_num*
  - [Setting] : Filter number (1...2147483647)
  - [Initial value] : -
- *nr* : Filter interpretation method
  - [Setting] :

Setting	Description
not	Import routes that do not match the IPv6 prefix
reject	Do not import routes that match the IPv6 prefix

- [Initial value] : -
- *kind* : IPv6 prefix interpretation method
- [Setting] :

Setting	Description
include	Routes included in the specified IPv6 prefix (including the IPv6 prefix itself)
refines	Routes included in the specified IPv6 prefix (not including the IPv6 prefix itself)
equal	Routes that match the specified IPv6 prefix

- [Initial value] : -
- *ipv6\_prefix/prefix\_len*
  - [Setting] : IPv6 prefix
  - [Initial value] : -

### [Description]

Defines the filter that is applied when importing a route received from another OSPFv3 router into the routing table through OSPFv3. The filter defined by this command takes effect when it is specified by the *filter* section of the **ipv6 ospf export from** command.

Set the IPv6 prefix with *ipv6\_prefix/prefix\_len*. This parameter can be specified multiple times, and the *kind* parameter specifies how the route is checked.

include	Filtering is applied to routes that match the IPv6 prefix and routes included in the IPv6 prefix
refines	Filtering is applied to the routes included in the IPv6 prefix, but not the routes that match the IPv6 prefix
equal	Filtering is applied to only the routes that match the IPv6 prefix

If *nr* is omitted, the route is imported when any filter matches (there is at least one applicable IPv6 prefix). When not is specified, the route is imported when none of the IPv6 prefixes in the filter matches. When reject is specified, the route is not imported when the filter matches (there is at least one applicable IPv6 prefix).

### [Note]

Caution must be exercised when a filter specified by not is used multiple times with the **ipv6 ospf export from ospf** command. Whether an IPv6 prefix that matches a filter specified by not is imported is not determined by that filter, and the address is checked by the next filter specified by **ipv6 ospf export from ospf**. Therefore, for example, setting the filters as shown below results in all routes being imported and is meaningless.

```
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 imports routes other than fec0:12ab:34cd:1::/64, and the second filter imports routes other than fec0:12ab:34cd:2::/64. In other words, the route fec0:12ab:34cd:1::/64 does not match the first filter, but it is imported by the second filter. On the other hand, because route fec0:12ab:34cd:2::/64 matches the first filter, it is imported regardless of the second filter. This means that there are no routes that are not imported.

If you do not want to import routes fec0:12ab:34cd:1::/64 and fec0:12ab:34cd:2::/64, you must set the filters as shown below.

```
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
```

RTX810 supports this command in Rev.11.01.23 or later.

### [Models]

RTX810, RTX5000

## 26.11 Route import using external protocol

### [Syntax]

```
ipv6 ospf import from protocol [filter filter_num ...]
no ipv6 ospf import from [protocol [filter filter_num...]]
```

### [Setting and Initial value]

- *protocol* : External protocol to be imported in the OSPFv3 routing table
  - [Setting] :

Setting	Description
static	Static route
rip	RIPng

- [Initial value] : -
- *filter\_num*
  - [Setting] : **ipv6 ospf import filter** command filter number (1...2147483647)
  - [Initial value] : -

### [Description]

Sets whether to import the route by an external protocol into the OSPFv3 routing table. The imported route is announced as an AS external route to other OSPFv3 routers. Set *filter\_num* to the filter number defined by the **ipv6 ospf import filter** command. The route being imported from an external protocol is checked by the specified filter. The first route to match the filter is applied to the OSPFv3 routing table. Routes that have been determined to be not for application and routes that do not match a filter are not applied. If the filter number after the filter keyword is omitted, all routes are imported into OSPFv3.

The metric value and metric type parameters for announcing the route use the values specified by the **ipv6 ospf import filter** command that matched the filter check. If the keywords after filter are omitted, the following parameters are used.

- metric=1
- type=2

### [Note]

RTX810 supports this command in Rev.11.01.23 or later.

### [Models]

RTX810, RTX5000

## 26.12 Filters applied to the importing of AS external routes

### [Syntax]

```
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 and Initial value]

- *filter\_num*
  - [Setting] : Filter number (1...2147483647)
  - [Initial value] : -
- *nr* : Filter interpretation method
  - [Setting] :

Setting	Description
not	Import routes that do not match the IPv6 prefix
reject	Do not import routes that match the IPv6 prefix

- [Initial value] : -
- *kind* : IPv6 prefix interpretation method
  - [Setting] :

Setting	Description
include	Routes included in the specified IPv6 prefix (including the IPv6 prefix itself)

Setting	Description
refines	Routes included in the specified IPv6 prefix (not including the IPv6 prefix itself)
equal	Routes that match the specified IPv6 prefix

- [Initial value] : -
- *ipv6\_prefix/prefix\_len*
  - [Setting] : IPv6 prefix
  - [Initial value] : -
- *parameters* : Parameter for announcing AS external routes
  - [Setting] :

Setting	Description
metric = <i>metric</i>	Metric value (1 ~ 16777215)
type = <i>type</i>	Metric type (1 or 2)

- [Initial value] : -

### [Description]

Defines the filter to be applied when importing external routes into the OSPFv3 routing table. The filter defined by this command takes effect when it is specified by the filter section of the **ipv6 ospf import from** command.

Set the IPv6 prefix with *ipv6\_prefix/prefix\_len*. This parameter can be specified multiple times, and the *kind* parameter specifies the interpretation method.

include	Filtering is applied to routes that match the IPv6 prefix and routes included in the IPv6 prefix
refines	Filtering is applied to the routes included in the IPv6 prefix, but not the routes that match the IPv6 prefix
equal	Filtering is applied to only the routes that match the IPv6 prefix

If *nr* is omitted, if there is at least one applicable IPv6 prefix, the filter matches and the route is imported. When not is specified, the route is imported when none of the IPv6 prefixes in the filter matches. When reject is specified, the route is not imported when the filter matches (there is at least one applicable IPv6 prefix).

In *parameters*, the parameter metric value and metric type for advertising the imported route as an AS external route of OSPFv3 can be specified by metric and type. If these keywords are omitted, the following values are used.

- metric=1
- type=2

### [Note]

Caution must be exercised when a filter specified by not is used multiple times with the **ipv6 ospf import from** command. Whether an IPv6 prefix that matches a filter specified by not is imported is not determined by that filter, and the address is checked by the next filter specified by **ipv6 ospf import from**. Therefore, for example, setting the filters as shown below results in all routes being imported and is meaningless.

```
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 imports routes other than fec0:12ab:34cd:1::/64, and the second filter imports routes other than fec0:12ab:34cd:2::/64. In other words, the route fec0:12ab:34cd:1::/64 does not match the first filter, but it is imported by the second filter. On the other hand, because route fec0:12ab:34cd:2::/64 matches the first filter, it is imported regardless of the second filter. This means that there are no routes that are not imported.

If you do not want to import routes fec0:12ab:34cd:1::/64 and fec0:12ab:34cd:2::/64, you must set the filters as shown below.

```
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
```

RTX810 supports this command in Rev.11.01.23 or later.

### [Models]

RTX810, RTX5000

## 26.13 Setting the OSPFv3 log output

---

### [Syntax]

```
ipv6 ospf log log ...  
no ipv6 ospf log [log...]
```

### [Setting and Initial value]

- *log*
- [Setting] :

Setting	Description
interface	Log for interface state and virtual links
neighbor	Log for neighbor router state
packet	Log for OSPFv3 packets

- [Initial value] : No logs of any type are output

### [Description]

Sets the type of log output for OSPFv3

### [Note]

RTX810 supports this command in Rev.11.01.23 or later.

### [Models]

RTX810, RTX5000

## Chapter 27

### Triggered Mail Notification Function

This function detects a preset trigger and notifies the details in a mail.

When a trigger specified by the **mail notify** command is detected, a message is created based on the mail template specified by the **mail template** command, and a mail describing the detected trigger content is sent using the mail server specified by the **mail server smtp** command.

The following SMTP authentication are supported: CRAM-MD5, DIGEST-MD5, and PLAIN. POP-before-SMTP is also supported.

#### 27.1 Set the Mail Configuration ID Name

##### [Syntax]

**mail server name** *id name*

**no mail server name** *id [name]*

##### [Setting and Initial value]

- *id*
  - [Setting] : Mail server configuration ID (1..10)
  - [Initial value] : -
- *name*
  - [Setting] : ID name
  - [Initial value] : -

##### [Description]

Sets the mail configuration ID name. If the ID name contains spaces, enclose the name in double quotation marks.

##### [Models]

RTX810, RTX5000

#### 27.2 Set the SMTP Mail Server

##### [Syntax]

**mail server smtp** *id address [port=port] [smtp-auth username password [auth\_protocol]] [pop-before-smtp]*

**no mail server smtp** *id [...]*

##### [Setting and Initial value]

- *id*
  - [Setting] : Mail server configuration ID (1..10)
  - [Initial value] : -
- *address*
  - [Setting] : IP address or host name of the server
  - [Initial value] : -
- *port*
  - [Setting] : Server port number (25 when omitted)
  - [Initial value] : -
- *username*
  - [Setting] : User name for authentication
  - [Initial value] : -
- *password*
  - [Setting] : Password for authentication
  - [Initial value] : -
- *auth\_protocol* : SMTP-AUTH authentication protocol
  - [Setting] :

Setting	Description
cram-md5	CRAM-MD5
digest-md5	DIGEST-MD5
plain	PLAIN authentication

- [Initial value] : -

- `pop-before-smtp`
  - [Setting] : Use POP before SMTP
  - [Initial value] : -

**[Description]**

Sets the server information used to send mail.

Specify the data (user name and password) for SMTP authentication when sending mail with the `smtp-auth` parameter. There is no need to set `smtp-auth` if authentication is not needed on the SMTP server.

The SMTP authentication protocols that are supported are CRAM-MD5, DIGEST-MD5, and PLAIN authentication. If a protocol is specified by the `smtp-auth` parameter, that protocol is used. If the protocol is omitted, authentication is negotiated in the order given above with the SMTP server.

If the `pop-before-smtp` parameter is specified, POP before SMTP is carried out when sending mail. The POP operation uses the same ID specified by the **mail server pop** command. If the `pop-before-smtp` parameter is specified but the corresponding setting by the **mail server pop** command is not available, mails cannot be sent.

**[Models]**

RTX810, RTX5000

## 27.3 Set the POP Mail Server

---

**[Syntax]**

**mail server pop** *id address [port=*port*] protocol username password*

**no mail server pop** *id [...]*

**[Setting and Initial value]**

- *id*
  - [Setting] : Mail server configuration ID (1..10)
  - [Initial value] : -
- *address*
  - [Setting] : IP address or host name of the server
  - [Initial value] : -
- *port*
  - [Setting] : Server port number (110 when omitted)
  - [Initial value] : -
- *protocol*
  - [Setting] :

Setting	Description
pop3	POP3
apop	APOP

- [Initial value] : -
- *username*
  - [Setting] : User name for authentication
  - [Initial value] : -
- *password*
  - [Setting] : Password for authentication
  - [Initial value] : -

**[Description]**

Sets the server information used to receive mail.

This setting is necessary when the `pop-before-smtp` parameter of the **mail server smtp** command is specified.

**[Models]**

RTX810, RTX5000

## 27.4 Set the Timeout Value for Mail Processing

---

**[Syntax]**

**mail server timeout** *id timeout*

**no mail server timeout** *id [timeout]*

**[Setting and Initial value]**

- *id*
  - [Setting] : Mail server configuration ID (1..10)
  - [Initial value] : -
- *timeout*
  - [Setting] : Timeout value (1..600 seconds)
  - [Initial value] : 60

**[Description]**

Sets the timeout value for processing the mail exchange.

If the processing of the mail does not finish within the specified time, the processing is aborted. After the wait time specified by the **mail template** command (30 seconds by default) elapses, the processing of the mail is started from the beginning. The restarting of the process is carried out up to three times excluding the first processing of the mail. If the maximum count is exceeded, the processing of the mail fails.

**[Models]**

RTX810, RTX5000

## 27.5 Set the Template Used to Send Mail

---

**[Syntax]**

**mail template** *template\_id mailserv\_id* From:*from\_address* To:*to\_address* [Subject:*subject*] [Date:*date*] [MIME-Version:*mime\_version*] [Content-Type:*content\_type*] [notify-log=*switch*] [notify-wait-time=*sec*]

**no mail template** *template\_id* [...]

**[Setting and Initial value]**

- *template\_id*
    - [Setting] : Mail template ID (1..10)
    - [Initial value] : -
  - *mailserv\_id*
    - [Setting] : Mail server ID used by this template (1..10)
    - [Initial value] : -
  - *from\_address*
    - [Setting] : Source mail address (From)
    - [Initial value] : -
  - *to\_address*
    - [Setting] : Destination mail address
    - [Initial value] : -
  - *subject*
    - [Setting] : Subject when sending mail
    - [Initial value] : Backup Info/Route Change Info/Filter Info/Status Info/Intrusion Info/QAC/TM Info
  - *date*
    - [Setting] : Time displayed in the mail header
    - [Initial value] : Time when sending mail
  - *mime\_version*
    - [Setting] : MIME-Version displayed in the mail header
    - [Initial value] : 1.0
  - *content\_type*
    - [Setting] : Content-Type displayed in the mail header
    - [Initial value] : text/plain;charset=iso-2022-jp
  - *switch*
    - [Setting] :

Setting	Description
on	Include syslog information in notification mails
off	Not include syslog information in notification mails
  - [Initial value] : off
- *sec*
  - [Setting] : Wait time until the notification mail is actually sent (1..86400 second)
  - [Initial value] : 30



**[Description]**

Sets the mail server configuration ID, source mail address, destination mail address, and header information that are used when sending mail.

Specify the source mail address with *from\_address*. Only one source mail address can be specified.

Specify the destination mail addresses with *to\_address*. Multiple destination mail addresses can be specified.

When specifying multiple addresses, delimit each address with a comma. Do not insert a space.

Only local-part@domain or local-part@ipaddress format of mail addresses are supported. Formats such as “NAME>local-part@domain<” are not supported.

Specify the subject of the mail with *subject*. If the subject includes a space, enclose the entire Subject:*subject* in double quotation marks.

Specify the time in the format indicated in RFC822 for *date*. Because the RFC822 format always includes a space, the entire Date:*date* must be enclosed in double quotation marks.

The type/subtype that can be specified in *content-type* is “text/plain” only. Only “charset=us-ascii” and “charset=iso-2022-jp” are supported as parameters.

**[Note]**

The required mail header information is the source mail address and destination mail address.

**[Example]**

```
mail template 1 1 From:test@test.com To:test1@test.com,test2@test.com
"Subject:Test Mail" notify-log=on
mail template 1 2 From:test@test.com To:test1@test.com
"Subject:RTX810 test" "Date:Tue Apr 2 14:31:48 2013 +0000"
MIME-Version:1.0 "Content-Type:text/plain; charset=iso-2022-jp"
```

**[Models]**

RTX810, RTX5000

## 27.6 Set the Mail Notification Trigger

---

**[Syntax]**

**mail notify** *id template\_id* trigger backup *if\_b* [*range\_b*] *if\_b* ...]]

**mail notify** *id template\_id* trigger route *route* [*route* ...]

**mail notify** *id template\_id* trigger filter ethernet *if\_f dir\_f* [*if\_f dir\_f* [...]]

**mail notify** *id template\_id* trigger status *type* [*type* [...]]

**mail notify** *id template\_id* trigger intrusion *if\_i* [*range\_i*] *dir\_i* [*if\_i* [*range\_i*] *dir\_i* [...]]

**no mail notify** *id* [...]

**[Setting and Initial value]**

- *id*
  - [Setting] : Setup number (1..10)
  - [Initial value] : -
- *template\_id*
  - [Setting] : Template ID (1..10)
  - [Initial value] : -
- *if\_b* : Backup interface for performing the mail notification
  - [Setting] :

Setting	Description
pp	PP backup
lanN	LAN backup
tunnel	TUNNEL backup

- [Initial value] : -
- *range\_b*
  - [Setting] :
    - Interface number and range specification
    - Only pp or tunnel (\*,xx-yy,zz etc)
  - [Initial value] : -
- *route*
  - [Setting] : Route with the netmask

- [Initial value] : -
- *if\_f*
  - [Setting] : LAN interface on which the filter for performing mail notification is set
  - [Initial value] : -
- *dir\_f* : Filter setting direction
  - [Setting] :

Setting	Description
in	Receive direction
out	Send direction

- [Initial value] : -
- *type* : Information included in the mail notification
  - [Setting] :

Setting	Description
all	All information
interface	Interface information
routing	Routing information
vpn	VPN information
nat	NAT information
firewall	Firewall information
config-log	Configuration and log information

- [Initial value] : -
- *if\_i* : Unauthorized access detection setup interface
  - [Setting] :

Setting	Description
pp	PP interface
lanN(N,M,N/M)	LAN interface
wan1	WAN interface
tunnel	TUNNEL interface
*	All interfaces

- [Initial value] : -
- *range\_i*
  - [Setting] :
    - Interface number and range specification
    - lan(\*,x)
    - pp,tunnel(\*,x,xx-yy,zz etc)
  - [Initial value] : -
- *dir\_i* : Unauthorized access detection setup direction
  - [Setting] :

Setting	Description
in	Receive direction
out	Send direction
in/out	Receive and send directions

- [Initial value] : -

#### [Description]

Sets the trigger operation for the mail notification. Backup, route change, Ethernet filter log display, the **mail notify status exec** command execution, and unauthorized access can be specified as triggers.

The items set by the following commands are applicable for backup and route.

PP backup	<b>pp backup</b> command
LAN backup	<b>lan backup</b> command
TUNNEL backup	<b>tunnel backup</b> command
Route backup	<b>ip route</b> command

Ethernet filters that are displayed in the log are applicable.

Ethernet filter.....

pass-log and reject-log parameter definitions

The **mail notify status exec** command must be executed for the internal condition to be reported.

When unauthorized access detection notification is enabled, mail notifications are sent for items that are detected by the **ip interface intrusion detection** command.

In addition, mail notification settings belonging to a single template ID are processed collectively.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Example]**

```
mail notify 1 1 trigger backup pp * lan2 lan3 tunnel 1-10,12
mail notify 2 1 trigger route 192.168.1.0/24 172.16.0.0/16
mail notify 3 1 trigger filter ethernet lan1 in
mail notify 4 1 trigger status all
mail notify 5 1 trigger intrusion lan1 in/out pp * in tunnel 1-3,5 out
```

**[Models]**

RTX810, RTX5000

## Chapter 28

### HTTP Server Function

#### 28.1 Common Configuration

##### 28.1.1 Enable/Disable the HTTP Server Function

**[Syntax]**

**httpd service** *switch*

**no httpd service**

**[Setting and Initial value]**

- *switch*

- [Setting] :

Setting	Description
on	Enable the HTTP server function
off	Disable the HTTP server function

- [Initial value] : on

**[Description]**

Selects whether to enable the HTTP server.

**[Models]**

RTX810

##### 28.1.2 Set the IP Address of the Host Allowed to Access the HTTP Server

**[Syntax]**

**httpd host** *ip\_range* [*ip\_range*]

**httpd host any**

**httpd host none**

**httpd host lan**

**no httpd host**

**[Setting and Initial value]**

- *ip\_range* : IP address of the host to allow access to the HTTP server or a mnemonic

- [Setting] :

Setting	Description
The IP address can be a single address, two IP addresses with a hyphen in between them (range designation)	Allow access from a specified host
lanN	Allow access from a specified LAN interface
wanN	Allow access from a specified WAN interface
bridgeN	Allow access from a specified bridge interface
vlanN	Allow access from a specified VLAN interface

- [Initial value] : -

- *any* : Allow access from all hosts

- [Initial value] : -

- *none* : Prohibit access from all hosts

- [Initial value] : -

- *lan* : Allow access from all LAN interface

- [Initial value] : lan

**[Description]**

Sets the hosts to allow access to the HTTP server.

**[Note]**

If the LAN interface is specified by this command, access from IP addresses excluding the network address and limited broadcast address is allowed. If neither the primary or secondary address is set on the specified LAN interface, access is not allowed.

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

**[Models]**

RTX810

### 28.1.3 Set the Session Timeout Value of the HTTP Server

---

**[Syntax]**

**httpd timeout** *time*

**no httpd timeout** [*time*]

**[Setting and Initial value]**

- *time*
  - [Setting] : Number of seconds (1..180)
  - [Initial value] : 5

**[Description]**

Sets the timeout value of the HTTP server.

**[Note]**

If this timeout occurs when accessing the router over the Internet, set a large value with this command.

**[Models]**

RTX810

### 28.1.4 Set the Listen Port of the HTTP Server Function

---

**[Syntax]**

**httpd listen** *port*

**no httpd listen**

**[Setting and Initial value]**

- *port*
  - [Setting] : Port number (1..65535)
  - [Initial value] : 80

**[Description]**

Sets the listen port of the HTTP server.

**[Models]**

RTX810

### 28.1.5 Set the GUI Language

---

**[Syntax]**

**httpd language** *language*

**httpd language file** *name*

**no httpd language**

**[Setting and Initial value]**

- *language*
  - [Setting] :

Setting	Description
english	Displays the GUI in English.
japanese	Displays the GUI in Japanese.

- [Initial value] : english
- *name* : Language file name
- [Setting] :

Setting	Description
<i>filename</i>	File name in RTFS
usb1: <i>filename</i>	File name in USB memory
sd1: <i>filename</i>	File name in microSD card

- [Initial value] : -

**[Description]**

Sets the language to use for GUI.

**[Note]**

If there is no language file, it will run in English.

**[Models]**

RTX810

### 28.1.6 Set the PP Interface and Tunnel Interface Names

---

**[Syntax]**

**pp name** *name*

**tunnel name** *name*

**no pp name**

**no tunnel name**

**[Setting and Initial value]**

- *name*
  - [Setting] : Name (up to 64 characters)
  - [Initial value] : -

**[Description]**

Sets the PP interface or tunnel interface name.

**[Note]**

This command can be used only through the Basic configuration page.

**[Models]**

RTX810

## 28.2 Set the Basic configuration page

---

The commands in this chapter are used to register provider connection information on the Basic configuration page of the RTX810. The information is automatically set by clicking the Apply button. Because using the commands in this chapter changes the information registered on the Basic configuration page, use them only after thoroughly understanding the function and operation of each command.

Information of up to 10 providers can be registered on the Basic configuration page. The **provider set** command is used to associate the provider with a preset peer number.

The **no provider set** command is used to clear the association.

Use the **provider select** command to select a preset provider. If the provider is changed with this command, items that are required to connect to the provider such as the DNS and default route are changed automatically.

You can check the provider setting status on the Basic configuration page or by using the **show config** command.

### 28.2.1 Set the Provider Connection Type

---

**[Syntax]**

**provider type** *provider\_type*

**no provider type** [*provider\_type*]

**[Setting and Initial value]**

- *provider\_type*
  - [Setting] :

Setting	Description
isdn-terminal	PPPoE terminal connection

Setting	Description
isdn-network	PPPoE network connection
none	None

- [Initial value] : none

#### [Description]

Sets the provider connection type.

#### [Models]

RTX810

### 28.2.2 Associate the Provider Information to PP and Assign the Name

---

#### [Syntax]

```
provider set peer_num [name]
no provider set peer_num [name]
```

#### [Setting and Initial value]

- *peer\_num*
  - [Setting] : Peer number
  - [Initial value] : -
- *name*
  - [Setting] : Name (up to 32 characters)
  - [Initial value] : -

#### [Description]

Register providers so that you can arbitrarily switch among different providers.

The associated peer number is handled as a provider. This command is invalid for peer numbers that are not configured.

#### [Models]

RTX810

### 28.2.3 Set the Provider Connection

---

#### [Syntax]

```
provider select peer_num
no provider select peer_num
```

#### [Setting and Initial value]

- *peer\_num*
  - [Setting] : Peer number
  - [Initial value] : -

#### [Description]

Selects the provider information and configures the parameters so that it can be used.

When this command is executed, the default route, DNS server, schedule, and the like are changed based on the information recorded in various provider setup commands.

This command is also executed and the destination is switched, when the destination is changed or manual connection is made in the Basic configuration Provider Connection Setting.

The commands that are overwritten through this command are as follows:

All provider information: **pp disable**

Selected provider information: **pp enable**, **ip route**, **dns server**, and **schedule at**.

#### [Note]

This command is invalid for peer numbers that are not set in the **provider set** command.

#### [Models]

RTX810

### 28.2.4 Setting the DNS Server Address of the Provider

---

#### [Syntax]

```
provider dns server peer_num ip_address [ip_address..]
no provider dns server peer_num [ip_address..]
```

**[Setting and Initial value]**

- *peer\_num*
  - [Setting] : Peer number
  - [Initial value] : -
- *ip\_address*
  - [Setting] : IP address of the DNS server (up to four)
  - [Initial value] : -

**[Description]**

Sets the DNS server address as provider-specific information.  
When a provider is selected, this address is overwritten by the **dns server** command.

**[Note]**

This command is invalid for peer numbers that are not set in the **provider set** command.  
When deleting the information, the setting of the **dns server** command is not cleared. Only the information set by the **provider dns server** command is cleared.

**[Models]**

RTX810

### 28.2.5 Set the DNS Server Address of the LAN Interface

---

**[Syntax]**

```
provider interface dns server ip_address [ip_address..]
no provider interface dns server [ip_address [ip_address]]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *ip\_address*
  - [Setting] : IP address of the DNS server (up to two)
  - [Initial value] : -

**[Description]**

Sets the DNS server IP address of the LAN interface as provider information on the Basic configuration page.

**[Models]**

RTX810

### 28.2.6 Set the Peer Number from Which the DNS Server Is to Be Notified

---

**[Syntax]**

```
provider dns server pp peer_num dns_peer_num
no provider dns server pp peer_num [dns_peer_num]
```

**[Setting and Initial value]**

- *peer\_num*
  - [Setting] : Peer number (1..30)
  - [Initial value] : -
- *dns\_peer\_num*
  - [Setting] : DNS notification peer number (1..30)
  - [Initial value] : -

**[Description]**

Sets the peer number from which the DNS server is to be notified as provider information.

**[Models]**

RTX810

### 28.2.7 Set the Type of Filter Type Routing

---

**[Syntax]**

```
provider filter routing type
no provider filter routing [type]
```



**[Setting and Initial value]**

- *type* : Type of filter type routing
  - [Setting] :

Setting	Description
off	The default destination changes automatically when a manual connection is made using Basic configuration.
connection	The active default route is selected only during auto connection when manual connection is made using Basic configuration. When the manual connection is disconnected, connection is made to the default destination.

- [Initial value] : off

**[Description]**

Command dedicated to Basic configuration. Sets the type of filter type routing that is selected on the Basic configuration page.

**[Note]**

The operation is not guaranteed when specified on the console.

**[Models]**

RTX810

## 28.2.8 Set the Provider Name of the LAN Interface

---

**[Syntax]**

```
provider interface name type:name
no provider interface name [type:name]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *protocol*
  - [Setting] :

Setting	Description
ipv4	Provider setting name using ipv4 address
ipv6	Provider setting name using ipv6 address

- [Initial value] : -
- *type*
  - [Setting] : Provider information ID information (e.g. "PRV")
  - [Initial value] : -
- *name*
  - [Setting] : Provider name that the user assigned, etc.
  - [Initial value] : -

**[Description]**

Identification command dedicated to Basic configuration. Sets the provider name or the like entered on the Basic configuration page.

The *protocol* option can be omitted. If omitted, the provider setting name using ipv4 address will be used.

**[Models]**

RTX810

## 28.2.9 Set the NTP Server

---

**[Syntax]**

```
provider ntpdate server_name
no provider ntpdate [server_name]
```

**[Setting and Initial value]**

- *server\_name*
  - [Setting] : NTP server name (IP address or FQDN)
  - [Initial value] : -

**[Description]**

Command dedicated to Basic configuration.

Sets one NTP server. The **provider ntp server** command sets the IP address information for each destination.

This command sets the IP address or FQDN of a single location.

**[Note]**

The operation is not guaranteed when manually specified on the console.

**[Models]**

RTX810

### 28.2.10 Setting the NTP Server Address of the Provider

---

**[Syntax]**

```
provider ntp server peer_num ip_address
no provider ntp server peer_num [ip_address]
```

**[Setting and Initial value]**

- *peer\_num*
  - [Setting] : Peer number
  - [Initial value] : -
- *ip\_address*
  - [Setting] : IP address of the NTP server
  - [Initial value] : -

**[Description]**

Sets the NTP server address as provider-specific information.

When an IP address is set with this command, the time is periodically queried when the respective provider is selected. The time query to the NTP server is entered in the schedule when the provider is selected.

**[Note]**

This command is invalid for peer numbers that are not set in the **provider set** command.

**[Models]**

RTX810

### 28.2.11 Set Whether to Automatically Connect When the Disconnect Button Is Pressed on the Basic configuration page

---

**[Syntax]**

```
provider auto connect forced disable switch
no provider auto connect forced disable [switch]
```

**[Setting and Initial value]**

- *switch*
  - [Setting] :

Setting	Description
on	Disable auto connection
off	Enable auto connection

- [Initial value] : off

**[Description]**

Set whether to automatically connect when the Disconnect button is pressed on the Basic configuration page.

**[Note]**

If set to off, the **pp enable** command is automatically set after the manual disconnect button is pressed on the Basic configuration page, after the **pp disable** command, and after the connection button is pressed.

Therefore, automatic connection is disabled after the Disconnect button is pressed. In addition, the **connect** command cannot be used to establish a connection. To connect, you must press the manual connection button or restart the router.

**[Models]**

RTX810

### 28.2.12 Set Whether to Carry Out IPv6 Connection on the Basic configuration page

---

#### [Syntax]

```
provider ipv6 connect pp peer_num connect
no provider ipv6 connect pp peer_num [connect]
```

#### [Setting and Initial value]

- *peer\_num*
  - [Setting] : Peer number
  - [Initial value] : -
- *connect*
  - [Setting] :

Setting	Description
on	Connect
off	Do not connect

- [Initial value] : off

#### [Description]

Sets whether to enable IPv6 connection as provider information on the Basic configuration page.

#### [Note]

This command is automatically turned on when IPv6 connection is set on the Basic configuration page.

#### [Models]

RTX810

### 28.2.13 Association Between Provider Information of a LAN Interface and Tunnel

---

#### [Syntax]

```
provider interface bind tunnel_num...
no provider interface bind [tunnel_num...]
```

#### [Setting and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *tunnel\_num*
  - [Setting] : Tunnel interface number
  - [Initial value] : -

#### [Description]

Sets the association between the provider information of the LAN interface and the tunnel.

#### [Models]

RTX810

## Chapter 29

### NetVolante DNS Service Configuration

NetVolante DNS is a type of dynamic DNS function. You can use it to register the router's IP address to Yamaha's NetVolante DNS server under a desired name. NetVolante can be used for Web server establishment, access point management, etc., in a dynamic IP address environment. Because NetVolante uses a unique protocol for IP address registration and updating, it is not compatible with other dynamic DNS services.

The Yamaha NetVolante DNS server is currently free of charge and not warranted. There is no cost to use the server, but there is also no guarantee that you will be able to register a desired name or look up a name that has been registered. Also, please be aware that the NetVolante server may go down without prior notice.

There are two NetVolante DNS services: a host address service and a telephone number service, but the telephone number service cannot be used by the models discussed in this manual.

Because the NetVolante DNS server identifies individual RT series and NetVolante series routers by their MAC addresses, there is no guarantee that you will be able to use the same name when you switch devices.

#### 29.1 Set Whether to Use the NetVolante DNS Service

##### [Syntax]

```
netvolante-dns use interface switch
netvolante-dns use pp switch
no netvolante-dns use interface [switch]
no netvolante-dns use pp [switch]
```

##### [Setting and Initial value]

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *switch*
  - [Setting] :

Setting	Description
auto	Update automatically
off	Do not update automatically

- [Initial value] : auto

##### [Description]

Sets whether to use the NetVolante DNS service.  
The NetVolante DNS server is notified automatically when the IP address is updated.

##### [Note]

RTX5000 does not support WAN interface for *interface* parameter.

##### [Models]

RTX810, RTX5000

#### 29.2 Manually Update the Data on the NetVolante DNS Server

##### [Syntax]

```
netvolante-dns go interface
netvolante-dns go pp peer_num
```

##### [Setting and Initial value]

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Peer number
  - [Initial value] : -

**[Description]**

Manually updates the IP address on the NetVolante DNS server.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 29.3 Delete Data from the NetVolante DNS Server

---

**[Syntax]**

```
netvolante-dns delete go interface [host]
netvolante-dns delete go pp peer_num [host]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Peer number
  - [Initial value] : -
- *host*
  - [Setting] : Host name
  - [Initial value] : -

**[Description]**

Deletes the registered IP address from the NetVolante DNS server.  
You can just delete the host name by specifying the host name after the interface.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 29.4 Set the Port Number to Use for the NetVolante DNS Service

---

**[Syntax]**

```
netvolante-dns port port
no netvolante-dns port [port]
```

**[Setting and Initial value]**

- *port*
  - [Setting] : Port number (1..65535)
  - [Initial value] : 2002

**[Description]**

Sets the port number to use for the NetVolante DNS service.

**[Models]**

RTX810, RTX5000

## 29.5 Acquire a List of Registered Host Names from the NetVolante DNS Server

---

**[Syntax]**

```
netvolante-dns get hostname list interface
netvolante-dns get hostname list pp peer_num
netvolante-dns get hostname list all
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *peer\_num*

- [Setting] : Peer number
- [Initial value] : -
- all : All interfaces
  - [Initial value] : -

**[Description]**

Acquires a list of registered host names from the NetVolante DNS server and displays them.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 29.6 Register a Host Name

---

**[Syntax]**

```
netvolante-dns hostname host interface host [duplicate]
netvolante-dns hostname host pp host [duplicate]
no netvolante-dns hostname host interface [host [duplicate]]
no netvolante-dns hostname host pp [host [duplicate]]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *host*
  - [Setting] : Host name (up to 63 characters)
  - [Initial value] : -

**[Description]**

Sets the host name to use with the NetVolante DNS service (host address service). Host names acquired from the NetVolante DNS server have the following format: (host name).(subdomain).netvolante.jp. You can set the host name. The subdomain is assigned by the NetVolante DNS server. You cannot specify the subdomain.

When you first use this command, just specify the host name. Once registration and updating have been performed successfully on the NetVolante DNS server, the command is saved in the complete FQDN format shown above.

You can register the same name for different interfaces on the same router by adding the duplicate keyword.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 29.7 Set the Communication Timeout

---

**[Syntax]**

```
netvolante-dns timeout interface time
netvolante-dns timeout pp time
no netvolante-dns timeout interface [time]
no netvolante-dns timeout pp [time]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *time*
  - [Setting] : Timeout value in seconds (1..180)
  - [Initial value] : 90

**[Description]**

Set the amount of time after which the communication between the router and the NetVolante server times out in seconds.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 29.8 Set Whether to Automatically Generate the Host Name

---

**[Syntax]**

```
netvolante-dns auto hostname interface switch
netvolante-dns auto hostname pp switch
no netvolante-dns auto hostname interface [switch]
no netvolante-dns auto hostname pp [switch]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *switch*
  - [Setting] :

Setting	Description
on	Automatically generate
off	Do not automatically generate

- [Initial value] : off

**[Description]**

Sets whether to use the automatic host name generation function. Host names are automatically generated in the following format: y + (last 6 digits of the MAC address).auto.netvolante.jp.

When you set this command to 'on' and execute the **netvolante-dns go** command, the NetVolante DNS server automatically assigns the host name described above to the router. You can check the assigned domain name by executing the **show status netvolante-dns** command.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 29.9 Register the Router's Serial Number as the Host Name

---

**[Syntax]**

```
netvolante-dns set hostname interface serial
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name, WAN interface name, or "pp"
  - [Initial value] : -

**[Description]**

Sets the command for using a host name containing a router serial number automatically.

When you perform this command, the **netvolante-dns hostname host** command is executed.

For example, when a router serial number is D000ABCDE and you perform the **netvolante-dns set hostname pp serial** command, the **netvolante-dns hostname host pp server=1 SER-D000ABCDE** command is executed.

**[Note]**

The sub-domain cannot be specified by a user.

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 29.10 Set the NetVolante DNS Server Location

---

**[Syntax]**

```
netvolante-dns server ip_address
```

**netvolante-dns server** *name*  
**no netvolante-dns server** [*ip\_address*]  
**no netvolante-dns server** [*name*]

**[Setting and Initial value]**

- *ip\_address*
  - [Setting] : IP address
  - [Initial value] : -
- *name*
  - [Setting] : Domain name
  - [Initial value] : netvolante-dns.netvolante.jp

**[Description]**

Sets the NetVolante DNS server IP address and host name.

**[Models]**

RTX810, RTX5000

## 29.11 Turn the NetVolante DNS Server Address Update Function ON/OFF

---

**[Syntax]**

**netvolante-dns server update address use** [*server=server\_num*] *switch*  
**no netvolante-dns server update address use** [*server=server\_num*]

**[Setting and Initial value]**

- *server\_num*
  - [Setting] :

Setting	Description
1 or 2	Server number
Omitted	When omitted, it is assumed that “1” is specified

- [Initial value] : -
- *switch*

- [Setting] :

Setting	Description
on	Enable the server address update function
off	Disable the server address update function

- [Initial value] : on

**[Description]**

Sets whether to update the setting automatically when receiving a notification indicating that the IP address is changed from the NetVolante DNS server.

**[Models]**

RTX810, RTX5000

## 29.12 Set the Port Number of the NetVolante DNS Server Address Update Function

---

**[Syntax]**

**netvolante-dns server update address port** [*server=server\_num*] *port*  
**no netvolante-dns server update address port** [*server=server\_num*]

**[Setting and Initial value]**

- *server\_num*
  - [Setting] :

Setting	Description
1 or 2	Server number
Omitted	When omitted, it is assumed that “1” is specified

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



- [Initial value] : 2002

#### [Description]

Sets the listen port number for IP address update notification of the NetVolante DNS server.

#### [Models]

RTX810, RTX5000

## 29.13 Set How Many Times and at What Interval to Retry after Automatic Updating Fails

#### [Syntax]

```
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 and Initial value]

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *interval*
  - [Setting] :
    - auto
    - Number of seconds (60-300)
  - [Initial value] : auto
- *count*
  - [Setting] : Count (1-50)
  - [Initial value] : 10

#### [Description]

Sets how many times and at what interval to retry after an automatic update to the NetVolante DNS server fails.

#### [Note]

If you set *interval* to auto, the router will attempt to perform an automatic update again after an interval of between 30 and 90 seconds. If that attempt fails, the router will perform subsequent update attempts at 60 second intervals. If automatic updating fails and manual updating is performed during the specified retry time, subsequent automatic updating is not performed.

RTX5000 does not support WAN interface for *interface* parameter.

#### [Models]

RTX810, RTX5000

## 29.14 Set the Periodical Update Interval of NetVolante DNS Registration

#### [Syntax]

```
netvolante-dns register timer [server=server_num] time
no netvolante-dns register timer [server=server_num]
```

#### [Setting and Initial value]

- *server\_num*
  - [Setting] :

Setting	Description
1 to 2	Server number
Omitted	When omitted, it is assumed that "1" is specified

- [Initial value] : -

- *time*

- [Setting] :

Setting	Description
3600 ... 2147483647	Number of seconds
off	Not update the NetVolante DNS registration periodically

- [Initial value] : off

**[Description]**

Specifies an interval to update the NetVolante DNS registration periodically.

**[Models]**

RTX810, RTX5000

## 29.15 Set the File for Saving the Configuration When Automatic NetVolante DNS Registration Succeed

---

**[Syntax]**

```
netvolante-dns auto save [server=server_num] file
```

```
no netvolante-dns auto save [server=server_num]
```

**[Setting and Initial value]**

- *server\_num*

- [Setting] :

Setting	Description
1 or 2	Server number
Omitted	When omitted, it is assumed that “1” is specified

- [Initial value] : -

- *file*

- [Setting] :

Setting	Description
off	Not automatically save the configuration
auto	Save automatically the configuration into the default configuration file
Number	Name of the file for saving the configuration automatically

- [Initial value] : auto

**[Description]**

Sets whether to save the configuration automatically, and if saving it, specifies a name of the file for saving when the router succeeds in automatic registration of NetVolante DNS, and also receives an address notification from the NetVolante DNS server.

**[Models]**

RTX810, RTX5000

## Chapter 30

### UPnP Configuration

#### 30.1 Set Whether to Use UPnP

##### [Syntax]

**upnp use** *use*

**no upnp use**

##### [Setting and Initial value]

- *use*
- [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : off

##### [Description]

Sets whether to use the UPnP function.

##### [Models]

RTX810

#### 30.2 Set the Interface That Is to Obtain the IP Address Used for UPnP

##### [Syntax]

**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 and Initial value]

- *interface*
- [Setting] :

Setting	Description
LAN interface name	Obtain an IP address of the specified LAN interface
WAN interface name	Obtain an IP address of the specified WAN interface
default	Default route interface

- [Initial value] : default
- *peer\_num*
  - [Setting] :
    - Peer number
    - anonymous
  - [Initial value] : -

##### [Description]

Sets the interface that is to obtain the IP address used for UPnP.

##### [Models]

RTX810

#### 30.3 Set the Type of Timer for Clearing the UPnP Port Mapping

##### [Syntax]

**upnp port mapping timer type** *type*

**no upnp mapping timer type**

**[Setting and Initial value]**

- *type*
- [Setting] :

Setting	Description
normal	Not refer to the ARP information
arp	Refer to the ARP information

- [Initial value] : arp

**[Description]**

Sets the type of timer used to clear the UPnP port mapping.

When a change is made with this command, the clearance timer value is set to 3600 seconds if arp is specified and 172800 seconds if normal is specified. The number of seconds of the clearance timer can be changed using the **upnp port mapping timer** command.

If you specify arp, it takes precedence over the **upnp port mapping timer** off setting. To allow the port mapping to remain without the influence of arp, specify normal.

**[Models]**

RTX810

## 30.4 Set the Timer for Clearing the UPnP Port Mapping

---

**[Syntax]**

**upnp port mapping timer** *time*  
**no upnp port mapping timer**

**[Setting and Initial value]**

- *time*
- [Setting] :

Setting	Description
600..21474836	Number of seconds
off	Not clear

- [Initial value] : 3600

**[Description]**

Sets the time until the port mapping generated by UPnP is cleared.

**[Note]**

Execute the **upnp port mapping timer type** command first and then change the setting using this command.

Even if you set this command to off, the port mapping will be cleared if the **upnp port mapping timer type** arp command has been executed. If you want the port mapping to remain even after an ARP timeout, execute the **upnp port mapping timer type normal** command.

**[Models]**

RTX810

## 30.5 Set Whether to Output the UPnP Syslog

---

**[Syntax]**

**upnp syslog** *syslog*  
**no upnp syslog**

**[Setting and Initial value]**

- *syslog*
- [Setting] :

Setting	Description
on	Output the UPnP syslog
off	Not output the UPnP syslog

- [Initial value] : off

**[Description]**

Sets whether to output the UPnP syslog. It is output at the debug level.

**[Models]**

RTX810

## Chapter 31

### USB Configuration

#### 31.1 Set Whether to Use the USB Host Function

##### [Syntax]

```
usbhost use switch
no usbhost use [switch]
```

##### [Setting and Initial value]

- *switch*
- [Setting] :

Setting	Description
on	Use the USB host function
off	Do not use the USB host function

- [Initial value] : on

##### [Description]

Sets whether to use the USB host function.

When this command is set to off, the router will not recognize USB memory that is connected to it.

Also, if the USB host function is impaired by excess current, you can restore it by executing this command when there is no USB memory connected to the router.

##### [Models]

RTX810

#### 31.2 Set the Time Until the Excess Current Protection Function in the USB Bus Is Activated

##### [Syntax]

```
usbhost overcurrent duration duration
no usbhost overcurrent duration [duration]
```

##### [Setting and Initial value]

- *duration*
- [Setting] : Time (5..100, on the 10-millisecond time scale)
- [Initial value] : 5 (50 milliseconds)

##### [Description]

Sets the time until the excess current protection function is activated. When excess current is detected continuously for the time specified here, the excess current protection function is activated.

##### [Models]

RTX810

## Chapter 32

### Schedule

#### 32.1 Set the Schedule

##### [Syntax]

**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*...

**no scudule at** *id* [[*date*]...]

##### [Setting and Initial value]

- *id*
  - [Setting] : Schedule number
  - [Initial value] : -
- *date* : Date (can be omitted)
  - [Setting] :
    - Month/Day
    - Assumed to be \*/\* if omitted

Month Setup Example	Setting
1,2	January and February
2-	February to December
2-7	February to July
-7	January to July
*	Every month

Date Setup Example	Setting
1	Day 1 only
1,2	Day 1 and 2
2-	Day 2 to the end of the month
2-7	Day 2 to 7
-7	Day 1 to 7
mon	Monday only
sat,sun	Saturday and Sunday
mon-fri	Monday through Friday
-fri	Sunday through Friday
*	Every day

- [Initial value] : -
- *time* : Time
- [Setting] :

Setting	Description
hh:mm[:ss]	Hour (0..23 or *): Minute (0..59 or *): Second (0..59). The second can be omitted.
startup	At startup
usb-attached	When a USB device is detected

Setting	Description
sd-attached	When a microSD is detected

- [Initial value] : -
- *peer\_num*
  - [Setting] :
    - Peer number
    - anonymous
  - [Initial value] : -
- *tunnel\_num*
  - [Setting] : Tunnel interface number
  - [Initial value] : -
- *switch* : Switch
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -
- *command*
  - [Setting] : Command to be executed (limitations exist)
  - [Initial value] : -

#### [Description]

Executes the command specified by *command* at the time specified by *time*.

If the second, third or fourth syntax is specified, the command operates as if the **pp select/tunnel select/switch select** command has been executed on the specified peer number, tunnel number or switch in advance.

Multiple **schedule at** commands can be specified. If multiple commands are specified at the same time, the commands are executed in ascending order of *id*.

When *time* is specified in the hh:mm format, the router determines that the second has been omitted. When it is specified in the hh:mm:ss format, the router determines that the second has been specified. You cannot use “-” for the number of seconds to specify a range, or “\*” for total specification.

The following commands cannot be specified.

**administrator, administrator password, administrator password encrypted, auth user, auth user group, bgp configure refresh, cold start,** commands starting with **console** excluding **console info** and **console prompt, copy, copy exec, date, delete, exit, external-memory performance-test go, help, http revision-up go, http revision-up schedule, interface reset,** commands starting with **less, login password, login password encrypted, login timer, login user, luac, make directory, nslookup, ospf configure refresh, packetdump, ping, ping6, pp select, quit, remote setup, rename, rfts format, rfts garbage collect, save, schedule at,** commands that start with **show, sshd host key generate, sshd session, ssl public key generate, system packet-buffer, telnet, telnetd session, time, timezone, traceroute, traceroute6, tunnel select, user attribute**

#### [Note]

Command completion using the TAB key is carried out for the *command* parameter when entering a command. However, errors such as syntax errors are not detected until the command is actually executed. When executing a command specified by the **schedule at** command, the command that was attempted is output to the SYSLOG of INFO type.

A number and a day of the week cannot be mixed in *date*.

A schedule with startup specified is executed when the router starts up. This is convenient for cases such as when you wish to originate a call as soon as the power is turned on.

#### [Example]

- Allow connection only between 8:00 and 17:00 on a weekday

```
# schedule at 1 */mon-fri 8:00 pp 1 wan1 auto connect on
# schedule at 2 */mon-fri 17:00 pp 1 wan1 auto connect off
# schedule at 3 */mon-fri 17:05 * disconnect 1
```

- Allow connection only for 15 minutes from minute 0 of every hour

```
# schedule at 1 *:00 pp 1 wan1 auto connect on
# schedule at 2 *:15 pp 1 wan1 auto connect off
# schedule at 3 *:15 * disconnect 1
```

- Switch the routing on the next New Years day



```
# schedule at 1 1/1 0:0 * ip route NETWORK gateway pp 2
```

- Execute a Lua script for 20 seconds every day between 12:00 and 13:00

```
# schedule at 1 12:*:00 * lua script.lua
```

```
# schedule at 2 12:*:20 * lua script.lua
```

```
# schedule at 3 12:*:40 * lua script.lua
```

- Switch is rebooted everyday at 3 o'clock.

```
# 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
```

#### **[Models]**

RTX810, RTX5000

## Chapter 33

### VLAN Configuration

#### 33.1 Set VLAN ID

##### [Syntax]

```
vlan interface/sub_interface 802.1q vid=vid name=name
```

```
no vlan interface/sub_interface 802.1q
```

##### [Setting and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *sub\_interface*
  - [Setting] : 1-32 (RTX5000), 1-8 (RTX810)
  - [Initial value] : -
- *vid*
  - [Setting] : VLAN ID (Value stored in the VID field of the IEEE802.1Q tag; 2-4094)
  - [Initial value] : -
- *name*
  - [Setting] : Arbitrary name assigned to the VLAN (up to 127 characters)
  - [Initial value] : -

##### [Description]

Sets the VLAN ID of the VLAN used on the LAN interface. Packets with an IEEE802.1Q tag containing the specified VID can be handled. Up to eight VLANs can be set on each LAN interface.

##### [Note]

If a tagged packet is received and the tag VID is not set on the receive LAN interface, the packet is discarded. This cannot be used simultaneously with the LAN division function (port-based-ks8995m=on of the **lan type** command) on the same LAN interface. The command entered first is valid, and the second command results in a command error.

##### [Models]

RTX810, RTX5000

#### 33.2 Assigning a Switching Hub Port to a VLAN

##### [Syntax]

```
vlan port mapping sw_port vlan_interface
```

```
no vlan port mapping sw_port [vlan_interface]
```

##### [Setting and Initial value]

- *sw\_port*
  - [Setting] : Switching hub port (lan1.1 - lan1.N)
  - [Initial value] : -
- *vlan\_interface*
  - [Setting] : VLAN interface (vlan1 - vlanN)
  - [Initial value] : -

##### [Description]

Uses the enhanced LAN division function to assign a switching hub port to a VLAN interface. Port names are specified in this format: lan1.N.

Ports that belong to the same VLAN interface operate as switches.

The VLAN interface that lan1. N belongs to is vlanN.

##### [Note]

This command only functions if you enable the LAN division function by specifying “port-based-option=dividenetwork” with

the **lan type** command.

You can execute **vlan port mapping** even when you have not specified “port-based-option=divide-network”, but the setting will have no effect on the operation of the switching hub.

**[Example]**

```
# vlan port mapping lan1.3 vlan7  
# vlan port mapping lan1.4 vlan7
```

**[Models]**

RTX810, RTX5000

## Chapter 34

### Heartbeat Function

#### 34.1 Set the Shared Heartbeat Key

##### [Syntax]

**heartbeat pre-shared-key** *key*

**no heartbeat pre-shared-key**

##### [Setting and Initial value]

- *key*
  - [Setting] : Key expressed using ASCII text characters (up to 32 characters)
  - [Initial value] : -

##### [Description]

Sets the shared key that the device that receives the heartbeat uses for authentication. The sending and receiving devices must both have the same key set.

When this command is not set, sent and received heartbeats are not logged.

##### [Models]

RTX810, RTX5000

#### 34.2 Set Whether to Receive Heartbeats

##### [Syntax]

**heartbeat receive** *switch* [*option=value ...*]

**no heartbeat receive** [*switch*]

##### [Setting and Initial value]

- *switch*
  - [Setting] :

Setting	Description
on	Receive heartbeat packets
off	Do not receive heartbeat packets

- [Initial value] : off
- *option=value*
  - [Setting] :

<i>option</i>	<i>value</i>	Description
log	on	Output the received contents to the syslog.
	off	Do not output the received contents to the syslog.
monitor	Monitor time [seconds] (30..21474836)	The router produces an alert when there is no heartbeat for the specified number of seconds.
	off	Even if it does not receive any heartbeats, the router does not produce an alarm.

- [Initial value] :
  - log=off
  - monitor=off

##### [Description]

Sets whether to output the contents of the received heartbeat to the syslog.

If the router does not receive any heartbeats within the time specified for the monitor option, it creates a log entry in the syslog and sends an SNMP trap.

**[Note]**

Before you set this command, you must specify the key shared with the sending router by using the **heartbeat pre-shared-key** command.

**[Models]**

RTX810, RTX5000

### 34.3 Send a Heartbeat

---

**[Syntax]**

**heartbeat send** *dest\_addr* [*log=switch*]

**[Setting and Initial value]**

- *dest\_addr*
  - [Setting] : IPv4 address or FQDN of the destination router
  - [Initial value] : -
- *switch* : syslog output
  - [Setting] :

Setting	Description
on	Output SYSLOG
off	Not output SYSLOG

- [Initial value] : off

**[Description]**

Sends the IP address and device name specified by **snmp sysname** to the IP address specified by *dest\_addr* to indicate that the router can communicate.

When log is set to on, packet transmissions are logged in the syslog.

**[Note]**

Before you execute this command, you must specify the key shared with the receiving router by using the **heartbeat pre-shared-key** command.

**[Models]**

RTX810, RTX5000

## Chapter 35

### Heartbeat Function Release 2

With the heartbeat function, a router connecting with the network sends a packet containing its own name and IP address to another router in the other site, and indicates that it can communicate. The router receiving the packet outputs the reported name and IP address in the log and saves them. With this function, a router of which WAN IP address is arbitrary can indicate that it communicate with another router in the other site.

#### Release

The conventional heartbeat function mentioned in the previous section is Release 1, and the new heartbeat function mentioned in this section is Release 2. Although the functional concept of both releases is same, note that their command systems and operations are not compatible.

#### Characteristics of Release 2

- Uses UDP/No. 8512 port for heartbeat packets (for both source and destination)
- The router receiving heartbeat packets identifies the source router with the reported name. Therefore, you have to specify a unique name for each router that sends heartbeat packets.
- When a sending router and a receiving router have a common encryption key and authentication key, they can encrypt information to be reported and detect interpolation.
- To simplify operations and management of multipoint communication, multiple transmitting/receiving settings are available by specifying individual identifier. In this case, a transmission setting of the transmission side and receiving setting of the receiving side, which make one pair, must have a same identifier. By including this setting identifier into heartbeat packets, the receiving side uniquely determines a receiving setting used for arbitrary heartbeat packets.
- Conventionally, periodical transmission of heartbeat packets needed the **schedule** command also. However, Release 2 allows periodical transmission of heartbeat packets only by the transmission setting command.
- An IP address to be reported is basically the IP address specified for the transmission interface of heartbeat packets. In this case, if NAT or IP masquerade is specified for a relevant interface, the IP address for which the NAT/IP masquerade setting is applied is used for heartbeat packets to be transmitted. However, when the unnumbered connection line is used to send a heartbeat packet, the router selects an IP address of the youngest number interface among the LAN interfaces with IP addresses, and reports that IP address (coincided with the source address in the IP header of the reported packet).
- You can display the received heartbeat information with the **show status heartbeat2** command.

### 35.1 Set the Notification Name

#### [Syntax]

```
heartbeat2 myname name
no heartbeat2 myname
```

#### [Setting and Initial value]

- *name*
  - [Setting] : The name used for the heartbeat (1 to 64 ASCII characters, or 1 to 32 SJIS characters)
  - [Initial value] : -

#### [Description]

Sets the device name to use in the heartbeat.

For the *name* parameter, you can specify ASCII characters or SJIS Japanese characters (except for half-width katakana). However, Japanese characters can only be specified and displayed properly when **console character** is set to *sjis*. When any other setting is selected, the Japanese characters may not be processed properly.

#### [Models]

RTX810, RTX5000

### 35.2 Configure Notification Settings

#### [Syntax]

```
heartbeat2 transmit trans_id [crypto crypto_key] auth auth_key dest_addr ...
no heartbeat2 transmit trans_id
```

#### [Setting and Initial value]

- *trans\_id*
  - [Setting] : Notification configuration ID (1..65535)
  - [Initial value] : -
- *crypto\_key*
  - [Setting] : Encryption key expressed using ASCII text characters (1 to 32 characters)

- [Initial value] : -
- *auth\_key*
  - [Setting] : Authentication key expressed using ASCII text characters (1 to 32 characters)
  - [Initial value] : -
- *dest\_addr*
  - [Setting] : IPv4 addresses or FQDNs of the source routers (you can specify up to four locations, delimiting each with a space)
  - [Initial value] : -

**[Description]**

Configures the settings for regular heartbeat transmission. Authentication information is attached to notification packets according to the *auth\_key* parameter specified by this command. If you set the *crypto\_key* parameter, the notification contents are encrypted further.

When you set the **heartbeat2 receive** command on the receiving device, the *recv\_id* setting must match the *trans\_id* setting specified by this command. The *crypto\_key* and *auth\_key* settings must also match.

The purpose of this command is to define the essential parameters for transmission and tie them to the ID specified by the *trans\_id* parameter. To actually enable transmission processing, you must set the **heartbeat2 transmit enable** command.

To diffuse the transmission load caused by multiple notification settings, for each notification configuration or destination, the router waits for a random interval of 30 seconds or less after the notification configuration is enabled before actually transmitting notification packets.

**[Models]**

RTX810, RTX5000

### 35.3 Enabling a Notification Configuration

---

**[Syntax]**

```
heartbeat2 transmit enable [one-shot] trans_id_list
no heartbeat2 transmit enable
```

**[Setting and Initial value]**

- *trans\_id\_list* : A list of the notification configurations to enable
  - [Setting] :
    - A number, two numbers with a hyphen in between them (range designation), or a list of numbers and ranges (up to 128)
  - [Initial value] : -

**[Description]**

Sets the notification configurations to enable.

You can list up to 128 ID entries, delimiting each with a space.

If you enter the 'one-shot' keyword, notifications for each configuration in the *trans\_id\_list* are only processed once. A command entered using this format cannot be saved.

**[Models]**

RTX810, RTX5000

### 35.4 Set a Notification Interval

---

**[Syntax]**

```
heartbeat2 transmit interval time
heartbeat2 transmit interval trans_id time
no heartbeat2 transmit interval [time]
no heartbeat2 transmit interval trans_id time
```

**[Setting and Initial value]**

- *trans\_id*
  - [Setting] : Notification configuration ID
  - [Initial value] : -
- *time*
  - [Setting] : Notification interval in seconds (30..65535)
  - [Initial value] : 30

**[Description]**

Sets the notification interval for the configuration specified by the *trans\_id* parameter.

If you omit the *trans\_id* parameter, the command affects all notification configurations. However, settings that specify individual notification configuration IDs take precedence.

**[Models]**

RTX810, RTX5000

## 35.5 Set Whether to Log Notification Transmissions

---

**[Syntax]**

```
heartbeat2 transmit log [trans_id] sw
no heartbeat2 transmit log [trans_id]
```

**[Setting and Initial value]**

- *trans\_id*
  - [Setting] : Notification configuration ID
  - [Initial value] : -
- *sw*
  - [Setting] :

Setting	Description
on	Output the transmitted contents to the syslog.
off	Do not output the transmitted contents to the syslog.

- [Initial value] : off

**[Description]**

Sets the log output for the notification configuration specified by the *trans\_id* parameter. When the *sw* parameter is set to 'on', heartbeat transmissions are output to the syslog at the INFO level.

If you omit the *trans\_id* parameter, the command affects all notification configurations. However, settings that specify individual notification configuration IDs take precedence.

**[Models]**

RTX810, RTX5000

## 35.6 Configuring Reception Settings

---

**[Syntax]**

```
heartbeat2 receive recv_id [crypto crypto_key] auth auth_key
no heartbeat2 receive recv_id
```

**[Setting and Initial value]**

- *recv\_id*
  - [Setting] : Reception configuration ID
  - [Initial value] : -
- *crypto\_key*
  - [Setting] : Encryption key expressed using ASCII text characters (1 to 32 characters)
  - [Initial value] : -
- *auth\_key*
  - [Setting] : Authentication key expressed using ASCII text characters (1 to 32 characters)
  - [Initial value] : -

**[Description]**

Configures the settings for heartbeat reception. When the router receives a packet, it uses the setting configuration whose *recv\_id* parameter matches the notification configuration ID (*trans\_id*) of the received packet to decrypt and authenticate the packet.

When you set the **heartbeat2 transmit** command on the sending device, the *trans\_id* must match the *recv\_id* specified by this command. The *crypto\_key* and *auth\_key* settings must also match.

The purpose of this command is to define the essential parameters for reception and tie them to the ID specified by the *recv\_id* parameter. To actually enable reception processing, you must set the **heartbeat2 receive enable** command.

**[Models]**

RTX810, RTX5000

## 35.7 Enabling a Reception Configuration

---



**[Syntax]****heartbeat2 receive enable** *recv\_id\_list***no heartbeat2 receive enable****[Setting and Initial value]**

- *recv\_id\_list* : A list of the reception configurations to enable
  - [Setting] :
    - A number, two numbers with a hyphen in between them (range designation), or a list of numbers and ranges (up to 128)
  - [Initial value] : -

**[Description]**

Sets the reception configurations to enable.

You can list up to 128 ID entries, delimiting each with a space.

**[Models]**

RTX810, RTX5000

## 35.8 Set Reception Interval Monitoring

---

**[Syntax]****heartbeat2 receive monitor** *time***heartbeat2 receive monitor** *recv\_id time***no heartbeat2 receive monitor** [*time*]**no heartbeat2 receive monitor** *recv\_id time***[Setting and Initial value]**

- *recv\_id*
  - [Setting] : Reception configuration ID
  - [Initial value] : -
- *time* : Monitor time
  - [Setting] :

Setting	Description
30..21474836	Number of seconds
off	Do not monitor the reception interval

- [Initial value] : off

**[Description]**

Sets the reception interval monitoring for the reception configuration specified by the *recv\_id* parameter. When monitoring is enabled, if no heartbeats are received within the specified interval, the router makes an INFO level entry in the syslog and sends an SNMP trap.

If you omit the *recv\_id* parameter, the command affects all reception configurations. However, settings that specify individual reception configuration IDs take precedence.

**[Models]**

RTX810, RTX5000

## 35.9 Set Whether to Log Received Notifications

---

**[Syntax]****heartbeat2 receive log** [*recv\_id*] *sw***no heartbeat2 receive log** [*recv\_id*]**[Setting and Initial value]**

- *recv\_id*
  - [Setting] : Reception configuration ID
  - [Initial value] : -
- *sw*
  - [Setting] :

Setting	Description
on	Output the received contents to the syslog.
off	Do not output the received contents to the syslog.

- [Initial value] : off

#### [Description]

Sets the log output for the reception configuration specified by the *recv\_id* parameter. When the *sw* parameter is set to 'on', received heartbeats are output to the syslog at the INFO level.

If you omit the *recv\_id* parameter, the command affects all reception configurations. However, settings that specify individual reception configuration IDs take precedence.

#### [Models]

RTX810, RTX5000

## 35.10 Set the Maximum Number of Heartbeats That Can Be Stored at the Same Time

---

#### [Syntax]

**heartbeat2 receive record limit** *num*

**no heartbeat2 receive record limit**

#### [Setting and Initial value]

- *num*
  - [Setting] : Maximum number of stored heartbeats (RTX5000, RTX3500, RTX3000: 64..10000, all other models: 64..1000)
  - [Initial value] : 64

#### [Description]

Sets the maximum number of received heartbeats that can be stored at the same time. New heartbeats cannot be acquired after the number of heartbeats exceeds this limit. If the limit is reached, erase unnecessary information using the **clear heartbeat2** command.

#### [Models]

RTX810, RTX5000

## 35.11 Show the Heartbeat Information

---

#### [Syntax]

**show status heartbeat2**

**show status heartbeat2 id** *recv\_id*

**show status heartbeat2 name** *string*

#### [Setting and Initial value]

- *recv\_id*
  - [Setting] : Reception configuration ID
  - [Initial value] : -
- *string*
  - [Setting] : Character string (1 to 64 ASCII characters, or 1 to 32 SJIS characters)
  - [Initial value] : -

#### [Description]

Shows the heartbeat information that has been received.

The first syntax shows all the stored information.

The second syntax only shows the information that has been received through the specified reception configuration.

The third syntax only shows the information for notifications that contain the specified string in their name.

For the *string* parameter, you can specify ASCII characters or SJIS Japanese characters (except for half-width katakana).

However, the command only processes Japanese characters properly when **console character** is set to *sjis*. When any other setting is selected, the command may not function properly.

#### [Models]

RTX810, RTX5000

## 35.12 Clear the Heartbeat Information

---

**[Syntax]**

**clear heartbeat2**

**clear heartbeat2 id** *recv\_id*

**clear heartbeat2 name** *string*

**[Setting and Initial value]**

- *recv\_id*
  - [Setting] : Reception configuration ID
  - [Initial value] : -
- *string*
  - [Setting] : Character string (1 to 64 ASCII characters, or 1 to 32 SJIS characters)
  - [Initial value] : -

**[Description]**

Clears the heartbeat information that has been received.

The first syntax clears all the stored information.

The second syntax only clears the information that has been received through the specified reception configuration.

The third syntax only clears the information for notifications that contain the specified string in their name.

For the *string* parameter, you can specify ASCII characters or SJIS Japanese characters (except for half-width katakana).

However, the command only processes Japanese characters properly when **console character** is set to sjis. When any other setting is selected, the command may not function properly.

**[Models]**

RTX810, RTX5000

## Chapter 36

### SNTP Server Function

SNTP is a protocol for using a network to synchronize the times of computers and network devices. You can use the SNTP server function to respond to a time query from the client with a value read from the router's internal clock. The SNTP server function uses SNTP version 4. It is also downward compatible with requests from SNTP versions 1 to 3.

To obtain accurate times with the SNTP server function, we recommend that you execute the **ntpdate** command regularly to synchronize the router's time with that of another NTP server.

#### 36.1 Set Whether to Enable the SNTP Server Function

##### [Syntax]

```
sntp service switch
no sntp service
```

##### [Setting and Initial value]

- *switch*
- [Setting] :

Setting	Description
on	Enable the SNTP server function
off	Disable the SNTP server function

- [Initial value] : on

##### [Description]

Sets whether to enable the SNTP server function.

##### [Models]

RTX810, RTX5000

#### 36.2 Set Which Hosts to Allow Access to the SNTP Server

##### [Syntax]

```
sntp host host
no sntp host
```

##### [Setting and Initial value]

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

Setting	Description
An IP address, two IP addresses with a hyphen (-) in between them (range designation), or a list containing these addresses	Allow access from a specified host
any	Allow access from all hosts
lan	Allow access from hosts in all LAN networks
lanN	Name of LAN interface that is allowed access to the SNTP server
vlanN	Name of VLAN interface that is allowed access to the SNTP server
none	Prohibit access from all hosts

- [Initial value] : lan

##### [Description]

Sets the hosts to allow access to the SNTP server.

##### [Note]

If the LAN interface is specified by this command, access from IPv4 addresses excluding the network address and the directed

broadcast address is allowed.

If neither the primary or secondary address is set on the specified LAN interface, access is not allowed.\

**[Models]**

RTX810, RTX5000

## Chapter 37

### External Memory Function

You can use this function to manipulate the data on an external memory device (USB memory or microSD memory card) connected to the router.

The types of external memory devices that you can use vary depending on the model.

This function makes the following operations possible.

- Operations Based on Commands and Command Settings
  - Transmit syslog messages to the external memory.
  - Copy setup files to the external memory.
  - Copy setup files from the external memory.
  - Copy firmware files from the external memory.
- Operations Performed Using the Router's External Memory and Download Buttons
  - You can copy setup and firmware files from the external memory by holding down an external memory button and the DOWNLOAD button for 3 seconds or more.
- Start the router from the external memory
- Batch file execution function

#### Batch File Execution Function

You can use this function to execute a list of commands stored in a batch file on the external memory.

You can configure the router so that you can execute the commands by pressing the DOWNLOAD button. You can also execute the commands using the **execute batch** command.

You can save files with the command execution results and log entries to the external memory.

Using this function, you can perform pinging and other operations in an environment where there are no PCs.

One way this function can be used is to greatly reduce the equipment and work required to install a router.

The execution results, settings, router conditions, etc., are saved to the external memory.

You can remove the external memory and check the saved data on a mobile phone.

You can also use the data as an operation log.

The following URL provides technical information of this function:

<http://www.yamaha.com/products/en/network/>

### 37.1 Set Whether to Use the microSD Card Slot

#### [Syntax]

**sd use** *switch*

**no sd use** [*switch*]

#### [Setting and Initial value]

- *switch*
- [Setting] :

Setting	Description
on	Use the microSD card slot
off	Do not use the microSD card slot

- [Initial value] : on

#### [Description]

Sets whether to use the microSD card slot. When this command is set to off, the router will not recognize a microSD memory card even if it is inserted in the card slot.

#### [Models]

RTX810, RTX5000

### 37.2 Set the Operational Mode of Cache Memory for the External Memory

#### [Syntax]

**external-memory cache mode** *mode*

**no external-memory cache mode** [*mode*]

**[Setting and Initial value]**

- *mode*
  - [Setting] :

Setting	Description
write-through	Write-through mode
copy-back1	Copy back mode 1
copy-back2	Copy back mode 2

- [Initial value] : copy-back1

**[Description]**

Sets the operational mode of the cache memory for the external memory. Three operational modes are supported: Write-through mode, copy-back mode 1, and copy-back mode 2. Each mode differs in the timing by which the data on each of the FAT, DIR, and FILE caches are written out to the external memory.

Each operational mode is explained below:

If you specify write-through, the caches assigned to FAT, DIR, and FILE will operate in write-through mode, and will always write to the external memory. This mode is the safest.

If you specify copy-back1, the FAT and DIR caches will operate in copy-back mode, and the FILE cache will operate in write-through mode. This allows for a faster operation than the write-through mode.

If you specify copy-back2, the FAT, DIR, and FILE caches will operate in copy-back mode. This setting operates at the highest speed, since writing to external memory is suppressed. However, since it will mean a prolonged state of no writing to external memory, if an unexpected power outage occurs, there is a higher possibility of the file system of the external memory suffering damage.

FAT: Abbreviation for File Allocation Table, DIR: Abbreviation for Directory Entry

**[Note]**

Changes to this command are applied when the external memory is connected. If the command is input while the external memory is already connected, it must be removed and then reconnected.

**[Models]**

RTX810, RTX5000

### 37.3 Set the Cache Memory Size for File Access Acceleration

**[Syntax]**

**external-memory accelerator cache size** *interface size*  
**no external-memory accelerator cache size** *interface* [*size*]

**[Setting and Initial value]**

- *interface*
  - [Setting] :

Setting	Description
usb1	USB port 1
sd1	microSD card slot

- [Initial value] : -

- *size*
  - [Setting] :

Setting	Description
1-5	Size of cache memory (the greater the value, the larger the memory size)
off	Disable the file access acceleration mechanism

- [Initial value] : 1

**[Description]**

Sets the size of the cache memory used to accelerate file access.

When you specify a value for *size*, a mechanism for accelerating file access activates, improving the access performance for the external memory, especially in structures where there are many directories and files. If the access performance does not

improve, it may improve by increasing the *size*. However, the greater the *size*, the longer it will take for the external memory to become available after it is connected.

If you set the *size* to "off", the cache memory for accelerating file access will not be secured.

In addition, if the external memory is connected to all interfaces simultaneously and the *size* is set to maximum for all interfaces, the system's overall performance may be affected. Therefore, it is recommended that you limit the use of this command to accelerate file access, to only one interface.

#### [Note]

Changes to this command are applied when the external memory is connected. If the command is input while the external memory is already connected, it must be removed and then reconnected.

Moreover, if the access performance does not improve even after increasing the *size*, it may improve by doing the following:

- If possible, reduce the number of files and directories in the external memory
- Adjust the total number of directories in the external memory, to less than 2,000
- Adjust the total number of files (including directories) in the directories that are frequently accessed, to less than 20,000
- If possible, shorten the names of files and directories (less than 32 characters recommended)

#### [Models]

RTX810, RTX5000

## 37.4 Specify the Name of the SYSLOG File to Save in External Memory

#### [Syntax]

```
external-memory syslog filename name [crypto password] [limit=size] [backup=num] [interval=interval] [line=line]
no external-memory syslog filename [name]
```

#### [Setting and Initial value]

- *name* : SYSLOG File Name
- [Setting] :

Setting	Description
usb1: <i>filename</i>	File name in the USB memory (cannot specify a name containing extension ".bak")
sd1: <i>filename</i>	File name in the microSD card (cannot specify a name containing extension ".bak")

- [Initial value] : -
- *crypto* : Select the encryption algorithm for encrypting and saving SYSLOG
- [Setting] :

Setting	Description
aes128	Encrypt in AES128
aes256	Encrypt in AES256

- [Initial value] : -
- *password*
  - [Setting] : Password expressed in ASCII (at least 8 half-width characters and less than 32 characters)
  - [Initial value] : -
- *size*
  - [Setting] : Maximum size of SYSLOG file (1 - 1024, Unit: MB)
  - [Initial value] : 10
- *num*
  - [Setting] : Maximum number of backup files (1-100)
  - [Initial value] : 10
- *interval*
  - [Setting] : Interval time for writing SYSLOG to external-memory (2-86400 seconds)
  - [Initial value] : 2
- *line*
  - [Setting] : The number of line for writing SYSLOG to external memory (1000-N lines) N...Maximum number of logging line
  - [Initial value] : 1000

#### [Description]

Specifies the name of the SYSLOG file to save in the external memory.



You cannot specify a name for *name* that contains the extension ".bak." In addition, if not encrypting, you cannot specify a file name for *name* that contains the extension ".rtfg".

If you specify *crypto* and *password*, SYSLOG will be encrypted and then saved to the external memory. To encrypt, you must include the extension ".rtfg" in *name*, or specify a name with no extension. If the extension is omitted, "rtfg" will be automatically added as the extension.

Once the SYSLOG file reaches the maximum size, a backup of the SYSLOG file will be performed. The name of the backup file created at this time will vary by firmware.

The name of the backup file will be the file name specified in *name*, appended with the date and time when the backup was performed, in the format *\_yyymmdd\_hhmmss*.

- *yyyy* ... Year (4 digits)
- *mm* ... Month (2 digits)
- *dd* ... Day (2 digits)
- *hh* ... Hour (2 digits)
- *mm* ... Minutes (2 digits)
- *ss* ... Seconds (2 digits)

When the number of backup files has reached its upper limit specified in *num*, or when the available space in the external memory runs out, the oldest backup file is deleted, and then the new backup file is created.

If the *name* has an extension:

- Saved without encryption ... The extension is replaced with ".bak".
- Encrypted and saved ... "\_bak" appended before the extension.

If the *name* does not contain file extension ... The extension ".bak" is added.

When the time specified by *interval* parameter is over, or the number of SYSLOG specified by *line* parameter is outputted, the SYSLOG will be outputted to external memory. Maximum number of logging line that can be specified by *line*:

- RTX810 ... 3000
- RTX5000 ... 20000

Unless this command is set, SYSLOG will not be written to the external memory.

#### [Note]

To make the following changes, *name* must be changed.

- To change from saving SYSLOG without encryption to saving with encryption
- To change from saving SYSLOG with encryption to saving without encryption
- To change the encryption algorithm or password

*name* must be within 99 half-width characters.

RTX810 supports *inerval* parameter and *line* parameter in Rev.11.01.23 or later.

#### [Models]

RTX810, RTX5000

## 37.5 Set Whether to Permit Setup File and Firmware File Copying through the Simultaneous Holding Down of an External Memory Button and the DOWNLOAD button

#### [Syntax]

**operation external-memory download permit** *switch*

**no operation external-memory download permit** [*switch*]

#### [Setting and Initial value]

- *switch*
  - [Setting] :

Setting	Description
on	Permit
off	Prohibit

- [Initial value] : on

**[Description]**

Sets whether to permit setup file and firmware file copying through the simultaneous holding down of an external memory button and the DOWNLOAD button.

**[Models]**

RTX810

## 37.6 Set Whether to Allow the Router to Start Using Files in the External Memory

---

**[Syntax]**

```
external-memory boot permit switch
no external-memory boot permit [switch]
```

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	Permit
off	Prohibit

- [Initial value] : on

**[Description]**

Sets whether to allow the router to start using files in the external memory. If this setting is set to OFF, the router cannot start by using files in the external memory.

You can set the name of the setup file and the firmware file that the router loads when it starts with the **external-memory config filename** and **external-memory exec filename** commands.

**[Models]**

RTX810, RTX5000

## 37.7 Set the Timeout for External Memory Detection at Router Startup

---

**[Syntax]**

```
external-memory boot timeout time
no external-memory boot timeout [time]
```

**[Setting and Initial value]**

- *time*
- [Setting] : Timeout in seconds (1..30)
- [Initial value] : 1

**[Description]**

Sets the timeout for detecting the external memory at router startup. This is valid if the **external-memory boot permit on** command has been set to allow booting from a file in the external memory. If the device takes a long time to be recognized, increasing the timeout value may help with the recognition.

**[Note]**

A good reference to use for this setting is the time displayed in "boot device attach" in the External Memory Performance Test command.

**[Models]**

RTX810

## 37.8 Specify the Name of the Firmware File That the Router Loads When It Starts or When an External Memory Button and the DOWNLOAD Button Are Held Down

---

**[Syntax]**

```
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 and Initial value]**

- *from* : External memory and firmware file name

- [Setting] :

Setting	Description
usb1: <i>filename</i>	A firmware file on the USB memory
sd1: <i>filename</i>	A firmware file on the microSD card
*: <i>filename</i>	A firmware file on the USB memory or microSD card

- [Initial value] :
  - \*:(Model name).bin (RTX810)
  - sd1:(Model name).bin (RTX5000)
- *to* : Copy destination file name
- [Setting] :

Setting	Description
num	Number of the executable firmware file on the internal flash ROM (0 or 1; 0 when omitted)

- [Initial value] : 0

### [Description]

Sets the name of the firmware file that is loaded when the router is started with external memory connected to it and when an external memory button and the DOWNLOAD button are held down at the same time.

You can specify what firmware file number on the internal flash ROM to copy to when an external memory button and the DOWNLOAD button are pressed at the same time.

If you use an asterisk to specify the external memory, the router starts searching the microSD memory card for the specified file. If the router can't find the file on the memory card, it searches for it in the USB memory. When you load the firmware file using buttons, only the external memory device that corresponds to the external memory button that you press is searched.

You can specify the *filename* parameter with an absolute path or a file name. If you only specify a file name, the router searches through the specified external memory device for the file.

If the router finds multiple files, it chooses the file in the directory that is closest to the root directory and first in alphabetical order.

If you specify off, the router does not search for and load a firmware file.

### [Note]

Depending on the file structure of the external memory and the number of files, it may take time for the router to search for the file.

To make searching faster, avoid creating deep directory structures, and save the firmware file in a directory that is close to the root directory, or specify the file directly using an absolute path.

You can set the timeout for automatic searching using the **external-memory auto-search time** command.

The number of characters used for *filename* is up to 99 characters.

### [Example]

- Search for the "rtx810.bin" file on the microSD card and load it as the firmware file.

```
# external-memory exec filename sd1:rtx810.bin
```

- Search for the "rtx810.bin" file in the "test" directory of the microSD card and load it as the firmware file.

```
# external-memory exec filename sd1:/test/rtx810.bin
```

### [Models]

RTX810, RTX5000

## 37.9 Specify the Name of the Setup File That the Router Loads When It Starts or When an External Memory Button and the DOWNLOAD Button Are Held Down

### [Syntax]

```
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 and Initial value]**

- *from* : External memory and setup file name
  - [Setting] :

Setting	Description
usb1: <i>filename</i>	A setup file on the USB memory
sd1: <i>filename</i>	A setup file on the microSD card
*: <i>filename</i>	A firmware file on the USB memory or microSD card

- [Initial value] :
  - \*:config.rtf,\*:config.txt (RTX810)
  - sd1:config.rtf,sd1:config.txt (RTX5000)
- *to* : Copy destination file name
  - [Setting] :

Setting	Description
num	Number of the setup file on the internal flash ROM (0..4; 0 when omitted)

- [Initial value] : 0
- *password*
  - [Setting] : Decryption password (ASCII text string between 8 and 32 characters in length)
  - [Initial value] : -

**[Description]**

Sets the name of the setup file that is loaded when the router is started with external memory connected to it and when the external memory and DOWNLOAD buttons are held down at the same time.

You can specify what setup file number on the internal flash ROM to copy to when the external memory and DOWNLOAD buttons are pressed at the same time.

If you use an asterisk to specify the external memory, the router starts searching the microSD memory card for the specified file. If the router can't find the file on the memory card, it searches for it in the USB memory. When you load the firmware file using buttons, only the memory that corresponds to the external memory button that you press is searched.

You can specify the *filename* parameter with an absolute path or a file name. If you only specify a file name, the router searches through the specified external memory device for the file.

If the router finds multiple files, it chooses the file in the directory that is closest to the root directory and first in alphabetical order.

To decrypt a file that was encrypted with a specified password, set the *password* parameter to the password that was used to encrypt the file.

If you specify off, the router does not search for and load a setup file.

**[Note]**

Depending on the file structure of the external memory and the number of files, it may take time for the router to search for the file.

To make searching faster, avoid creating deep directory structures, and save the firmware file in a directory that is close to the root directory, or specify the file directly using an absolute path.

You can set the timeout for automatic searching using the **external-memory auto-search time** command.

The number of characters used for *filename* is up to 99 characters.

**[Example]**

- Search for the “config.txt” file on the microSD card and load it as the setup file.

```
# external-memory config filename sd1:config.txt
```

- Search for the “config.txt” file in the “test” directory of the microSD card and load it as the setup file.

```
# external-memory config filename sd1:/test/config.txt
```

**[Models]**

RTX810, RTX5000

**37.10 Set the File Search Timeout**

**[Syntax]**

**external-memory auto-search time** *time*  
**no external-memory auto-search time** [*time*]

**[Setting and Initial value]**

- *time*
  - [Setting] :
    - Number of seconds (1..600)
  - [Initial value] : 300

**[Description]**

Set the timeout time for when the router is searching for a file on the external memory.

**[Models]**

RTX810, RTX5000

## 37.11 Execute the Batch File

---

**[Syntax]**

**execute batch**

**[Description]**

Executes the batch file in the external memory. You can specify the name of the batch file to execute using the **external-memory batch filename** command.

**[Note]**

If you want to stop the execution of a batch file, enter Ctrl+C.

**[Models]**

RTX810, RTX5000

## 37.12 Set the Batch and Execution Result Files

---

**[Syntax]**

**external-memory batch filename** *batchfile* [*logfile*]  
**no external-memory batch filename** [*batchfile* [*logfile*]]

**[Setting and Initial value]**

- *batchfile* : Batch file name
  - [Setting] :

Setting	Description
<i>usb1:filename</i>	A batch file in the USB memory
<i>sd1:filename</i>	A batch file in the microSD card
<i>*:filename</i>	A batch file in the USB memory or microSD card

- [Initial value] :
  - \*:command.txt (RTX810)
  - sd1:command.txt (RTX5000)

- *logfile*

- [Setting] :

Setting	Description
<i>filename</i>	The name of the execution result file

- [Initial value] : command-log.txt

**[Description]**

Specifies the names of the batch file and the execution result file on the external memory.

If you use an asterisk to specify the external memory, the router starts searching the microSD card for the specified file. If the router can't find the file on the memory card, it searches for it in the USB memory.

You can specify the *filename* parameter with an absolute path or a file name. If you only specify a file name for the *filename* parameter, the router will automatically search through the external memory for the file. If the router finds multiple files, it chooses the file in the directory that is closest to the root directory and first in alphabetical order.

If you omit the *logfile* parameter, the router creates an execution result file with the name (batch file name)-log.txt.

**[Note]**

when *logfile* is specified, the number of characters that can be specified for *batchfile* is up to 99 characters. When *logfile* is omitted, the number is up to 91 characters excluding an extension. The number of characters that can be specified for *filename* is up to 99 characters.

**[Example]**

- Search for the “command\_test.txt” file on the microSD card and use it as the batch file.

```
# external-memory batch filename sd1:command_test.txt
```

- Load “command\_test.txt” from the “test” directory on the microSD card.

```
# external-memory batch filename sd1:/test/command_test.txt
```

**[Models]**

RTX810, RTX5000

### 37.13 External Memory Performance Test Command

---

**[Syntax]**

**external-memory performance-test go** *interface*

**[Setting and Initial value]**

- *interface*
  - [Setting] :

Setting	Description
usb1	USB interface
sd1	microSD interface

- [Initial value] : -

**[Description]**

Check whether the memory performance is appropriate for the external memory function.

After the router performs tests and checks the time required to identify the external memory and the data load speed, if the memory performance is deemed appropriate, the following message appears:

- OK:succeeded

Otherwise, this message appears:

- NG:failed

**[Note]**

The test is meant for external memory that has just been formatted.

This function must be executed when other functions are not being used.

When this command is running, **syslog debug** on and **no syslog host** are specified. Therefore, when **syslog debug** is off, a DEBUG type SYSLOG may be output in some cases. Also, even if the **syslog host** command is specified, no log is transferred to the SYSLOG server.

This command tests the external memory for the minimum performance necessary to use the external memory function of a Yamaha router, and does not guarantee all the operations of the external memory.

When you use the external memory function, we recommend that you execute the **show status external-memory** command regularly to make sure that external memory write errors and other problems are not occurring.

**[Models]**

RTX810, RTX5000

### 37.14 Set the Function to Execute When the DOWNLOAD Button Is Pressed

---

**[Syntax]**

**operation button function download** *function* [*script\_file* [*args* ...]]

**no operation button function download** [*function* [*script\_file* [*args* ...]]]

**[Setting and Initial value]**

- *function* : The function to execute when the DOWNLOAD button is pressed

- [Setting] :

Setting	Description
http revision-up	HTTP revision update
execute batch	Batch file execution
mobile signal-strength	Acquisition of the signal reception level of a mobile terminal
execute lua	Lua script execution

- [Initial value] : http revision-up
- *script\_file*
  - [Setting] : Specify the absolute or relative path of a script file or bytecode file.
  - [Initial value] : -
- *args*
  - [Setting] : The variable arguments to pass to *script\_file*.
  - [Initial value] : -

#### [Description]

Sets the function that is executed when the DOWNLOAD button is pressed. While the function is being executed, the LED below the DOWNLOAD button lights. The LED turns off when the execution of the function is completed.

If you set the *function* parameter to execute lua, you must specify a file for the *script\_file* parameter. If you set *script\_file* to a relative path, it is interpreted as a path starting with the PWD environment variable. You can change PWD with the **set** command. Its initial value is “/”.

#### [Note]

When you execute a Lua script, if the LUA\_INIT environment variable has been specified, it will be executed before the file specified by the *script\_file* parameter.

#### [Models]

RTX810

## 37.15 Set Whether to Allow Batch File Execution through the Pressing of the DOWNLOAD Button

#### [Syntax]

**operation execute batch permit** *permit*  
**no operation execute batch permit** [*permit*]

#### [Setting and Initial value]

- *permit*
  - [Setting] :

Setting	Description
on	Allow batch file execution through the pressing of the DOWNLOAD button
off	Do not allow batch file execution through the pressing of the DOWNLOAD button

- [Initial value] : off

#### [Description]

Sets whether to allow batch file execution through the pressing of the DOWNLOAD button.

#### [Models]

RTX810

## Chapter 38

### Mobile Internet Connection Function

You can use this function to send data using an Internet connection from a mobile terminal connected to the router. Even if there is no fixed line, you can connect to the Internet if you have a mobile terminal that supports this function. This function only supports transmission, it does not support reception.

Currently, only mobile terminals that can be connected to the router with a USB cable are supported. The router controls the connected mobile terminal as a PP (USB modem), or WAN (network adapter). To use this function, you must have:

- A router that supports the function.
- A mobile terminal that supports the function.
- A provider contract that enables data transmission on the mobile terminal(mopera, etc.).

This function has preset packet transmission quantity and packet transmission time limits. When these limits are reached, the router stops transmission and is unable to transmit afterwards. You can change the limits by using the **mobile access limit length** and **mobile access limit time** commands when the router controls the mobile terminal as a PP (USB modem), and **wanaccess limit time** and **wanaccess limit length** commands when the router controls the mobile terminal as WAN (network adapter).

#### 38.1 Set Whether to Use a Mobile Terminal

##### [Syntax]

```
mobile use interface use [first-connect-wait-time=time]
no mobile use interface [use]
```

##### [Setting and Initial value]

###### • interface

- [Setting] :

Setting	Description
usb1	Use USB1 for the mobile Internet connection.

- [Initial value] : -

###### • use

- [Setting] :

Setting	Description
on	Use the mobile terminal.
off	Do not use the mobile terminal.

- [Initial value] : off

###### • time

- [Setting] :

Setting	Description
0-300	The wait time of connection after the device is attached.

- [Initial value] : 0

##### [Description]

Specify whether to use the mobile terminal connected to the specified bus to connect to the Internet.

When the *first-connect-wait-time* is set, the connection is inhibited in specified time after the device is attached. The connection request by following commands is also inhibited by this command.

- **mobile auto connect**
- **wan1 auto connect**
- **pp always-on**
- **wan1 always-on**

##### [Note]

RTX810 supports *first-connect-wait-time* option in Rev.11.01.23 or later.



**[Models]**  
RTX810

## 38.2 Set the PIN Code to Be Input to Mobile Terminal

---

### [Syntax]

**mobile pin code** *interface pin*  
**no mobile pin code** *interface [pin]*

### [Setting and Initial value]

- *interface*
  - [Setting] :

Setting	Description
usb1	USB1 interface

- [Initial value] : -
- *pin*
  - [Setting] : PIN code
  - [Initial value] : -

### [Description]

Sets a PIN code to be used when it is necessary for the use of mobile terminal to be connected to the USB interface. If a mobile terminal needs no PIN code, you can use it regardless of how this command is set.

### [Note]

When using a PIN code, you must register the PIN code in a SIM card of your mobile terminal with a connection utility of the terminal in advance. The router cannot register the PIN code in the SIM card.

If the PIN code registered in the SIM card and this command configuration do not match and matching fails three times continuously, the mobile terminal is locked automatically (PIN lock). If so, the router cannot cancel the lock. You must input a code to cancel PIN lock with the connection utility of the mobile terminal.

**[Models]**  
RTX810

## 38.3 Send a Direct Command to the Mobile Interface

---

### [Syntax]

**execute at-command** *interface command*

### [Setting and Initial value]

- *interface*
  - [Setting] :
    - usb1
  - [Initial value] : -
- *command*
  - [Setting] :
    - AT command
  - [Initial value] : -

### [Description]

Sends an AT command directly to the mobile terminal connected to the specified interface.

The following command also sends AT commands. You must be careful when using these two commands together.

**usbhost modem initialize**

### [Note]

This command is only necessary under special circumstances.

### [Example]

```
execute at-command usb1 AT+CGDCONT=<1>,"PPP","mopera.ne.jp"
```

You have to escape double quotes with a “\”.

**[Models]**  
RTX810

## 38.4 Release the Transmission Restriction on a Specified Peer

### [Syntax]

```
clear mobile access limitation [interface]
clear mobile access limitation pp [peer_num]
```

### [Setting and Initial value]

- *interface*
  - [Setting] :

Setting	Description
usb1	USB interface
wan1	WAN interface

- [Initial value] : -
- *peer\_num*

- [Setting] :

Setting	Description
Peer number	The selected peer when omitted

- [Initial value] : -

### [Description]

Releases the transmission restriction on an interface that has been imposed by the **mobile access limit** command so that the interface can send data again.

The transmission restriction is also released when you restart the router.

### [Models]

RTX810

## 38.5 Set the Interface Used for PP

### [Syntax]

```
pp bind interface
no pp bind [interface]
```

### [Setting and Initial value]

- *interface*
  - [Setting] :

Setting	Description
usb1	Use usb1

- [Initial value] : -

### [Description]

Sets the interface used for the selected peer.

### [Models]

RTX810

## 38.6 Set Automatic Transmission from the Mobile Terminal

### [Syntax]

```
mobile auto connect auto
no mobile auto connect [auto]
```

### [Setting and Initial value]

- *auto*
  - [Setting] :

Setting	Description
on	Automatically transmit from the mobile terminal

Setting	Description
off	Do not automatically transmit from the mobile terminal

- [Initial value] : off

**[Description]**

Sets whether to auto connect to the selected destination.

**[Models]**

RTX810

### 38.7 Set the Timer for Disconnecting from the Mobile Terminal

---

**[Syntax]**

**mobile disconnect time** *time*

**no mobile disconnect time** [*time*]

**[Setting and Initial value]**

- *time*
- [Setting] :

Setting	Description
1-21474836	Number of seconds
off	Disable the timer

- [Initial value] : 60

**[Description]**

Sets the time to disconnect the line when there is no data exchange on the remote pp interface for the selected peer.

**[Models]**

RTX810

### 38.8 Set the Timer for Disconnecting from the Mobile Terminal When There Is No Input

---

**[Syntax]**

**mobile disconnect input time** *time*

**no mobile disconnect input time** [*time*]

**[Setting and Initial value]**

- *time*
- [Setting] :

Setting	Description
1-21474836	Seconds
off	Disable the timer

- [Initial value] : 120

**[Description]**

Sets the time to disconnect the line when there is no data received from the remote pp interface for the selected peer.

**[Models]**

RTX810

### 38.9 Set the Timer for Disconnecting from the Mobile Terminal When There Is No Output

---

**[Syntax]**

**mobile disconnect output time** *time*

**no mobile disconnect output time** [*time*]

**[Setting and Initial value]**

- *time*
- [Setting] :

Setting	Description
1-21474836	Seconds
off	Disable the timer

- [Initial value] : 120

**[Description]**

Sets the time to disconnect the line when there is no data transmission to the remote pp interface for the selected peer.

**[Models]**

RTX810

## 38.10 Set the Access Point to Transmit To

---

**[Syntax]**

**mobile access-point name** *apn* *cid=cid* [*pdp=type*]

**no mobile access-point name** [*apn cid=cid*]

**[Setting and Initial value]**

- *apn*
  - [Setting] : Name of an access point that supports packet communication (Access Point Name)
  - [Initial value] : -
- *cid*
  - [Setting] :

Setting	Description
1-10	CID number

- [Initial value] : -
- *type*
  - [Setting] :

Setting	Description
ppp	PDP type: PPP
ip	PDP type: IP

- [Initial value] : -

**[Description]**

Sets the access point name (APN), CID number, and PDP type to assign to the selected destination. In addition, if *pdp=type* is omitted, it will usually be set to *ip*.

**[Example]**

```
mobile access-point name mopera.ne.jp cid=1 (for mopera)
mobile access-point name mopera.net cid=3 (for mopera U)
```

**[Models]**

RTX810

## 38.11 Set a Point to Transmit Which Is Specified to the Mobile Terminal

---

**[Syntax]**

**mobile dial number** *dial\_string*

**no mobile dial number** [*dial\_string*]

**[Setting and Initial value]**

- *dial\_string*
  - [Setting] : Text string to specify a point to transmit
  - [Initial value] : -

**[Description]**

Sets a point to transmit issued after ATD to the mobile terminal for the selected peer.

**[Note]**

When no setting is available, issue “ATD\*99\*\*[CID]#” with the *cid* number [CID] specified with the **mobile access-point name** command.

[Models]  
RTX810

## 38.12 Set the Packet Transmission Quantity Limit

### [Syntax]

**mobile access limit length** *length* [alert=*alert*[,*alert\_cancel*]]

**no mobile access limit length** [*length*]

### [Setting and Initial value]

- *length*
  - [Setting] :

Setting	Description
1-2147483647	The maximum number of total packet data bytes that can be sent and received
off	No limit

- [Initial value] : 200000
- *alert*
  - [Setting] : The alert value. Specify a data length or a percentage.
  - [Initial value] : -
- *alert\_cancel*
  - [Setting] : The alert cancel value. Specify a data length or a percentage.
  - [Initial value] : -

### [Description]

Sets the maximum amount of total packet data that can be sent and received for the selected peer. When the limit is reached, the router stops transmission and is unable to transmit afterwards.

Totaled values are cleared when:

- The **clear mobile access limitation** command is executed.
- The setting of the **mobile access limit duration** command is changed.
- The system is restarted.

You can check the current packet data total by using the **show status pp** command.

If you specify an *alert* value, a log entry is created when that value is exceeded.

If you specify an *alert\_cancel* cancel value, a log entry is created when the **mobile access limit duration** setting is changed and the resulting total is below the cancel value.

If you do not specify an alert cancel value, the alert will not be cancelled until the amount of total packet data for the period falls to 0.

### [Note]

The alarm value must be lower than the limit value, and the alarm cancel value must be lower than the alarm value.

Mobile terminal packet transmission fees are counted in units of 128 bytes, but there is no guarantee that the data that is actually sent and received between the router and the mobile terminal is organized in 128-byte units.

For example, if the router sends 512 bytes of data (128 bytes × 4), there is no guarantee that this corresponds to four packets worth of transmission fees. The data may be divided into more packets when it is sent and received on the mobile network.

Also, the data that flows between the router and the mobile terminal is asynchronous, and depending on the type of data, the amount of sent and received data may be greater than the amount of original data.

Therefore, you must be careful because the data length specified by this command is only an estimate.

An alert is displayed when you set this command to OFF.

[Models]  
RTX810

## 38.13 Set the Packet Transmission Time Limit

### [Syntax]

**mobile access limit time** *time* [alert=*alert*[,*alert\_cancel*]] [unit=*unit*]

**no mobile access limit time** [*time*]

### [Setting and Initial value]

- *time*

- [Setting] :

Setting	Description
1-2147483647	The maximum transmission time in seconds
off	Disable the timer

- [Initial value] : 3600
- *alert*
  - [Setting] : The alert value. Specify a number of seconds or a percentage.
  - [Initial value] : -
- *alert\_cancel*
  - [Setting] : The alert cancel value. Specify a number of seconds or a percentage.
  - [Initial value] : -
- *unit*
  - [Setting] : The unit. Specify “second” or “minute”.
  - [Initial value] : second

#### [Description]

Sets the total transmission time limit for the selected peer.

When the limit is reached, the router stops transmission and is unable to transmit afterwards.

This command operates independently from the **mobile disconnect time** command.

Totaled values are cleared when:

- The **clear mobile access limitation** command is executed.
- The setting of the **mobile access limit duration** command is changed.
- The system is restarted.

You can check the current packet transmission time total by using the **show status pp** command.

If you specify an *alert* value, a log entry is created when that value is exceeded.

If you specify an *alert\_cancel* value, a log entry is created when the **mobile access limit duration** setting is changed and the resulting total is below the cancel value.

The router will not reconnect after the total transmission time has reached the alert value. The router will reconnect again after the total transmission time goes below the alert cancel value.

If you do not specify an alert cancel value, the alert will not be cancelled until the total transmission time falls to 0.

You can make the router calculate the connection time in minutes by setting the *unit* parameter to “minute”. Seconds are rounded up to minutes.

#### [Note]

The alarm value must be lower than the limit value, and the alarm cancel value must be lower than the alarm value.

If the **mobile access limit duration** command is set, the router calculates the total transmission time within the specified duration in seconds even if the *unit* parameter is set to “minute”.

An alert is displayed when you set this command to OFF.

#### [Models]

RTX810

## 38.14 Set the Maximum Number of Consecutive Authentication Failures for a Single Peer

#### [Syntax]

**mobile call prohibit auth-error count** *count*

**no mobile call prohibit auth-error count** [*count*]

#### [Setting and Initial value]

- *count*
  - [Setting] :

Setting	Description
1-21474836	Maximum number of consecutive authentication failures
off	No transmission limit

- [Initial value] : 5

**[Description]**

Sets the maximum number of consecutive authentication failures for the selected peer. After authentication fails consecutively for the number of times specified by this command, the router will not send to the selected peer.

Transmission becomes possible again after you execute one of the following commands.

**pp auth accept / pp auth request / pp auth myname / pp auth username / no pp auth accept / no pp auth request / no pp auth myname / no pp auth username**

The transmission restriction is also released when you restart the router.

**[Models]**

RTX810

### 38.15 Set the LCP Async Control Character Map Option

---

**[Syntax]**

**ppp lcp accm** *accm*  
**no ppp lcp accm** [*accm*]

**[Setting and Initial value]**

- *accm*
- [Setting] :

Setting	Description
on	Use
off	Not use

- [Initial value] : off

**[Description]**

Sets whether to use the Async-Control-Character-Map option of [PPP, LCP] for the selected peer.

Enabling this setting can reduce communication traffic.

This setting can only used with the mobile Internet connection function.

**[Note]**

Even if on is specified, the option is not used if it is rejected by the peer. Also, whether the Async-Control-Character- Map value is sent from the router or the peer, 0x00000000 is always used.

**[Models]**

RTX810

### 38.16 Set Whether to Attach a Caller ID (186)

---

**[Syntax]**

**mobile display caller id** *switch*  
**no mobile display caller id** [*switch*]

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	Send caller ID (attach 186 to transmissions)
off	Do not send caller ID (do not attach 186 to transmissions)

- [Initial value] : off

**[Description]**

Sets whether to attach 186 to transmissions to notify the peer of the caller ID.

**[Models]**

RTX810

### 38.17 Set Whether to Output a Detailed Syslog

---

**[Syntax]**

**mobile syslog** *switch*

**no mobile syslog** [*switch*]

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	Output a detailed syslog
off	Do not output a detailed syslog

- [Initial value] : off

**[Description]**

Sets whether to output to the syslog details about AT commands transmitted to the mobile terminal. Only events after the mobile internet connection was established are logged. Events before transmission starts are not logged. The **syslog debug** on command must also be executed.

**[Models]**

RTX810

### 38.18 Set Whether to Sound an Alarm When the Mobile Terminal Is Connected

---

**[Syntax]**

**alarm mobile** *switch*

**no alarm mobile** [*switch*]

**[Setting and Initial value]**

- *switch*
- [Setting] :

Setting	Description
on	Sound alarms.
off	Do not sound alarms.

- [Initial value] : on

**[Description]**

Sets whether to sound an alarm when the mobile terminal is connected.

**[Models]**

RTX810

### 38.19 Set the Packet Transmission Quantity Limit for Each Connection

---

**[Syntax]**

**mobile access limit connection length** *length* [*alert=alert*]

**no mobile access limit connection length** [*length*]

**[Setting and Initial value]**

- *length*
- [Setting] :

Setting	Description
1-2147483647	The maximum number of packet data bytes that can be sent and received
off	No limit

- [Initial value] : off
- *alert*
  - [Setting] : The alert value. Specify a data length or a percentage.
  - [Initial value] : -

**[Description]**

Sets the maximum amount of packet data that can be sent and received in a single connection for the selected destination. The



router stops transmission when the limit is reached.

You can set the *alert* parameter to produce an alarm before the limit is reached. The alert appears in the log.

**[Note]**

Mobile terminal packet transmissions are counted in units of 128 bytes, but there is no guarantee that the data that is actually sent and received between the router and the mobile terminal is organized in 128-byte units.

For example, if the router sends 512 bytes of data (128 bytes × 4), there is no guarantee that four packets worth of transmission data have been sent. The data may be divided into more packets when it is sent and received on the mobile network.

Also, the data that flows between the router and the mobile terminal is asynchronous, and depending on the type of data, the amount of sent and received data may be greater than the amount of original data.

Therefore, you must be careful because the data length specified by this command is only an estimate.

**[Models]**

RTX810

## 38.20 Set the Packet Transmission Time Limit for Each Connection

---

**[Syntax]**

**mobile access limit connection time** *time* [*alert=alert*]

**no mobile access limit connection time** [*time*]

**[Setting and Initial value]**

- *time*

- [Setting] :

Setting	Description
1-2147483647	Maximum amount of transmission time in seconds
off	Disable the timer

- [Initial value] : off

- *alert*

- [Setting] : The alert value. Specify a number of seconds or a percentage.
- [Initial value] : -

**[Description]**

Sets the maximum amount of time over which packet data can be sent and received in a single connection for the selected destination.

The router stops transmission when the limit is reached.

This command operates independently from the **mobile disconnect time** command.

You can set the *alert* parameter to produce an alarm before the limit is reached. The alert appears in the log.

**[Models]**

RTX810

## 38.21 Set the Duration That the Transmission Limits Apply To

---

**[Syntax]**

**mobile access limit duration** *duration*

**no mobile access limit duration** [*duration*]

**[Setting and Initial value]**

- *duration*

- [Setting] :

Setting	Description
1-604800	The duration of the period that the transmission limits apply to in seconds
off	Apply the limits to all past transmissions

- [Initial value] : off

**[Description]**

Sets the period over which the transmission limits for the specified peer are applied to.

**[Models]**

RTX810

## 38.22 Acquire the Signal Reception Level

### [Syntax]

**mobile signal-strength go**

### [Description]

Acquires the signal reception level.

### [Models]

RTX810

## 38.23 Configure Signal Reception Level Acquisition

### [Syntax]

**mobile signal-strength switch** [*option=value*]

**no mobile signal-strength** [...]

### [Setting and Initial value]

- *switch* : Set whether to permit signal reception level acquisition.
- [Setting] :

Setting	Description
on	Permit
off	Do not permit

- [Initial value] : on
- *option=value* : Acquisition options
- [Setting] :
  - interface
    - The interface from which to acquire the signal reception level
  - syslog
    - Whether to output the acquisition result to an INFO level entry in the syslog

Setting	Description
on	Output
off	Not output
trans	Output only when the state transition (out-of-range or within-range) occurs

- interval
  - The interval at which to regularly acquire the signal reception level
  - Interval

Setting	Description
1..3600	Number of seconds
off	Do not acquire regularly

- Count

Setting	Description
1..1000	Count
infinity	Infinity

- [Initial value] :
  - interface=usb1
  - syslog=on
  - interval=off

### [Description]

Configures the various signal reception level acquisition settings.

The settings of this command are applied when the signal reception level is acquired for GUI display or through the **mobile**

**signal-strength go** command or the pressing of the DOWNLOAD button.

For the interval option, you can specify the number of seconds and times by separating them with commas.

If you specify the number of seconds and times for the interval option, the reception level will be obtained regularly according to the specified number after this command is executed.

You can check the regularly acquired results by executing the **show status mobile signal-strength** command. The reception level is always acquired regardless of how this command is set immediately before data transmission starts and immediately after it stops.

When the signal reception level is acquired regularly with the 'trans' is set to *syslog* option, the signal reception level is output to SYSLOG when the state transition occurs from out-of-range to within-range or from within-range to out-of-range.

When the *syslog* is set to 'on', the signal reception level is output to SYSLOG every time, and in addition, the signal reception level is output to SYSLOG when the state transition occurs from out-of-range to within-range or from within-range to out-of-range

**[Note]**

The router cannot acquire the signal reception level while it is connected to a PP interface.

**[Models]**

RTX810

## 38.24 Displaying Regularly Acquired Signal Reception Levels

---

**[Syntax]**

**show status mobile signal-strength** [reverse]

**[Setting and Initial value]**

- reverse : Shows the log from the newest event.
  - [Initial value] : -

**[Description]**

Shows up to 256 acquisition results when the router has been configured by the **mobile signal-strength** command to regularly acquire signal reception levels. If the number of acquired levels exceeds 256, older levels are deleted. This command normally shows the log from the oldest event. However, you can show the log from the newest event by specifying reverse.

**[Note]**

When a mobile terminal is connected, the information displayed by this command is cleared when you press the USB button for 2 or more seconds and release the connection between the terminal and the router.

**[Models]**

RTX810

## 38.25 Set the AT Commands to Use to Initialize the Device Connected to the USB Port

---

**[Syntax]**

**usbhost modem initialize** *interface command* [*command\_list*]  
**no usbhost modem initialize** *interface*

**[Setting and Initial value]**

- *interface* : Interface Name
  - [Setting] :
    - usb1
  - [Initial value] : -
- *command*
  - [Setting] : AT command string (up to 64 characters)
  - [Initial value] : -
- *command\_list*
  - [Setting] : List of AT command strings delimited by spaces
  - [Initial value] : -

**[Description]**

Sets the AT commands to use to initialize the device connected to the USB port.

The AT commands that you specify using this command are sent to the device when the router is started with the device connected to it and when the device is connected to a running router.

Specify the commands using AT command strings that start with AT (for attention).

It is possible to specify multiple commands in a single AT command string.

**[Note]**

This initialization setting is not necessary when you perform remote setup through FOMA.

**[Models]**

RTX810

## 38.26 Set Whether to Perform Flow Control on the Device Connected to the USB Port

---

**[Syntax]**

**usbhost modem flow control** *interface sw*  
**no usbhost modem flow control** *interface*

**[Setting and Initial value]**

- *interface* : Interface Name

- [Setting] :

- usb1

- [Initial value] : -

- *sw*

- [Setting] :

Setting	Description
on	Perform flow control.
off	Do not perform flow control.

- [Initial value] :

- off

**[Description]**

Sets whether to perform flow control on the device connected to the USB port.

When you are performing remote setup communication using the connected device, if the device is being disconnected when you don't want it to be, setting this command to off may be effective.

**[Models]**

RTX810

## 38.27 Set Its Own Name and Password

---

**[Syntax]**

**wan auth myname** *myname password*  
**no wan auth myname** [*myname password*]

**[Setting and Initial value]**

- *wan*

- [Setting] :

Setting	Description
wan1	WAN interface name

- [Initial value] : -

- *myname*

- [Setting] : Name (up to 64 characters)

- [Initial value] : -

- *password*

- [Setting] : Password (up to 64 characters)

- [Initial value] : -

**[Description]**

Sets its own name and password that are sent at the time of connection on the mobile Internet.

**[Models]**

RTX810

## 38.28 Set the Interface Used for WAN

---

**[Syntax]**

*wan bind interface*  
**no wan bind** [*interface*]

**[Setting and Initial value]**

- *wan*
  - [Setting] :

Setting	Description
wan1	WAN interface name

- [Initial value] : -
- *interface*
  - [Setting] :

Setting	Description
usb1	USB interface name

- [Initial value] : -

**[Description]**

Sets the specified WAN interface that is actually used.

**[Models]**

RTX810

## 38.29 Set Automatic Transmission from the Mobile Terminal

---

**[Syntax]**

*wan auto connect auto*  
**no wan auto connect** [*auto*]

**[Setting and Initial value]**

- *wan*
  - [Setting] :

Setting	Description
wan1	WAN interface name

- [Initial value] : -
- *auto*
  - [Setting] :

Setting	Description
on	Automatically transmit from the mobile terminal
off	Do not automatically transmit from the mobile terminal

- [Initial value] : off

**[Description]**

Sets whether to automatically connect to the specified WAN interface.

**[Models]**

RTX810

## 38.30 Set the Timer for Disconnecting from the Mobile Terminal

---

**[Syntax]**

*wan disconnect time time*  
**no wan disconnect time** [*time*]

**[Setting and Initial value]**

- *wan*
  - [Setting] :

Setting	Description
wan1	WAN interface name

- [Initial value] : -
- *time*
- [Setting] :

Setting	Description
1-21474836	Number of seconds
off	Disable the timer

- [Initial value] : 60

**[Description]**

Sets the time to disconnect the line when there is no data exchange on the specified WAN interface.

**[Models]**

RTX810

### 38.31 Set the Timer for Disconnecting from the Mobile Terminal When There Is No Input

---

**[Syntax]**

```
wan disconnect input time time
no wan disconnect input time [time]
```

**[Setting and Initial value]**

- *wan*
- [Setting] :

Setting	Description
wan1	WAN interface name

- [Initial value] : -
- *time*
- [Setting] :

Setting	Description
1-21474836	Number of seconds
off	Disable the timer

- [Initial value] : 120

**[Description]**

Sets the time to disconnect the line when there is no data received on the specified WAN interface.

**[Models]**

RTX810

### 38.32 Set the Timer for Disconnecting from the Mobile Terminal When There Is No Output

---

**[Syntax]**

```
wan disconnect output time time
no wan disconnect output time [time]
```

**[Setting and Initial value]**

- *wan*
- [Setting] :

Setting	Description
wan1	WAN interface name

- [Initial value] : -
- *time*
- [Setting] :

Setting	Description
1-21474836	Number of seconds
off	Disable the timer

- [Initial value] : 120

#### [Description]

Sets the time to disconnect the line when there is no data transmission from the specified WAN interface.

#### [Models]

RTX810

## 38.33 Set Permanent Connection

#### [Syntax]

*wan always-on switch [time]*

**no wan always-on**

#### [Setting and Initial value]

- *wan*

- [Setting] :

Setting	Description
wan1	WAN interface name

- [Initial value] : -

- *switch*

- [Setting] :

Setting	Description
on	Enable permanent connection
off	Disable permanent connection

- [Initial value] : off

- *time*

- [Setting] : Number of seconds until reconnection is requested (60..21474836)

- [Initial value] : -

#### [Description]

Sets whether or not to enable permanent connection for the specified WAN interface. Also, sets the time interval for requesting a reconnection, when the permanent connection is terminated. When permanent connection is set, connection is started at startup, and reconnection is started when the communication is terminated. If the connection fails or the communication terminates abnormally, a reconnection request is made after waiting the time interval specified in *time*. If the communication terminates normally, a reconnection request is made immediately. If *switch* is set to on, the *time* setting is activated. If *time* is not specified, *time* of 60 will be used.

#### [Models]

RTX810

## 38.34 Set the Access Point to Transmit To

#### [Syntax]

*wan access-point name apn*

**no wan access-point name [apn]**

#### [Setting and Initial value]

- *wan*

- [Setting] :

Setting	Description
wan1	WAN interface name

- [Initial value] : -

- *apn*

- [Setting] : Name of an access point that supports the mobile Internet communication (Access Point Name)

- [Initial value] : -

**[Description]**

Sets the access point name (APN) to assign to the specified WAN interface.

**[Models]**

RTX810

### 38.35 Set the Packet Transmission Quantity Limit

---

**[Syntax]**

*wan* **access limit length** *length* [*alert=alert*[,*alert\_cancel*]]

**no wan access limit length** [*length*]

**[Setting and Initial value]**

- *wan*

- [Setting] :

Setting	Description
wan1	WAN interface name

- [Initial value] : -

- *length*

- [Setting] :

Setting	Description
1-2147483647	The maximum number of total packet data bytes that can be sent and received
off	No limit

- [Initial value] : 200000

- *alert*

- [Setting] : The alert value. Specify a data length or a percentage.

- [Initial value] : -

- *alert\_cancel*

- [Setting] : The alert cancel value. Specify a data length or a percentage.

- [Initial value] : -

**[Description]**

Sets the maximum amount of total packet data that can be sent and received for the specified WAN interface.

When the limit is reached, the router stops transmission and is unable to transmit afterwards.

Totaled values are cleared when:

- The **clear mobile access limitation** command is executed.
- The setting of the **wan access limit duration** command is changed.
- The system is restarted.

You can check the current packet data total by using the **show status wan1** command.

If you specify an *alert* value, a log entry is created when that value is exceeded.

If you specify an *alert\_cancel* value, a log entry is created when the **wan access limit duration** setting is changed and the resulting total is below the cancel value.

If you do not specify an alert cancel value, the alert will not be cancelled until the amount of total packet data for the period falls to 0.

**[Note]**

The alarm value must be lower than the limit value, and the alarm cancel value must be lower than the alarm value.

Mobile terminal packet transmissions are counted in units of 128 bytes, but there is no guarantee that the data that is actually sent and received between the router and the mobile terminal is organized in 128-byte units.

For example, if the router sends 512 bytes of data (128 bytes  $\times$  4), there is no guarantee that four packets worth of transmission data have been sent. The data may be divided into more packets when it is sent and received on the mobile network.

Also, the data that flows between the router and the mobile terminal is asynchronous, and depending on the type of data, the amount of sent and received data may be greater than the amount of original data.

Therefore, you must be careful because the data length specified by this command is only an estimate.

An alert is displayed when you set this command to OFF.



[Models]  
RTX810

## 38.36 Set the Packet Transmission Time Limit

### [Syntax]

*wan* **access limit time** *time* [alert=*alert*[,*alert\_cancel*]] [unit=*unit*]

**no** *wan* **access limit time** [*time*]

### [Setting and Initial value]

- wan*

- [Setting] :

Setting	Description
wan1	WAN interface name

- [Initial value] : -

- time*

- [Setting] :

Setting	Description
1-2147483647	The maximum transmission time in seconds
off	Disable the timer

- [Initial value] : 3600

- alert*

- [Setting] : The alert value. Specify a number of seconds or a percentage.

- [Initial value] : -

- alert\_cancel*

- [Setting] : The alert cancel value. Specify a number of seconds or a percentage.

- [Initial value] : -

- unit*

- [Setting] : The unit. Specify “second” or “minute”.

- [Initial value] : second

### [Description]

Sets the total transmission time limit for the specified WAN interface.

When the limit is reached, the router stops transmission and is unable to transmit afterwards.

This command operates independently from the **wan disconnect time** command.

Totaled values are cleared when:

- The **clear mobile access limitation** command is executed.
- The setting of the **wan access limit duration** command is changed.
- The system is restarted.

You can check the current packet transmission time total by using the **show status wan1** command.

If you specify an *alert* value, a log entry is created when that value is exceeded.

If you specify an *alert\_cancel* value, a log entry is created when the **wan access limit duration** setting is changed and the resulting total is below the cancel value.

The router will not reconnect after the total transmission time has reached the alert value. The router will reconnect again after the total transmission time goes below the alert cancel value.

If you do not specify an alert cancel value, the alert will not be cancelled until the total transmission time falls to 0.

You can make the router calculate the connection time in minutes by setting the *unit* parameter to “minute”. Seconds are rounded up to minutes.

### [Note]

The alarm value must be lower than the limit value, and the alarm cancel value must be lower than the alarm value.

If the **wan access limit duration** command is set, the router calculates the total transmission time within the specified duration in seconds even if the *unit* parameter is set to “minute”.

An alert is displayed when you set this command to OFF.

[Models]  
RTX810

### 38.37 Set the Packet Transmission Quantity Limit for Each Connection

#### [Syntax]

*wan* **access limit connection length** *length* [*alert=alert*]

**no** *wan* **access limit connection length** [*length*]

#### [Setting and Initial value]

- *wan*

- [Setting] :

Setting	Description
wan1	WAN interface name

- [Initial value] : -

- *length*

- [Setting] :

Setting	Description
1-2147483647	The maximum number of packet data bytes that can be sent and received
off	No limit

- [Initial value] : off

- *alert*

- [Setting] : The alert value. Specify a data length or a percentage.

- [Initial value] : -

#### [Description]

Sets the maximum amount of packet data that can be sent and received in a single connection for the specified WAN interface. The router stops transmission when the limit is reached.

You can set the *alert* parameter to produce an alarm before the limit is reached. The alert appears in the log.

#### [Note]

Mobile terminal packet transmissions are counted in units of 128 bytes, but there is no guarantee that the data that is actually sent and received between the router and the mobile terminal is organized in 128-byte units.

For example, if the router sends 512 bytes of data (128 bytes × 4), there is no guarantee that four packets worth of transmission data have been sent. The data may be divided into more packets when it is sent and received on the mobile network.

Also, the data that flows between the router and the mobile terminal is asynchronous, and depending on the type of data, the amount of sent and received data may be greater than the amount of original data.

Therefore, you must be careful because the data length specified by this command is only an estimate.

#### [Models]

RTX810

### 38.38 Set the Packet Transmission Time Limit for Each Connection

#### [Syntax]

*wan* **access limit connection time** *time* [*alert=alert*]

**no** *wan* **access limit connection time** [*time*]

#### [Setting and Initial value]

- *wan*

- [Setting] :

Setting	Description
wan1	WAN interface name

- [Initial value] : -

- *time*

- [Setting] :

Setting	Description
1-2147483647	Maximum amount of transmission time in seconds
off	Disable the timer

- [Initial value] : off
- *alert*
  - [Setting] : The alert value. Specify a number of seconds or a percentage.
  - [Initial value] : -

**[Description]**

Sets the maximum amount of time over which packet data can be sent and received in a single connection for the specified WAN interface.

The router stops transmission when the limit is reached.

This command operates independently from the **wan disconnect time** command.

You can set the *alert* parameter to produce an alarm before the limit is reached. The alert appears in the log.

**[Models]**

RTX810

### 38.39 Set the Duration That the Transmission Limits Apply To

---

**[Syntax]**

*wan access limit duration duration*

**no wan access limit duration** [*duration*]

**[Setting and Initial value]**

- *wan*
  - [Setting] :

Setting	Description
wan1	WAN interface name

- [Initial value] : -
- *duration*

- [Setting] :

Setting	Description
1-604800	The duration of the period that the transmission limits apply to in seconds
off	Apply the limits to all past transmissions

- [Initial value] : off

**[Description]**

Sets the past period over which the transmission limits for the specified WAN interfaced are applied to.

**[Models]**

RTX810

## Chapter 39

### Bridge Interface(Bridge function)

Bridge interface is a feature that is housed in a single virtual interface multiple interfaces, which performs the bridging between housed interfaces.

A physical segment connected by each housed interface will be treated as a single segment.

#### Notes

- Bridge processing in this function does not mean a wire rate.
- QoS features are not supported. Dynamic Traffic Control in QoS function is not available.
- Spanning tree protocol is not supported.
- BPDU frames are transmitted.
- IEEE802.1Q tagged packets are transmitted.

### 39.1 Configuring member interfaces for bridge interface

#### [Syntax]

```
bridge member bridge_interface interface interface [...]
```

```
no bridge member bridge_interface [interface ...]
```

#### [Setting and Initial value]

- *bridge\_interface*
  - [Setting] : Bridge interface name
  - [Initial value] : -
- *interface*
  - [Setting] :

Setting	Description
lanN	LAN interface name
lanN.M	LAN division interface name
vlanN	VLAN interface name
tunnelN	TUNNEL interface name
tunnelN-tunnelM	TUNNEL interface range

- [Initial value] : -

#### [Description]

Defines the interface that will be a member of the bridge virtual interface. The bridge operates between interfaces that are members. If a tunnel interface is a member, the bridge will only operate on tunnel interfaces that are certified as L2TPv3 tunnels.

#### [Note]

- About member LAN interfaces  
IPv4,IPv6 addresses are not assigned to actual interfaces that are members. The IPv6 link local address of an actual interface that is a member is deleted. The MTU value must be identical for all member LAN interfaces. An actual interface that is a member of one bridge interface cannot be a member of a different bridge interface. If the member interface has a switching hub, the bridge operation for this feature does not operate on the communications between the ports of the switching hub, but it is processed internally within the switching hub LSI. Specification of VLAN interface name is only supported on models that have the expanded features for the LAN division feature.
- About member tunnel interfaces  
The MTU for member tunnel interface are invalid, and fragmentation of the tunnel interface is not carried out. Fragmentation occurs based on the MTU of the sending interface for the encapsulated packet. An interface that is a member of one bridge interface cannot be a member of a different bridge interface. Specification of a tunnel interface as a member interface is only possible on models that have the L2TPv3 feature enabled.
- About bridge interfaces  
The link status of the bridge interface depends on the link status of the member LAN interfaces or member tunnel interfaces. If

either of the member interfaces is up, the bridge interface is up. If all interfaces are down, the bridge interface is down. The smallest interface number of all the member LAN interfaces is used as the MAC address of the bridge interface.

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

## 39.2 Setting whether to automatically execute learning

**[Syntax]**

**bridge learning** *bridge\_interface* *switch*  
**no bridge learning** *bridge\_interface* [*switch*]

**[Setting and Initial value]**

- *bridge\_interface*
  - [Setting] : Bridge interface name
  - [Initial value] : -
- *switch*
  - [Setting] :

Setting	Description
on	Learning is active
off	Learning is disabled

- [Initial value] : on

**[Description]**

Configure whether or not the bridge feature will automatically learn MAC addresses. *bridge\_interface* specifies the affected bridge interface name. If learning is executed, when a packet is received by the interface inside the bridge interface, the MAC address and receiving interface of that packet will be learned and registered in the learning table.

The learned information will be referenced during bridge processing, and the packet will reduce unnecessary output by the interface.

**[Note]**

If the learning table exceeds the maximum limit during learning, the oldest entry will be deleted and the new entry will be registered. When the learning table is referenced during bridge processing, if a corresponding entry does not exist, all included interfaces (with the exception of the receiving interface) will output the packet. It operates in the same way as a repeater.

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

## 39.3 Setting the deletion timer for bridge learning information

**[Syntax]**

**bridge learning** *bridge\_interface* **timer** *time*  
**no bridge learning** *bridge\_interface* **timer** [*time*]

**[Setting and Initial value]**

- *bridge\_interface*
  - [Setting] : Bridge interface name
  - [Initial value] : -
- *time*
  - [Setting] :

Setting	Description
30..32767	Number of seconds
off	Timer is not configured

- [Initial value] : 300

**[Description]**

Configures the lifetime for the information that the bridge automatically learns. The bridge interface name is specified by *bridge\_interface*. If a packet with a certain source MAC address is not received within the specified time, the learned information for that MAC address will be deleted.

If off is selected, the learned information will not be automatically deleted.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

## 39.4 Configuring the static learning information

---

**[Syntax]**

```
bridge learning bridge_interface static mac_address interface
no bridge learning bridge_interface static mac_address [interface]
```

**[Setting and Initial value]**

- *bridge\_interface*
  - [Setting] : Bridge interface name
  - [Initial value] : -
- *mac\_address*
  - [Setting] : MAC address
  - [Initial value] : -
- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -

**[Description]**

Configures the static registration information that the bridge will reference. The bridge interface name is specified by *bridge\_interface*. The address packet with the MAC address specified in *mac\_address* will be output to the interface specified in *interface*. *interface* specifies the LAN interface that is a member of the *bridge\_interface*.

**[Note]**

Information that has been statically registered is given precedence over automatically learned information. If the LAN interface specified in *interface* is not a member of *bridge\_interface*, the registered information will be ignored.

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

## Chapter 40

### Lua Script Function

This function allows execution of scripts described with the Lua language. By integration of API dedicated for Yamaha router into the Lua scripts, you can change the router configuration and program actions according to the router condition.

#### 40.1 Set Whether to Enable the Lua Script Function

##### [Syntax]

**lua use** *switch*  
**no lua use** [*switch*]

##### [Setting and Initial value]

- *switch*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : on

##### [Description]

Sets whether to enable the Lua script function.

If you use this command to disable the Lua script function, any Lua scripts that are running are stopped.

##### [Models]

RTX810, RTX5000

#### 40.2 Execute a Lua Script

##### [Syntax]

**lua** [-e *stat*] [-l *module*] [-v] [--] [*script\_file* [*args* ...]]

##### [Setting and Initial value]

- *stat*
  - [Setting] : Script character string
  - [Initial value] : -
- *module*
  - [Setting] : The module to load (require)
  - [Initial value] : -
- *script\_file*
  - [Setting] : Specify the absolute or relative path of a script file or bytecode file.
  - [Initial value] : -
- *args*
  - [Setting] : The variable arguments to pass to *script\_file*.
  - [Initial value] : -

##### [Description]

Executes a Lua script.

The basic syntax is the same as that for standard **lua** commands, however, the router does not support execution without parameters or the “-i” and “-” options for using the standard input (stdin) as the script's input. The “-v” option outputs the version information.

-- The “--” option terminates the option at the described point, and you can specify a file name and text string starting from “-” for *script\_file* and *args*.

The “-e”, “-l”, and “-v” options can be specified multiple times, but they cannot be specified after *script\_file*. You can only specify one file for the *script\_file* parameter. Any parameters listed after the *script\_file* parameter are ignored. No error message appears to indicate ignored parameters.

If you set *script\_file* to a relative path, it is interpreted as a path starting with the PWD environment variable. You can change PWD with the **set** command. Its initial value is “/”.

**[Note]**

If the `LUA_INIT` environment variable has been set, the script that is specified is executed first.

For the `script_file` parameter, you can only specify bytecode files that were created on the router. You cannot execute bytecode files that have been created by other devices, such as a PC with Lua installed on it.

**[Models]**

RTX810, RTX5000

## 40.3 Execute the Lua Compiler

---

**[Syntax]**

```
luac [-l] [-o output_file] [-p] [-s] [-v] [--] script_file [script_file ..]
```

**[Setting and Initial value]**

- *output\_file*
  - [Setting] : Specify the absolute or relative path of the bytecode file to output to.
  - [Initial value] : luac.out (relative path)
- *script\_file*
  - [Setting] : Specify the absolute or relative path of the script file to compile.
  - [Initial value] : -

**[Description]**

Executes the Lua compiler and creates a bytecode file.

The fundamental syntax is the same as that of the standard Lua `luac` command, except that the “-” option cannot be specified. The “-l” option generates a list of the bytecode. The “-p” option only performs syntax analysis. The “-s” option removes comments and other debugging information. The “-v” option outputs the version information.

-- The “--” option terminates the option at the described point, and you can specify a file name starting from “-“ for *script\_file*. You can include multiple *script\_file* specifications and make them into a single bytecode file.

If you set *script\_file* or *output\_file* to a relative path, it is interpreted as a path starting with the PWD environment variable. You can change PWD with the `set` command. Its initial value is “/”.

**[Models]**

RTX810, RTX5000

## 40.4 Show the Status of Running Lua Scripts

---

**[Syntax]**

```
show status lua [info]
```

**[Setting and Initial value]**

- *info* : Type of information to be shown
  - [Setting] :

Setting	Description
running	Information about currently running scripts
history	Information about scripts that ran in the past
Omitted	All information is displayed

- [Initial value] : -

**[Description]**

Displays status of the Lua script running currently, and its past operation history. This information is cleared if you disable the Lua script function using the `lua use` command.

- Lua version information
- Running scripts [running]
  - Lua task number
  - Running status

RUN	Running
SLEEP	Sleeping
WATCH	Monitoring SYSLOG (the Lua task is sleeping)



COMMUNICATE	Sending and receiving the HTTP message
TERMINATE	Stopping forcedly

- Trigger
  - **lua** command
  - **luac** command
  - Schedule
  - DOWNLOAD button
- Command line
- Script file name
- Text string to be monitored (when SYSLOG is being monitored)
- Starting date and time and run time
- Scripts ran in the past[history] (the most recent 10 with the newest script listed first)
  - Trigger
    - **lua** command
    - **luac** command
    - Schedule
    - DOWNLOAD button
  - Command line
  - Script file name
  - Number of times ran/number of errors/Error history (the most recent five with the newest message listed first)
  - The latest start date and time, end time, and result

**[Models]**

RTX810, RTX5000

## 40.5 Stop a Lua Script

**[Syntax]****terminate lua** *task\_id***terminate lua file** *script\_file***[Setting and Initial value]**

- *task\_id* : The number of the Lua task that you want to stop
  - [Setting] :

Setting	Description
all	All Lua task numbers
1..10 (for models without DOWNLOAD button 1..9)	A Lua task number

- [Initial value] : -
- *script\_file*
  - [Setting] : Specify the absolute or relative path of the script file or bytecode file that you want to stop.
  - [Initial value] : -

**[Description]**

Stops the specified Lua task or script.

In the first syntax, the Lua task specified by the *task\_id* parameter is stopped. You can view Lua task numbers and scripts that are currently being executed by executing the **show status lua** command.

In the second syntax, all Lua tasks that are executing the script that matches perfectly with the path and file name specified by *script\_file* are stopped. If you specify a relative path for *script\_file*, the router searches for Lua tasks after first converting the path to an absolute path that starts with environment variable PWD.

To stop Lua scripts that are using the -e option and running without a script file, use the first syntax.

**[Models]**

RTX810, RTX5000

## 40.6 Set Whether to Sound Alarms for the Lua Script Function

**[Syntax]****alarm lua** *switch*

**no alarm lua** [*switch*]

**[Setting and Initial value]**

- *switch*

- [Setting] :

Setting	Description
on	Sound alarms.
off	Do not sound alarms.

- [Initial value] : on

**[Description]**

Sets whether to sound alarms for the Lua script function.

**[Models]**

RTX810

# Chapter 41

## Custom GUI

The custom GUI function allows users to design and integrate unique GUI (user interface to support the WWW browser). The router has an interface to transfer settings from the host with HTTP. Use JavaScript to create your GUI.

Although the Yamaha router has the WWW browser setup assistance function, the configuration GUI could not be changed for each user. With multiple custom GUIs integrated in the router, this function allows each user to switch the configuration GUI.

### 41.1 Set Whether to Use the Custom GUI

#### [Syntax]

```
httpd custom-gui use use
no httpd custom-gui use [use]
```

#### [Setting and Initial value]

- *use*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : off

#### [Description]

Sets whether to use the custom GUI.

#### [Models]

RTX810

### 41.2 Configure Custom GUI User Settings

#### [Syntax]

```
httpd custom-gui user [user] directory=path [index=name]
no httpd custom-gui user [user...]
```

#### [Setting and Initial value]

- *user*
  - [Setting] : User name
  - [Initial value] : -
- *path*
  - [Setting] : The absolute or relative path of the starting directory
  - [Initial value] : -
- *name*
  - [Setting] : The file that appears when the user accesses the GUI through a URL that ends with a slash
  - [Initial value] : index.html

#### [Description]

Configures custom GUI user settings. When you access `http://(the IP address of the router)/` and login with a user name specified by this command, you will be redirected to `http://(the IP address of the router)/custom/user/`.

If you omit the *user* parameter, the settings for an anonymous user are configured. The URL in this case is `http://(the IP address of the router)/custom/anonymous.user/`.

Set the *path* parameter to the absolute directory of the starting path or to a relative path. If you set to a relative path, it is interpreted as a path starting with the PWD environment variable. You can change PWD with the set command. Its initial value is `"/`.

Set the *name* parameter to the file name that you want to display when the user accesses the GUI through a URL that ends with a slash.

#### [Note]

Before you configure the settings for any user other than an anonymous user with this command, you must first register the user with **login user** user command. An error will occur if you execute this command using the name of an unregistered user.

The users whose settings are configured by this command cannot access the normal internal router GUI.

**[Models]**  
RTX810

### 41.3 Set Whether to Use the Custom GUI API

---

**[Syntax]**

```
httpd custom-gui api use use
no httpd custom-gui api use [use]
```

**[Setting and Initial value]**

- *use*
- [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : off

**[Description]**

Sets whether to accept POST requests to the API URL, which is “http://(the IP address of the router)/custom/api”.

**[Note]**

To use the API URL, in addition to setting this command, you must also execute the **httpd custom-gui use on** command. Even when setting this command on, you cannot use the URL for the API without specifying the **httpd custom-gui api password** command.

**[Models]**  
RTX810

### 41.4 Set the Password for Accessing the Custom GUI API

---

**[Syntax]**

```
httpd custom-gui api password password
no httpd custom-gui api password [password]
```

**[Setting and Initial value]**

- *password*
- [Setting] : Password
- [Initial value] : -

**[Description]**

Sets the password that is used when POST requests are sent to the API URL. The password can be set using up to 32 alphanumeric characters.

For example, if you use this command to set the password to doremi, the URL will be http://(the IP address of the router)/custom/api?password=doremi.

**[Models]**  
RTX810

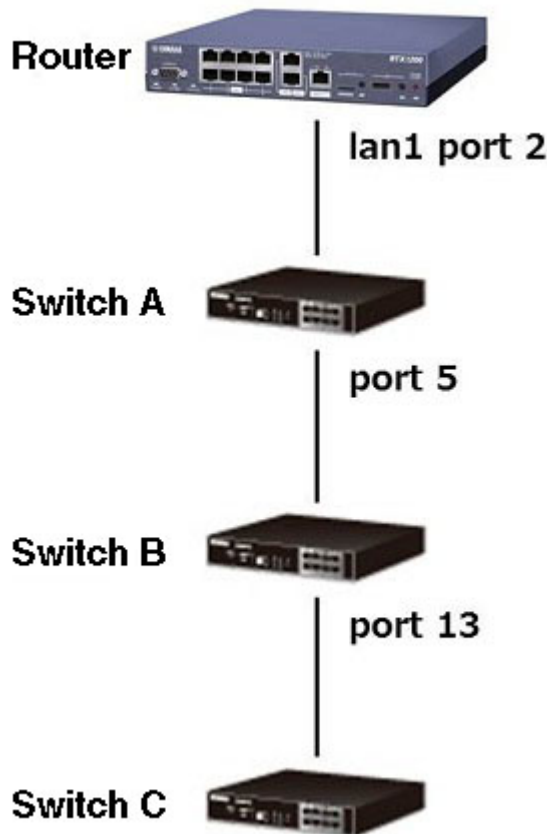
## Chapter 42

### Switch Control Function

The switch control function allows control of the Yamaha switches and wifi access point from the router. Refer the related command for each models in addition to the common settings for management of them.

You can specify a switch or wifi access point with each command of this switch with two ways: specify with a MAC address, and specifying with a route.

When specifying with a route, describe port numbers of each switch on the way from the router as a starting point in sequence.



A notation to specify the switch C in the configuration above is "lan1:2-5-13".

- Specify a LAN interface of the router first.
- When the LAN interface is a switching hub, specify a port number. Delimit the LAN interface name and the port number with ":" (colon).
- When the LAN interface is not a switching hub, you don't have to specify a port number.
- Specify port numbers between the router and switch C from the closest in sequence. Delimit the port numbers with "-" (hyphen).

#### 42.1 Switch Control Function

##### 42.1.1 Set Whether to Use the Switch Control Function

###### [Syntax]

**switch control use** *interface use*

**no switch control use** *interface*

###### [Setting and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *use*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : off

#### [Description]

Sets whether to use the switch control function for each LAN interface. An interface for which this command is set on communicates to control the switch supporting the switch control function. For the interface that does not connect a switch supporting the switch control function underneath, set this command off to prevent transmission of unnecessary packets.

#### [Note]

You can specify a physical LAN interface (lanN) only for *interface*. For the interface for which the LAN division function or the port division function is enabled, you cannot specify this command.

#### [Models]

RTX810

### 42.1.2 Set the Time Interval for Watching Switch

---

#### [Syntax]

```
switch control watch interval time [count]
no switch control watch interval
```

#### [Setting and Initial value]

- *time*
  - [Setting] : Number of seconds (2 .. 10)
  - [Initial value] : 3
- *count*
  - [Setting] : Count (2 .. 10)
  - [Initial value] : 3

#### [Description]

Sets the time interval for sending a packet to search a switch, and the number of times to send a search packet until the router receives no response packet from the switch and decides that the switch is down.

When a large value is specified for *time*, frequency of sending a search packet is decreased, but time that the router needs to identify a switch after connecting it gets longer. On the contrary, when a small value is specified for *time*, frequency of sending a search packet is increased, but time that the router needs to identify a switch after connecting it gets shorter.

When the router receives no response packet from the switch even after sending a search packet the number of times specified in *count*, it decides that the switch is down.

#### [Note]

If an Ethernet cable connecting the switch is removed, the router may decide that the switch is down earlier than the setting specified with this command.

#### [Models]

RTX810

### 42.1.3 Select the Switch

---

#### [Syntax]

```
switch select switch
no switch select
```

#### [Setting and Initial value]

- *switch*
  - [Setting] :

Setting	Description
Switches	MAC address or route
none	Not select a switch

- [Initial value] : -

#### [Description]

Selects a target switch. After this command, the prompt shows the text string selected by the console prompt command followed by the selected switch.

When the **switch select** none command or the **no switch select** command is executed, the prompt stops showing the switch.

**[Models]**

RTX810

#### 42.1.4 Set the Functions That the Switch Has

---

**[Syntax]**

**switch control function set** *function* [*index ...*] *value*  
**no switch control function set** *function* [*index ...*]

**[Setting and Initial value]**

- *function*
  - [Setting] : Function name
  - [Initial value] : -
- *index*
  - [Setting] : Index
  - [Initial value] : -
- *value*
  - [Setting] : Setting
  - [Initial value] : -

**[Description]**

Sets the configuration of functions that the switch has. Specify a setting value for the function you want to configure as a parameter. For the function needing multiple settings, specify an index.

To stop the running command, hold down Ctrl-C. However, if synchronous process starts after execution, you cannot stop.

**[Note]**

Before executing this command, you must specify a switch with the **switch select** command.

**[Models]**

RTX810

#### 42.1.5 Obtain the Configuration and Operation Status of the Functions That the Switch Has

---

**[Syntax]**

**switch control function get** *function* [*index ...*] [*switch*]

**[Setting and Initial value]**

- *function*
  - [Setting] : Function name
  - [Initial value] : -
- *index*
  - [Setting] : Index
  - [Initial value] : -
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Obtains the configuration and operation status of the functions that the switch has. Specify a name of function that you want to obtain as a parameter. For the function having multiple targets to be obtained, specify an index.

To stop the running command, hold down Ctrl-C.

**[Note]**

If you do not specify *switch*, you must specify a switch with the **switch select** command before executing this command.

**[Models]**

RTX810

#### 42.1.6 Execute a Specified Operation for the Switch

---

**[Syntax]**

**switch control function execute** *function* [*index ...*] [*switch*]

**[Setting and Initial value]**

- *function*
  - [Setting] : Function name
  - [Initial value] : -
- *index*
  - [Setting] : Index
  - [Initial value] : -
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Lets the router execute a specified operation for the switch. Specify a name of function that you want to execute as a parameter. For the function having multiple targets to be executed, specify an index.

To stop the running command, hold down Ctrl-C.

**[Note]**

If you do not specify *switch*, you must specify a switch with the **switch select** command before executing this command.

**[Models]**

RTX810

### 42.1.7 Delete the Switch Setting

---

**[Syntax]**

**switch control function default** [both] [*switch*]

**[Setting and Initial value]**

- *both* : Deletes all applicable settings of the target switch
  - [Initial value] : -
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Deletes the settings on the router about the selected switch. At the same time, performs synchronous process when the router controls the switch.

If the both option is not specified and when another applicable setting about the switch exists, the switch is synchronized according to that setting. For example, when you select a setting by MAC address specification instead of another setting by route specification, which is also available, and execute this command, the switch is synchronized according to the setting by route specification after the setting by MAC address specification is deleted.

When the both option is specified and when another applicable setting about the switch exists, that setting is deleted simultaneously. In the example above, both settings by MAC address specification and by route specification are deleted.

In other words, when you want to initialize a switch reliably, specify the both option.

**[Note]**

If you do not specify *switch*, you must specify a switch with the **switch select** command before executing this command.

**[Models]**

RTX810

### 42.1.8 Update the Firmware of the Switch

---

**[Syntax]**

**switch control firmware upload go file** [*switch*]

**[Setting and Initial value]**

- *file*
  - [Setting] : Relative path or absolute path to the firmware file
  - [Initial value] : -
- *switch* : Switches
  - [Setting] :



- MAC address
- Route
- [Initial value] : -

**[Description]**

Updates the firmware of the switch. Store the firmware file in the flash or external memory in advance, and specify a path in *file*. When the firmware is successfully updated, the switch automatically starts up.

To stop the running command, hold down Ctrl-C.

If you set *file* to a relative path, it is interpreted as a path starting with the PWD environment variable. You can change PWD with the **set** command. Its initial value is “/”.

**[Note]**

If you do not specify *switch*, you must specify a switch with the **switch select** command before executing this command.

**[Models]**

RTX810

### 42.1.9 Set the Ethernet Cable Redundancy

---

**[Syntax]**

**switch control route backup** *route port*

**no switch control route backup** *route*

**[Setting and Initial value]**

- *route*
  - [Setting] : Master Route
  - [Initial value] : -
- *port*
  - [Setting] : Port number for use as a backup route
  - [Initial value] : -

**[Description]**

Set the main route and backup route for ethernet cable redundancy.

**[Note]**

Following port can not be set as the port for use as a backup route.

- The port set as main route
- The port ethernet cable redundancy is already configured

When this command is configured to switching-hub on router, the ethernet cable redundancy is enabled only when the switch control function is enable on LAN interface which has switching-hub.

When this command is configured to the switches, target port is linked down temporarily.

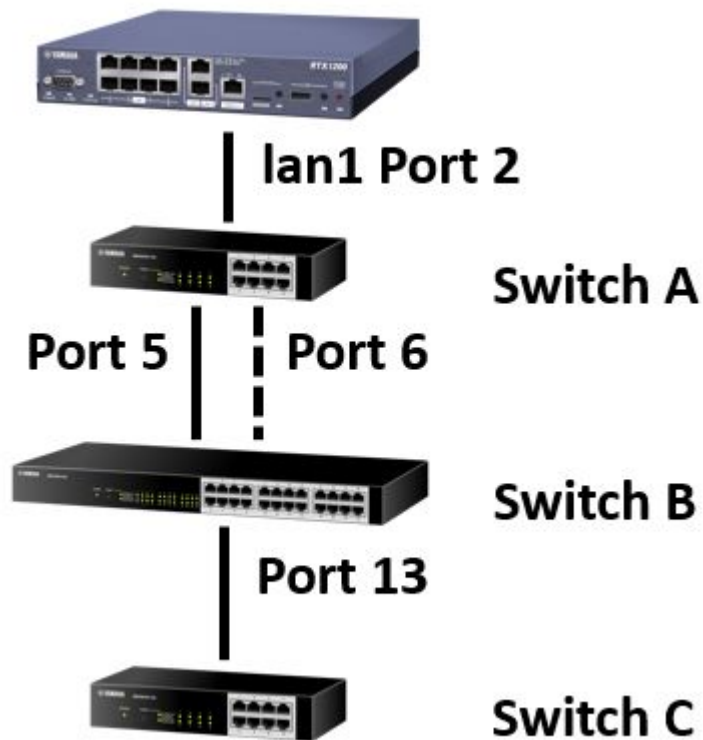
The status of ethernet cable redundancy can be refer by **show status switch control route backup** command.

RTX810 supports this command in Rev.11.01.23 or later.

**[Example]**

Sample configuration in case of port number 5 on Switch-A is master route and port number 6 is backup route.

```
switch control route backup lan1:2-5 6
```



[Models]  
RTX810

## 42.2 Switch Function

---

### 42.2.1 System

---

#### 42.2.1.1 Obtain the BootROM Version

---

[Syntax]

```
switch control function get boot-rom-version [switch]
```

[Setting and Initial value]

- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

[Description]

Obtains the BootROM version.

[Models]  
RTX810

#### 42.2.1.2 Obtain the Firmware Revision

---

[Syntax]

```
switch control function get firmware-revision [switch]
```

[Setting and Initial value]

- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

[Description]

Obtains the firmware revision.

**[Models]**

RTX810

**42.2.1.3 Obtain the Serial Number**

---

**[Syntax]****switch control function get serial-number** [*switch*]**[Setting and Initial value]**

- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Obtains the serial number.

**[Models]**

RTX810

**42.2.1.4 Obtain the Model Name**

---

**[Syntax]****switch control function get model-name** [*switch*]**[Setting and Initial value]**

- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Obtains the model name.

**[Models]**

RTX810

**42.2.1.5 Obtain the MAC Address**

---

**[Syntax]****switch control function get system-macaddress** [*switch*]**[Setting and Initial value]**

- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Obtains the MAC address.

**[Models]**

RTX810

**42.2.1.6 Obtain the System Name**

---

**[Syntax]**

**switch control function set system-name** *name*  
**no switch control function set system-name**  
**switch control function get system-name** [*switch*]

**[Setting and Initial value]**

- *name*
  - [Setting] : System name (between 1 and 64 characters)
  - [Initial value] : (model name)\_(Serial number)
- *switch* : Switches

- [Setting] :
  - MAC address
  - Route
- [Initial value] : -

**[Description]**

Specify the system name. Characters that can be used for *name* are alphanumeric characters, hyphen, and underscore.

**[Models]**

RTX810

**42.2.1.7 Set Whether to Use the Energy Saving Function**

---

**[Syntax]**

```
switch control function set energy-saving mode
no switch control function set energy-saving
switch control function get energy-saving [switch]
```

**[Setting and Initial value]**

- *mode*
- [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : off
- *switch* : Switches
- [Setting] :
  - MAC address
  - Route
- [Initial value] : -

**[Description]**

Sets whether to use the energy saving function of the LAN port.

**[Note]**

When this function setting is changed, link of all ports are down temporarily.

**[Models]**

RTX810

**42.2.1.8 Adjust the LED Brightness**

---

**[Syntax]**

```
switch control function set led-brightness mode
no switch control function set led-brightness
switch control function get led-brightness [switch]
```

**[Setting and Initial value]**

- *mode*
- [Setting] :

Setting	Description
normal	Bright
economy	Dark

- [Initial value] : normal
- *switch* : Switches
- [Setting] :
  - MAC address
  - Route
- [Initial value] : -

**[Description]**

Adjusts the LED brightness.

**[Models]**

RTX810

**42.2.1.9 Obtain the LED Display Mode****[Syntax]****switch control function get status-led-mode** [*switch*]**[Setting and Initial value]**

- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Obtains the current LED display mode of each LAN port.

Display mode	Description
link/act	Display the link state of each port. <ul style="list-style-type: none"> <li>• Lighted on in green: The link is established</li> <li>• Flashing in green: Data is being transferred</li> <li>• Light-off: The link is lost</li> </ul>
speed	Display the connection speed of each port. <ul style="list-style-type: none"> <li>• Lighted on in green: Connect to 1000BASE-T</li> <li>• Lighted on in orange: Connect to 100BASE-TX</li> <li>• Light-off: Connect to 10BASE-T</li> </ul>
duplex	Display the connection state (full duplex / half duplex) of each port. <ul style="list-style-type: none"> <li>• Lighted on in green: Connect at full duplex</li> <li>• Lighted on in orange: Connect at half duplex</li> </ul>
status	Display the system state. <ul style="list-style-type: none"> <li>• Lighted on in orange: A loop is detected</li> </ul> When a failure of the fan is detected in SWX2200-24G, the lower mode LED starts flashing in orange.

**[Models]**

RTX810

**42.2.1.10 Obtain the Fan State****[Syntax]****switch control function get status-fan** [*switch*]**[Setting and Initial value]**

- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Obtains the fan state.

Condition	Description
normal	Normal
lock	Abnormal

**[Note]**

Only SWX2200-24G can use this function.

**[Models]**

RTX810

**42.2.1.11 Restart**

---

**[Syntax]****switch control function execute restart** [*switch*]**[Setting and Initial value]**

- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Restarts the system.

**[Models]**

RTX810

**42.2.1.12 Obtain the Time Since the System Starts Up**

---

**[Syntax]****switch control function get system-uptime** [*switch*]**[Setting and Initial value]**

- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Obtains the time since the system starts up.

**[Models]**

RTX810

**42.2.2 Port**

---

**42.2.2.1 Set the Port Speed and Operation Mode**

---

**[Syntax]**

**switch control function set port-speed** *port speed*  
**no switch control function set port-speed** *port*  
**switch control function get port-speed** *port* [*switch*]

**[Setting and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *speed* : Transmission speed and operation mode
  - [Setting] :

Setting	Description
auto	Auto speed detection
1000-fdx	Full duplex 1000BASE-T
100-fdx	Full duplex 100BASE-TX
100-hdx	Half duplex 100BASE-TX
10-fdx	Full duplex 10BASE-T
10-hdx	Half duplex 10BASE-T

- [Initial value] : auto
- *switch* : Switches

- [Setting] :
  - MAC address
  - Route
- [Initial value] : -

**[Description]**

Sets the transmission speed and operation mode of the port.

**[Note]**

When this function setting is changed, link of the relevant port is down temporarily.

**[Models]**

RTX810

**42.2.2.2 Set Whether to Use the Port****[Syntax]**

```
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 and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *mode*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : on
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets whether to use the port. If this function setting is off, link is not established even when the LAN cable is connected to the relevant port.

**[Models]**

RTX810

**42.2.2.3 Set Whether to Use the Auto Crossover Function****[Syntax]**

```
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 and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *mode*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : on
- *switch* : Switches

- [Setting] :
  - MAC address
  - Route
- [Initial value] : -

**[Description]**

Sets whether to use the auto crossover function.

The auto crossover function automatically detects whether the LAN cable is a straight cable or a crossover cable and makes the connection accordingly. Enabling this function frees you from worrying about the cable type.

**[Note]**

When this function setting is changed, link of the relevant port is down temporarily.

**[Models]**

RTX810

**42.2.2.4 Set Whether to Use the Speed-Downshift Function**

---

**[Syntax]**

```
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 and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *mode*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : on
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets whether to use the speed-downshift function.

One use of the speed-downshift function is to try to establish a link at a reduced speed when a LAN cable that does not support 1000BASE-T is connected.

**[Note]**

When this function setting is changed, link of the relevant port is down temporarily.

**[Models]**

RTX810

**42.2.2.5 Set Whether to Use the Flow Control Function**

---

**[Syntax]**

```
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 and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *mode*
  - [Setting] :



Setting	Description
on	Enable
off	Disable

- [Initial value] : off
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets whether to use the flow control function.

When this function setting is on, both the reception side and the transmission side can control flow. When the link is up at full duplex, IEEE802.3x is used for controlling flow. In case of half duplex, the back pressure method is used.

**[Note]**

When this function setting is changed, link of the relevant port is down temporarily.

**[Models]**

RTX810

**42.2.2.6 Set Whether to Block the Switch control Packet****[Syntax]**

```
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 and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *mode*
  - [Setting] :

Setting	Description
on	Block the switch control packet
off	Pass the switch control packet

- [Initial value] : off
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets whether to block the switch control packet. When this function is enabled, the switch control packets do not forwarded on the port.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810

**42.2.2.7 Set Whether to Block Non-Switch Control Packet****[Syntax]**

```
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 and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *mode*
  - [Setting] :

Setting	Description
on	Block non-switch control packet
off	Pass non-switch control packet

- [Initial value] : off
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets whether to block non-switch control packet. When this function is enabled, non-switch control packets do not forwarded on the port.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810

**42.2.2.8 Obtain the Port Link State****[Syntax]**

**switch control function get status-port-speed** *port* [*switch*]

**[Setting and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Obtains the current link state of the port.

Condition	Description
1000-fdx	Full duplex 1000BASE-T
100-fdx	Full duplex 100BASE-TX
100-hdx	Half duplex 100BASE-TX
10-fdx	Full duplex 10BASE-T
10-hdx	Half duplex 10BASE-T
down	Linkdown

**[Models]**

RTX810

**42.2.3 MAC Address Table**

The size of the MAC address table of the Yamaha switch is indicated below.

Model	Maximum Number of Entries
SWX2200-24G	8192
SWX2200-8G, @swx2200-8poe@	

#### 42.2.3.1 Set Whether to Use the MAC Address-Aging Function

##### [Syntax]

```
switch control function set macaddress-aging mode
no switch control function set macaddress-aging
switch control function get macaddress-aging [switch]
```

##### [Setting and Initial value]

- *mode*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : on
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

##### [Description]

Sets whether to use the MAC address-aging function.

The MAC address-aging function clears at a given interval the MAC address table entries that the switch stores. When this function is turned off, the MAC addresses that the switch learned are not cleared automatically.

Specify a time interval to clear entries with the **macaddress-aging-timer** command.

##### [Models]

RTX810

#### 42.2.3.2 Set the MAC Address-Aging Time Interval

##### [Syntax]

```
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 and Initial value]

- *time*
  - [Setting] : Number of seconds (10 .. 64800)
  - [Initial value] : 300

##### [Description]

Sets the time interval for clearing the MAC addresses that the switch learned for the MAC address-aging function.

The time from when the switch learns the MAC addresses until it clears the entries is from the number of seconds specified with this function at shortest, up to twice of that number of seconds at longest. For example, if the setting value is 300 seconds, the time interval is a value from 300 seconds up to 600 seconds.

Note that if the switch receives a frame from the MAC address that it already learned, the time until that entry is cleared is reset.

##### [Models]

RTX810

#### 42.2.3.3 Search the MAC Address Table According to the MAC Address

##### [Syntax]

```
switch control function get status-macaddress-addr mac_address [switch]
```

##### [Setting and Initial value]

- *mac\_address*
  - [Setting] : MAC address

- [Initial value] : -
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Searches a MAC address table according to the MAC address and obtains a port number, which learned that MAC address. When several VLANs have learned a same MAC address, multiple port numbers may be displayed.

**[Models]**

RTX810

#### 42.2.3.4 Search the MAC Address Table According to the Port Number

---

**[Syntax]**

```
switch control function get status-macaddress-port port [switch]
```

**[Setting and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Searches a MAC address table according to the port number and obtains a MAC address, which the port learned. When several VLANs have learned a same MAC address, multiple port numbers may display a same MAC address.

**[Models]**

RTX810

#### 42.2.3.5 Clear the MAC Address Table Entries

---

**[Syntax]**

```
switch control function execute clear-macaddress-table [switch]
```

**[Setting and Initial value]**

- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Clears all entries in the MAC address table.

**[Models]**

RTX810

### 42.2.4 VLAN

---

When specifying the port VLAN/tag VLAN for the Yamaha switch, specify a VLAN registration number, instead of entering a VLAN ID directly for the command. To tie the VLAN registration number to the VLAN ID, use the **vlan-id** command. For example, in case of the following setting, the VLAN ID of the port 2 is “4”.

```
switch control function set vlan-id 10 4
switch control function set vlan-access 2 10
```

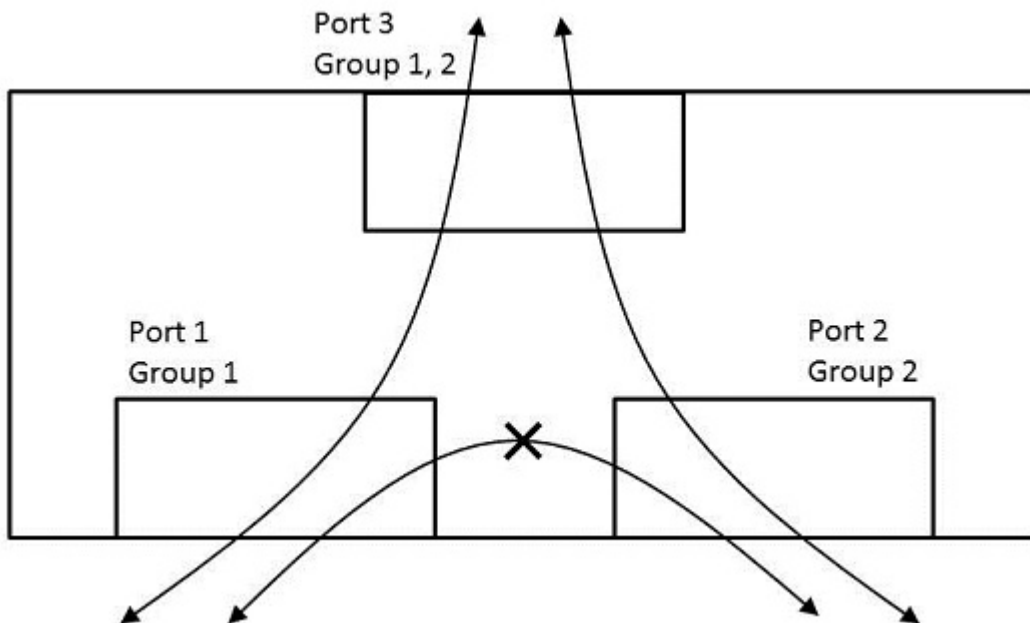
A packet the switch receives is grouped into any VLAN ID regardless of availability of VLAN tag, and transferred according to that information. The VLAN operation mode of the port is specified with the **vlan-port-mode** command.

vlan-port-mode	Receiving operation	Sending operation
access	Receive only a packet without a VLAN tag. The VLAN ID is grouped according to the <b>vlan-access</b> command setting.	At the time of receiving, send a packet grouped into the VLAN ID ( <b>vlan-access</b> ) of the destination port without a VLAN tag.
trunk	Receive only a packet with a VLAN tag. Note that the port must participate in the VLAN ID in the VLAN tag. The VLAN ID where the port participates can be specified with the <b>vlan-trunk</b> command. The VLAN ID is grouped according to the VLAN tag information.	At the time of receiving, send a packet grouped into the VLAN ID ( <b>vlan-trunk</b> ) where the destination port participates with a VLAN tag.
hybrid	Receive both types, a packet with a VLAN tag and a packet without a VLAN tag. When receiving a packet without a VLAN tag, the switch operates similarly to the access port. When receiving a packet with a VLAN tag, it operates similarly to the trunk port.	At the time of receiving, send a packet grouped into the VLAN ID ( <b>vlan-access</b> ) of the destination port without a VLAN tag. Also, at the time of receiving, send a packet grouped into the VLAN ID ( <b>vlan-trunk</b> ) where the destination port participates with a VLAN tag. If a packet is corresponding to both types, send without a VLAN tag.

The multiple VLAN function allows grouping of ports of one port and prohibits communication between the groups

After enabling this function with the **vlan-multiple-use** command, specify a group number where the port belongs with the **vlan-multiple** command. One port can belong to multiple groups. A packet received at a certain port is sent from another port that belongs to the same group number with that port.

For example, consider the following setting:



```
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
```

- A packet the port 1 receives is sent from the port 3 only.
- A packet the port 2 receives is sent from the port 3 only.
- A packet the port 3 receives is sent from the port 1 and port 2.

Since the multiple VLAN does not divide a network, a same network address is assigned to several groups.

When the port VLAN/tag VLAN, and the multiple VLAN are used at the same time, ports belonging to a same group in the multiple VLAN cannot communicate each other unless they belong to a same VLAN defined in the port VLAN/tag VLAN.

#### 42.2.4.1 Set VLAN ID

---

##### [Syntax]

```
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 and Initial value]

- *vlan\_register\_num*
  - [Setting] : VLAN registration number (1 .. 256)
  - [Initial value] : -
- *vid*
  - [Setting] : VLAN ID (1 .. 4094)
  - [Initial value] : Same value with the VLAN registration number
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

##### [Description]

Sets a VLAN ID to the VLAN registration number.

##### [Models]

RTX810

#### 42.2.4.2 Set the Port VLAN Operation Mode

---

##### [Syntax]

```
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 and Initial value]

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *mode* : VLAN operation mode
  - [Setting] :

Setting	Description
access	Access port
trunk	Trunk port
hybrid	Hybrid port

- [Initial value] : access
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

##### [Description]

Sets the port VLAN operation mode.

##### [Models]

RTX810

#### 42.2.4.3 Set the Access Port

---

##### [Syntax]

```
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 and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *vlan\_register\_num*
  - [Setting] : VLAN registration number (1 .. 256)
  - [Initial value] : 1
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets a VLAN ID of the port of which **vlan-port-mode** command setting is access or hybrid. Specify the VLAN ID using a VLAN registration number.

**[Note]**

Even if this function setting is changed for the port of which **vlan-port-mode** command setting is trunk, it does not affect operation.

**[Models]**

RTX810

**42.2.4.4 Set the Trunk Port**

---

**[Syntax]**

```
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 and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *vlan\_register\_num*
  - [Setting] : VLAN registration number (1 .. 256)
  - [Initial value] : -
- *mode*
  - [Setting] :

Setting	Description
join	Participate
leave	Not participate

- [Initial value] : leave
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets a VLAN ID to participate for the port of which **vlan-port-mode** command setting is trunk or hybrid. Specify the VLAN ID using a VLAN registration number.

**[Note]**

Even if this function setting is changed for the port of which **vlan-port-mode** command setting is access, it does not affect operation.

**[Models]**

RTX810

#### 42.2.4.5 Set Whether to Use Multiple VLAN

---

##### [Syntax]

```
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 and Initial value]

- *mode*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : off
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

##### [Description]

Sets whether to use the multiple VLAN.

##### [Models]

RTX810

#### 42.2.4.6 Set the Multiple VLAN Group

---

##### [Syntax]

```
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 and Initial value]

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *group\_num* : Group number
  - [Setting] :

Model	Range
SWX2200-24G	1 .. 24
SWX2200-8G	1 .. 8

- [Initial value] : -
- *mode*
  - [Setting] :

Setting	Description
join	Participate
leave	Not participate

- [Initial value] : leave
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

##### [Description]

Sets a group number of the multiple VLAN where the port belongs.



**[Note]**

When the **vlan-multiple-use** setting is off, even a change of this function setting does not affect operation.

**[Models]**

RTX810

**42.2.5 QoS**

The DSCP remarking function allows rewriting of 6-bit DSCP value in the DS field of the IP header. The class (**qos-dscp-remark-class**) of the port that receives a packet, and the rewriting method (**qos-dscp-remark-type**) of the destination port determine a value to be rewritten. For more detail, see below:

qos-dscp-remark-type	qos-dscp-remark-class	DSCPvalue	PHB
af	class1	001100	AF12
	class2	010100	AF22
	class3	011100	AF32
	class4	100100	AF42
cs	class1	000000	default
	class2	001000	Class Selector
	class3	010000	
	class4	011000	

**42.2.5.1 Set the DSCP Remarking Rewriting Method****[Syntax]**

```
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 and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *type* : Rewriting method
  - [Setting] :

Setting	Description
off	Not rewrite
af	Rewrite with AF (Assured Forwarding)
cs	Rewrite with CS (Class Selector)

- [Initial value] : off
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets the method to rewrite a DSCP value of the IP packet sent from the switch.

**[Models]**

RTX810

**42.2.5.2 Set the Received Packets Classification****[Syntax]**

```
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 and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *class*
  - [Setting] :

Setting	Description
off	Not classify
class1	Group into Class 1
class2	Group into Class 2
class3	Group into Class 3
class4	Group into Class 4

- [Initial value] : off
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Groups the packets that the switch received with the DSCP remarking function.

**[Models]**

RTX810

**42.2.5.3 Set the Speed Unit for Band Limit**

---

**[Syntax]**

```
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] :
    - 128k
    - 1m
    - 10m
    - 32m
  - [Initial value] : 32m
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets a speed unit to police incoming traffic and to shape outgoing traffic.

**[Note]**

Only SWX2200-24G can use this function.

**[Models]**

RTX810

**42.2.5.4 Set Whether to Police Incoming Traffic**

---

**[Syntax]**

```
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
  - [Initial value] : -
- *mode*
  - [Setting] :

Setting	Description
on	Yes
off	No

- [Initial value] : off
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets whether to police incoming traffic.

**[Note]**

Only SWX2200-24G can use this function.

**[Models]**

RTX810

**42.2.5.5 Set a Bandwidth for Incoming Traffic**

---

**[Syntax]**

```
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]
```

**[Setting and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *level*
  - [Setting] : Bandwidth (1 .. 31)
  - [Initial value] : 1
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets a bandwidth for policing incoming traffic. Multiply the **qos-speed-unit** command setting value by *level* to find the actual bandwidth.

**[Note]**

Only SWX2200-24G can use this function.

When the **qos-policing-use** command setting is off, even a change of this function setting does not affect operation.

**[Models]**

RTX810

**42.2.5.6 Set Whether to Shape Outgoing Traffic**

---

**[Syntax]**

```
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]
```

**[Setting and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *mode*
  - [Setting] :

Setting	Description
on	Yes
off	No

- [Initial value] : off
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets whether to shape outgoing traffic.

**[Note]**

Only SWX2200-24G can use this function.

**[Models]**

RTX810

**42.2.5.7 Set a Bandwidth for Outgoing Traffic****[Syntax]**

```
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]
```

**[Setting and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *level*
  - [Setting] : Bandwidth (1 .. 31)
  - [Initial value] : 1
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets a bandwidth for shaping outgoing traffic. Multiply the **qos-speed-unit** command setting value by *level* to find the actual bandwidth.

**[Note]**

Only SWX2200-24G can use this function.

When the **qos-shaping-use** command setting is off, even a change of this function setting does not affect operation.

**[Models]**

RTX810

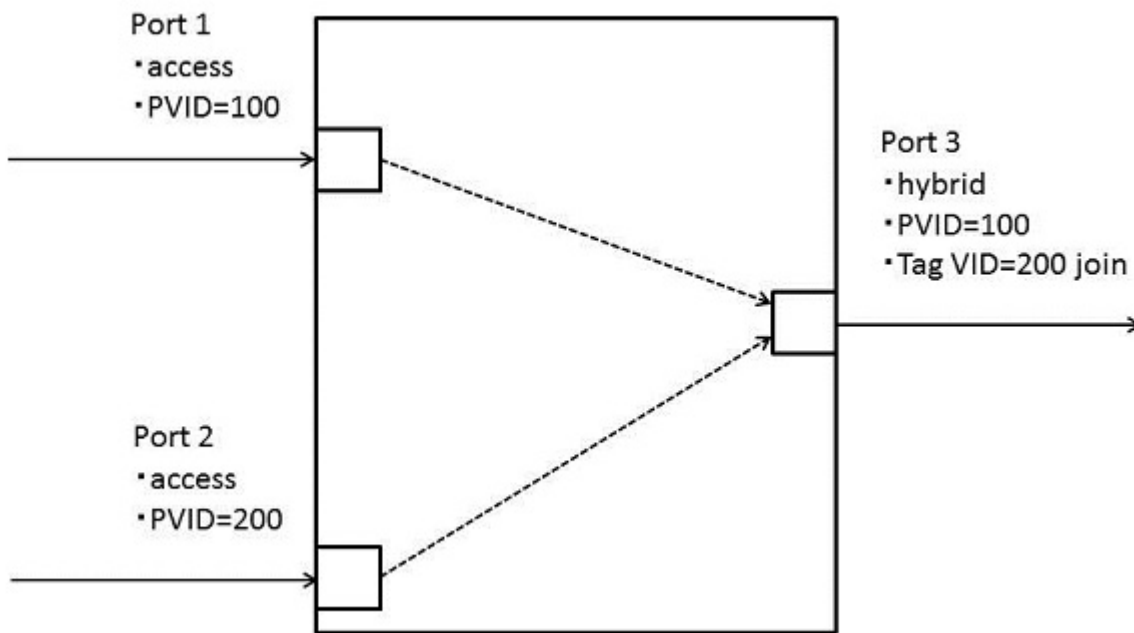
**42.2.6 Mirroring**

The mirroring function enables the communication on a certain port to be monitored on another port.

The mirroring function and the port blocking function can not be used simultaneously.

When the mirroring function, the port VLAN/tag VLAN, and the multiple VLAN are used simultaneously, a port that operates mirroring (**mirroring-src-rx** and **mirroring-src-tx**) and a destination port (**mirroring-dest**) must belong to a same VLAN and also a same group number.

In some cases, availability of VLAN tag is different between a mirroring packet and an original packet. Whether a VLAN tag is attached to the mirroring packet depends on the VLAN operation mode of the destination port. The figure below shows an example:



- Port 1: Access port with VLAN ID=100
- Port 2: Access port with VLAN ID=200
- Port 3: Hybrid port which participates in the access port with VLAN ID=100 and the tag VLAN with VLAN ID=200.
- The port 3 mirrors a packet that the port 1 and the port 2 receive.

```
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 the port 3 mirrors a packet that the port 1 receives, no VLAN tag is attached to that packet.
- When the port 3 mirrors a packet that the port 2 receives, the VLAN tag with VLAN ID=200 is attached to that packet.

#### 42.2.6.1 Set Whether to Use the Mirroring Function

##### [Syntax]

```
switch control function set mirroring-use mode
no switch control function set mirroring-use
switch control function get mirroring-use [switch]
```

##### [Setting and Initial value]

- *mode*
- [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : off
- *switch* : Switches
- [Setting] :
  - MAC address
  - Route
- [Initial value] : -

**[Description]**

Sets whether to use the mirroring function.

**[Models]**

RTX810

**42.2.6.2 Set a Destination Port for Mirroring Packets****[Syntax]**

```
switch control function set mirroring-dest port
no switch control function set mirroring-dest
switch control function get mirroing-dest [switch]
```

**[Setting and Initial value]**

- *port*
  - [Setting] : Destination port number for mirroring packets
  - [Initial value] :

Model	Port Number
SWX2200-24G	24
SWX2200-8G	8

- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets a destination port for mirroring packets.

**[Note]**

When the **mirroring-use** command setting is off, even a change of this function setting does not affect operation.

**[Models]**

RTX810

**42.2.6.3 Set Whether to Mirror Received Packets****[Syntax]**

```
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 and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *mode*
  - [Setting] :

Setting	Description
on	Mirror received packets
off	Not mirror received packets

- [Initial value] : off
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets whether to mirror received packets.

**[Note]**

Even when this function is turned on for the port specified in the **mirroring-dest** command, the mirroring function is not activated.

When the **mirroring-use** command setting is off, even a change of this function setting does not affect operation.

**[Models]**

RTX810

**42.2.6.4 Set Whether to Mirror Packets to Be Transmitted****[Syntax]**

```
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 and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *mode*
  - [Setting] :

Setting	Description
on	Mirror packets to be transmitted
off	Not mirror packets to be transmitted

- [Initial value] : off
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets whether to mirror packets to be transmitted.

**[Note]**

Even when this function is turned on for the port specified in the **mirroring-dest** command, the mirroring function is not activated.

When the **mirroring-use** command setting is off, even a change of this function setting does not affect operation.

**[Models]**

RTX810

**42.2.7 Counter**

Every port has a frame counter and an octet counter, which can individually count incoming packets and outgoing packets. The frame counter can count multiple types of packets simultaneously.

To use the frame counter, specify a packet type with the **counter-frame-rx-type** command or the **counter-frame-tx-type** command in advance. You can obtain the counter value with the **status-counter-frame-rx** command or the **status-counter-frame-tx** command.

You can obtain the octet counter value with the **status-counter-octet-rx** command or the **status-counter-octet-tx** command.

Among the types of packets that the frame counter counts, the class-0 to class-3 support the DSCP remarking classification (**qos-dscp-remark-class**). The table below shows relation between them:

DSCP classification	Class of outgoing queue or incoming queue
class1	class-0
class2	class-1
class3	class-2
class4	class-3
No classification (off)	

When a packet that the switch receives is transmitted, the class of the incoming queue is always same with the class of the outgoing queue.

#### 42.2.7.1 Set a Type of Frames That the Incoming Frame Counter Counts

##### [Syntax]

**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 and Initial value]

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *counter* : Counter number
  - [Setting] :

Model	Range
SWX2200-24G	1 .. 5
SWX2200-8G	1 .. 3

- [Initial value] : -
- *type* : Packet type to be counted
  - [Setting] :

Setting	Description
packets	All packets
broadcast-and-multicast-packets	Broadcast packets and multicast packets
total-error-packets	Packets containing CRC error, alignment error, and/or frame size error
broadcast-packets	Broadcast packets
multicast-packets	Multicast packets
packets-64-octets	64-octet packets
packets-65-to-127-octets	65- to 127-octet packets
packets-128-to-255-octets	128- to 255-octet packets
packets-256-to-511-octets	256- to 511-octet packets
packets-512-to-1023-octets	512- to 1023-octet packets
packets-1024-to-1526-octets	1024- to 1526-octet packets
pause	PAUSE packets
fifo-drops	Packets discarded due to overflow of the receive buffer
total-good-packets	Packets normally received
class-0	Packets grouped into the incoming queue class-0
class-1	Packets grouped into the incoming queue class-1
class-2	Packets grouped into the incoming queue class-2
class-3	Packets grouped into the incoming queue class-3
backward-drops	Packets discarded due to buffer congestion
classifier-drops	Packets of which originating or destination MAC address is 00:00:00:00:00:00, packets with VLAN tag received on the access port, and packets without VLAN tag received on the trunk port
crc-align-errors	Packets in which CRC error, alignment error, and/or physical layer error is detected
under-size-packets	Packets less than 64-byte, of which CRC is normal



Setting	Description
over-size-packets	Packets equal to or larger than 1519-byte (without VLAN tag) or equal to or larger than 1523-byte (with VLAN tag), of which CRC is normal
fragments	Packets less than 64-byte, of which CRC is abnormal
jabbers	Packets equal to or larger than 1519-byte (without VLAN tag) or equal to or larger than 1523-byte (with VLAN tag), of which CRC is abnormal
control-packets	Packets of which Ethernet type is 0x8808

- [Initial value] :

Model	Counter number	Type
SWX2200-24G	1	packets
	2	total-good-packets
	3	total-error-packets
	4	fifo-drops
	5	crc-align-errors
SWX2200-8G	1	packets
	2	total-good-packets
	3	total-error-packets

- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

#### [Description]

Sets a type of frames that the incoming frame counter counts up. Obtain the counter value with the **status-counter-frame-rx** command.

#### [Note]

When this function setting is changed, all counters (outgoing, incoming, frame, and octet) of the relevant port are reset.

#### [Models]

RTX810

### 42.2.7.2 Set a Type of Frames That the Outgoing Frame Counter Counts

#### [Syntax]

```
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 and Initial value]

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *counter* : Counter number
  - [Setting] :

Model	Range
SWX2200-24G	1 .. 5
SWX2200-8G	1 .. 3

- [Initial value] : -
- *type* : Packet type to be counted
  - [Setting] :

Setting	Description
packets	All packets
broadcast-and-multicast-packets	Broadcast packets and multicast packets
total-error-packets	The number of times to stop transmission due to error occurrence during packet transmission
broadcast-packets	Broadcast packets
multicast-packets	Multicast packets
packets-64-octets	64-octet packets
packets-65-to-127-octets	65- to 127-octet packets
packets-128-to-255-octets	128- to 255-octet packets
packets-256-to-511-octets	256- to 511-octet packets
packets-512-to-1023-octets	512- to 1023-octet packets
packets-1024-to-1526-octets	1024- to 1526-octet packets
pause	PAUSE packets
fifo-drops	Packets discarded due to overflow of the transmission buffer
total-good-packets	Packets normally transmitted
class-0	Packets transmitted from the outgoing queue class-0
class-1	Packets transmitted from the outgoing queue class-1
class-2	Packets transmitted from the outgoing queue class-2
class-3	Packets transmitted from the outgoing queue class-3
drops	Packets discarded due to frequent collision, late collision, or long-time retention in the transmission buffer
collisions	The number of times of collision occurrence
cfi-drop	Packets discarded because the CFI bit is 1 (When a packet of which CFI is 1 is received and transmitted without a tag, the packet is discarded.)

- [Initial value] :

Model	Counter number	Type
SWX2200-24G	1	packets
	2	total-good-packets
	3	total-error-packets
	4	fifo-drops
	5	collisions
SWX2200-8G	1	packets
	2	total-good-packets
	3	total-error-packets

- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

#### [Description]

Sets a type of frames that the outgoing frame counter counts up. Obtain the counter value with the **status-counter-frame-tx** command.

**[Note]**

When this function setting is changed, all counters (outgoing, incoming, frame, and octet) of the relevant port are reset.

**[Models]**

RTX810

**42.2.7.3 Obtain the Incoming Frame Counter Value**

---

**[Syntax]**

**switch control function get status-counter-frame-rx** *port counter* [*switch*]

**[Setting and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *counter* : Counter number
  - [Setting] :

Model	Range
SWX2200-24G	1 .. 5
SWX2200-8G	1 .. 3

- [Initial value] : -
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Obtains the incoming frame counter value.

**[Models]**

RTX810

**42.2.7.4 Obtain the Outgoing Frame Counter Value**

---

**[Syntax]**

**switch control function get status-counter-frame-tx** *port counter* [*switch*]

**[Setting and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *counter* : Counter number
  - [Setting] :

Model	Range
SWX2200-24G	1 .. 5
SWX2200-8G	1 .. 3

- [Initial value] : -
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Obtains the outgoing frame counter value.

**[Models]**

RTX810

#### 42.2.7.5 Obtain the Incoming Octet Counter Value

---

##### [Syntax]

**switch control function get status-counter-octet-rx** *port* [*switch*]

##### [Setting and Initial value]

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

##### [Description]

Obtains the incoming octet counter value. This counter counts the number of octets for all received packets, regardless of the **counter-frame-rx-type** command setting.

##### [Models]

RTX810

#### 42.2.7.6 Obtain the Outgoing Octet Counter Value

---

##### [Syntax]

**switch control function get status-counter-octet-tx** *port* [*switch*]

##### [Setting and Initial value]

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

##### [Description]

Obtains the outgoing octet counter value. This counter counts the number of octets for all transmitted packets, regardless of the **counter-frame-tx-type** command setting.

##### [Models]

RTX810

#### 42.2.7.7 Clear the Counter

---

##### [Syntax]

**switch control function execute clear-counter** [*switch*]

##### [Setting and Initial value]

- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

##### [Description]

Clear all counters (all ports, outgoing, incoming, frame, and octet).

##### [Models]

RTX810

### 42.2.8 Detect a Loop

---

The Yamaha switch detects a packet loop on the network by monitoring transfer of MAC address or switch control packet.

Transfer of MAC address means that multiple ports learn one MAC address. The switch monitor the number of MAC address migration in a second. When the number exceeds the threshold specified by **loopdetect-count** command, and that state lasts in specified time configured by **loopdetect-time**, the switch determine the packet loop happened.

For the packet loop detection method by using switch control packet, the switch monitors the number of receiving switch control packet that is sent by itself. When the number exceeds the threshold specified by **loopdetect-count** command, and that state lasts in specified time configured by **loopdetect-time**, the switch determine the packet loop happened.

Even if it is detected by either method, the LED will blink on a port that the packet loop is detected.

Enable the **loopdetect-port-use** command on the port use the packet loop detection.

Specify the operation after a loop is detected with the **loopdetect-linkdown** command. When the **loopdetect-linkdown** command setting is linkdown or linkdown-recovery, among the ports where a loop occurs, the switch turns down a link from the port with the largest number in sequence until the loop stops. To keep communication with the router even in the loop condition, we recommend using the port 1 for the uplink port.

Note that the LED of the port of which link is down due to the loop blinks in orange.

#### 42.2.8.1 Set the Threshold for Detecting the Packet Loop Per Second

---

##### [Syntax]

```
switch control function set loopdetect-count count
no switch control function set loopdetect-count count
switch control function get loopdetect-count [switch]
```

##### [Setting and Initial value]

- *count*
  - [Setting] : The threshold for detecting the packet loop per second (3 .. 65535)
  - [Initial value] : 3
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

##### [Description]

Sets the threshold for detecting the packet loop per second. When the number of MAC address translation or the number of received switch control packet which is sent from itself exceed the threshold set by this command, and that state lasts in time set by **loopdetect-time** command, the switch determine the packet loop happened.

##### [Models]

RTX810

#### 42.2.8.2 Set the Time Until the Switch Determines That the Loop Occurs

---

##### [Syntax]

```
switch control function set loopdetect-time time
no switch control function set loopdetect-time
switch control function get loopdetect-time [switch]
```

##### [Setting and Initial value]

- *time*
  - [Setting] : Number of seconds (2 .. 60)
  - [Initial value] : 3
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

##### [Description]

Sets the time for detecting the packet loop. When the number of MAC address translation or the number of received switch control packet which is sent from itself exceed the threshold set by **loopdetect-count** command, and that state lasts in time set by this command, the switch determine the packet loop happened.

##### [Models]

RTX810

#### 42.2.8.3 Set the Operation When a Loop Occurs

---

##### [Syntax]

```
switch control function set loopdetect-linkdown action
no switch control function set loopdetect-linkdown
```

**switch control function get loopdetect-linkdown** [*switch*]**[Setting and Initial value]**

- *action*
- [Setting] :

Setting	Description
none	No operation
linkdown	Turn down the port where the loop occurs
linkdown-recovery	After tuning down the port where the loop occurs, recover it when a given length of time passes

- [Initial value] : none
- *switch* : Switches
- [Setting] :
  - MAC address
  - Route
- [Initial value] : -

**[Description]**

Sets the operation when a loop occurs.

When the *action* command setting is linkdown or linkdown-recovery, among the ports where a loop occurs, the switch turns down a link from the port with the largest number in sequence until the loop stops. To recover the port of which link is down, execute the **reset-loopdetect** command, or hold down the MODE button.

When the *action* command setting is linkdown-recovery, the switch turns down the port link and then recover it automatically after the time specified in the **loopdetect-recovery-timer** command passes.

**[Note]**

Since a port for which the **loopdetect-port-use** command setting is off does not detect a loop, it does not perform the operation specified with this function.

**[Models]**

RTX810

**42.2.8.4 Set the Time from When a Port Link Is Down Until It Is Recovered****[Syntax]**

```
switch control function set loopdetect-recovery-timer time
no switch control function set loopdetect-recovery-timer
switch control function get loopdetect-recovery-timer [switch]
```

**[Setting and Initial value]**

- *time*
  - [Setting] : Number of seconds (1 .. 86400)
  - [Initial value] : 300
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

When the **loopdetect-linkdown** command setting is linkdown-recovery, sets the time from when a port link is down until it is recovered.

**[Models]**

RTX810

**42.2.8.5 Set Whether to Use the Loop Detection Function****[Syntax]**

```
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]
```

**[Setting and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *mode*
  - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : on
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets whether to use the loop detection function. When a loop occurs in a port for which this function is on and also in another port for which the function is off, the switch detects that the loop occurs in the port for which the function is on. When a loop occurs only in the port for which the function is off, the switch does not detect the loop.

**[Models]**

RTX810

**42.2.8.6 Set Whether to Use the Loop Detection Function by Using Switch Control Packet****[Syntax]**

```
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 and Initial value]**

- *mode*
  - [Setting] :

Setting	Description
on	Enable the loop detection function by using switch control packet
off	Disable the loop detection function by using switch control packet

- [Initial value] : on
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Sets whether to use loop detection function by using switch control packet. When this function is enabled, the switches will detect packet loop when receiving switch control packet sent by itself.

**[Note]**

When the switch control packets are not forwarded by congestion or something, the packet loop may not be able to be detected.

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810

**42.2.8.7 Obtain the Port Status Related to the Loop Detection Function****[Syntax]**

```
switch control function get status-loopdetect-port port [switch]
```

**[Setting and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Obtains the port status related to the loop detection function.

Condition	Description
normal	Normal
loopdetect	A loop occurs
linkdown	The link is down due to the loop occurrence

**[Models]**

RTX810

#### 42.2.8.8 Obtain the Remaining Time Until the Port Is Recovered from Linkdown

---

**[Syntax]**

**switch control function get status-loopdetect-recovery-timer** *port* [*switch*]

**[Setting and Initial value]**

- *port*
  - [Setting] : Port Number
  - [Initial value] : -
- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Obtains the remaining time until the port of which link is down due to the loop occurrence is recovered.

**[Models]**

RTX810

#### 42.2.8.9 Recover the Port of Which Link Is Down due to the Loop Occurrence

---

**[Syntax]**

**switch control function execute reset-loopdetect** [*switch*]

**[Setting and Initial value]**

- *switch* : Switches
  - [Setting] :
    - MAC address
    - Route
  - [Initial value] : -

**[Description]**

Recover all ports of which links are down due to the loop occurrence.

**[Models]**

RTX810



## Chapter 43

### Operation

#### 43.1 Select the Peer Number

##### [Syntax]

**pp select** *peer\_num*

**no pp select**

##### [Setting and Initial value]

- *peer\_num*
- [Setting] :

Setting	Description
Number	Peer number
none	Not select a peer
anonymous	Setting for anonymous peers

- [Initial value] : -

##### [Description]

Selects the peer number to be configured or displayed. After this command, the prompt shows the text string specified by the **console prompt** command followed by the peer number.

If none is specified, the peer number is not shown at the prompt.

##### [Note]

This operation command can also be executed by a general user.

The **no pp select** command is equivalent to the **pp select none** command.

For information about the different peer numbers that can be selected on different models, see 1.6.

##### [Models]

RTX810, RTX5000

#### 43.2 Select the Tunnel Interface Number

##### [Syntax]

**tunnel select** *tunnel\_num*

**no tunnel select**

##### [Setting and Initial value]

- *tunnel\_num*
- [Setting] :

Setting	Description
Number	Tunnel interface number
none	Not select the tunnel interface

- [Initial value] : -

##### [Description]

Selects the tunnel interface number for setting and displaying the tunnel mode.

##### [Note]

This operation command can also be executed by a general user.

If the prompt shows tunnel, command related to pp cannot be entered.

The **no tunnel select** command is equivalent to the **tunnel select none** command.

For information about the different tunnel interface numbers that can be selected on different models, see 15.

##### [Models]

RTX810, RTX5000

## 43.3 Configuration Operation

---

### 43.3.1 Switch to Administrator

---

**[Syntax]**

**administrator**

**[Description]**

This command must be executed before the router can be configured. In addition, operation commands cannot be executed. There are no parameters. Enter the command, and then enter the administrator password at the prompt. The password that you enter does not appear on the screen.

**[Models]**

RTX810, RTX5000

### 43.3.2 Quit

---

**[Syntax]**

**quit**

**quit save**

**exit**

**exit save**

**[Setting and Initial value]**

- **save** : If this keyword is specified when exiting from administrator mode, the configuration is saved to the non-volatile memory before exiting
  - [Initial value] : -

**[Description]**

End the login to the router or exit from administrator mode.

If you attempt to exit from administrator mode after changing the configuration but not saving it, the router asks whether to save the new configuration to the non-volatile memory. If you save the configuration to the non-volatile memory, you can start with the same settings even after restarting.

**[Models]**

RTX810, RTX5000

### 43.3.3 Save the Configuration

---

**[Syntax]**

**save** *[filename [comment]]*

**[Setting and Initial value]**

- *filename* : Name of the file for saving the configuration
  - [Setting] :

Setting	Description
Number	Configuration file number of the internal Flash ROM (0..4)
usb1: <i>filename</i>	A setup file on the USB memory
sd1: <i>filename</i>	A setup file on the microSD card

- [Initial value] : -
- *comment*
  - [Setting] : Comment for the configuration file (up to 200 characters)
  - [Initial value] : -

**[Description]**

Saves the current configuration to the non-volatile memory.

If the file is not specified, the configuration is saved to the configuration file used at startup.

**[Note]**

the number of characters used for *filename* is up to 99 characters.

[Models]  
RTX810, RTX5000

### 43.3.4 Duplicate the Configuration File

#### [Syntax]

**copy config** *from to*  
**copy config** *from to crypto* [*password*]  
**copy config** *from to* [*password*]

#### [Setting and Initial value]

- *from* : Duplicate the Configuration File
  - [Setting] :

Setting	Description
0..4.2	Configuration file number of the internal Flash ROM
usb1: <i>filename</i>	A setup file on the USB memory
sd1: <i>filename</i>	A setup file on the microSD card
*: <i>filename</i>	A firmware file on the USB memory or microSD card

- [Initial value] : -
- *to* : Copy destination file name
  - [Setting] :

Setting	Description
0..4	Configuration file number of the internal Flash ROM
usb1: <i>filename</i>	A setup file on the USB memory ( <i>filename</i> must be 64 characters or less)
sd1: <i>filename</i>	A setup file on the microSD card ( <i>filename</i> must be 64 characters or less)

- [Initial value] : -
- *crypto* : The encryption algorithm
  - [Setting] :

Setting	Description
aes128	Encrypt using AES128.
aes256	Encrypt using AES256.

- [Initial value] : -
- *password*
  - [Setting] : Password expressed using ASCII text characters (between 8 and 32 characters in length)
  - [Initial value] : -

#### [Description]

Duplicate a saved configuration file.

The copy source and copy destination cannot both be located on the external memory.

There is no setup file after a **cold start**, so the router cannot copy the setup file from the internal flash ROM to the external memory. In this case, you have to save the settings by executing the **save** command before you execute this command.

To apply the settings that you copy to the internal flash ROM, you need to restart the router after executing this command.

If you use an asterisk to specify the external memory, the router starts searching the microSD card for the specified file. If the router can't find the file on the memory card, it searches for it in the USB memory. You can specify the *filename* parameter with an absolute path or a file name. If you only specify a file name for the *filename* parameter, the router will automatically search through the external memory for the file.

If the router finds multiple files, it chooses the file in the directory that is closest to the root directory and first in alphabetical order.

When you specify a copy destination in the external memory, set the *filename* parameter to an absolute path.

You can use the encryption function on the external memory.

If you specify CRYPTO, the setup file is encrypted before it is saved to the external memory. To encrypt a file before copying

it, you must include the .rtfg extension in the file name or omit the extension when you specify the file name. If you omit the extension, the .rtfg extension is automatically added to the filename.  
you can encrypt files without specifying a password.

**[Note]**

You cannot copy an encrypted setup file from the external memory to the internal flash ROM without decrypting it. The second syntax can only be used to copy a file from the internal flash ROM to the external memory and encrypt it. The third syntax can only be used to decrypt an encrypted file and copy it from the external memory to the internal flash ROM. When the file is decrypted, the encryption algorithm is determined automatically. Therefore, the encryption algorithm does not need to be specified at the time of decryption.

You can only specify a file in the external memory on models that have external memory interfaces.

If you specify a configuration file number on the internal flash ROM as the copy destination, the original file that was at that file number becomes a backup file after this command is executed.

Automatic file searching is possible.

Depending on the file structure of the external memory and the number of files, it may take time for the router to search for the file.

To make searching faster, avoid creating deep directory structures, and save the firmware file in a directory that is close to the root directory, or specify the file directly using an absolute path.

You can set the timeout for automatic searching using the **external-memory auto-search time** command.

the number of characters used for *filename* is up to 99 characters.

**[Models]**

RTX810, RTX5000

### 43.3.5 Copy the Firmware File to the Internal Flash ROM

**[Syntax]**

**copy exec** *from to*

**[Setting and Initial value]**

- *from* : Duplicate the Configuration File
  - [Setting] :

Setting	Description
Number	Number of an executable firmware file on the internal flash ROM (only 0 on the RTX810)
usb1: <i>filename</i>	A firmware file on the USB memory (only on models with USB interfaces)
sd1: <i>filename</i>	A firmware file on the microSD card (only on models with microSD interfaces)
*: <i>filename</i>	A firmware file on the USB memory or microSD card

- [Initial value] : -
- *to* : Copy destination file name
  - [Setting] :

Setting	Description
Number	Number of the executable firmware file on the internal flash ROM (can be specified on all units except RTX810), can be specified as 0

- [Initial value] : -

**[Description]**

Copies the executable firmware file to the internal Flash ROM.

To apply the settings that you copy to the internal flash ROM, you need to restart the router after executing this command.

If you use an asterisk to specify the external memory, the router starts searching the microSD card for the specified file. If the router can't find the file on the memory card, it searches for it in the USB memory.

You can specify the *filename* parameter with an absolute path or a file name. If you only specify a file name for the *filename* parameter, the router will automatically search through the external memory for the file.

If the router finds multiple files, it chooses the file in the directory that is closest to the root directory and first in alphabetical order.

**[Note]**

You can only specify a file in the external memory on models that have external memory interfaces.

You can only set the copy destination firmware file number to a value other than 0 on models that have the multiple firmware function.

Automatic file searching is possible.

Depending on the file structure of the external memory and the number of files, it may take time for the router to search for the file.

To make searching faster, avoid creating deep directory structures, and save the firmware file in a directory that is close to the root directory, or specify the file directly using an absolute path.

You can set the timeout for automatic searching using the **external-memory auto-search time** command.

the number of characters used for *filename* is up to 99 characters.

**[Models]**

RTX810, RTX5000

**43.3.6 Delete a Configuration File**

---

**[Syntax]**

**delete config** *filename*

**[Setting and Initial value]**

- *filename* : Name of the file to be deleted
  - [Setting] :

Setting	Description
all	All configuration files for the built-in Flash ROM
Number	Configuration file number of the internal Flash ROM (0..4.2)

- [Initial value] : -

**[Description]**

Deletes a saved configuration file.

**[Models]**

RTX810, RTX5000

**43.3.7 Deleting an executable firmware file**

---

**[Syntax]**

**delete exec** *filename*

**[Setting and Initial value]**

- *filename* : File name to be deleted
  - [Setting] :

Setting	Description
Number	Executable firmware file number (only 1 can be specified)

- [Initial value] : -

**[Description]**

Delete a saved executable firmware file.

**[Models]**

RTX5000

**43.3.8 Set the Default Configuration File**

---

**[Syntax]**

**set-default-config** *filename*

**[Setting and Initial value]**

- *filename*
  - [Setting] : Configuration file number (0..4.2)
  - [Initial value] : -

**[Description]**

Sets the configuration file to be used at startup.

**[Models]**

RTX810, RTX5000

### 43.3.9 Setting the default firmware file

---

**[Syntax]**

**set-default-exec** *filename*

**[Setting and Initial value]**

- *filename*
  - [Setting] : Executable firmware file number (0..1)
  - [Initial value] : -

**[Description]**

Sets the firmware file to use when booting up.

**[Models]**

RTX5000

### 43.3.10 Reset the Configuration

---

**[Syntax]**

**cold start**

**[Description]**

Resets the configuration to factory default and restarts the router.  
You must enter the administrator password when executing this command.

**[Note]**

Note that all configuration files in the internal Flash ROM are deleted.

**[Models]**

RTX810, RTX5000

## 43.4 Clear Operation of Dynamic Information

---

### 43.4.1 Clear an Account

---

**[Syntax]**

**clear account**  
**clear account** *interface*

**[Setting and Initial value]**

- *interface*
  - [Setting] :
    - BRI interface name
    - PRI interface name
  - [Initial value] : -

**[Description]**

Clears the account related to the specified interface (the first syntax is a combination of the other two syntaxes).

**[Models]**

RTX5000

### 43.4.2 Clear the PP Account

---

**[Syntax]**

**clear account pp** [*peer\_num*]

**[Setting and Initial value]**

- *peer\_num*
  - [Setting] :
    - Peer number
    - The selected peer when omitted
  - [Initial value] : -

**[Description]**

Clears the account related to the specified PP interface.

**[Models]**

RTX5000

**43.4.3 Clear the ARP Table**

---

**[Syntax]**

**clear arp**

**[Description]**

Clears the ARP table.

**[Models]**

RTX810, RTX5000

**43.4.4 Clear the Dynamic Routing Information of IP**

---

**[Syntax]**

**clear ip dynamic routing**

**[Description]**

Clears the routing information of an IP configure dynamically.

**[Models]**

RTX810, RTX5000

**43.4.5 Clearing the bridge learning information**

---

**[Syntax]**

**clear bridge learning** *bridge\_interface*

**[Setting and Initial value]**

- *bridge\_interface*
  - [Setting] : Bridge interface name
  - [Initial value] : -

**[Description]**

Erase all dynamically acquired bridge learning information.

**[Note]**

Statically specified registration information is not erased. RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

**43.4.6 Clear the Log**

---

**[Syntax]**

**clear log**

**[Description]**

Clears the log.

**[Models]**

RTX810, RTX5000

**43.4.7 Clear InARP**

---

**[Syntax]**

**clear inarp**

**[Description]**

Clears the peer IP address acquired via InARP for the selected peer. If InARP is on, then InARP will start again.

**[Models]**

RTX5000

**43.4.8 Clear the DNS Cache**

---

**[Syntax]**

**clear dns cache**

**[Description]**

Clears the cache held by the DNS recursive server.

**[Models]**

RTX810, RTX5000

**43.4.9 Clear the Interface Counter Information**

---

**[Syntax]**

**clear status** *interface*

**clear status pp** *peer\_num*

**clear status tunnel** *tunnel\_num*

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN or Bridge interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Peer number
  - [Initial value] : -
- *tunnel\_num*
  - [Setting] : Tunnel interface number
  - [Initial value] : -

**[Description]**

Clears the counter data for the specified interface.

**[Note]**

Cumulative reception count, cumulative transmission count, and cumulative error count on the interface used for mobile Internet function are not cleared, to prevent operations related to restriction of outgoing calls. These cumulative counter data can be cleared by using the **clear mobile access limitation** command.

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

**43.4.10 Clear the NAT Address Table**

---

**[Syntax]**

**clear nat descriptor dynamic** *nat\_descriptor*

**[Setting and Initial value]**

- *nat\_descriptor*
  - [Setting] :

Setting	Description
1..2147483647	NAT descriptor number
all	All NAT descriptor numbers

- [Initial value] : -

**[Description]**

Clears the NAT address table.

**[Note]**

If the address management table is cleared in the middle of the communication, the communication may become temporarily unstable.

**[Models]**

RTX810, RTX5000

**43.4.11 Clear the NAT Address Table of the Interface**

---

**[Syntax]**

**clear nat descriptor interface dynamic** *interface*

**clear nat descriptor interface dynamic pp** [*peer\_num*]



**clear nat descriptor interface dynamic tunnel** [*tunnel\_num*]

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] :
    - Peer number
    - anonymous
    - The selected peer when omitted
  - [Initial value] : -
- *tunnel\_num*
  - [Setting] :
    - Tunnel interface number
    - The selected tunnel interface when omitted
  - [Initial value] : -

**[Description]**

Clears the NAT address table applied to the interface.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

#### 43.4.12 Clear the Dynamic Routing Information of IPv6

---

**[Syntax]**

**clear ipv6 dynamic routing**

**[Description]**

Clears the IPv6 routing information that the routing control protocol has obtained.

**[Models]**

RTX810, RTX5000

#### 43.4.13 Clear the Neighbor Cache

---

**[Syntax]**

**clear ipv6 neighbor cache**

**[Description]**

Clears the neighbor cache.

**[Models]**

RTX810, RTX5000

#### 43.4.14 Delete the Startup Information History

---

**[Syntax]**

**clear boot list**

**[Description]**

Delete the startup information history.

**[Models]**

RTX810, RTX5000

#### 43.4.15 Clear the SYSLOG Saved in the External Memory and Deleting the Backup Files

---

**[Syntax]**

**clear external-memory syslog**

**[Description]**

Clears the log entries in the current SYSLOG file stored in the external memory, and deletes all SYSLOG backup files. The backup files of SYSLOG to be deleted are those that exist in the path specified in the **external-memory syslog filename**

command. Note that this command works only if the SYSLOG file name has been set by the **external-memory syslog filename** command, and the external memory is connected to the specified external storage interface.

**[Models]**

RTX810, RTX5000

## 43.5 File and Directory Operation

---

### 43.5.1 Create Directories

---

**[Syntax]**

**make directory** *path*

**[Setting and Initial value]**

- *path*
  - [Setting] : Relative or absolute path
  - [Initial value] : -

**[Description]**

Creates a directory with the specified name.

If you set *path* to a relative path, it is interpreted as a path starting with the PWD environment variable. You can change PWD with the **set** command. Its initial value is *"/*".

**[Models]**

RTX810, RTX5000

### 43.5.2 Delete a File or Directory

---

**[Syntax]**

**delete** *path*

**[Setting and Initial value]**

- *path*
  - [Setting] : Relative or absolute path
  - [Initial value] : -

**[Description]**

Deletes the specified file or directory.

When the directory is not empty, all of the files and directories within it are deleted simultaneously.

If you set *path* to a relative path, it is interpreted as a path starting with the PWD environment variable. You can change PWD with the **set** command. Its initial value is *"/*".

**[Note]**

If you set the *path* parameter to a relative path of "config" or "exec", the **delete config** or **delete exec** command is executed instead of this command. In such a case, do not specify a relative path. Instead, use an absolute path to specify a file or directory.

**[Models]**

RTX810, RTX5000

### 43.5.3 Copy a File or Directory

---

**[Syntax]**

**copy** *path1 path2*

**[Setting and Initial value]**

- *path1*
  - [Setting] : The relative or absolute path of the copy source file or directory
  - [Initial value] : -
- *path2*
  - [Setting] : The relative or absolute copy destination path
  - [Initial value] : -

**[Description]**

Copies a file or directory. When the copy source is a directory, all of the files and directories within it are copied recursively.

When *path1* specifies a file, the following operations are performed:

If there is a file with the same name specified by *path2*, that file is overwritten by the file from *path1*.

If there is a directory with the same name specified by *path2*, a file with the same name as that specified by *path1* is created in the directory specified by *path2*.

If the file or directory specified by *path2* does not exist, it is created.

When *path1* is a directory, the following operations are performed:

If there is a file with the same name specified by *path2*, the copy operation cannot be performed.

If there is a directory with the same name specified by *path2*, a directory with the same name as that specified by *path1* is created in the directory specified by *path2*.

If the file or directory specified by *path2* does not exist, it is created.

If you set *path1* and *path2* to relative paths, they are interpreted as a path starting with the PWD environment variable. You can change PWD with the **set** command. Its initial value is “/”.

**[Note]**

If you set the *path1* parameter to a relative path of “config” or “exec”, the **copy config** or **copy exec** command is executed instead of this command. In such a case, do not specify a relative path. Instead, use an absolute path to specify a file or directory.

**[Models]**

RTX810, RTX5000

### 43.5.4 Change a File or Directory Name

---

**[Syntax]**

**rename** *path name*

**[Setting and Initial value]**

- *path*
  - [Setting] : The relative or absolute path of the file or directory whose name you want to change
  - [Initial value] : -
- *name*
  - [Setting] : The name that you want to change to
  - [Initial value] : -

**[Description]**

Changes the name of the specified file or directory.

If you set *path* to a relative path, it is interpreted as a path starting with the PWD environment variable. You can change PWD with the **set** command. Its initial value is “/”.

**[Note]**

When specifying a new name for the *name* parameter, you cannot specify a name that includes a slash.

**[Models]**

RTX810, RTX5000

## 43.6 Other Operations

---

### 43.6.1 Enable the Peer

---

**[Syntax]**

**pp enable** *peer\_num*  
**no pp enable** *peer\_num*

**[Setting and Initial value]**

- *peer\_num*
  - [Setting] :

Setting	Description
Number	Peer number
anonymous	anonymous interface
all	All peer numbers

- [Initial value] : -

**[Description]**

Enables the peer. By factory default, all peers are disabled. Therefore, you must enable the peer using this command before using the peer.

**[Models]**

RTX810, RTX5000

**43.6.2 Disable the Peer**

---

**[Syntax]****pp disable** *peer\_num***[Setting and Initial value]**

- *peer\_num*
- [Setting] :

Setting	Description
Number	Peer number
anonymous	anonymous interface
all	All peer numbers

- [Initial value] : -

**[Description]**

Disables the peer.

It is desirable that the peer be disabled when configuring the peer.

**[Models]**

RTX810, RTX5000

**43.6.3 Restart**

---

**[Syntax]****restart** [*binary* [*config*]]**restart** [*config*]**[Setting and Initial value]**

- *binary*
  - [Setting] : Number of the executable firmware file (0..1)
  - [Initial value] : -
- *config*
  - [Setting] : Number of the configuration file on the internal flash ROM (0..4.2)
  - [Initial value] : -

**[Description]**

Restarts the router.

You can specify the configuration file and the configuration file used to start the router.

**[Note]**

Only second syntax can be used with RTX810.

Only first syntax can be used with models not listed above.

**[Models]**

RTX810, RTX5000

**43.6.4 Restart the Interface**

---

**[Syntax]****interface reset** *interface* [*interface ...*]**[Setting and Initial value]**

- *interface*
  - [Setting] :
    - LAN interface name
    - WAN interface name
  - [Initial value] : -

**[Description]**

Restarts the specified interface.

If auto negotiation is specified on a LAN interface, the auto negotiation procedure is started.

**[Note]**

If this command is executed on lan1 or lan2 on the RTX810, the lan1 and lan2 interfaces are reset simultaneously. RTX5000 does not support WAN interface for *interface* parameter.

Execute this command after adjusting all settings such as those specified by the **pp bind** commands and the routing information. Execute this command with the communication to all peer numbers bound to the target interface stopped.

**[Models]**

RTX810, RTX5000

**43.6.5 Reset the PP interface**

---

**[Syntax]**

```
interface reset pp [peer_num]
```

**[Setting and Initial value]**

- *peer\_num*
  - [Setting] :
    - Peer number
    - anonymous
  - [Initial value] : -

**[Description]**

Resets the interface bound to the select peer number. Used on interfaces which are using MP.

**[Models]**

RTX5000

**43.6.6 Connect**

---

**[Syntax]**

```
connect interface
connect peer_num
connect pp peer_num
connect tunnel tunnel_num
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : WAN interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Peer number to be connected
  - [Initial value] : -
- *tunnel\_num*
  - [Setting] : L2TPv3 tunnel number
  - [Initial value] : -

**[Description]**

Manually connects the line.

**[Note]**

Models that do not support the data connect connection feature cannot use **connect pp** command.

Models that do not have data connect connection functionality and L2TPv3 functionality implemented cannot use the **connect tunnel** command.

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

### 43.6.7 Disconnect

#### [Syntax]

**disconnect** *interface*

**disconnect** *peer\_num*

**disconnect pp** *peer\_num*

**disconnect tunnel** *tunnel\_num*

#### [Setting and Initial value]

- *interface*
  - [Setting] : WAN interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] :

Setting	Description
Number	Peer number to be disconnected
all	All peer numbers
anonymous	All anonymous peers
anonymous1 ..	Specified anonymous peer

- [Initial value] : -
- *tunnel\_num*
  - [Setting] : The NGN network mediated tunnel number or the L2TPv3 tunnel number
  - [Initial value] : -

#### [Description]

Manually disconnects the line.

#### [Note]

Models that do not support the data connect connection feature cannot use **disconnect pp** command.

Models that do not have data connect connection functionality and L2TPv3 functionality implemented cannot use the **disconnect tunnel** command.

RTX5000 does not support WAN interface for *interface* parameter.

#### [Models]

RTX810, RTX5000

### 43.6.8 ping

#### [Syntax]

**ping** [-s *datalen*] [-c *count*] [-sa *ip\_address*] [-w *wait*] *host*

#### [Setting and Initial value]

- *datalen*
  - [Setting] : Data length (1..65535 bytes)
  - [Initial value] : 64
- *count*
  - [Setting] : Execution count (1..21474836)
  - [Initial value] : Repeat until the Ctrl+c is pressed
- *ip\_address*
  - [Setting] : Source IP address (xxx.xxx.xxx.xxx where xxx is a decimal number)
  - [Initial value] : Select one from addresses granted to the router interface
- *wait*
  - [Setting] : Packet transmission interval in seconds
  - [Setting] :

Setting	Description
0.1 ... 3600.0	RTX810 Rev.11.01.23 or later
0.1 ... 99.9	Except above one

- [Initial value] : 1

- *host*
  - [Setting] :
    - IP address of the host to pings (xxx.xxx.xxx.xxx where xxx is a decimal number)
    - Name of the host to ping
  - [Initial value] : -

#### [Description]

Sends ICMP Echo to the specified host and waits for ICMP Echo Reply to be returned. When the reply is returned, the router notifies of that fact. When the command is complete, the router shows a simple statistical information.

If the *count* parameter is omitted, the operation repeats until the Ctrl+c key is pressed.

If the *-w* option is specified and the router does not detect a reply from the peer until the next packet is sent, the router shows a message notifying this fact. If the *-w* option is not specified, the router does not show any message even if the packet is not received.

#### [Models]

RTX810, RTX5000

### 43.6.9 Execute ping6

#### [Syntax]

```
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
ping6 destination [count]
ping6 destination%scope_id [count]
ping6 destination interface [count]
ping6 destination pp peer_num [count]
ping6 destination tunnel tunnel_num [count]
```

#### [Setting and Initial value]

- *datalen*
  - [Setting] : Data length (1..65535 bytes)
  - [Initial value] : 64
- *count*
  - [Setting] : Execution count (1..21474836)
  - [Initial value] : Repeat until the Ctrl+c is pressed
- *ipv6\_address*
  - [Setting] : Source IPv6 address
  - [Initial value] : Select one from addresses granted to the router interface
- *wait*
  - [Setting] : Packet transmission interval in seconds
  - [Setting] :

Setting	Description
0.1 ... 3600.0	RTX810 Rev.11.01.23 or later
0.1 ... 99.9	Except above one

- [Initial value] : 1
- *destination*
  - [Setting] : Destination IPv6 address or name
  - [Initial value] : -
- *scope\_id*
  - [Setting] : Scope ID
  - [Initial value] : -
- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Peer number

- [Initial value] : -
- *tunnel\_num*
  - [Setting] : Tunnel interface number
  - [Initial value] : -

**[Description]**

Sends ICMPv6 Echo Request to the specified destination.

The scope ID can be shown using the **show ipv6 address** command.

If the *count* parameter is omitted, the operation repeats until the Ctrl+c key is pressed.

If the -w option is specified and the router does not detect a reply from the peer until the next packet is sent, the router shows a message notifying this fact. If the -w option is not specified, the router does not show any message even if the packet is not received.

**[Models]**

RTX810, RTX5000

**43.6.10 traceroute**

---

**[Syntax]**

**traceroute** *host* [noresolv] [-sa *source*]

**[Setting and Initial value]**

- *host*
  - [Setting] :
    - IP address of the host to traceroute (xxx.xxx.xxx.xxx)
    - Name of the host to traceroute
  - [Initial value] : -
- noresolv : Keyword indicating that DNS resolution is not to be carried out
  - [Initial value] : -
- *source*
  - [Setting] : Source IP address
  - [Initial value] : -

**[Description]**

Traces the route to the specified host and shows the result.

**[Models]**

RTX810, RTX5000

**43.6.11 Execute traceroute6**

---

**[Syntax]**

**traceroute6** *destination*

**[Setting and Initial value]**

- *destination*
  - [Setting] : Destination IPv6 address or name
  - [Initial value] : -

**[Description]**

Traces the route to the specified destination and shows the result.

**[Models]**

RTX810, RTX5000

**43.6.12 nslookup**

---

**[Syntax]**

**nslookup** *host*

**[Setting and Initial value]**

- *host*
  - [Setting] :
    - IP address (xxx.xxx.xxx.xxx where xxx is a decimal number)
    - Host name
  - [Initial value] : -



**[Description]**

Performs name resolution through DNS.

**[Models]**

RTX810, RTX5000

### 43.6.13 Delete the Connection Management Information of the Dynamic IPv4 Filter

---

**[Syntax]**

**disconnect ip connection** *session\_id* [*channel\_id*]

**[Setting and Initial value]**

- *session\_id*
  - [Setting] : Session ID
  - [Initial value] : -
- *channel\_id*
  - [Setting] : Channel ID
  - [Initial value] : -

**[Description]**

Deletes a specified channel belonging to the specified session. If the channel is not specified, all channels belonging to the session are deleted.

**[Models]**

RTX810, RTX5000

### 43.6.14 TELNET Client

---

**[Syntax]**

**telnet** *host* [*port* [*mode* [*negotiation* [*abort*]]]]

**[Setting and Initial value]**

- *host*
  - [Setting] : IP address or host name of the peer to TELNET
  - [Initial value] : -
- *port* : Port number to be used
  - [Setting] :
    - Decimal Number
    - Port number mnemonic
    - 23 (TELNET) when omitted
  - [Initial value] : 23
- *mode* : TELNET communication (transmission) operation mode
  - [Setting] :

Setting	Description
character	Communicate at the character level
line	Communicate at the line level
auto	Select character or line according to the <i>port</i> parameter
Omitted	When omitted, auto is specified.

- [Initial value] : auto
- *negotiation* : Select the negotiation of the TELNET options
  - [Setting] :

Setting	Description
on	Negotiate
off	Not negotiate
auto	Select on or off according to the <i>port</i> parameter
Omitted	When omitted, auto is specified.

- [Initial value] : auto
- *abort* : Abort key for terminating the TELNET client
  - [Setting] :

- ASCII code in decimal notation
- .29(^) when omitted.
- [Initial value] : 29

**[Description]**

Executes the TELNET client.

**[Note]**

In character mode, transparent communication is carried out for connecting to a normal TELNET server.

In line mode, the input line is edited, and communication is performed at the line level. The end of the line editing is determined by the line feed code (CR:0x0d or LF:0x0a).

Regarding auto selection of functions according to the port number

**1.** Auto selection of the TELNET communication operation mode

If the port number is 23, character mode is selected. If not, line mode is selected.

**2.** Auto selection of the negotiation of the TELNET options

If the port number is 23, the options are negotiated. If not, the options are not negotiated.

**[Models]**

RTX810, RTX5000

### 43.6.15 Delete the Connection Management Information of the Dynamic IPv6 Filter

---

**[Syntax]**

**disconnect ipv6 connection** *session\_id* [*channel\_id*]

**[Setting and Initial value]**

- *session\_id*
  - [Setting] : Session ID
  - [Initial value] : -
- *channel\_id*
  - [Setting] : Channel ID
  - [Initial value] : -

**[Description]**

Deletes a specified channel belonging to the specified session. If the channel is not specified, all channels belonging to the session are deleted.

**[Models]**

RTX810, RTX5000

### 43.6.16 Delete the Switching Hub MAC Address Table

---

**[Syntax]**

**clear switching-hub macaddress** [*interface*]

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -

**[Description]**

Deletes the dynamic MAC address table held inside the switching hub LSI.

**[Note]**

If this command is executed when the *macaddress-aging* parameter of the **lan type** command is set to off, the table entry information is not deleted. The information is deleted the next time when the *macaddress-aging* parameter is set to on.

**[Models]**

RTX810, RTX5000

### 43.6.17 Send a Magic Packet

---

**[Syntax]**

**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 and Initial value]**

- *interval*
  - [Setting] : Packet transmission interval (s)
  - [Initial value] : 1
- *count*
  - [Setting] : Packet transmission count
  - [Initial value] : 4
- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *mac\_address*
  - [Setting] : MAC Address
  - [Initial value] : -
- *ip\_address*
  - [Setting] : IPv4 address
  - [Initial value] : -
- *port*
  - [Setting] : UDP port number
  - [Initial value] : -
- *type*
  - [Setting] : Ethernet type field value (1501..65535)
  - [Initial value] : -

**[Description]**

Sends a Magic Packet to the specified LAN interface.

In the first syntax, a packet with the Magic Packet data sequence stored in the UDP payload is sent as an IPv4 UDP packet. The source IP address and the destination UDP port number can be specified. However, if they are omitted, the source IP address is set to the directed broadcast address of the interface, and the destination port number is set to 9 (discard).

If the destination IP address is specified, the router sends the packet as unicast. In this case, the normal routing and ARP procedures are not carried out, and the destination MAC address is set to the address specified by the command. If the destination IP address is omitted, the router sends the packet as a broadcast.

In the second syntax, the router sends a packet in which the Magic Packet data sequence starts immediately after the Ethernet header.

For either syntax, the transmission interval and count of the Magic Packet can be specified by the *-i* and *-c* options. The command can be aborted using the ^C key even while the packet is being sent.

**[Note]**

Magic Packets can be sent only to LAN interfaces to which the Yamaha router is directly connected.

**[Models]**

RTX810, RTX5000

### 43.6.18 Check and Update the Firmware by Using HTTP

---

**[Syntax]**

**http revision-up go** [no-confirm [prompt]]

**[Setting and Initial value]**

- no-confirm : Do not ask whether to update the firmware when an overwritable revision of the firmware is available
  - [Initial value] : -
- prompt : Display a prompt immediately after the command is executed so that other commands can be executed
  - [Initial value] : -

**[Description]**

Checks the revision numbers of the firmware available on the WEB server and that of the firmware currently being used and updates the firmware if the firmware can be overwritten. When a firmware of an overwritable revision is available, a confirmation message “Update? (Y/N)” appears. You must enter “Y” to update the firmware or “N” to not update the firmware.

If the no-confirm option is specified, the firmware is updated without confirmation. If the prompt option is specified, a prompt appears immediately after the command is executed so that other commands can be executed. However, the router cannot perform other operations while it is writing the firmware onto the flash ROM.

The firmware can only be overwritten if you have permitted HTTP revision updating by executing the **http revision-up permit** command.

If downgrading is permitted by the **http revision-down permit** command, the firmware is overwritten even when the firmware on the WEB server is older than the current firmware.

If the firmware on the WEB server and the current firmware are of the same revision, the firmware is not overwritten.

**[Models]**

RTX810

### 43.6.19 Clear the Statistical Information for the URL Filter

---

**[Syntax]**

**clear url filter**

**clear url filter** [*interface*]

**clear url filter pp** [*peer\_num*]

**clear url filter tunnel** [*tunnel\_num*]

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Peer number
  - [Initial value] : -
- *tunnel\_num*
  - [Setting] : Tunnel interface number
  - [Initial value] : -

**[Description]**

Clears the statistical information for the URL filter. If no interface is specified, the information for all interfaces is cleared.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

### 43.6.20 Execute the Mail Notification

---

**[Syntax]**

**mail notify status exec** *id*

**[Setting and Initial value]**

- *id*
  - [Setting] : Setup number (1..10)
  - [Initial value] : -

**[Description]**

Sends the status information using mail.

**[Models]**

RTX810, RTX5000

### 43.6.21 Rotate (Back Up) the SYSLOG Files Stored in the External Memory

---

**[Syntax]**

**rotate external-memory syslog**

**[Description]**

Rotates (backs up) the SYSLOG files stored in the external memory. Saves the current SYSLOG file to a backup file, and creates a new SYSLOG file to write to. If the backup file with a same name already exists, this is not performed. Moreover, when creating the backup file, if the number of backup files has reached the maximum specified in the **external-memory syslog filename** command, or if you run out of available space in the external memory, the oldest backup file is deleted, and then the new backup file is created. For the naming format of the backup file, refer to the **external-memory syslog filename** command. Note that this command works only if the SYSLOG file name has been set by the **external-memory syslog filename** command, and the external memory is connected to the specified external storage interface.

**[Note]**

By executing this command regularly using the schedule at command, you will be able to to automatically create backup files of SYSLOG on a daily, weekly or monthly basis.

**[Example]**

```
schedule at 1 */* 00:00 * rotate external-memory syslog # Run backup daily
schedule at 1 */mon 00:00 * rotate external-memory syslog # Run backup every Monday
schedule at 1 */1 00:00 * rotate external-memory syslog # Run backup every 1st of the month
```

**[Models]**

RTX810, RTX5000

---

## Chapter 44

---

### Configuration Display

---

---

#### 44.1 Show the Router Configuration

---

**[Syntax]**

**show environment** [detail]

**[Setting and Initial value]**

- detail
  - [Setting] : In addition to the overall average CPU load, the CPU load for each individual core is displayed.
  - [Initial value] : -

**[Description]**

The following items are shown.

- Policy filtering module version (on models with the policy filter function)
- System revision
- CPU and memory usage (%)
- Packet buffer usage (%)
- Firmware and configuration file that are running
- Firmware and configuration file used at startup
- Fan status (RTX5000)
- Internal temperature Status (RTX5000)

RTX5000 supports the detail option. On the RTX5000, if the detail option is omitted, the overall average CPU load is displayed. If the detail option is specified, in addition to the overall average CPU load, the CPU load for each individual core is displayed.

**[Models]**

RTX810, RTX5000

---

#### 44.2 Show All Configurations

---

**[Syntax]**

**show config**  
**show config** *filename*  
**less config**  
**less config** *filename*

**[Setting and Initial value]**

- *filename*
  - [Setting] : Configuration file name or backup file name (0..4.2)
  - [Initial value] : -

**[Description]**

Shows all the configurations.

If a file is specified, you are prompted to enter the login password and administrator password.

**[Models]**

RTX810, RTX5000

---

#### 44.3 Show the Configuration of a Specified AP

---

**[Syntax]**

**show config ap** [*ap*]  
**less config ap** [*ap*]

**[Setting and Initial value]**

- *ap*
  - [Setting] :
    - MAC address or route
    - When it is omitted, the configuration of the selected AP is shown.
  - [Initial value] : -

**[Description]**

Shows only the configuration of the specified AP from the configuration shown by the **show config** and **less config** command.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810

## 44.4 Show the Configuration of a Specified PP

---

**[Syntax]**

```
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 and Initial value]**

- *peer\_num*
  - [Setting] :
    - Peer number
    - anonymous
    - If omitted, the configuration of the selected peer is shown.
  - [Initial value] : -

**[Description]**

Shows only the information related to the selected peer number among the items shown using the **show config** and **less config** commands.

Second syntax can be used on all Rev.14.00 series and later firmwares. If a range is specified by putting a hyphen (-) between two peer information numbers, the information for the specified range of peer information numbers will be displayed.

**[Models]**

RTX810, RTX5000

## 44.5 Show the Configuration of a Specified Switch

---

**[Syntax]**

```
show config switch [switch]
less config switch [switch]
```

**[Setting and Initial value]**

- *switch*
  - [Setting] :
    - MAC address or route
    - When it is omitted, the configuration of the selected switch is shown
  - [Initial value] : -

**[Description]**

Shows only the configuration of the specified switch from the configuration shown by the **show config** and **less config** command.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810

## 44.6 Show the Configuration of a Specified Tunnel

---

**[Syntax]**

```
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 and Initial value]**

- *tunnel\_num*
  - [Setting] :
    - Tunnel number
    - If omitted, the configuration of the selected tunnel is shown.
  - [Initial value] : -

**[Description]**

Shows only the configuration of the specified tunnel number from the configuration shown by the **show config** and **less config** commands.

Second syntax can be used with Rev.14.00 series and later firmwares. If a range is specified by putting a hyphen (-) between two tunnel numbers, the information for the specified range of tunnel numbers will be displayed.

If you specify the expand keyword, the command shows the settings that are actually referenced after the template specified by the **tunnel template** command is applied.

**[Models]**

RTX810, RTX5000

## 44.7 List the Configuration Files

---

**[Syntax]**

**show config list**

**less config list**

**[Description]**

Shows a list of the file names, dates, and comments of the configuration files saved on the internal Flash ROM.

**[Models]**

RTX810, RTX5000

## 44.8 Show a List of File Information

---

**[Syntax]**

**show file list** *location* [all] [file-only]

**less file list** *location* [all] [file-only]

**[Setting and Initial value]**

- *location* : Location of the file to be shown
  - [Setting] :

Setting	Description
internal	List of the config files that are stored in the internal flash ROM
Relative or absolute path	Internal flash ROM RTFS and external memory

- [Initial value] : -
- all : Show the contents of all the directories at the specified path
  - [Initial value] : -
- file-only : Only display file names
  - [Initial value] : -

**[Description]**

Shows a list of files and directories stored at the specified location.

If you set *location* to a relative path, it is interpreted as a path starting with the PWD environment variable. You can change PWD with the **set** command. Its initial value is “/”.

**[Note]**

all and file-only are available only when you set *location* to an absolute path or relative path.

**[Models]**

RTX810, RTX5000

## 44.9 Show the IPv6 Address Granted to the Interface

---

**[Syntax]**

**show ipv6 address** [*interface*]



```
show ipv6 address pp [peer_num]
show ipv6 address tunnel [tunnel_num]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name, loopback interface name, null interface name, or bridge interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] :
    - Peer number
    - anonymous
    - If omitted, the configuration of the selected peer is shown.
  - [Initial value] : -
- *tunnel\_num*
  - [Setting] : Tunnel interface number
  - [Initial value] : -

**[Description]**

Shows the IPv6 addresses that are granted to each interface.  
If no interface is specified, the information for all interfaces is displayed.  
RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

## 44.10 Showing lines acquired by masterclock

---

**[Syntax]**

```
show line masterclock
```

**[Description]**

Shows the lines acquired by the clock for communication use. If in free run, this will be indicated.

**[Models]**

RTX5000

## 44.11 Show the SSH Server Public Key

---

**[Syntax]**

```
show sshd public key
```

**[Description]**

Shows the SSH server public key.

**[Models]**

RTX810, RTX5000

## 44.12 Display the Filter Contents of the Specified Interface

---

**[Syntax]**

```
show ip secure filter interface [dir]
show ip secure filter pp [peer_num] [dir]
show ip secure filter tunnel [tunnel_num] [dir]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : Name of an interface that has a filter applied to it
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Peer number
  - [Initial value] : -
- *tunnel\_num*
  - [Setting] : Tunnel interface number
  - [Initial value] : -
- *dir*

- [Setting] : The filter direction, 'in' or 'out'
- [Initial value] : -

**[Description]**

The contents of the filter definition for the specified interface are displayed.

**[Models]**

RTX810, RTX5000

## 44.13 List of firmware files

---

**[Syntax]**

**show exec list**

**less exec list**

**[Description]**

Displays information for the firmware files saved in the internal Flash ROM. The operating firmware file is indicated with an asterisk (\*). When the external memory where the firmware is stored is connected, the information including that firmware is displayed.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

---

## Chapter 45

---

### Status Display

---

---

#### 45.1 Show the ARP Table

---

**[Syntax]**

```
show arp [interface[/sub_interface]]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *sub\_interface*
  - [Setting] : 1-32 (RTX5000), 1-8 (models not listed)
  - [Initial value] : -

**[Description]**

Shows the ARP table. If an interface name is specified, the router shows only the ARP table information obtained through that interface.

**[Models]**

RTX810, RTX5000

---

#### 45.2 Show the Interface Status

---

**[Syntax]**

```
show status interface
```

**[Setting and Initial value]**

- *interface*
  - [Setting] :
    - LAN interface name
    - WAN interface name
    - Bridge interface name
  - [Initial value] : -

**[Description]**

Shows the interface status.

**[Note]**

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.  
RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

---

#### 45.3 Show the Peer Status

---

**[Syntax]**

```
show status pp [peer_num]
```

**[Setting and Initial value]**

- *peer\_num*
  - [Setting] :
    - Peer number
    - anonymous
    - If omitted, the configuration of the selected peer is shown.
  - [Initial value] : -

**[Description]**

Shows the status of the peer that is connected or the status of the last connection.

- Currently connected or not
- Call status immediately before

- Date/Time of connection (disconnection)
- Line type
- Communication time
- Cause of disconnection
- Communication charge
- IP addresses on the local PP interface and remote PP interface
- Number of packets sent successfully
- Number of transmission errors and their breakdown
- Number of packets received successfully
- Number of receive errors and their breakdown
- PPP status
- CCP status
- Miscellaneous

**[Models]**

RTX810, RTX5000

## 45.4 Show the IP Routing Information Table

**[Syntax]****show ip route** [*destination*]**show ip route** detail**show ip route** summary**[Setting and Initial value]**

- *destination*
  - [Setting] :
    - Peer IP address
    - When omitted, the entire routing information table is shown.
  - [Initial value] : -
- detail : Shows dynamic routes that are hidden by the routes obtained by the dynamic routing protocol in addition to the current active IPv4 routes.
  - [Initial value] : -
- summary : Shows the number of IPv4 routes as a total for each protocol
  - [Initial value] : -

**[Description]**

Shows the IP routing information table of the gateway to the peer IP address.

The netmask is expressed as a number of consecutive bits regardless of the expression used when it was set.

In case of frame relay, the DLCI value is shown.

If detail is specified, static routes that are hidden by the comparison of the routes obtained by the dynamic routing protocol and the preference value are shown in addition to the current active IPv4 routes.

If summary is specified, the number of IPv4 routes is shown as a total for each protocol.

**[Note]**

For routes obtained by the dynamic routing protocol, the router shows auxiliary information according to the protocol. The following auxiliary information is shown.

Protocol	Metric value
RIP	Metric value
OSPF	Cost value and metric value (external routes only) for each internal and external route For a type 1 external route, the cost value is the cost value to the route including the metric value. For a type 2 external route, the cost value is the cost value to the ASBR.
BGP	None

**[Models]**

RTX810, RTX5000

## 45.5 Show Routing Information Obtained by RIP

---

### [Syntax]

**show ip rip table**

### [Description]

Shows routing information obtained by RIP.

### [Models]

RTX810, RTX5000

## 45.6 Show IPv6 Routing Information

---

### [Syntax]

**show ipv6 route**  
**show ipv6 route detail**  
**show ipv6 route summary**

### [Setting and Initial value]

- detail : Show active IPv6 routes as well as hidden IPv6 routes
  - [Initial value] : -
- summary : Shows the number of IPv6 routes as a total for each protocol
  - [Initial value] : -

### [Description]

Shows IPv6 routing information.

When detail is specified, IPv6 routes that are hidden by the preference comparison are shown in addition to the currently active IPv6 routes.

If summary is specified, the number of IPv6 routes as a total for each protocol is shown.

### [Models]

RTX810, RTX5000

## 45.7 Show the IPv6 RIP Table

---

### [Syntax]

**show ipv6 rip table**

### [Description]

Shows the IPv6 RIP table.

### [Models]

RTX810, RTX5000

## 45.8 Show the Neighbor Cache

---

### [Syntax]

**show ipv6 neighbor cache**

### [Description]

Shows the status of the neighbor cache.

### [Models]

RTX810, RTX5000

## 45.9 Showing bridge learning information

---

### [Syntax]

**show bridge learning *bridge\_interface***

### [Setting and Initial value]

- *bridge\_interface*
  - [Setting] : Bridge interface name
  - [Initial value] : -

### [Description]

Shows the MAC address learning information for the bridge.

**[Note]**

RTX810 supports bridge interface for *interface* parameter in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

## 45.10 Show IPsec SA

---

**[Syntax]**

**show ipsec sa** [*id*]

**show ipsec sa gateway** [*gateway\_id*] [detail]

**[Setting and Initial value]**

- *id*
  - [Setting] :
    - SA ID
    - When omitted, all SAs are shown.
  - [Initial value] : -
- *gateway\_id*
  - [Setting] :
    - Security Gateway ID
    - When omitted, a summary of all security gateway SAs is shown.
  - [Initial value] : -
- detail : Show detailed information of the SA.
  - [Initial value] : -

**[Description]**

Shows the IPsec SA status.

Shows information on the SA with an ID specified by *id*.

**[Note]**

If XAUTH authentication was performed at the creation of the displayed SA, the following items are displayed at the same time: The user name used for authentication.

- Whether RADIUS authentication was performed
- The reported internal IP address
- The added route information
- Information about the applied filter

**[Models]**

RTX810, RTX5000

## 45.11 Show the Certificate Information

---

**[Syntax]**

**show pki certificate summary** [*cert\_id*]

**[Setting and Initial value]**

- *cert\_id*
  - [Setting] :

Setting	Description
1..8	Certificate file identifier

- [Initial value] : -

**[Description]**

Shows the certification information.

The following information is shown:

- Subject
- SubjectAltName
- Usable period (Not Before, Not After)
- Certificate type (CA certificate/device certificate)

When *cert\_id* is specified, information of the certificate of the specified file identifier is shown only.

**[Models]**  
RTX810, RTX5000

## 45.12 Show the CRL File Information

---

**[Syntax]**

**show pki crl** [*crl\_id*]

**[Setting and Initial value]**

- *crl\_id*
  - [Setting] :

Setting	Description
1..8	CRL file identifier

- [Initial value] : -

**[Description]**

Shows the CRL file information.

The following information is shown:

- Version
- Issuer
- Update date and time
- Next update date and time

**[Models]**  
RTX810, RTX5000

## 45.13 Show VRRP Information

---

**[Syntax]**

**show status vrrp** [*interface* [*vrid*]]

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *vrid*
  - [Setting] : VRRP group ID (1..255)
  - [Initial value] : -

**[Description]**

Shows VRRP information.

**[Models]**  
RTX810, RTX5000

## 45.14 Show the Address Map of the Dynamic NAT Descriptor

---

**[Syntax]**

**show nat descriptor address** [*nat\_descriptor*] [detail]

**[Setting and Initial value]**

- *nat\_descriptor*
  - [Setting] :

Setting	Description
1..2147483647	NAT descriptor number
all	All NAT descriptor numbers

- [Initial value] : -
- detail : Show all dynamic IP masquerade entries.
- [Initial value] : -

**[Description]**

Shows the address map of the dynamic NAT descriptor.

If *nat\_descriptor* is omitted, the address map of all NAT descriptor numbers is shown.

**[Note]**

if the detail option is omitted, the dynamic IP masquerade entries are arranged by internal IP address and displayed, and the IP masquerade entries derived and generated by the static IP masquerade entries are not displayed. Therefore, the detail option is prepared as an option for displaying in all previous entry display formats.

When there is many IP masquerading entries, it may take time to display all the entries if you specify the detail option, and do so may interfere with communication. Therefore, we recommend that you avoid using the detail option, or use the **show nat descriptor masquerade port summary** command when you want to check how many ports are being used by IP masquerading.

**[Models]**

RTX810, RTX5000

## 45.15 Show the List of Active NAT Descriptor Applications

---

**[Syntax]**

**show nat descriptor interface bind** *interface*

**show nat descriptor interface bind pp**

**show nat descriptor interface bind tunnel**

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -

**[Description]**

Shows a list of NAT descriptors and the applied interfaces.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 45.16 Show the Address Map of the NAT Descriptor of the LAN Interface

---

**[Syntax]**

**show nat descriptor interface address** *interface*

**show nat descriptor interface address pp** *peer\_num*

**show nat descriptor interface address tunnel** *tunnel\_num*

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Peer number
  - [Initial value] : -
- *tunnel\_num*
  - [Setting] : Tunnel interface number
  - [Initial value] : -

**[Description]**

Shows the address map of the NAT descriptor applied to the interface.

**[Note]**

the dynamic IP masquerade entries are arranged by internal IP address and displayed, and the IP masquerade entries derived and generated by the static IP masquerade entries are not displayed.

RTX5000 does not support WAN interface for *interface* parameter.



**[Models]**  
RTX810, RTX5000

## 45.17 Show the Number of Ports Being Used by IP Masquerading

---

**[Syntax]**

**show nat descriptor masquerade port** [*nat\_descriptor*] **summary**

**[Setting and Initial value]**

- *nat\_descriptor*
  - [Setting] :
    - NAT descriptor number (1..2147483647)
    - When *nat\_descriptor* is omitted, the command shows the information for all NAT descriptors.
  - [Initial value] : -

**[Description]**

Shows the number of ports being used by dynamic IP masquerading. The number of ports secured by static IP masquerading is not included.

**[Models]**  
RTX810, RTX5000

## 45.18 Show the L2TP Status

---

**[Syntax]**

**show status l2tp** [*tunnel\_tunnel\_num*]

**[Setting and Initial value]**

- *tunnel\_num*
  - [Setting] : Tunnel number
  - [Initial value] : -

**[Description]**

Shows the L2TP status.

**[Note]**

Tunnel numbers can be specified only on models that support the L2TPv3 function.

**[Models]**  
RTX810, RTX5000

## 45.19 Show the PPTP Status

---

**[Syntax]**

**show status pptp**

**[Description]**

Shows the PPTP status and GRE statistical information.

**[Models]**  
RTX810

## 45.20 Show OSPF Information

---

**[Syntax]**

**show status ospf info**

**[Setting and Initial value]**

- *info* : Type of information to be shown
  - [Setting] :

Setting	Description
database	OSPF database
neighbor	Neighbor router
interface	Status of each interface

Setting	Description
virtual-link	Virtual link status

- [Initial value] : -

**[Description]**

Shows OSPF information.

**[Models]**

RTX810, RTX5000

## 45.21 Show the BGP Status

---

**[Syntax]**

```
show status bgp neighbor [ip-address]
show status bgp neighbor ip-address route-type
```

**[Setting and Initial value]**

- *ip-address*
  - [Setting] : IP address of the adjacent router
  - [Initial value] : -
- *route-type* : Routing information display
  - [Setting] :

Setting	Description
advertised-routes	Show the routes advertised to the adjacent router
received-routes	Show the routes received from the adjacent router
routes	Shows valid routes received from the adjacent router

- [Initial value] : -

**[Description]**

Shows information related to the adjacent router of BGP.

If the *ip-address* is specified, information on a specific adjacent router is shown. If the *ip-address* is omitted, information on all adjacencies is shown.

If *route-type* is specified, routing information exchanged with adjacencies is shown. If *advertised-routes* is specified, the routes advertised to adjacencies are shown. If *received-routes* is specified, all routes received from adjacencies are shown. If *routes* is specified, only the routes accepted by the **bgp export filter** and so forth among the routes received from the adjacencies are shown.

**[Models]**

RTX810, RTX5000

## 45.22 Show the DHCP Server Status

---

**[Syntax]**

```
show status dhcp [summary] [scope_n]
```

**[Setting and Initial value]**

- *summary* : Show a summary of the IP address assignment status of each DHCP scope
  - [Initial value] : -
- *scope\_n*
  - [Setting] : Scope number (1-65535)
  - [Initial value] : -

**[Description]**

Shows the lease status of each DHCP. The following items are shown.

- Lease status of the DHCP scope
- DHCP scope number
- Network address
- Assigned IP address
- MAC address of the assigned client
- Remaining lease time
- Reserved (unused) IP address
- Number of all IP addresses in the DHCP scope

- Number of IP addresses that are excluded.
- Number of assigned IP addresses.
- Number of addresses that can be used and the number of reserved IP address in parentheses.

**[Models]**

RTX810, RTX5000

## 45.23 Show the DHCP Client Status

---

**[Syntax]****show status dhcpc****[Description]**

Shows the DHCP client status.

- Client status
  - Interface
  - IP address (the status if the address cannot be retrieved)
  - DHCP server
  - Remaining lease time
  - Client ID
  - Host name (when specified)
- Common information
  - DNS server
  - Gateway

**[Models]**

RTX810, RTX5000

## 45.24 Show the DHCPv6 Status

---

**[Syntax]****show status ipv6 dhcp****[Description]**

Shows the status related to DHCPv6.

**[Models]**

RTX810, RTX5000

## 45.25 Show the Backup Status

---

**[Syntax]****show status backup****[Description]**

Shows the backup status of the interface set to backup.

**[Models]**

RTX810, RTX5000

## 45.26 Show the Connections Managed by Dynamic Filters

---

**[Syntax]****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 [*interface* [*direction*]]**show ip connection** detail **pp** [*peer\_num* [*direction*]]**show ip connection** detail **tunnel** [*tunnel\_num* [*direction*]]**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *peer\_num*

- [Setting] : Peer number
- [Initial value] : -
- *tunnel\_num*
  - [Setting] : Tunnel interface number
  - [Initial value] : -
- *direction*
  - [Setting] :

Setting	Description
in	Input direction
out	Output direction

- [Initial value] : -
- *ip\_address*
  - [Setting] : IP address xxx.xxx.xxx.xxx (where xxx is a decimal number)
  - [Initial value] : -
- *summary* : Show the number of managed connections for each interface and direction and the total.
  - [Initial value] : -
- *detail* : Shows all connections managed by dynamic filters
  - [Initial value] : -

**[Description]**

On the Rev.14.00 or later, in case of without detail option, the managed connections which is aggregated by each source IP address are displayed. In case of without interface option, all information of every interface is displayed.

If detail is not specified, the connections managed by dynamic filters will be displayed as a summary of each originating IP address. However, if *ip\_address* has been specified, the source address from the information specified in detail will be displayed as the results of *ip\_address*.

**[Note]**

**show ip connection detail** command is available on the RTX5000 models.

**show ip connection** command as a summary of each originating IP address is available on the RTX5000 models.

RTX5000 does not support WAN interface for *interface* parameter.

*ip\_address* can be specified on the RTX5000 models.

**[Models]**

RTX810, RTX5000

## 45.27 Show the Connections Managed by IPv6 Dynamic Filters

---

**[Syntax]**

**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 interface** [*direction*]

**show ipv6 connection pp** [*peer\_num*] [*direction*]

**show ipv6 connection tunnel** [*tunnel\_num*] [*direction*]

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Peer number
  - [Initial value] : -
- *tunnel\_num*
  - [Setting] : Tunnel interface number
  - [Initial value] : -
- *direction*
  - [Setting] :

Setting	Description
in	Input direction
out	Output direction

- [Initial value] : -
- *ipv6\_address*
  - [Setting] : IPv6 address portion
  - [Initial value] : -
- summary : Show the number of managed connections for each interface and direction and the total.
  - [Initial value] : -
- detail : Shows all connections managed by dynamic filters
  - [Initial value] : -

**[Description]**

On the Rev.14.00 or later, in case of without detail option, the managed connections which is aggregated by each source IP address are displayed. In case of without interface option, all information of every interface is displayed.

If detail is not specified, the connections managed by dynamic filters will be displayed as a summary of each originating IP address. However, if *ipv6\_address* has been specified, the source address from the information specified in detail will be displayed as the results of *ipv6\_address*.

**[Note]**

**show ipv6 connection detail** command is available on the RTX5000 models.

**show ipv6 connection** command as a summary of each originating IP address is available on the RTX5000 models.

The WAN interface can be specified for RTX810.

*ipv6\_address* can be specified on the RTX5000 models.

**[Models]**

RTX810, RTX5000

## 45.28 Show the Status of the Network Monitor Function

---

**[Syntax]**

```
show status ip keepalive
```

**[Description]**

Shows the status of the network monitor function.

**[Models]**

RTX810, RTX5000

## 45.29 Show the History of Intrusion Information

---

**[Syntax]**

```
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 and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] : Peer number
  - [Initial value] : -
- *tunnel\_num*
  - [Setting] : Tunnel interface number
  - [Initial value] : -
- *direction*
  - [Setting] :

Setting	Description
in	Input direction
out	Output direction

- [Initial value] : -

**[Description]**

Shows the recent intrusion information. Intrusion information is shown for each direction of each interface. The maximum number of incidents that are shown is the value specified by the **ip intrusion detection report** command.

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 45.30 Show the Connection Time for Each Peer

---

**[Syntax]**

**show pp connect time** [*peer\_num*]

**[Setting and Initial value]**

- *peer\_num*
  - [Setting] :
    - Peer number
    - anonymous
    - If omitted, the configuration of the selected peer is shown.
  - [Initial value] : -

**[Description]**

Shows the connection time of the selected peer.

**[Models]**

RTX810

## 45.31 Display the Status of GUI Language Setting

---

**[Syntax]**

**show status httpd language**

**[Description]**

Shows the settings for the currently valid GUI language.

**[Example]**

```
> show status httpd language
config: English
execute: English
```

**[Models]**

RTX810

## 45.32 Show Settings Related to the NetVolante DNS Service

---

**[Syntax]**

**show status netvolante-dns** *interface*

**show status netvolante-dns pp** [*peer\_num*]

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN or WAN interface name
  - [Initial value] : -
- *peer\_num*
  - [Setting] :
    - Peer number
    - If omitted, the configuration of the selected peer is shown.

- [Initial value] : -

**[Description]**

Shows settings that relate to dynamic DNS.

Displayed Contents

NetVolante DNS service	AUTO/OFF
Interface	INTERFACE
Host address	aaa.bbb.netvolante.jp
IP address	aaa.bbb.ccc.ddd
Most recent update	2001/01/25 15:00:00
Timeout	90 seconds

**[Note]**

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

### 45.33 Show the Switching Hub MAC Address Table

---

**[Syntax]**

```
show status switching-hub macaddress [interface [port]] [mac_address]
```

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *port*
  - [Setting] : Port number 1..4
  - [Initial value] : -
- *mac\_address*
  - [Setting] : MAC Address
  - [Initial value] : -

**[Description]**

Shows the dynamic MAC address table of each port held inside the switching hub LSI. If a port number is specified, only the information of that port is shown. Only the interfaces that have a switching hub can be specified for the LAN interface name.

**[Models]**

RTX810, RTX5000

### 45.34 Show the UPnP Status Information

---

**[Syntax]**

```
show status upnp
```

**[Description]**

Shows the UPnP status information.

**[Models]**

RTX810

### 45.35 Show the Tunnel Interface Status

---

**[Syntax]**

```
show status tunnel [tunnel_num]
show status tunnel [state]
```

**[Setting and Initial value]**

- *tunnel\_num*
  - [Setting] : Tunnel interface number
  - [Initial value] : -

- *state* : Connection status
  - [Setting] :

Setting	Description
up	Displays a list of connected tunnel interfaces
down	Displays a list of unconnected tunnel interfaces

- [Initial value] : -

**[Description]**

Shows the tunnel interface status. Second syntax does not support PPTP tunnel. On PPTP enabled models, PPTP tunnels are designated as unconnected tunnel interfaces. In addition, for models that have the L2TP/IPsec function and L2TPv3/IPsec function enabled, L2TP tunnels are designated according to the connection status of the IPsec tunnel.

**[Note]**

On the Rev.14.00 or later, the second syntax is available.

**[Models]**

RTX810, RTX5000

## 45.36 Show the VLAN Interface Status

---

**[Syntax]**

**show status vlan** [*interface/sub\_interface*]

**[Setting and Initial value]**

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -
- *sub\_interface*
  - [Setting] : 1-32 (RTX5000), 1-8 (RTX810)
  - [Initial value] : -

**[Description]**

Shows the VLAN interface information. If a VLAN interface name is specified, only the information of that interface is shown.

**[Models]**

RTX810, RTX5000

## 45.37 Show Information Regarding the Triggered Mail Notification Function

---

**[Syntax]**

**show status mail service** [*template\_id*] [debug]

**[Setting and Initial value]**

- *template\_id*
  - [Setting] : Template ID (1..10)
  - [Initial value] : -
- debug : Show the internal information for debugging
  - [Initial value] : -

**[Description]**

Shows the internal state of the triggered mail notification function.  
If a template ID is not specified, information of all template IDs is shown.

**[Models]**

RTX810, RTX5000

## 45.38 Show MLD Group Management Information

---

**[Syntax]**

**show status ipv6 mld**

**[Description]**

Shows a list of information managed by MLD.  
If an MLD proxy is running, this command can be used to check the forwarding destination.



**[Models]**  
RTX810, RTX5000

## 45.39 Show IPv6 Multicast Routing Information

### [Syntax]

**show ipv6 mroute fib**

### [Description]

Shows forwarding routes of IPv6 multicast packets.  
This command shows the following information for each forwarding route.

Item	Description
Inbound IF	Inbound interface
Source	Source address of the multicast packet
Group	Group address of the multicast packet
Outbound IFs	Output interface. When output to multiple interfaces, each interface is separated by a comma.

**[Models]**  
RTX810, RTX5000

## 45.40 Show Information about the Logged in User

### [Syntax]

**show status user**

### [Description]

Shows information of the user logged in to the router. The following items are shown.

- User name
- Connection type
- Date of login
- Idle time
- Peer IP address

Also, the following marks are attached before the user name according to user status.

Mark	Condition
Asterisk	Current user
Plus	Administrator mode
At mark	Authenticated via RADIUS

### [Example]

```
> show status user
(*: 自分自身のユーザー情報, +: 管理者モード, @: RADIUS での認証)
ユーザー名   接続種別   ログイン   アイドル   IP アドレス
-----
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)
username     connection login time  idle   IP address
-----
user-local   serial   09/16 10:21 0:02:08
@user-radius2 remote   09/16 10:22 0:02:27
*+@user-radius1 telnet1  09/16 10:22 0:00:00 192.168.0.100
```

**[Models]**  
RTX810, RTX5000

## 45.41 Show the Packet Buffer Status

### [Syntax]

**show status packet-buffer** [*group*]

### [Setting and Initial value]

- *group* : Specify the packet buffer group to be displayed.
  - [Setting] :

Setting	Description
Group name (small, middle, large, jumbo, huge)	Show the specified group status
Omitted	All groups are displayed

- [Initial value] : -

### [Description]

Shows the packet buffer status. The following items are shown.

- Group name
- Packet size that can be stored
- Management parameter
- Number of packet buffers currently assigned
- Number of packet buffers currently linked to the free list
- Number of chunks currently allotted
- Number of times packet buffer assignment requests have been received
- Number of successful packet buffer assignments
- Number of failed packet buffer assignments
- Number of released packet buffers
- Number of times chunks were allotted
- Number of failed chunk allotments
- Number of times chunks that were released

### [Note]

Jumbo groups can only be used on models that support the 1000BASE-T LAN interface and can send and received jumbo packets.

### [Example]

```
# show status packet-buffer large
large group: 2048 bytes length
parameters: max-buffer=10000 max-free=2812 min-free=62
            buffers-in-chunk=625 initial-chunk=4
2372 buffers in free list
128 buffers are allocated, req/succ/fail/rel = 137/137/0/9
4 chunks are allocated, req/succ/fail/rel = 4/4/0/0
```

### [Models]

RTX810, RTX5000

## 45.42 Show the QoS Status

### [Syntax]

**show status qos info** [*interface* [*class*]]

### [Setting and Initial value]

- *info* : Type of information to be shown
  - [Setting] :

Setting	Description
bandwidth	Used bandwidth
length	Number of packets in queue
dcc	Dynamic Class Control status

Setting	Description
all	All information

- [Initial value] : -
- *interface*
  - [Setting] : LAN interface name (If omitted, the status is shown for all LAN interfaces.)
  - [Initial value] : -
- *class*
  - [Setting] : Class (RTX5000: 1..100; other models: 1..16)
  - [Initial value] : -

**[Description]**

Shows QoS setup information and the usage status of each class for the interface.

- LAN interface name
- Queuing algorithm
- Interface speed
- Number of classes
- The configured bandwidth, the used bandwidth, and the peak value of the used bandwidth of each class and the recording date/time
- Total of the configured bandwidths
- Number of successful/failed enqueues, number of dequeues, number of held packets, and peak value of the number of packets of each class and the recording date/time
- Information about hosts being controlled through Dynamic Class Control and how they are being controlled

**[Models]**

RTX810, RTX5000

## 45.43 Show the Cooperation Status

---

**[Syntax]**

**show status cooperation** *type* [*id*]

**[Setting and Initial value]**

- *type* : Cooperation type
  - [Setting] :

Setting	Description
bandwidth-measuring	Line bandwidth detection
load-watch	Load watch notification

- [Initial value] : -
- *id*
  - [Setting] : Peer ID number (1-100)
  - [Initial value] : -

**[Description]**

Shows cooperation information.

The following items are shown for line bandwidth detection.

- Peer information
- Status display
  - Count
  - Time of measurement
  - Measured result (client operation only)
  - Current status (client operation only)
  - Configuration change history (client operation only)
  - Remaining time until the next measurement (client operation only)

The following items are shown for load watch notification.

- Peer information
- Status display
  - Suppression request county
  - Suppression release count
  - History

**[Models]**

RTX810, RTX5000

**45.44 Showing OSPFv3 information**

---

**[Syntax]****show ipv6 ospf info****[Setting and Initial value]**• *info*

- [Setting] :

Setting	Description
database	OSPFv3 database
neighbor	Neighboring router
interface	Status of each interface
virtual-link	Status of virtual link

- [Initial value] : -

**[Description]**

Shows the OSPFv3 status.

**[Note]**

RTX810 supports this command in Rev.11.01.23 or later.

**[Models]**

RTX810, RTX5000

**45.45 Show the URL Filter Information**

---

**[Syntax]****show url filter****show url filter interface****show url filter pp** [*peer\_num*]**show url filter tunnel** [*tunnel\_num*]**[Setting and Initial value]**• *interface*

- [Setting] : LAN or WAN interface name

- [Initial value] : -

• *peer\_num*

- [Setting] : Peer number

- [Initial value] : -

• *tunnel\_num*

- [Setting] : Tunnel interface number

- [Initial value] : -

**[Description]**

Shows statistical information about which of the specified interfaces matched with the filter and how many times. If no interface is specified, the information for all interfaces is shown.

The following items are shown.

- Filter number
- Source IP address
- The number of times that the HTTP connection matched with the filter

**[Note]**

If an asterisk is entered for both the keyword and the IP address in the **url filter** command, the number of times that the HTTP connection matched with that filter is not displayed.

RTX5000 does not support WAN interface for *interface* parameter.

**[Models]**

RTX810, RTX5000

## 45.46 Show the Heartbeat Information

---

### [Syntax]

**show status heartbeat**

### [Description]

Shows the heartbeat information that has been received.

The following items are shown.

- Reported name
- Reported IP address
- Time when the last heartbeat was received
- Reception interval (s)

### [Models]

RTX810, RTX5000

## 45.47 Show the USB Host Function Operation Status

---

### [Syntax]

**show status usbhost** [modem]

### [Description]

Shows the USB host function operation status.

If you specify modem, the connection information for the device that is connected to the USB port is displayed. The current connection status, the total number of errors that have occurred during connection, the total number of bytes that have been sent and received, the total number of transmissions and receptions, information about the most recent connection, etc., are displayed.

### [Models]

RTX810

## 45.48 Show Connection Information Related to the Remote Setup Function

---

### [Syntax]

**show status remote setup**

### [Description]

Shows connection information related to the remote setup function.

The current connection status, the total number of errors that have occurred during connection, the total number of frames that have been sent and received, the total number of transmissions and receptions, information about the most recent connection, etc., are displayed.

### [Models]

RTX810, RTX5000

## 45.49 Show Technical Info

---

### [Syntax]

**show techinfo**

### [Description]

Shows information necessary for technical support.

In contrast to other **show** commands, the **show techinfo** command is output all at once, regardless of the setting of the console **console columns/lines** command. The output is not stopped for each screen. This means that it is best to use the log function of a terminal software application to save the output to a file on a PC.

The setting of the **console character** command is also ignored, and the contents are always output in English mode.

If you want to check the output contents one screen at a time, we recommend that you use the **less** command as indicated below. However, because the **less** command outputs multiple screen control sequences, if you log the output while using the **less** command, the log file will be difficult to read.

**show techinfo | less**

### [Note]

If you access the router from a TFTP client on a PC and get the 'techinfo' file, the result will be the same as the output of the

**show techinfo** command.

The following is an example using TFTP.EXE on Windows XP:

```
C:\>tftp 192.168.0.1 get techinfo techinfo.txt
```

**[Models]**

RTX810, RTX5000

## 45.50 Show the Operation Status of the microSD Slot

---

**[Syntax]**

```
show status sd
```

**[Description]**

Shows the operation status of the microSD slot.

**[Models]**

RTX810, RTX5000

## 45.51 Show the Operation Status of the External Memory

---

**[Syntax]**

```
show status external-memory
```

**[Description]**

Shows the status and common information about the external memory connected to the USB port and the microSD slot.

**[Note]**

If a mobile terminal is connected to the USB port, this command will indicate that external memory is not connected to the router.

You can check the status of a mobile terminal by executing the **show status usbhost** modem command.

**[Models]**

RTX810, RTX5000

## 45.52 Show the RTFS Status

---

**[Syntax]**

```
show status rtfs
```

**[Description]**

Shows the status of the RTFS area of the internal flash ROM. The following items are shown.

- Capacity
- Available memory
- Number of entries that can be created
- Number of files
- Number of directories

The example is shown below:

```
# show status rtfs
Capacity          : 1572864 bytes
Available memor   : 1566025 bytes
Number of entries that can be created : 995
Number of files   : 2
Number of directories : 3
#
```

**[Models]**

RTX810, RTX5000

## 45.53 Show the Startup Information

---

**[Syntax]**

```
show status boot [num]
```

**[Setting and Initial value]**

- *num* : History number
- [Setting] :

Setting	Description
0..4	Shows the specified number's history
Omitted	0, when omitted

- [Initial value] : -

#### [Description]

Shows the startup information.

Specify a history number displayed with the **show status boot list** command, and detail of that history is displayed.

When *num* is omitted, history of the history number =0 is displayed.

#### [Models]

RTX810, RTX5000

## 45.54 Show Detail of the Startup Information History

---

#### [Syntax]

**show status boot all**

#### [Description]

Shows detail of the history of up to 5 items of startup information.

When the **cold start** command and the **clear boot list** command are executed, the information is cleared.

#### [Models]

RTX810, RTX5000

## 45.55 Show a List of the Startup Information History

---

#### [Syntax]

**show status boot list**

#### [Description]

Shows the history of up to 5 items of startup information.

When the **cold start** command and the **clear boot list** command are executed, the information is cleared.

#### [Models]

RTX810, RTX5000

## 45.56 Show a List of the Switches Controlled by the Router

---

#### [Syntax]

**show status switch control** *interface*

#### [Setting and Initial value]

- *interface*
  - [Setting] : LAN interface name
  - [Initial value] : -

#### [Description]

Shows a list of switches controlled by the router. If no interface is specified, the information for all interfaces is displayed.

- MAC address
- Model name
- System name
- Route from router
- Uplink port
- Setting currently used

#### [Example]

```
> show status switch control
LAN1
[00:a0:de:01:02:03]
機種名   : SWX2200-24G
機器名   : SWX2200-24G_0123456
経路     : lan1:1
```

```

アップリンク : 1
設定      : switch select lan1:1
---
LAN2
スイッチ制御機能が有効になっていません
---
LAN3
スイッチ制御機能が有効になっていません

```

```

> show status switch control
LAN1
[00:a0:de:01:02:03]
Model name : SWX2200-24G
System name: SWX2200-24G_0123456
Route      : lan1:1
Uplink     : 1
Config     : switch select lan1:1
---
LAN2
Switch control function is not available.
---
LAN3
Switch control function is not available.

[Models]
RTX810

```

## 45.57 Show the Operation Status of Ethernet Cable Redundancy

### [Syntax]

**show status switch control route backup *route***

### [Setting and Initial value]

- *route*
  - [Setting] : Route
  - [Initial value] : -

### [Description]

Shows the operation status of ethernet cable redundancy

Status	Description
none	Ethernet cable redundancy is disabled.
active	Ethernet cable redundancy is enabled.
force-linkdown	The port is linked down by ethernet cable redundancy
blocking	The communication is blocked by ethernet cable redundancy

### [Note]

When the port on master route is linked up, the port is enabled as main route. The port on backup route works as force-linkdown status and it does not link up if the cable is connected.

When the port on master route is linked down, the port on backup route is enabled as main route. The port on master route works as blocking status and the communication is blocked even if the port is linked up.

RTX810 supports this command in Rev.11.01.23 or later.

### [Models]

RTX810

## 45.58 Display the DNS Cache

### [Syntax]

**show dns cache**

### [Description]

Displays the DNS cache content.

### [Models]

RTX810, RTX5000



## 45.59 Show the Status of CPU Packet Scheduling

### [Syntax]

**show status packet-scheduling**

### [Description]

Shows the current status of CPU packet scheduling function.

- CPU packet scheduling mode
  - Mode

Value	Description
hash	Hash mode
load-balance	load-balance mode
lan-based	LAN interface mode

- CPU usage
  - CPU usage of each CPU core
- Flow(IPv4/IPv6)
  - Total number of IPv4/IPv6 flow
  - Number of IPv4/IPv6 flow on each CPU core
- Received packet
  - Number of received packet on each CPU core

When the *mode* is 'load-balance', the number of IPv4/IPv6 flow on each CPU core is not displayed.

The number of received packet is cleared by **system packet-scheduling** command.

### [Example]

```
# show status packet-scheduling
Mode:                hash
CPU usage:
  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 entries / 1 entries
  CPU1:      1 entries / 0 entries
  CPU2:      1 entries / 0 entries
  CPU3:      0 entries / 1 entries
Received packet:
  CPU0:      23155524 packets
  CPU1:      14018842 packets
  CPU2:      23624407 packets
  CPU3:      22886347 packets
```

### [Models]

RTX5000

## Chapter 46

### Logging

#### 46.1 Show the Log

##### [Syntax]

```
show log [saved] [reverse]
show log external-memory [backup fileid]
less log [saved] [reverse]
```

##### [Setting and Initial value]

- saved
  - [Setting] : Show the Log Directly Before Reboot
  - [Initial value] : -
- reverse
  - [Setting] : Show the log in reverse order
  - [Initial value] : -
- external-memory
  - [Setting] : Show the SYSLOG file content specified with the **external-memory syslog filename** command
  - [Initial value] : -
- backup
  - [Setting] : Show the SYSLOG backup file content, or a list of the SYSLOG backup file
  - [Initial value] : -
- *fileid* : Show the specified SYSLOG backup file content
  - [Setting] : `yyyymmdd_hhmmss`
  - [Initial value] : -

##### [Description]

Show the log of the router operating status.

Maximum number of line for logging is following:

Model	Number of line
RTX5000	20000
RTX810	3000

To save the log exceeding the maximum number, you must use the **syslog host** command to transfer the log to a SYSLOG server and store the information there.

When an unintended reboot occurs, specify 'saved' and the router can show the log directly before the reboot.

This command normally shows the log from the oldest event. However, the log can be shown from the newest event by specifying reverse.

For models that do not support the power off log retention feature, the log is erased when the router power is turned off.

When external-memory is specified, the SYSLOG file in the external memory is displayed.

If external-memory backup has been specified, a list of the backup files will be shown from oldest to newest. To show the content of the backup file, it can be displayed by specifying the displayed file name's date/time data (15 digits in `yyyymmdd_hhmmss` format) in *fileid*.

##### [Note]

Even when the router is restarted without power-off due to the **restart** command execution or firmware version up via TFTP, the log is saved unless you turn off power.

For models other than the RTX5000, the log configured for display in the saved parameter will be deleted.

The following limitations apply when you specify external-memory:

- Encrypted log files in the external memory cannot be displayed.
- The redirect function cannot be specified.

When the **external-memory syslog filename** command is not specified even if external-memory is specified, an execution error occurs.

**[Models]**

RTX810, RTX5000

## 46.2 Show the Account

---

**[Syntax]**

**show account**

**show account** *interface*

**[Setting and Initial value]**

- *interface*
  - [Setting] :
    - BRI interface name
    - PRI interface name
  - [Initial value] : -

**[Description]**

The following items are shown:

- Number of originated calls
- Number of received calls
- Total fee

**[Note]**

All charging amount information is cleared when the router is turned OFF or restarted.

**[Models]**

RTX5000

## 46.3 Show the PP Account

---

**[Syntax]**

**show account pp** [*peer\_num*]

**[Setting and Initial value]**

- *peer\_num*
  - [Setting] :
    - Peer number
    - anonymous
    - If omitted, the configuration of the selected peer is shown.
  - [Initial value] : -

**[Description]**

Shows the account about the specified PP interface.

**[Models]**

RTX5000

## 46.4 Display the Tunnel Account

---

**[Syntax]**

**show account tunnel** [*tunnel\_num*]

**[Setting and Initial value]**

- *tunnel\_num*
  - [Setting] :
    - Peer number
    - If omitted, shows the settings of the selected peer.
  - [Initial value] : -

**[Description]**

Displays the number of originated/received calls and charges for the tunnel interface for which the specified data connection is set. The number of originated and received calls are counted at the time of disconnecting. The charges are cleared by rebooting.

The charges for data connection are not included in the calculation to determine whether the threshold value set by the **account threshold** command has been exceeded.

**[Models]**

RTX5000

## 46.5 Show the Communication History

---

**[Syntax]**

**show history**

**[Description]**

Shows the communication history.

**[Models]**

RTX810

# Index

## Symbols

> 38  
>> 38

## A

administrator 458  
 administrator password 41  
 administrator password encrypted 41  
 administrator radius auth 43  
 alarm batch 77  
 alarm entire 76  
 alarm http revision-up 78  
 alarm lua 417  
 alarm mobile 400  
 alarm sd 77  
 alarm startup 78  
 alarm usbhost 77  
 auth user 198  
 auth user attribute 199  
 auth user group 200  
 auth user group attribute 200

## B

bgp aggregate 300  
 bgp aggregate filter 300  
 bgp autonomous-system 301  
 bgp configure refresh 305  
 bgp export 302  
 bgp export aspath 302  
 bgp export filter 303  
 bgp import 304  
 bgp import filter 305  
 bgp log 307  
 bgp neighbor 306  
 bgp preference 302  
 bgp router id 301  
 bgp use 300  
 bridge learning 413  
 bridge learning bridge\_interface static 414  
 bridge learning bridge\_interface timer 413  
 bridge member 412

## C

clear account 462  
 clear account pp 462  
 clear arp 463  
 clear boot list 465  
 clear bridge learning 463  
 clear dns cache 463  
 clear external-memory syslog 465  
 clear heartbeat2 378  
 clear heartbeat2 id 378  
 clear heartbeat2 name 378  
 clear inarp 463  
 clear ip dynamic routing 463  
 clear ip traffic list 127  
 clear ip traffic list pp 127  
 clear ip traffic list tunnel 127

clear ipv6 dynamic routing 465  
 clear ipv6 neighbor cache 465  
 clear log 463  
 clear mobile access limitation 394  
 clear mobile access limitation pp 394  
 clear nat descriptor dynamic 464  
 clear nat descriptor interface dynamic 464  
 clear nat descriptor interface dynamic pp 464  
 clear nat descriptor interface dynamic tunnel 464  
 clear status 464  
 clear switching-hub macaddress 474  
 clear url filter 476  
 clear url filter pp 476  
 clear url filter tunnel 476  
 cold start 462  
 connect 469  
 connect pp 469  
 connect tunnel 469  
 console character 49  
 console columns 50  
 console info 50  
 console lines 50  
 console prompt 49  
 cooperation 280  
 cooperation bandwidth-measuring remote 280  
 cooperation load-watch control 285  
 cooperation load-watch remote 282  
 cooperation load-watch trigger 283  
 cooperation port 280  
 cooperation type go 285  
 copy 466  
 copy config 459  
 copy exec 460

## D

date 47  
 delete 466  
 delete config 461  
 delete exec 461  
 description 64  
 dhcp client client-identifier 164  
 dhcp client client-identifier pool 164  
 dhcp client client-identifier pp 164  
 dhcp client hostname 162  
 dhcp client hostname pool 162  
 dhcp client hostname pp 162  
 dhcp client option 165  
 dhcp client option pool 165  
 dhcp client option pp 165  
 dhcp client release linkdown 166  
 dhcp convert lease to bind 159  
 dhcp duplicate check 155  
 dhcp manual lease 160  
 dhcp manual release 161  
 dhcp relay select 161  
 dhcp relay server 161  
 dhcp relay threshold 162  
 dhcp scope 155  
 dhcp scope bind 156  
 dhcp scope lease type 158  
 dhcp scope option 159

[dhcp server rfc2131 compliant 154](#)  
[dhcp service 153](#)  
[disconnect 470](#)  
[disconnect ip connection 473](#)  
[disconnect ipv6 connection 474](#)  
[disconnect pp 470](#)  
[disconnect tunnel 470](#)  
[disconnect user 45](#)  
[dns cache max entry 270](#)  
[dns cache use 269](#)  
[dns domain 263](#)  
[dns host 269](#)  
[dns notice order 264](#)  
[dns private address spoof 265](#)  
[dns server 263](#)  
[dns server dhcp 163](#)  
[dns server pp 264](#)  
[dns server select 266](#)  
[dns service 263](#)  
[dns service fallback 270](#)  
[dns srcport 268](#)  
[dns static 267](#)  
[dns syslog resolv 265](#)

## E

[ethernet filter 130](#)  
[ethernet interface filter 131](#)  
[execute at-command 393](#)  
[execute batch 389](#)  
[exit 458](#)  
[external-memory accelerator cache size 383](#)  
[external-memory auto-search time 388](#)  
[external-memory batch filename 389](#)  
[external-memory boot permit 386](#)  
[external-memory boot timeout 386](#)  
[external-memory cache mode 382](#)  
[external-memory config filename 387](#)  
[external-memory exec filename 386](#)  
[external-memory performance-test go 390](#)  
[external-memory syslog filename 384](#)

## G

[grep 36](#)

## H

[heartbeat pre-shared-key 372](#)  
[heartbeat receive 372](#)  
[heartbeat send 373](#)  
[heartbeat2 myname 374](#)  
[heartbeat2 receive 376](#)  
[heartbeat2 receive enable 376](#)  
[heartbeat2 receive log 377](#)  
[heartbeat2 receive monitor 377](#)  
[heartbeat2 receive record limit 378](#)  
[heartbeat2 transmit 374](#)  
[heartbeat2 transmit enable 375](#)  
[heartbeat2 transmit interval 375](#)  
[heartbeat2 transmit log 376](#)  
[help 40](#)  
[http revision-down permit 68](#)  
[http revision-up go 475](#)  
[http revision-up permit 67](#)  
[http revision-up proxy 67](#)

[http revision-up schedule 69](#)  
[http revision-up timeout 68](#)  
[http revision-up url 67](#)  
[httpd custom-gui api password 420](#)  
[httpd custom-gui api use 420](#)  
[httpd custom-gui use 419](#)  
[httpd custom-gui user 419](#)  
[httpd host 348](#)  
[httpd language 349](#)  
[httpd listen 349](#)  
[httpd service 348](#)  
[httpd timeout 349](#)

## I

[interface reset 468](#)  
[interface reset pp 469](#)  
[ip arp timer 102](#)  
[ip filter 89](#)  
[ip filter directed-broadcast 92](#)  
[ip filter dynamic 93](#)  
[ip filter dynamic timer 94](#)  
[ip filter set 92](#)  
[ip filter source-route 92](#)  
[ip flow limit 105](#)  
[ip flow timer 104](#)  
[ip forward filter 128](#)  
[ip fragment remove df-bit 100](#)  
[ip host 267](#)  
[ip icmp echo-reply send 167](#)  
[ip icmp echo-reply send-only-linkup 167](#)  
[ip icmp error-decrypted-ipsec send 170](#)  
[ip icmp log 170](#)  
[ip icmp mask-reply send 167](#)  
[ip icmp parameter-problem send 168](#)  
[ip icmp redirect receive 168](#)  
[ip icmp redirect send 168](#)  
[ip icmp time-exceeded send 169](#)  
[ip icmp timestamp-reply send 169](#)  
[ip icmp unreachable send 169](#)  
[ip icmp unreachable-for-truncated send 172](#)  
[ip implicit-route preference 104](#)  
[ip interface address 84](#)  
[ip interface arp log 103](#)  
[ip interface arp mtu discovery 171](#)  
[ip interface arp queue length 103](#)  
[ip interface arp static 102](#)  
[ip interface dhcp lease time 163](#)  
[ip interface dhcp retry 164](#)  
[ip interface forward filter 129](#)  
[ip interface intrusion detection 95](#)  
[ip interface intrusion detection notice-interval 96](#)  
[ip interface intrusion detection repeat-control 96](#)  
[ip interface intrusion detection report 97](#)  
[ip interface intrusion detection threshold 97](#)  
[ip interface mtu 86](#)  
[ip interface nat descriptor 254](#)  
[ip interface ospf area 295](#)  
[ip interface ospf neighbor 298](#)  
[ip interface proxyarp 101](#)  
[ip interface proxyarp vrrp 101](#)  
[ip interface rebound 86](#)  
[ip interface rip auth key 114](#)  
[ip interface rip auth key text 114](#)  
[ip interface rip auth type 113](#)  
[ip interface rip filter 112](#)

ip interface rip force-to-advertise 117  
 ip interface rip hop 113  
 ip interface rip receive 112  
 ip interface rip send 111  
 ip interface rip trust gateway 110  
 ip interface secondary address 85  
 ip interface secure filter 99  
 ip interface secure filter name 99  
 ip interface tcp mss limit 98  
 ip interface traffic list 126  
 ip interface traffic list threshold 127  
 ip interface vrrp 119  
 ip interface vrrp shutdown trigger 120  
 ip interface wol relay 63  
 ip keepalive 124  
 ip local forward filter 129  
 ip pp address 84  
 ip pp forward filter 129  
 ip pp intrusion detection 95  
 ip pp intrusion detection notice-interval 96  
 ip pp intrusion detection repeat-control 96  
 ip pp intrusion detection report 97  
 ip pp intrusion detection threshold 97  
 ip pp mtu 86  
 ip pp nat descriptor 254  
 ip pp ospf area 295  
 ip pp ospf neighbor 298  
 ip pp rebound 86  
 ip pp remote address 105  
 ip pp remote address pool 106  
 ip pp rip auth key 114  
 ip pp rip auth key text 114  
 ip pp rip auth type 113  
 ip pp rip backup interface 116  
 ip pp rip connect interval 115  
 ip pp rip connect send 115  
 ip pp rip disconnect interval 116  
 ip pp rip disconnect send 115  
 ip pp rip filter 112  
 ip pp rip force-to-advertise 117  
 ip pp rip hold routing 114  
 ip pp rip hop 113  
 ip pp rip receive 112  
 ip pp rip send 111  
 ip pp rip trust gateway 110  
 ip pp secure filter 99  
 ip pp secure filter name 99  
 ip pp tcp mss limit 98  
 ip pp traffic list 126  
 ip pp traffic list threshold 127  
 ip route 87  
 ip route change log 99  
 ip routing 84  
 ip routing process 55  
 ip simple-service 87  
 ip stealth 171  
 ip tos supersede 101  
 ip tunnel address 179  
 ip tunnel forward filter 129  
 ip tunnel intrusion detection 95  
 ip tunnel intrusion detection notice-interval 96  
 ip tunnel intrusion detection repeat-control 96  
 ip tunnel intrusion detection report 97  
 ip tunnel intrusion detection threshold 97  
 ip tunnel mtu 86  
 ip tunnel nat descriptor 254  
 ip tunnel ospf area 295  
 ip tunnel ospf neighbor 298  
 ip tunnel rebound 86  
 ip tunnel remote address 179  
 ip tunnel rip auth key 114  
 ip tunnel rip auth key text 114  
 ip tunnel rip auth type 113  
 ip tunnel rip filter 112  
 ip tunnel rip force-to-advertise 117  
 ip tunnel rip hop 113  
 ip tunnel rip receive 112  
 ip tunnel rip send 111  
 ip tunnel rip trust gateway 110  
 ip tunnel secure filter 99  
 ip tunnel secure filter name 99  
 ip tunnel tcp mss limit 98  
 ip tunnel traffic list 126  
 ip tunnel traffic list threshold 127  
 ipsec auto refresh 185  
 ipsec ike always-on 187  
 ipsec ike auth method 182  
 ipsec ike backward-compatibility 196  
 ipsec ike duration 207  
 ipsec ike eap myname 184  
 ipsec ike eap request 184  
 ipsec ike eap send certreq 185  
 ipsec ike encryption 193  
 ipsec ike esp-encapsulation 205  
 ipsec ike group 194  
 ipsec ike hash 195  
 ipsec ike keepalive log 192  
 ipsec ike keepalive use 191  
 ipsec ike license-key 203  
 ipsec ike license-key use 204  
 ipsec ike local address 190  
 ipsec ike local id 191  
 ipsec ike local name 189  
 ipsec ike log 205  
 ipsec ike message-id-control 206  
 ipsec ike mode-cfg address 203  
 ipsec ike mode-cfg address pool 202  
 ipsec ike mode-cfg method 202  
 ipsec ike nat-traversal 210  
 ipsec ike negotiate-strictly 186  
 ipsec ike payload type 196  
 ipsec ike pfs 197  
 ipsec ike pki file 183  
 ipsec ike pre-shared-key 183  
 ipsec ike proposal-limitation 205  
 ipsec ike queue length 194  
 ipsec ike remote address 188  
 ipsec ike remote id 189  
 ipsec ike remote name 188  
 ipsec ike restrict-dangling-sa 210  
 ipsec ike retry 187  
 ipsec ike send info 197  
 ipsec ike version 182  
 ipsec ike xauth myname 198  
 ipsec ike xauth request 201  
 ipsec ipcomp type 213  
 ipsec log illegal-spi 195  
 ipsec refresh sa 209  
 ipsec sa delete 211  
 ipsec sa policy 208  
 ipsec transport 216  
 ipsec transport template 216

ipsec tunnel 213  
 ipsec tunnel fastpath-fragment-function follow df-bit 212  
 ipsec tunnel outer df-bit 212  
 ipsec use 181  
 ipv6 filter 325  
 ipv6 filter dynamic 327  
 ipv6 icmp echo-reply send 172  
 ipv6 icmp echo-reply send-only-linkup 172  
 ipv6 icmp error-decrypted-ipsec send 175  
 ipv6 icmp log 175  
 ipv6 icmp packet-too-big send 175  
 ipv6 icmp packet-too-big-for-truncated send 176  
 ipv6 icmp parameter-problem send 173  
 ipv6 icmp redirect receive 173  
 ipv6 icmp redirect send 173  
 ipv6 icmp time-exceeded send 174  
 ipv6 icmp unreachable send 174  
 ipv6 interface address 310  
 ipv6 interface dad retry count 314  
 ipv6 interface dhcp service 313  
 ipv6 interface mld 329  
 ipv6 interface mld static 329  
 ipv6 interface mtu 308  
 ipv6 interface ospf area 334  
 ipv6 interface prefix 311  
 ipv6 interface prefix change log 312  
 ipv6 interface rip filter 321  
 ipv6 interface rip hop 320  
 ipv6 interface rip receive 319  
 ipv6 interface rip send 319  
 ipv6 interface rip trust gateway 320  
 ipv6 interface rtadv send 316  
 ipv6 interface secure filter 326  
 ipv6 interface tcp mss limit 308  
 ipv6 interface vrrp 323  
 ipv6 interface vrrp shutdown trigger 324  
 ipv6 max auto address 314  
 ipv6 nd ns-trigger-dad 330  
 ipv6 ospf area 333  
 ipv6 ospf area network 333  
 ipv6 ospf configure refresh 332  
 ipv6 ospf export 337  
 ipv6 ospf export from ospf 337  
 ipv6 ospf import 339  
 ipv6 ospf import from 339  
 ipv6 ospf log 341  
 ipv6 ospf preference 337  
 ipv6 ospf router id 332  
 ipv6 ospf use 332  
 ipv6 ospf virtual-link 336  
 ipv6 pp address 310  
 ipv6 pp dad retry count 314  
 ipv6 pp dhcp service 313  
 ipv6 pp mld 329  
 ipv6 pp mld static 329  
 ipv6 pp mtu 308  
 ipv6 pp ospf area 334  
 ipv6 pp prefix 311  
 ipv6 pp prefix change log 312  
 ipv6 pp rip connect interval 322  
 ipv6 pp rip connect send 321  
 ipv6 pp rip disconnect interval 322  
 ipv6 pp rip disconnect send 322  
 ipv6 pp rip filter 321  
 ipv6 pp rip hold routing 323  
 ipv6 pp rip hop 320

ipv6 pp rip receive 319  
 ipv6 pp rip send 319  
 ipv6 pp rip trust gateway 320  
 ipv6 pp rtadv send 316  
 ipv6 pp secure filter 326  
 ipv6 pp tcp mss limit 308  
 ipv6 prefix 315  
 ipv6 rh0 discard 309  
 ipv6 rip preference 323  
 ipv6 rip use 319  
 ipv6 route 318  
 ipv6 routing 308  
 ipv6 routing process 309  
 ipv6 source address selection rule 314  
 ipv6 stealth 176  
 ipv6 tunnel address 310  
 ipv6 tunnel dhcp service 313  
 ipv6 tunnel mld 329  
 ipv6 tunnel mld static 329  
 ipv6 tunnel ospf area 334  
 ipv6 tunnel prefix 311  
 ipv6 tunnel prefix change log 312  
 ipv6 tunnel rip filter 321  
 ipv6 tunnel rip receive 319  
 ipv6 tunnel rip send 319  
 ipv6 tunnel secure filter 326  
 ipv6 tunnel tcp mss limit 308

## L

l2tp always-on 222  
 l2tp hostname 222  
 l2tp keepalive log 221  
 l2tp keepalive use 220  
 l2tp local router-id 222  
 l2tp remote end-id 223  
 l2tp remote router-id 223  
 l2tp service 219  
 l2tp syslog 221  
 l2tp tunnel auth 220  
 l2tp tunnel disconnect time 220  
 lan backup 122  
 lan backup recovery time 122  
 lan count-hub-overflow 56  
 lan keepalive interval 123  
 lan keepalive log 124  
 lan keepalive use 123  
 lan link-aggregation static 62  
 lan linkup send-wait-time 57  
 lan port-mirroring 57  
 lan shutdown 56  
 lan type 58  
 leased keepalive down 109  
 less 37  
 less config 478  
 less config ap 478  
 less config list 480  
 less config pp 479  
 less config switch 479  
 less config tunnel 479  
 less exec list 482  
 less file list 480  
 less log 506  
 login password 41  
 login password encrypted 41  
 login radius use 42



login timer [63](#)  
 login user [42](#)  
 lua [415](#)  
 lua use [415](#)  
 luac [416](#)

## M

mail notify [345](#)  
 mail notify status exec [476](#)  
 mail server name [342](#)  
 mail server pop [343](#)  
 mail server smtp [342](#)  
 mail server timeout [343](#)  
 mail template [344](#)  
 make directory [466](#)  
 mobile access limit connection length [400](#)  
 mobile access limit connection time [401](#)  
 mobile access limit duration [401](#)  
 mobile access limit length [397](#)  
 mobile access limit time [397](#)  
 mobile access-point name [396](#)  
 mobile auto connect [394](#)  
 mobile call prohibit auth-error count [398](#)  
 mobile dial number [396](#)  
 mobile disconnect input time [395](#)  
 mobile disconnect output time [395](#)  
 mobile disconnect time [395](#)  
 mobile display caller id [399](#)  
 mobile pin code [393](#)  
 mobile signal-strength [402](#)  
 mobile signal-strength go [402](#)  
 mobile syslog [399](#)  
 mobile use [392](#)

## N

nat descriptor address inner [256](#)  
 nat descriptor address outer [255](#)  
 nat descriptor ftp port [260](#)  
 nat descriptor log [261](#)  
 nat descriptor masquerade incoming [259](#)  
 nat descriptor masquerade port range [259](#)  
 nat descriptor masquerade remove df-bit [261](#)  
 nat descriptor masquerade rlogin [257](#)  
 nat descriptor masquerade session limit [262](#)  
 nat descriptor masquerade static [257](#)  
 nat descriptor masquerade unconvertible port [260](#)  
 nat descriptor sip [261](#)  
 nat descriptor static [256](#)  
 nat descriptor timer [258](#)  
 nat descriptor type [254](#)  
 netvolante-dns auto hostname [359](#)  
 netvolante-dns auto hostname pp [359](#)  
 netvolante-dns auto save [362](#)  
 netvolante-dns delete go [357](#)  
 netvolante-dns delete go pp [357](#)  
 netvolante-dns get hostname list [357](#)  
 netvolante-dns get hostname list pp [357](#)  
 netvolante-dns go [356](#)  
 netvolante-dns go pp [356](#)  
 netvolante-dns hostname host [358](#)  
 netvolante-dns hostname host pp [358](#)  
 netvolante-dns port [357](#)  
 netvolante-dns register timer [361](#)  
 netvolante-dns retry interval [361](#)

netvolante-dns retry interval pp [361](#)  
 netvolante-dns server [359](#)  
 netvolante-dns server update address port [360](#)  
 netvolante-dns server update address use [360](#)  
 netvolante-dns set hostname [359](#)  
 netvolante-dns timeout [358](#)  
 netvolante-dns timeout pp [358](#)  
 netvolante-dns use [356](#)  
 netvolante-dns use pp [356](#)  
 nslookup [472](#)  
 ntp backward-compatibility [49](#)  
 ntp local address [48](#)  
 ntpdate [48](#)

## O

operation button function download [390](#)  
 operation execute batch permit [391](#)  
 operation external-memory download permit [385](#)  
 operation http revision-up permit [68](#)  
 ospf area [292](#)  
 ospf area network [292](#)  
 ospf area stubhost [293](#)  
 ospf configure refresh [287](#)  
 ospf export filter [289](#)  
 ospf export from ospf [288](#)  
 ospf import filter [290](#)  
 ospf import from [288](#)  
 ospf log [298](#)  
 ospf merge equal cost stub [298](#)  
 ospf preference [287](#)  
 ospf router id [288](#)  
 ospf use [287](#)  
 ospf virtual-link [293](#)

## P

ping [470](#)  
 ping6 [471](#)  
 pki certificate file [217](#)  
 pki crl file [218](#)  
 pp always-on [109](#)  
 pp auth accept [137](#), [226](#)  
 pp auth multi connect prohibit [139](#)  
 pp auth myname [138](#)  
 pp auth request [138](#), [226](#)  
 pp auth username [137](#)  
 pp backup [121](#)  
 pp backup pp [121](#)  
 pp backup recovery time [121](#)  
 pp backup tunnel [121](#)  
 pp bind [224](#), [394](#)  
 pp disable [468](#)  
 pp enable [467](#)  
 pp keepalive interval [107](#)  
 pp keepalive log [108](#)  
 pp keepalive use [107](#)  
 pp name [350](#)  
 pp select [457](#)  
 ppp ccp maxconfigure [148](#)  
 ppp ccp maxfailure [148](#)  
 ppp ccp maxterminate [147](#)  
 ppp ccp no-encryption [229](#)  
 ppp ccp restart [147](#)  
 ppp ccp type [146](#)  
 ppp chap maxchallenge [143](#)

ppp chap restart [143](#)  
 ppp ipcp ipaddress [143](#)  
 ppp ipcp maxconfigure [144](#)  
 ppp ipcp maxfailure [145](#)  
 ppp ipcp maxterminate [144](#)  
 ppp ipcp msex [145](#)  
 ppp ipcp remote address check [145](#)  
 ppp ipcp restart [144](#)  
 ppp ipcp vjc [143](#)  
 ppp ipv6cp use [148](#)  
 ppp lcp accm [399](#)  
 ppp lcp acfc [139](#)  
 ppp lcp magicnumber [139](#)  
 ppp lcp maxconfigure [141](#)  
 ppp lcp maxfailure [141](#)  
 ppp lcp maxterminate [141](#)  
 ppp lcp mru [140](#)  
 ppp lcp pfc [140](#)  
 ppp lcp restart [141](#)  
 ppp lcp silent [142](#)  
 ppp msccp maxretry [146](#)  
 ppp msccp restart [146](#)  
 ppp pap maxauthreq [142](#)  
 ppp pap restart [142](#)  
 pppoe access concentrator [149](#)  
 pppoe auto connect [149](#)  
 pppoe auto disconnect [149](#)  
 pppoe disconnect time [151](#)  
 pppoe invalid-session forced close [152](#)  
 pppoe padi maxretry [150](#)  
 pppoe padi restart [150](#)  
 pppoe padr maxretry [150](#)  
 pppoe padr restart [150](#)  
 pppoe service-name [151](#)  
 pppoe tcp mss limit [151](#)  
 pppoe use [148](#)  
 pptp hostname [225](#)  
 pptp keepalive interval [228](#)  
 pptp keepalive log [228](#)  
 pptp keepalive use [228](#)  
 pptp service [224](#)  
 pptp service type [225](#)  
 pptp syslog [226](#)  
 pptp tunnel disconnect time [227](#)  
 pptp window size [225](#)  
 provider auto connect forced disable [354](#)  
 provider dns server [351](#)  
 provider dns server pp [352](#)  
 provider filter routing [352](#)  
 provider interface bind [355](#)  
 provider interface dns server [352](#)  
 provider interface name [353](#)  
 provider ipv6 connect pp [355](#)  
 provider ntp server [354](#)  
 provider ntpdate [353](#)  
 provider select [351](#)  
 provider set [351](#)  
 provider type [350](#)

## Q

queue class filter [271](#)  
 queue interface class control [277](#)  
 queue interface class filter list [274](#)  
 queue interface class property [277](#)  
 queue interface default class [276](#)

queue interface default class secondary [276](#)  
 queue interface length [275](#)  
 queue interface length secondary [275](#)  
 queue interface type [274](#)  
 queue pp class filter list [274](#)  
 queue pp class property [277](#)  
 queue pp default class [276](#)  
 queue pp length [275](#)  
 queue pp type [274](#)  
 queue tunnel class filter list [274](#)  
 quit [458](#)

## R

radius account [250](#)  
 radius account port [252](#)  
 radius account server [251](#)  
 radius auth [250](#)  
 radius auth port [252](#)  
 radius auth server [251](#)  
 radius retry [252](#)  
 radius secret [252](#)  
 radius server [250](#)  
 rdate [47](#)  
 rename [467](#)  
 restart [468](#)  
 rip filter rule [117](#)  
 rip preference [110](#)  
 rip timer [118](#)  
 rip use [109](#)  
 rotate external-memory syslog [476](#)  
 rtf format [83](#)  
 rtf garbage-collect [83](#)

## S

save [458](#)  
 schedule at [367](#)  
 scp [74](#)  
 sd use [382](#)  
 security class [46](#)  
 set [79](#)  
 set-default-config [461](#)  
 set-default-exec [462](#)  
 sftpd host [72](#)  
 show account [507](#)  
 show account pp [507](#)  
 show account tunnel [507](#)  
 show arp [483](#)  
 show bridge learning [485](#)  
 show command [40](#)  
 show config [478](#)  
 show config ap [478](#)  
 show config list [480](#)  
 show config pp [479](#)  
 show config switch [479](#)  
 show config tunnel [479](#)  
 show dns cache [504](#)  
 show environment [478](#)  
 show exec list [482](#)  
 show file list [480](#)  
 show history [508](#)  
 show ip connection [491](#)  
 show ip connection pp [491](#)  
 show ip connection tunnel [491](#)  
 show ip intrusion detection [493](#)

show ip intrusion detection pp 493  
 show ip intrusion detection tunnel 493  
 show ip rip table 485  
 show ip route 484  
 show ip secure filter 481  
 show ip secure filter pp 481  
 show ip secure filter tunnel 481  
 show ip traffic list 127  
 show ip traffic list pp 127  
 show ip traffic list tunnel 127  
 show ipsec sa 486  
 show ipsec sa gateway 486  
 show ipv6 address 480  
 show ipv6 address pp 480  
 show ipv6 address tunnel 480  
 show ipv6 connection 492  
 show ipv6 connection pp 492  
 show ipv6 connection tunnel 492  
 show ipv6 mroute fib 497  
 show ipv6 neighbor cache 485  
 show ipv6 ospf 500  
 show ipv6 rip table 485  
 show ipv6 route 485  
 show line masterclock 481  
 show log 506  
 show nat descriptor address 487  
 show nat descriptor interface address 488  
 show nat descriptor interface address pp 488  
 show nat descriptor interface address tunnel 488  
 show nat descriptor interface bind 488  
 show nat descriptor interface bind pp 488  
 show nat descriptor interface bind tunnel 488  
 show nat descriptor masquerade port summary 489  
 show pki certificate summary 486  
 show pki crl 487  
 show pp connect time 494  
 show sshd public key 481  
 show status 483  
 show status backup 491  
 show status bgp neighbor 490  
 show status boot 502  
 show status boot all 503  
 show status boot list 503  
 show status cooperation 499  
 show status dhcp 490  
 show status dhcpc 491  
 show status ethernet filter 132  
 show status external-memory 502  
 show status heartbeat 501  
 show status heartbeat2 378  
 show status heartbeat2 id 378  
 show status heartbeat2 name 378  
 show status httpd language 494  
 show status ip keeplive 493  
 show status ipv6 dhcp 491  
 show status ipv6 mld 496  
 show status l2tp 489  
 show status lua 416  
 show status mail service 496  
 show status mobile signal-strength 403  
 show status netvolante-dns 494  
 show status netvolante-dns pp 494  
 show status ospf 489  
 show status packet-buffer 498  
 show status packet-scheduling 505  
 show status pp 483  
 show status pptp 489  
 show status qos 498  
 show status remote setup 501  
 show status rfts 502  
 show status sd 502  
 show status switch control 503  
 show status switch control route backup 504  
 show status switching-hub macaddress 495  
 show status tunnel 495  
 show status upnp 495  
 show status usbhost 501  
 show status user 497  
 show status vlan 496  
 show status vrrp 487  
 show techinfo 501  
 show url filter 500  
 show url filter pp 500  
 show url filter tunnel 500  
 sip 100rel 231  
 sip arrive address check 233  
 sip arrive ringing p-n-uatype 232  
 sip arrive session timer method 232  
 sip arrive session timer refresher 232  
 sip ip protocol 231  
 sip log 234  
 sip outer address 234  
 sip response code busy 233  
 sip session timer 230  
 sip use 230  
 sip user agent 231  
 snmp community read-only 236  
 snmp community read-write 236  
 snmp display ipcp force 246  
 snmp host 235  
 snmp ifindex switch static index 247  
 snmp local address 242  
 snmp syscontact 242  
 snmp syslocation 243  
 snmp sysname 243  
 snmp trap community 236  
 snmp trap enable snmp 243  
 snmp trap enable switch 248  
 snmp trap enable switch common 248  
 snmp trap host 236  
 snmp trap link-updown separate-l2switch-port 246  
 snmp trap mobile signal-strength 247  
 snmp trap send linkdown 244  
 snmp trap send linkdown pp 244  
 snmp trap send linkdown tunnel 244  
 snmp yrifppdisplayatmib2 245  
 snmp yrifswitchdisplayatmib2 245  
 snmp yriftunneldisplayatmib2 245  
 snmp yrswindex switch static index 247  
 snmpv2c community read-only 237  
 snmpv2c community read-write 238  
 snmpv2c host 237  
 snmpv2c trap community 238  
 snmpv2c trap host 238  
 snmpv3 context name 239  
 snmpv3 engine id 239  
 snmpv3 host 240  
 snmpv3 trap host 242  
 snmpv3 usm user 239  
 snmpv3 vacm access 241  
 snmpv3 vacm view 240  
 sntpd host 380

- sntpd service 380
- speed 271
- speed pp 271
- ssh 73
- ssh encrypt algorithm 74
- ssh known hosts 75
- sshd client alive 72
- sshd encrypt algorithm 71
- sshd host 70
- sshd host key generate 71
- sshd listen 70
- sshd service 69
- sshd session 71
- switch control firmware upload go 424
- switch control function default 424
- switch control function execute 423
- switch control function execute clear-counter 452
- switch control function execute clear-macaddress-table 436
- switch control function execute reset-loopdetect 456
- switch control function execute restart 430
- switch control function get 423
- switch control function get boot-rom-version 426
- switch control function get counter-frame-rx-type 448
- switch control function get counter-frame-tx-type 449
- switch control function get energy-saving 428
- switch control function get firmware-revision 426
- switch control function get led-brightness 428
- switch control function get loopdetect-count 453
- switch control function get loopdetect-linkdown 453
- switch control function get loopdetect-port-use 454
- switch control function get loopdetect-recovery-timer 454
- switch control function get loopdetect-time 453
- switch control function get loopdetect-use-control-packet 455
- switch control function get macaddress-aging 435
- switch control function get macaddress-aging-timer 435
- switch control function get mirroring-dest 446
- switch control function get mirroring-src-rx 446
- switch control function get mirroring-src-tx 447
- switch control function get mirroring-use 445
- switch control function get model-name 427
- switch control function get port-auto-crossover 431
- switch control function get port-blocking-control-packet 433
- switch control function get port-blocking-data-packet 433
- switch control function get port-flow-control 432
- switch control function get port-speed 430
- switch control function get port-speed-downshift 432
- switch control function get port-use 431
- switch control function get qos-dscp-remark-class 441
- switch control function get qos-dscp-remark-type 441
- switch control function get qos-policing-speed 443
- switch control function get qos-policing-use 442
- switch control function get qos-shaping-speed 444
- switch control function get qos-shaping-use 443
- switch control function get qos-speed-unit 442
- switch control function get serial-number 427
- switch control function get status-counter-frame-rx 451
- switch control function get status-counter-frame-tx 451
- switch control function get status-counter-octet-rx 452
- switch control function get status-counter-octet-tx 452
- switch control function get status-fan 429
- switch control function get status-led-mode 429
- switch control function get status-loopdetect-port 455
- switch control function get status-loopdetect-recovery-timer 456
- switch control function get status-macaddress-addr 435
- switch control function get status-macaddress-port 436
- switch control function get status-port-speed 434
- switch control function get system-macaddress 427
- switch control function get system-name 427
- switch control function get system-uptime 430
- switch control function get vlan-access 438
- switch control function get vlan-id 438
- switch control function get vlan-multiple 440
- switch control function get vlan-multiple-use 440
- switch control function get vlan-port-mode 438
- switch control function get vlan-trunk 439
- switch control function set 423
- switch control function set counter-frame-rx-type 448
- switch control function set counter-frame-tx-type 449
- switch control function set energy-saving 428
- switch control function set led-brightness 428
- switch control function set loopdetect-count 453
- switch control function set loopdetect-linkdown 453
- switch control function set loopdetect-port-use 454
- switch control function set loopdetect-recovery-timer 454
- switch control function set loopdetect-time 453
- switch control function set loopdetect-use-control-packet 455
- switch control function set macaddress-aging 435
- switch control function set macaddress-aging-timer 435
- switch control function set mirroring-dest 446
- switch control function set mirroring-src-rx 446
- switch control function set mirroring-src-tx 447
- switch control function set mirroring-use 445
- switch control function set port-auto-crossover 431
- switch control function set port-blocking-control-packet 433
- switch control function set port-blocking-data-packet 433
- switch control function set port-flow-control 432
- switch control function set port-speed 430
- switch control function set port-speed-downshift 432
- switch control function set port-use 431
- switch control function set qos-dscp-remark-class 441
- switch control function set qos-dscp-remark-type 441
- switch control function set qos-policing-speed 443
- switch control function set qos-policing-use 442
- switch control function set qos-shaping-speed 444
- switch control function set qos-shaping-use 443
- switch control function set qos-speed-unit 442
- switch control function set system-name 427
- switch control function set vlan-access 438
- switch control function set vlan-id 438
- switch control function set vlan-multiple 440
- switch control function set vlan-multiple-use 440
- switch control function set vlan-port-mode 438
- switch control function set vlan-trunk 439
- switch control route backup 425
- switch control use 421
- switch control watch interval 422
- switch select 422
- syslog debug 52
- syslog execute command 53
- syslog facility 51
- syslog host 51
- syslog info 52
- syslog local address 53
- syslog notice 51
- syslog sreport 53
- system led brightness 78
- system packet-buffer 75
- system packet-scheduling 79
- system packet-scheduling filter 80
- system packet-scheduling filter list 82
- system temperature threshold 55

**T**

[tcp log 65](#)  
[tcp session limit 98](#)  
[telnet 473](#)  
[telnetd host 54](#)  
[telnetd listen 54](#)  
[telnetd service 53](#)  
[telnetd session 55](#)  
[terminate lua 417](#)  
[terminate lua file 417](#)  
[tftp host 63](#)  
[time 47](#)  
[timezone 46](#)  
[traceroute 472](#)  
[traceroute6 472](#)  
[tunnel backup 213](#)  
[tunnel backup pp 213](#)  
[tunnel backup tunnel 213](#)  
[tunnel disable 178](#)  
[tunnel enable 178](#)  
[tunnel encapsulation 178](#)  
[tunnel endpoint address 180](#)  
[tunnel endpoint name 227](#)  
[tunnel name 350](#)  
[tunnel select 457](#)  
[tunnel template 214](#)

**U**

[upnp external address refer 363](#)  
[upnp external address refer pp 363](#)  
[upnp port mapping timer 364](#)  
[upnp port mapping timer type 363](#)  
[upnp syslog 364](#)  
[upnp use 363](#)  
[url filter 133](#)

[url filter log 135](#)  
[url filter port 134](#)  
[url filter reject 135](#)  
[url filter use 134](#)  
[url interface filter 133](#)  
[url pp filter 133](#)  
[url tunnel filter 133](#)  
[usbhost modem flow control 404](#)  
[usbhost modem initialize 403](#)  
[usbhost overcurrent duration 366](#)  
[usbhost use 366](#)  
[user attribute 43](#)

**V**

[vlan interface 802.1q 370](#)  
[vlan port mapping 370](#)

**W**

[wan access limit connection length 410](#)  
[wan access limit connection time 410](#)  
[wan access limit duration 411](#)  
[wan access limit length 408](#)  
[wan access limit time 409](#)  
[wan access-point name 407](#)  
[wan always-on 407](#)  
[wan auth myname 404](#)  
[wan auto connect 405](#)  
[wan bind 404](#)  
[wan disconnect input time 406](#)  
[wan disconnect output time 406](#)  
[wan disconnect time 405](#)  
[wins server 145](#)  
[wol send 474](#)

