

Command Reference

Rev.8.03.30, Rev.9.00.08, Rev.10.01.40

**Yamaha Corporation
August 2012, 1st edition**

Contents

Preface: Introduction	23
Chapter 1: How to Read the Command Reference	24
1.1 Applicable Firmware Revision	24
1.2 How to Read the Command Reference	24
1.3 Interface Names	24
1.4 Command Syntax Starting with the Word “no”	25
1.5 Number of Input Characters in a Command and Escape Sequence	25
1.6 Range of Peer Numbers by Model	25
1.7 About the Factory Default Settings	25
Chapter 2: How to Use the Commands	26
2.1 Console	26
2.1.1 Configuration Procedure Using the Console	26
2.1.2 Configuration Using TELNET	27
2.1.3 Remote Setup	28
2.2 SSH Server	29
2.2.1 Notes Regarding the Use of the SSH Server Function	29
2.2.2 Setting the SSH Server	29
2.3 TFTP	30
2.3.1 Configuration Procedure Using TFTP	30
2.3.2 Reading the Configuration File	31
2.3.3 Writing the Configuration File	31
2.4 Keyboard Operation When Using the Console	32
2.5 Commands That Start with the Word “show”	33
2.5.1 Extracting Only the Contents That Match the Search Pattern from the Display Contents of the Show Command	33
2.5.2 Making the Display Contents of the Show Command Easier to View	34
2.5.3 Redirection to External Memory	35
Chapter 3: Help	37
3.1 Showing a Brief Explanation of the Console	37
3.2 Showing a List of Commands	37
Chapter 4: Router Configuration	38
4.1 Set the Login Password	38
4.2 Encrypt and Save the Login Password	38
4.3 Set the Administrator Password	38
4.4 Encrypt and Save the Administrator Password	38
4.5 Set the Login User Name and Login Password	39
4.6 Set Whether to Use RADIUS for Password Authentication When Logging in	39
4.7 Set Whether to Use RADIUS for Password Authentication When Switching to Administrator	40
4.8 Set User Attributes	40
4.9 Disconnect Another User Connection by Force	42
4.10 Set the Security Class	43
4.11 Set the Time Zone	43
4.12 Set the Current Date	44
4.13 Set the Current Time	44
4.14 Set the Clock through a Remote Host	44
4.15 Set the Clock Using NTP	45
4.16 Set the Source IP Address for Sending NTP Packets	45

4.17 Set the Console Prompt Display	46
4.18 Set the Console Language and Code	46
4.19 Set the Number of Characters Shown on the Console	46
4.20 Set the Number of Lines Shown on the Console	47
4.21 Set Whether to Show System Messages on the Console	47
4.22 Set the IP Address of the Host Receiving the SYSLOG	48
4.23 Set the SYSLOG Facility	48
4.24 Set Whether to Output SYSLOGs of NOTICE Type	48
4.25 Set the Output of SYSLOG of INFO Type	49
4.26 Set Whether to Output SYSLOGs of DEBUG Type	49
4.27 Set the Source IP Address for Sending SYSLOG	49
4.28 Set the Source Port Number for SYSLOG Packets	50
4.29 Set Whether to Output Executed Commands to the SYSLOG	50
4.30 Turn the TELNET Server Function ON/OFF	50
4.31 Set the Listen Port of the TELNET Server Function	51
4.32 Set the IP Address of the Host Allowed to Access the TELNET Server	51
4.33 Set the Number of Users That Can Connect Simultaneously to the TELNET Server	51
4.34 Set the Monitored Temperature Threshold	52
4.35 Set the Fast Path Function	52
4.36 Set the LAN Interface Operation	53
4.37 Set How Long after Linkup through the LAN Interface to Wait before Sending	53
4.38 Set the Port Mirroring Function	53
4.39 Set the Operation Type of the LAN Interface	54
4.40 Set the Size of the Buffer for Packets Received through the LAN Interface	59
4.41 Set the Login Timer	59
4.42 Set the IP Address of the Host Allowed to Access the Router Using TFTP	60
4.43 Set Whether to Relay Magic Packets to the LAN	60
4.44 Set the Interface or System Description	61
4.45 Set Whether to Output the Syslog at the TCP Connection Level	61
4.46 Set Whether to Allow HTTP Revision Update	63
4.47 Set the URL for the HTTP Revision Update	64
4.48 Set the Proxy Server for HTTP Revision Update	64
4.49 Set the HTTP Revision Update Timeout	64
4.50 Set Whether to Allow Downgrade	65
4.51 Set Whether to Allow Updating Using the DOWNLOAD Button	65
4.52 Revision Update Schedule	65
4.53 Turn the SSH Server Function ON/OFF	66
4.54 Set the Listen Port of the SSH Server Function	67
4.55 Set the IP Address of the Host Allowed to Access the SSH Server	67
4.56 Set the Number of Users That Can Connect Simultaneously to the SSH Server	67
4.57 Set the SSH Server Host Key	68
4.58 Set the Encryption Algorithms That the SSH Server Can Use	68
4.59 Check Whether the SSH Client Is Alive	69
4.60 Set the IP Address of the Host Allowed to Access the SFTP Server	69
4.61 Change the Packet Buffer Parameters	70
4.62 Set Whether to Sound Active Alarms or to Not Sound Them at All	71
4.63 Set Whether to Sound Alarms for the USB Host Function	71
4.64 Set Whether to Sound Alarms for the microSD Function	72
4.65 Set Whether to Sound Alarms for the Batch File Execution Function	72
4.66 Set Whether to Sound an Alarm at Startup	72
4.67 Set Whether to Sound Alarms for the HTTP Revision Update Function	73
4.68 Adjust the LED Brightness	73

4.69 Set Environment Variables	74
Chapter 5: File System for Yamaha router: RTFS	75
5.1 Format the RTFS	75
5.2 Perform Garbage Collection on the RTFS	75
Chapter 6: ISDN Configuration	76
6.1 Common Configuration	76
6.1.1 Specify the BRI Line Type	76
6.1.2 Set the Local ISDN Number	76
6.1.3 Set the Terminator	77
6.1.4 Set the Interface Used for PP	77
6.1.5 Set Transmission Restriction According to Charging Amount	77
6.1.6 Set Whether to Permit Incoming PIAFS	78
6.1.7 Specify an Activation Side at PIAFS Connection	78
6.1.8 Set the PIAFS Transmission Method	79
6.2 Set the Peer Side	80
6.2.1 Set Permanent Connection	80
6.2.2 Set the Remote ISDN Number	80
6.2.3 Set the Auto Connection	81
6.2.4 Set the Order in Which Calls are Made to the Remote Device	81
6.2.5 Permit Incoming Calls	82
6.2.6 Permit Outgoing Calls	82
6.2.7 Set the Call Block Timer	83
6.2.8 Set the Call Prohibit Timer after an Erroneous Disconnection	83
6.2.9 Set Whether to Make a Callback Request to the Peer	83
6.2.10 Set Whether to Answer Callback Requests from the Destination	84
6.2.11 Set the Callback Request Type	84
6.2.12 Sets the Callback Permit Type	84
6.2.13 Set Whether to Permit Number Designation from the User in MS Callback	85
6.2.14 Set the Callback Timer	85
6.2.15 Set the Callback Wait Timer	85
6.2.16 Specify the Timer Type for Disconnecting the ISDN Line	86
6.2.17 Set the Disconnection Timer (Normal)	86
6.2.18 Set the Disconnection Timer (Fast)	86
6.2.19 Set the Disconnection Timer (Forced)	87
6.2.20 Set the Input Disconnection Timer (Normal)	87
6.2.21 Set the Output Disconnection Timer (Normal)	88
6.2.22 Set the Charging Unit Time and Monitor Time for the Charging Unit Time Type	88
Chapter 7: IP Configuration	90
7.1 Common Interface Settings	90
7.1.1 Set Whether to Process IP Packets	90
7.1.2 Set the IP Address	90
7.1.3 Set the Secondary IP Address	91
7.1.4 Set the Interface MTU	92
7.1.5 Set Whether to Send Returning Packets to the Same Interface	92
7.1.6 Set Whether to Run the Echo, Discard, and Time Services	93
7.1.7 Set the Statistic IP Routing Information	93
7.1.8 Set the IP Packet Filter	95
7.1.9 Define the Filter Set	98
7.1.10 Set Whether to Filter Out IP Packets with the Source-route Option	98
7.1.11 Set Whether to Filter Out Directed Broadcast Packets	98
7.1.12 Define a Dynamic Filter	99

7.1.13 Set the Dynamic Filter Timeout	100
7.1.14 Set the Operation of the Intrusion Detection Function	101
7.1.15 Set the Frequency of Intrusion Detection Notifications in a Second	102
7.1.16 Control the Repeated Intrusion Detection Notifications	102
7.1.17 Set the Number of Maximum Displayed Notifications of the Intrusion Detection	103
7.1.18 Set the Intrusion Detection Threshold Value	103
7.1.19 Set the MSS Limit of the TCP Session	104
7.1.20 Set the Number of TCP Sessions of Which the Router Is an Endpoint	105
7.1.21 Set Whether to Log Changes in the IPv4 Route Information	105
7.1.22 Set the Security by Filtering	105
7.1.23 Set Whether to Rewrite the DF Bit of the IP Packet That Matches the Rule with 0	107
7.1.24 Set the TOS Field Overwriting of the IP Packet	107
7.1.25 Set the Proxy ARP	108
7.1.26 Set the ARP Entry Lifetime	108
7.1.27 Set a Static ARP Entry	108
7.1.28 Limit the Number of Transmission Packets That Are Held until ARP Is Resolved	109
7.1.29 Set Whether to Log ARP Entry Changes	110
7.2 Setting the Remote PP Interface	110
7.2.1 Set the IP Address on the Remote PP Interface	110
7.2.2 Set the Remote IP Address Pool	111
7.2.3 Set the Time Interval of Keepalive via the PP	111
7.2.4 Set Whether to Use Keepalive via the PP	112
7.2.5 Set Whether to Log Keepalive via the PP	113
7.2.6 Set the Operation When Disconnection of the Exclusive Line is Detected	113
7.3 RIP Configuration	114
7.3.1 Set Whether to Use RIP	114
7.3.2 Set the RIP Trusted Gateway	114
7.3.3 Set the RIP Routing Preference	115
7.3.4 Set the RIP Packet Transmission	115
7.3.5 Set the RIP Packet Reception	116
7.3.6 Set the RIP Filtering	116
7.3.7 Set the Number of Hops to Be Added for RIP	117
7.3.8 Set the RIP2 Authentication	117
7.3.9 Set the RIP2 Authentication Key	118
7.3.10 Set the Route Hold When the Line Is Disconnected	118
7.3.11 Set the RIP Operation on the Remote PP Interface When the Line Is Connected	119
7.3.12 Set the RIP Transmission Interval on Remote PP Interface When the Line Is Connected	119
7.3.13 Set the RIP Operation on the Remote PP Interface When the Line Is Disconnected	119
7.3.14 Set the RIP Transmission Interval on the Remote PP Interface When the Line Is Disconnected	120
7.3.15 Set Whether to Switch the RIP Source Interface during Backup	120
7.3.16 Force RIP Route Advertisement	121
7.3.17 Method of Comparison for the RIP2 Filter	121
7.3.18 Adjust the RIP Timer	122
7.4 VRRP Configuration	123
7.4.1 Set the VRRP for Each Interface	123
7.4.2 Set the Shutdown Trigger	123
7.5 Backup Configuration	125
7.5.1 Set the Destination for PP Backup When the Provider Connection Goes Down	125
7.5.2 Set the Recovery Time from Backup	125
7.5.3 Set the Destination for Backup When the Provider Connection via the LAN Goes Down	126
7.5.4 Set the Recovery Time from Backup	126

7.5.5 Set Whether to Use Keepalive via the LAN	127
7.5.6 Set the Time Interval of Keepalive via the LAN	127
7.5.7 Set Whether to Log Keepalive via the LAN	128
7.5.8 Set the Network Monitor Function	128
7.6 IGMP Configuration	130
7.6.1 Set IGMP for Each Interface	130
7.6.2 Static IGMP Settings	131
7.7 PIM-SM Configuration	132
7.7.1 Set PIM-SM for Each Interface	132
7.7.2 Specify the Static Relationship between the Group and RP	133
7.7.3 Set the Detailed Log Output Related to PIM-SM	133
7.7.4 Set the Checksum Calculation Method of the Register	134
7.7.5 Set the Level of Preference of Implicit Routes	134
7.7.6 Set the Lifetime of Each Flow Table Entry	135
7.8 Set Packet Transfer Filters	135
7.8.1 Define a Packet Transfer Filter	135
7.8.2 Applying a Packet Transfer Filter to an Interface	136
Chapter 8: Ethernet Filter Configuration	138
8.1 Define a Filter	138
8.2 Set the Application to the Interface	139
8.3 Show the Ethernet Filter Status	140
Chapter 9: Input Cut-Off Filter Configuration	141
9.1 Set the Filter Definition	141
9.2 Setting the Filter Application	143
Chapter 10: Policy Filter Configuration	144
10.1 Define a Service	144
10.2 Define an Interface Group	144
10.3 Define an Address Group	145
10.4 Define a Service Group	146
10.5 Define a Policy Filter	146
10.6 Define a Policy Set	148
10.7 Enabling a Policy Set	149
10.8 Automatically Switch Policy Sets	149
10.9 Set the Timer	150
Chapter 11: URL Filter Configuration	152
11.1 Define a Filter	152
11.2 Apply a URL Filter to an Interface	152
11.3 Set the HTTP Port Numbers to Apply the URL Filter To	153
11.4 Set Whether to Use the URL Filter	153
11.5 Set the HTTP Response to the Source of a Packet Discarded by the URL Filter	154
11.6 Set Whether to Log Filter Matches	154
Chapter 12: PPP Configuration	156
12.1 Set the Peer Name and Password	156
12.2 Set the Type of Authentication to Accept	157
12.3 Set the Authentication Type to Be Requested	157
12.4 Set Its Own Name and Password	158
12.5 Set Whether to Prohibit Multiple Connections from a Peer with the Same Username	158
12.6 LCP Configuration	159
12.6.1 Set the Address and Control Field Compression Option	159
12.6.2 Set the Magic Number Option	159

12.6.3 Set the Maximum Receive Unit Option	159
12.6.4 Set the Protocol Field Compression Option	160
12.6.5 Set the lcp-restart Parameter	160
12.6.6 Set the lcp-max-terminate Parameter	160
12.6.7 Set the lcp-max-configure Parameter	161
12.6.8 Set the lcp-max-failure Parameter	161
12.6.9 Set Whether to Send Configure-Request Immediately	161
12.7 PAP Configuration	161
12.7.1 Set the pap-restart Parameter	162
12.7.2 Set the pap-max-authreq Parameter	162
12.8 CHAP Configuration	162
12.8.1 Set the chap-restart Parameter	162
12.8.2 Set the chap-max-challenge Parameter	162
12.9 IPCP Configuration	163
12.9.1 Set the Van Jacobson Compressed TCP/IP	163
12.9.2 Set the IP Address Negotiation with the Remote PP Interface	163
12.9.3 Set the ipcp-restart Parameter	163
12.9.4 Set the ipcp-max-terminate Parameter	164
12.9.5 Set the ipcp-max-configure Parameter	164
12.9.6 Set the ipcp-max-failure Parameter	164
12.9.7 Set the IP Address of the WINS Server	164
12.9.8 Set Whether to Use the IPCP MS Extension Option	165
12.9.9 Set Whether to Accept a Peer IP Address That Has a Host Route	165
12.10 MSCBCP Configuration	165
12.10.1 Set the mscbcpr-restart Parameter	165
12.10.2 Set the mscbcpr-maxretry Parameter	166
12.11 CCP Configuration	166
12.11.1 Set the Compression Type of All Packets	166
12.11.2 Set the ccp-restart Parameter	167
12.11.3 Set the ccp-max-terminate Parameter	167
12.11.4 Set the ccp-max-configure Parameter	167
12.11.5 Set the ccp-max-failure Parameter	167
12.12 IPV6CP Configuration	168
12.12.1 Set Whether to Use IPV6CP	168
12.13 MP Configuration	168
12.13.1 Set Whether to Use MP	168
12.13.2 Set the MP Control Method	168
12.13.3 Set the Load Threshold for MP	169
12.13.4 Set the Maximum Number of MP Links	169
12.13.5 Set the Minimum Number of MP Links	169
12.13.6 Set the Load Measurement Interval for MP	170
12.13.7 Set Whether to Divide MP Packets	170
12.14 BACP Configuration	170
12.14.1 Set the bacp-restart Parameter	170
12.14.2 Set the bacp-max-terminate Parameter	171
12.14.3 Set the bacp-max-configure Parameter	171
12.14.4 Set the bacp-max-failure Parameter	171
12.15 BAP Configuration	171
12.15.1 Set the bap-restart Parameter	171
12.15.2 Set the bap-max-retry Parameter	172
12.16 PPPoE Configuration	172
12.16.1 Specify the LAN Interface Used by PPPoE	172

12.16.2 Set the Access Concentrator Name	172
12.16.3 Set the Session Auto Connection	172
12.16.4 Set the Session Auto Disconnection	173
12.16.5 Set the Maximum Retry Count of PADI Packets	173
12.16.6 Set the Retransmission Time of PADI Packets	173
12.16.7 Set the Maximum Retry Count of PADR Packets	174
12.16.8 Set the Retransmission Time of PADR Packets	174
12.16.9 Set the Disconnection Timer of PPPoE Sessions	174
12.16.10 Set the Service Name	174
12.16.11 Turn ON/OFF the MSS Limit of TCP Packets and the Size	175
12.16.12 Set Whether to Forcefully Disconnect PPPoE Sessions That Do Not Exist on the Router	175
Chapter 13: DHCP Configuration	176
13.1 DHCP Server and Relay Agent Function	176
13.1.1 Set the DHCP Operation	176
13.1.2 Set the RFC2131 Compliant Operation	177
13.1.3 Set Whether to Check Duplications in the Leased IP Address	178
13.1.4 Define the DHCP Scope	178
13.1.5 Set the Reserved DHCP Address	179
13.1.6 Set the DHCP Address Assignment Operation	181
13.1.7 Generate Reserved Settings Based on the DHCP Assignment Information	182
13.1.8 Set the DHCP Options	182
13.1.9 Manually Add DHCP Lease Information	183
13.1.10 Manually Release DHCP Lease Information	184
13.1.11 Set the DHCP Server Designation	184
13.1.12 Set the DHCP Server Selection Method	185
13.1.13 Set the Relay Reference of the DHCP BOOTREQUEST Packet	185
13.2 DHCP Client Function	185
13.2.1 Set the Host Name of the DHCP Client	185
13.2.2 Set the Interface to Obtain the DNS Server Address	186
13.2.3 Set the Lease Period of the Requested IP Address	186
13.2.4 Set the Retry Count and Interval of the IP Address Get Request	187
13.2.5 Set the DHCP Client ID Option	187
13.2.6 Set the Options to Be Stored in the Message That the DHCP Client Sends to the DHCP Server	188
13.2.7 Set Whether to Release the Information When the Link Is Down	189
Chapter 14: ICMP Configuration	190
14.1 IPv4 Configuration	190
14.1.1 Set Whether to Send ICMP Echo Reply	190
14.1.2 Set Whether to Send ICMP Echo Reply When the Link Is Down	190
14.1.3 Set Whether to Send ICMP Mask Reply	190
14.1.4 Set Whether to Send ICMP Parameter Problem	191
14.1.5 Set Whether to Send ICMP Redirect	191
14.1.6 Set the Processing When ICMP Redirect Is Received	191
14.1.7 Set Whether to Send ICMP Time Exceeded	192
14.1.8 Set Whether to Send ICMP Timestamp Reply	192
14.1.9 Set Whether to Send ICMP Destination Unreachable	192
14.1.10 Set Whether to Send ICMP Error for Packets Decoded with IPsec	193
14.1.11 Set Whether to Log Received ICMP	193
14.1.12 Set the Stealth Function	193
14.1.13 Set Whether to Perform MTU Discovery Using ARP	194

14.1.14 Set Whether to Send ICMP Destination Unreachable for Truncated Packets	194
14.2 IPv6 Configuration	195
14.2.1 Set Whether to Send ICMP Echo Reply	195
14.2.2 Set Whether to Send ICMP Echo Reply When the Link Is Down	195
14.2.3 Set Whether to Send ICMP Parameter Problem	196
14.2.4 Set Whether to Send ICMP Redirect	196
14.2.5 Set the Processing When ICMP Redirect Is Received	196
14.2.6 Set Whether to Send ICMP Time Exceeded	197
14.2.7 Set Whether to Send ICMP Destination Unreachable	197
14.2.8 Set Whether to Log Received ICMP	197
14.2.9 Set Whether to Send ICMP Packet-Too-Big	198
14.2.10 Set Whether to Send ICMP Error for Packets Decoded with IPsec	198
14.2.11 Set the Stealth Function	198
14.2.12 Set Whether to Send ICMP Error (Packet Too Big) for Frames Truncated due to Size Error	199
Chapter 15: Tunneling	200
15.1 Enable the Tunnel Interface	200
15.2 Disable the Tunnel Interface	200
15.3 Set the Tunnel Interface Type	200
15.4 Set the IPv4 Address of the Tunnel Interface	201
15.5 Set the Peer IPv4 Address of the Tunnel Interface	201
15.6 Set the End Point IP Address of the Tunnel Interface	202
Chapter 16: IPsec Configuration	203
16.1 Set the IPsec Operation	203
16.2 Set the IKE Version	204
16.3 Set the IKE Authentication Method	204
16.4 Register the Pre-Shared Key	205
16.5 Set the PKI Files to Use in IKEv2 Authentication	206
16.6 Set Its Own Name and Password Used for EAP-MD5 Authentication	206
16.7 Configure EAP-MD5 User Authentication	207
16.8 Set Whether to Send the Certificate Request Payload in EAP-MD5 Authentication	207
16.9 Set Whether to Start IKE	208
16.10 Set Whether to Reject Key Exchange When the Setting Differs	208
16.11 Set Whether to Continue Key Exchange When IKE Fails	209
16.12 Set the Retry Count and Interval of Key Exchange	209
16.13 Set the Remote Security Gateway Name	210
16.14 Set the IP Address of the Remote Security Gateway	211
16.15 Set the Remote ID	211
16.16 Set the Local Security Gateway Name	212
16.17 Set the IP Address of the Local Security Gateway	213
16.18 Set the Local ID	213
16.19 Set the IKE Keepalive Function	214
16.20 Set Whether to Output SYSLOG Related to IKE Keepalive	215
16.21 Set the Encryption Algorithm That IKE Uses	216
16.22 Set the Length of the Queue That Stores the Received IKE Packets	216
16.23 Set the Group That IKE Uses	217
16.24 Set the Hash Algorithm That IKE Uses	218
16.25 Set Whether to Output to the Log When the SPI Value of the Received Packet Is Invalid	218
16.26 Set the IKE Payload Type	219
16.27 Set Whether to Send the IKE Information Payload	219
16.28 Set Whether to Use PFS	220

16.29 Set XAUTH	220
16.30 Set the User ID to Use in XAUTH Authentication or EAP-MD5 Authentication	221
16.31 Set the Attributes of the User ID to Use in XAUTH Authentication or EAP-MD5 Authentication ..	221
16.32 Set the User Group to Use in XAUTH Authentication or EAP-MD5 Authentication	222
16.33 Set the Attribute to Use in XAUTH Authentication or EAP-MD5 Authentication	222
16.34 Configure XAUTH User Authentication	223
16.35 Set an Internal IP Address Pool	224
16.36 Set the IKE XAUTH Mode-Cfg Method	224
16.37 Set the Internal IP Address Pool That Is Assigned to the IPsec Client	225
16.38 Register the Simultaneous Connection Limit License of the VPN Client	225
16.39 Apply the Simultaneous Connection Limit License of the VPN Client	226
16.40 Set the IKE Log Type	226
16.41 Set Whether to Exchange ESP by Encapsulating It in UDP	227
16.42 SA Configuration	227
16.42.1 Set the SA Life Time	227
16.42.2 Define the SA Policy	228
16.42.3 Manually Refresh the SA	230
16.42.4 Set the Dangling SA Operation	230
16.42.5 Configure Settings for IPsec NAT Traversal	231
16.42.6 Deleting SAs	232
16.43 Tunnel Interface Configuration	232
16.43.1 Set the DF Bit Control of the IPv4 Packet on the Outside of the IPsec Tunnel	232
16.43.2 Set the SA Policy to Be Used	233
16.43.3 Set Data Compression Using IPComp	233
16.43.4 Set the Tunnel Backup	234
16.43.5 Set a Tunnel Template	234
16.44 Transport Mode Configuration	236
16.44.1 Define the Transport Mode	236
16.45 PKI Configuration	237
16.45.1 Set the Certification File	237
16.45.2 Set the CRL File	238

Chapter 17: Set the L2TP/IPsec Function239

17.1 Set Whether to Run L2TP/IPsec	239
17.2 L2TP Tunnel Authentication Configuration	239
17.3 Set the Disconnection Timer of L2TP Tunnel	240
17.4 Set the L2TP Keepalive	240
17.5 Set L2TP Keepalive Logging	241
17.6 Set Whether to Output L2TP Connection Control to the Syslog	241

Chapter 18: PPTP Configuration243

18.1 Common Configuration	243
18.1.1 Set Whether to Operate as a PPTP Server	243
18.1.2 Set the Tunnel Interfaces That Are Bound to the Peer Information Number	243
18.1.3 Set the PPTP Operation Type	244
18.1.4 Set the PPTP Host Name	244
18.1.5 Set the PPTP Packet Window Size	244
18.1.6 Set the Authentication Method to Request for Creating PPTP Encryption Keys	245
18.1.7 Set the Acceptable Authentication Methods for Creating PPTP Encryption Keys	245
18.1.8 Set Whether to Output PPTP Connection Control to the Syslog	246
18.2 Remote Access VPN Function	246
18.2.1 Set the PPTP Tunnel Disconnection Timer	246
18.2.2 Set the Tunnel Endpoint Name	246

18.2.3 Set the PPTP Keepalive	247
18.2.4 Set PPTP Keepalive Logging	247
18.2.5 Set the PPTP Keepalive Interval and Count	248
18.2.6 Set Whether to Allow Connection According to the Encryption of the PPTP Connection	248
Chapter 19: Set the SIP Function	249
19.1 Common Configuration	249
19.1.1 Set Whether to Use SIP	249
19.1.2 Set the Additional User-Agent Header to SIP Packet to Be Sent	249
19.1.3 Setting When refresher Is Not Specified in INVITE at the Time of Call Reception Using SIP	249
19.1.4 Set Session Timer Request at the Time of Call Reception Using SIP	250
19.1.5 Set Whether to Verify the User Name at the Time of SIP Reception	250
19.1.6 Set an SIP Response Code to Be Returned When No Port to Receive Calls Is Available	251
19.1.7 Set Whether to Log SIP Messages	251
Chapter 20: SNMP Configuration	252
20.1 Set the Host to Allow Access Using SNMPv1	252
20.2 Set the SNMPv1 Read-Only Community Name	252
20.3 Set the SNMPv1 Read-Write Community Name	253
20.4 Set the SNMPv1 Trap Transmission Destination	253
20.5 Set the SNMPv1 Trap Community Name	253
20.6 Set the Hosts to Allow Access Using SNMPv2c	254
20.7 Set the SNMPv2c Read-Only Community Name	254
20.8 Set the SNMPv2c Read-Write Community Name	254
20.9 Set the SNMPv2c Trap Transmission Destination	255
20.10 Set the SNMPv2c Trap Community Name	255
20.11 Set the SNMPv3 Engine ID	255
20.12 Set the SNMPv3 Context Name	256
20.13 Set the User Managed with SNMPv3 USM	256
20.14 Set the Host to Allow Access Using SNMPv3	257
20.15 Set the MIB View Family Managed with SNMPv3 VACM	257
20.16 Set the Access Policy Managed with SNMPv3 VACM	258
20.17 Set the SNMPv3 Trap Transmission Destination	258
20.18 Set the Source Address of the SNMP Transmission Packet	259
20.19 Set sysContact	259
20.20 Set sysLocation	259
20.21 Set sysName	260
20.22 Set Whether to Send the SNMP Standard Traps	260
20.23 Set the Transmission Control of SNMP LinkDown Traps	261
20.24 Set Whether to Display the PP Interface Information in the MIB2 Range	261
20.25 Set Whether to Display the Tunnel Interface Information in the MIB2 Range	262
20.26 Set Whether to Display the Switch Interface Information in the MIB2 Range	262
20.27 Set the Forced Display of the PP Interface Address	263
20.28 Set Whether to Send a Trap When the Link of Each Port of the LAN Interface Goes Up or Down ..	263
20.29 Set Whether to Send the Signal Strength Trap	263
20.30 Set the Interface Number Statically Added to the Switch	264
20.31 Set the Switch Number Statically Added to the Switch	264
20.32 Set the Conditions of SNMP Trap According to Switch Status	265
20.33 Set Conditions of Common SNMP Trap for Switches	265
Chapter 21: RADIUS Configuration	267
21.1 Set Whether to Use RADIUS Authentication	267
21.2 Set Whether to Use RADIUS Account	267

21.3 Set the RADIUS Server	267
21.4 Set the RADIUS Authentication Server	268
21.5 Set the RADIUS Account Server	268
21.6 Set the UDP Port of the RADIUS Authentication Server	269
21.7 Set the UDP Port of the RADIUS Account Server	269
21.8 Set the RADIUS Secret Key	269
21.9 Set the RADIUS Retry Parameter	269
Chapter 22: NAT Function	271
22.1 Apply the NAT Descriptor to the Interface	271
22.2 Set the Operation Type of the NAT Descriptor	271
22.3 Set the Outer IP Address of the NAT Process	272
22.4 Set the Inner IP Address of the NAT Process	273
22.5 Set a Static NAT Entry	273
22.6 Set Whether to Use rlogin, rcp, and ssh When Using IP Masquerade	274
22.7 Set the Static IP Masquerade Entry	274
22.8 Set the Timer for Clearing the NAT IP Address Map	275
22.9 Set the TTL Synchronization Method of the IP Masquerade Table	276
22.10 Set the Action Taken When a Conversion Table Corresponding to the Packet Received from the Outside Does Not Exist	276
22.11 Set the Range of Ports Used for IP Masquerade	277
22.12 Set the Port Number Identified as FTP	277
22.13 Set the Range of Ports Not Converted by IP Masquerade	278
22.14 Set Whether to Log NAT Address Assignments	278
22.15 Set Whether to Overwrite the IP Address Included in SIP Messages	278
22.16 Set Whether to Remove the DF Bit during IP Masquerade Conversion	279
22.17 Set the Number of Sessions Converted by IP Masquerade	279
Chapter 23: DNS Configuration	281
23.1 Set Whether to Use the DNS	281
23.2 Set the IP Address of the DNS Server	281
23.3 Set the DNS Domain Name	281
23.4 Set the Peer Number from Which the DNS Server Is to Be Notified	282
23.5 Set the Order in Which the DNS Servers Are Notified in the DHCP/PCP MS Extension	282
23.6 Set Whether to Process Queries Directed at a Private Address	283
23.7 Set Whether to Resolve Names Using DNS on the SYSLOG Display	283
23.8 Select the DNS Server According to the Contents of the DNS Query	284
23.9 Register the Static DNS Record	285
23.10 Set the Source Port Number of the DNS Query Packet	286
23.11 Set the IP Address of the Host Allowed to Access the DNS Server	287
23.12 Set Whether to Use DNS Cache	287
23.13 Set the Maximum Number of DNS Cache Entries	288
23.14 Set Whether to Unify the DNS Fallback Operations of the Router	288
Chapter 24: Priority Control and Bandwidth Control	290
24.1 Set the Interface Speed	290
24.2 Set the Filter for Classification	290
24.3 Select the Queuing Algorithm Type	293
24.4 Set the MP Interleave	294
24.5 Apply the Classification Filter	294
24.6 Set the Queue Length for Each Class	295
24.7 Set the Queue Length of the Secondary Class	296
24.8 Set the Default Class	296
24.9 Set the Default Secondary Class	296

24.10 Set the Class Property	297
24.11 Set Dynamic Class Control	298
Chapter 25: Cooperation Function	301
25.1 Set Whether to Use the Cooperation Function	301
25.2 Set the Port Number to Be Used by the Cooperation Function	301
25.3 Set the Operation of Each Peer That Is to Cooperate in the Bandwidth Measurement	301
25.4 Set the Operation of Each Peer That Is to Cooperate in the Load Watch Notification	303
25.5 Set the Operation Trigger for the Load Watch Server	304
25.6 Set the Operation Trigger for the Load Watch Client	306
25.7 Manually Execute the Cooperation Function	306
Chapter 26: OSPF	308
26.1 Apply OSPF	308
26.2 Enable/Disable OSPF	308
26.3 Set the Level of Precedence of the OSPF Routing	308
26.4 Set the OSPF Router ID	308
26.5 Set Whether to Apply the Route Received through OSPF to the Routing Table	309
26.6 Route Import Using External Protocol	309
26.7 Set the Filter for Handling the Route Received through OSPF	310
26.8 Define Filters Applied to the Importing of AS External Routes	311
26.9 Set the OSPF Area	313
26.10 Advertise the Route to an Area	313
26.11 Advertise Stub Connections	314
26.12 Set the Virtual Link	314
26.13 Set the OSPF Area of the Specified Interface	315
26.14 Specify the OSPF Router Connected to a Non-Broadcast Network	318
26.15 Set the Handling of the Network Route When Stubs Are Present	319
26.16 Set Whether to Log OSPF State Transitions and Packet Exchanges	319
Chapter 27: BGP	321
27.1 Set the BGP Startup	321
27.2 Set Aggregate Routes	321
27.3 Set the Filter for Route Aggregation	321
27.4 Set the AS Number	322
27.5 Set the Router ID	322
27.6 Set the BGP Route Preference	323
27.7 Apply the Filter to the Route Received with BGP	323
27.8 Set the Filter to Be Applied to the Routes Received with BGP	324
27.9 Apply the Filter to the Route to Be Imported in BGP	325
27.10 Activate the BGP Configuration	326
27.11 Set the Filter to Be Applied to the Routes to Be Imported in BGP	326
27.12 Set the BGP Destination	327
27.13 Set the BGP Log	328
Chapter 28: IPv6	329
28.1 Common Configuration	329
28.1.1 Set Whether to Process IPv6 Packets	329
28.1.2 Set the Link MTU of the IPv6 Interface	329
28.1.3 Set the MSS Limit of the TCP Session	329
28.1.4 Set Whether to Discard IPv6 Packets with Type 0 Routing Headers	330
28.1.5 Set the IPv6 Fast Path Function	330
28.2 IPv6 Address Management	331
28.2.1 Set the IPv6 Address of the Interface	331
28.2.2 Set the IPv6 Address Based on the Prefix to the Interface	332

28.2.3 Set the DHCPv6 Operation	334
28.2.4 Set the DAD (Duplicate Address Detection) Retry Count	334
28.2.5 Set the Maximum Number of Automatically Set IPv6 Addresses	335
28.2.6 Set the Rule for Determining the Source IPv6 Address	335
28.3 Neighbor Discovery	335
28.3.1 Define the Prefix Distributed by the Router Advertisement	335
28.3.2 Control the Router Advertisement Transmission	337
28.4 Route Control	338
28.4.1 Add IPv6 Routing Information	338
28.5 RIPng	339
28.5.1 Set Whether to Use RIPng	339
28.5.2 Set the Transmission Policy of RIPng on the Interface	340
28.5.3 Set the Reception Policy of RIPng on the Interface	340
28.5.4 Set the Number of Hops to Be Added for RIPng	341
28.5.5 Set the Trusted RIPng Gate on the Interface	341
28.5.6 Set the Filtering to Be Applied to the Route Exchanging RIPng Packets	341
28.5.7 Set the RIPng Operation on the Remote PP Interface When the Line Is Connected	342
28.5.8 Set the RIPng Transmission Interval on the Remote PP Interface When the Line Is Connected	342
28.5.9 Set the RIPng Operation on the Remote PP Interface When the Line Is Disconnected	343
28.5.10 Set the RIPng Transmission Interval on the Remote PP Interface When the Line Is Disconnected	343
28.5.11 Set Whether to Hold the Route Obtained by RIPng When the Line Is Disconnected	343
28.5.12 Set the RIPng Routing Preference	344
28.6 Filter Configuration	344
28.6.1 Define an IPv6 Filter	344
28.6.2 Apply the IPv6 Filter	345
28.6.3 Define a Dynamic IPv6 Filter	346
28.7 IPv6 Multicast Packet Forwarding Configuration	347
28.7.1 Set the MLD Operation	348
28.7.2 Set Static MLD	348
28.7.3 Set the IPv6 Multicast Packet Transmission Mode	349
28.8 Neighbor Solicitation	350
28.8.1 Set Whether to Respond to Address Duplication Checking by Performing Neighbor Solicitation	350

Chapter 29: OSPFv3351

29.1 Apply OSPFv3	351
29.2 Enable/Disable OSPFv3	351
29.3 Set the OSPFv3 Router ID	351
29.4 Set the OSPFv3 Area	352
29.5 Advertise the Route to an Area	352
29.6 Set the OSPFv3 Area of the Specified Interface	353
29.7 Set the Virtual Link	355
29.8 Set the Level of Precedence of the OSPFv3 Routing	356
29.9 Set Whether to Apply the Route Received through OSPFv3 to the Routing Table	356
29.10 Set the Filter for Handling the Route Received through OSPFv3	356
29.11 Route Import Using External Protocol	358
29.12 Define Filters Applied to the Importing of AS External Routes	358
29.13 Set the OSPFv3 Log Output	360

Chapter 30: Status Mail Notification Function361

30.1 Set the Operation of the Status Mail Notification Function	361
---	-----

30.2 E-mail Server Settings	361
30.3 Set the Source Mail Address	361
30.4 Set the Destination Mail Address	361
30.5 Set the Subject	362
30.6 Set the Transmission Timeout	362
30.7 Set the Notified Information	362
30.8 Execute the Status Mail Notification	363
Chapter 31: Triggered Mail Notification Function	364
31.1 Set the Mail Configuration ID Name	364
31.2 Set the SMTP Mail Server	364
31.3 Set the POP Mail Server	365
31.4 Set the Timeout Value for Mail Processing	366
31.5 Set the Template Used to Send Mail	366
31.6 Set the Mail Notification Trigger	367
Chapter 32: HTTP Server Function	370
32.1 Common Configuration	370
32.1.1 Enable/Disable the HTTP Server Function	370
32.1.2 Set the IP Address of the Host Allowed to Access the HTTP Server	370
32.1.3 Set the Session Timeout Value of the HTTP Server	371
32.1.4 Set the Listen Port of the HTTP Server Function	371
32.1.5 Set the PP Interface and Tunnel Interface Names	371
32.2 Set the Easy Setup Page	371
32.2.1 Set the Provider Connection Type	372
32.2.2 Associate the Provider Information to PP and Assign the Name	372
32.2.3 Set the Provider Connection	372
32.2.4 Setting the DNS Server Address of the Provider	373
32.2.5 Set the DNS Server Address of the LAN Interface	373
32.2.6 Set the Peer Number from Which the DNS Server Is to Be Notified	374
32.2.7 Set the Type of Filter Type Routing	374
32.2.8 Set the Provider Name of the LAN Interface	374
32.2.9 Set the NTP Server	375
32.2.10 Setting the NTP Server Address of the Provider	375
32.2.11 Set Whether to Automatically Connect When the Disconnect Button Is Pressed on the Easy Setup Page	375
32.2.12 Set Whether to Carry Out IPv6 Connection on the Easy Setup Page	376
Chapter 33: NetVolante DNS Service Configuration	377
33.1 Set Whether to Use the NetVolante DNS Service	377
33.2 Manually Update the Data on the NetVolante DNS Server	377
33.3 Delete Data from the NetVolante DNS Server	378
33.4 Set the Port Number to Use for the NetVolante DNS Service	378
33.5 Acquire a List of Registered Host Names from the NetVolante DNS Server	378
33.6 Register a Host Name	379
33.7 Set the Communication Timeout	379
33.8 Set Whether to Automatically Generate the Host Name	379
33.9 Register the Router's Serial Number as the Host Name	380
33.10 Set the NetVolante DNS Server Location	380
33.11 Turn the NetVolante DNS Server Address Update Function ON/OFF	381
33.12 Set the Port Number of the NetVolante DNS Server Address Update Function	381
33.13 Set How Many Times and at What Interval to Retry after Automatic Updating Fails	382
33.14 Set the Periodical Update Interval of NetVolante DNS Registration	382
33.15 Set the File for Saving the Configuration When Automatic NetVolante DNS Registration Succeed ..	383

Chapter 34: UPnP Configuration	384
34.1 Set Whether to Use UPnP	384
34.2 Set the Interface That Is to Obtain the IP Address Used for UPnP	384
34.3 Set the Type of Timer for Clearing the UPnP Port Mapping	384
34.4 Set the Timer for Clearing the UPnP Port Mapping	385
34.5 Set Whether to Output the UPnP Syslog	385
Chapter 35: USB Configuration	387
35.1 Set Whether to Use the USB Host Function	387
35.2 Set the Time Until the Excess Current Protection Function in the USB Bus Is Activated	387
Chapter 36: Schedule	388
36.1 Set the Schedule	388
Chapter 37: VLAN Configuration	391
37.1 Set VLAN ID	391
37.2 Assigning a Switching Hub Port to a VLAN	391
Chapter 38: Heartbeat Function	393
38.1 Set the Shared Heartbeat Key	393
38.2 Set Whether to Receive Heartbeats	393
38.3 Send a Heartbeat	394
Chapter 39: Heartbeat Function Release 2	395
39.1 Set the Notification Name	395
39.2 Configure Notification Settings	395
39.3 Enabling a Notification Configuration	396
39.4 Set a Notification Interval	396
39.5 Set Whether to Log Notification Transmissions	397
39.6 Configuring Reception Settings	397
39.7 Enabling a Reception Configuration	398
39.8 Set Reception Interval Monitoring	398
39.9 Set Whether to Log Received Notifications	399
39.10 Set the Maximum Number of Heartbeats That Can Be Stored at the Same Time	399
39.11 Show the Heartbeat Information	400
39.12 Clear the Heartbeat Information	400
Chapter 40: SNTP Server Function	401
40.1 Set Whether to Enable the SNTP Server Function	401
40.2 Set Which Hosts to Allow Access to the SNTP Server	401
Chapter 41: External Memory Function	403
41.1 Set Whether to Use the microSD Card Slot	403
41.2 Set the Prefix for Statistical Information Files Saved to the External Memory	403
41.3 Set the Name of the Syslog File to Save to the External Memory	405
41.4 Set Whether to Permit Setup File and Firmware File Copying through the Simultaneous Holding Down of an External Memory Button and the DOWNLOAD button	406
41.5 Set Whether to Allow the Router to Start Using Files in the External Memory	407
41.6 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	407
41.7 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	408
41.8 Set the File Search Timeout	409
41.9 Execute the Batch File	409
41.10 Set the Batch and Execution Result Files	410
41.11 External Memory Performance Test Command	410

41.12 Set the Function to Execute When the DOWNLOAD Button Is Pressed	411
41.13 Set Whether to Allow Batch File Execution through the Pressing of the DOWNLOAD Button	412

Chapter 42: HTTP Upload Function413

42.1 Set a File to Upload to the HTTP Server	413
42.2 Set the HTTP Upload Destination URL	414
42.3 Set Whether to Allow HTTP Uploading	414
42.4 Set the HTTP Upload Timeout Time	414
42.5 Set the HTTP Upload Retry Count and Interval	415
42.6 Set the Proxy Server to Use for HTTP Uploading	415
42.7 Upload to an HTTP Server	415
42.8 Set Whether to Sound Alarms for the HTTP Upload Function	416

Chapter 43: Mobile Internet Connection Function417

43.1 Set Whether to Use a Mobile Terminal	417
43.2 Set the PIN Code to Be Input to Mobile Terminal	417
43.3 Send a Direct Command to the Mobile Interface	418
43.4 Release the Transmission Restriction on a Specified Peer	418
43.5 Set Automatic Transmission from the Mobile Terminal	419
43.6 Set the Timer for Disconnecting from the Mobile Terminal	419
43.7 Set the Timer for Disconnecting from the Mobile Terminal When There Is No Input	419
43.8 Set the Timer for Disconnecting from the Mobile Terminal When There Is No Output	420
43.9 Set the Access Point to Transmit To	420
43.10 Set a Point to Transmit Which Is Specified to the Mobile Terminal	421
43.11 Set the Packet Transmission Quantity Limit	421
43.12 Set the Packet Transmission Time Limit	422
43.13 Set the Maximum Number of Consecutive Authentication Failures for a Single Peer	423
43.14 Set the LCP Async Control Character Map Option	423
43.15 Set Whether to Attach a Caller ID (186)	424
43.16 Set Whether to Output a Detailed Syslog	424
43.17 Set Whether to Sound an Alarm When the Mobile Terminal Is Connected	424
43.18 Set the Packet Transmission Quantity Limit for Each Connection	425
43.19 Set the Packet Transmission Time Limit for Each Connection	425
43.20 Set the Duration That the Transmission Limits Apply To	426
43.21 Acquire the Signal Reception Level	426
43.22 Configure Signal Reception Level Acquisition	426
43.23 Displaying Regularly Acquired Signal Reception Levels	427
43.24 Set the AT Commands to Use to Initialize the Device Connected to the USB Port	428
43.25 Set Whether to Perform Flow Control on the Device Connected to the USB Port	428
43.26 Set Its Own Name and Password	429
43.27 Set the Interface Used for WAN	429
43.28 Set Automatic Transmission from the Mobile Terminal	430
43.29 Set the Timer for Disconnecting from the Mobile Terminal	430
43.30 Set the Timer for Disconnecting from the Mobile Terminal When There Is No Input	431
43.31 Set the Timer for Disconnecting from the Mobile Terminal When There Is No Output	431
43.32 Set Permanent Connection	432
43.33 Set the Access Point to Transmit To	432
43.34 Set the Packet Transmission Quantity Limit	433
43.35 Set the Packet Transmission Time Limit	434
43.36 Set the Packet Transmission Quantity Limit for Each Connection	435
43.37 Set the Packet Transmission Time Limit for Each Connection	436
43.38 Set the Duration That the Transmission Limits Apply To	436

Chapter 44: Lua Script Function438

44.1 Set Whether to Enable the Lua Script Function	438
44.2 Execute a Lua Script	438
44.3 Execute the Lua Compiler	439
44.4 Show the Status of Running Lua Scripts	439
44.5 Stop a Lua Script	440
44.6 Set Whether to Sound Alarms for the Lua Script Function	441
Chapter 45: Custom GUI	442
45.1 Set Whether to Use the Custom GUI	442
45.2 Configure Custom GUI User Settings	442
45.3 Set Whether to Use the Custom GUI API	443
45.4 Set the Password for Accessing the Custom GUI API	443
Chapter 46: Switch Control Function	444
46.1 Set the Switch Control Function	444
46.1.1 Set Whether to Use the Switch Control Function	444
46.1.2 Set the Time Interval for Watching Switch	445
46.1.3 Select the Switch	445
46.1.4 Set the Functions That the Switch Has	446
46.1.5 Obtain the Configuration and Operation Status of the Functions That the Switch Has	446
46.1.6 Execute a Specified Operation for the Switch	446
46.1.7 Delete the Switch Setting	447
46.1.8 Update the Firmware of the Switch	447
46.2 Switch Function	448
46.2.1 System	448
46.2.1.1 Obtain the BootROM Version	448
46.2.1.2 Obtain the Firmware Revision	448
46.2.1.3 Obtain the Serial Number	448
46.2.1.4 Obtain the Model Name	449
46.2.1.5 Obtain the MAC Address	449
46.2.1.6 Obtain the System Name	449
46.2.1.7 Set Whether to Use the Energy Saving Function	449
46.2.1.8 Adjust the LED Brightness	450
46.2.1.9 Obtain the LED Display Mode	450
46.2.1.10 Obtain the Fan State	451
46.2.1.11 Restart	451
46.2.1.12 Obtain the Time Since the System Starts Up	452
46.2.2 Port	452
46.2.2.1 Set the Port Speed and Operation Mode	452
46.2.2.2 Set Whether to Use the Port	452
46.2.2.3 Set Whether to Use the Auto Crossover Function	453
46.2.2.4 Set Whether to Use the Speed-Downshift Function	453
46.2.2.5 Set Whether to Use the Flow Control Function	454
46.2.2.6 Obtain the Port Link State	455
46.2.3 MAC Address Table	455
46.2.3.1 Set Whether to Use the MAC Address-Aging Function	455
46.2.3.2 Set the MAC Address-Aging Time Interval	456
46.2.3.3 Search the MAC Address Table According to the MAC Address	456
46.2.3.4 Search the MAC Address Table According to the Port Number	456
46.2.3.5 Clear the MAC Address Table Entries	457
46.2.4 VLAN	457
46.2.4.1 Set VLAN ID	458
46.2.4.2 Set the Port VLAN Operation Mode	458

46.2.4.3 Set the Access Port	459
46.2.4.4 Set the Trunk Port	459
46.2.4.5 Set Whether to Use Multiple VLAN	460
46.2.4.6 Set the Multiple VLAN Group	460
46.2.5 QoS	461
46.2.5.1 Set the DSCP Remarking Rewriting Method	461
46.2.5.2 Set the Received Packets Classification	462
46.2.5.3 Set the Speed Unit for Band Limit	462
46.2.5.4 Set Whether to Police Incoming Traffic	463
46.2.5.5 Set a Bandwidth for Incoming Traffic	463
46.2.5.6 Set Whether to Shape Outgoing Traffic	464
46.2.5.7 Set a Bandwidth for Outgoing Traffic	464
46.2.6 Mirroring	465
46.2.6.1 Set Whether to Use the Mirroring Function	466
46.2.6.2 Set a Destination Port for Mirroring Packets	466
46.2.6.3 Set Whether to Mirror Received Packets	467
46.2.6.4 Set Whether to Mirror Packets to Be Transmitted	467
46.2.7 Counter	468
46.2.7.1 Set a Type of Frames That the Incoming Frame Counter Counts	468
46.2.7.2 Set a Type of Frames That the Outgoing Frame Counter Counts	470
46.2.7.3 Obtain the Incoming Frame Counter Value	471
46.2.7.4 Obtain the Outgoing Frame Counter Value	472
46.2.7.5 Obtain the Incoming Octet Counter Value	472
46.2.7.6 Obtain the Outgoing Octet Counter Value	472
46.2.7.7 Clear the Counter	473
46.2.8 Detect a Loop	473
46.2.8.1 Set the Threshold for the Number of Times That a MAC Address Transfers Per Second	473
46.2.8.2 Set the Time Until the Switch Determines That the Loop Occurs	473
46.2.8.3 Set the Operation When a Loop Occurs	474
46.2.8.4 Set the Time from When a Port Link Is Down Until It Is Recovered	474
46.2.8.5 Set Whether to Use the Loop Detection Function	475
46.2.8.6 Obtain the Port Status Related to the Loop Detection Function	475
46.2.8.7 Obtain the Remaining Time Until the Port Is Recovered from Linkdown	476
46.2.8.8 Recover the Port of Which Link Is Down due to the Loop Occurrence	476
Chapter 47: Diagnosis	477
47.1 Port Availability Diagnosis	477
47.2 Diagnosis of Access Ranges That Can Reach a Port	477
47.3 Set the Maximum Number of Passed Packets That Can Be Detected in the Port Availability Diagnosis	478
47.4 Set the Number of Port Availability Diagnosis Results to Store in the History	478
47.5 Display the Results of the Port Availability Diagnosis	479
47.6 Display the Results of the Diagnosis of Access Ranges That Can Reach a Port	479
47.7 Delete the Results of the Port Availability Diagnosis	479
Chapter 48: Statistics	480
48.1 Set Whether to Enable the Statistics Function	480
Chapter 49: Operation	481
49.1 Select the Peer Number	481
49.2 Select the Tunnel Interface Number	481
49.3 Configuration Operation	482
49.3.1 Switch to Administrator	482

49.3.2 Quit	482
49.3.3 Save the Configuration	482
49.3.4 Duplicate the Configuration File	483
49.3.5 Copy the Firmware File to the Internal Flash ROM	484
49.3.6 Delete a Configuration File	485
49.3.7 Delete an Executable Firmware File	485
49.3.8 Set the Default Configuration File	486
49.3.9 Set the Default Firmware File	486
49.3.10 Reset the Configuration	486
49.3.11 Configure a Router at a Remote Location	486
49.3.12 Limit Configuration from a Router at a Remote Location	487
49.4 Clear Operation of Dynamic Information	487
49.4.1 Clear an Account	487
49.4.2 Clear the PP Account	488
49.4.3 Clear the ARP Table	488
49.4.4 Clear the Dynamic Routing Information of IP	488
49.4.5 Clear the Log	488
49.4.6 Clear the InARP	488
49.4.7 Clear the DNS Cache	488
49.4.8 Clear the Interface Counter Information	489
49.4.9 Clear the NAT Address Table	489
49.4.10 Clear the NAT Address Table of the Interface	489
49.4.11 Clear the Dynamic Routing Information of IPv6	490
49.4.12 Clear the Neighbor Cache	490
49.4.13 Delete the Startup Information History	490
49.5 File and Directory Operation	490
49.5.1 Create Directories	490
49.5.2 Delete a File or Directory	491
49.5.3 Copy a File or Directory	491
49.5.4 Change a File or Directory Name	492
49.6 Other Operations	492
49.6.1 Enable the Peer	492
49.6.2 Disable the Peer	492
49.6.3 Restart	493
49.6.4 Restart the Interface	493
49.6.5 Restart the PP Interface	494
49.6.6 Connect	494
49.6.7 Disconnect	494
49.6.8 ping	495
49.6.9 Execute ping6	496
49.6.10 traceroute	497
49.6.11 Execute traceroute6	497
49.6.12 nslookup	497
49.6.13 Delete the Connection Management Information of the Dynamic IPv4 Filter	497
49.6.14 TELNET Client	498
49.6.15 Delete the Connection Management Information of the Dynamic IPv6 Filter	499
49.6.16 Delete the Switching Hub MAC Address Table	499
49.6.17 Send a Magic Packet	499
49.6.18 Check and Update the Firmware by Using HTTP	500
49.6.19 Clear the Input Cut-Off Filter Information	501
49.6.20 Clear the Policy Filter Information	501
49.6.21 Clear the Statistical Information for the URL Filter	501

49.6.22 Execute the Mail Notification	502
Chapter 50: Configuration Display	503
50.1 Show the Router Configuration	503
50.2 Show All Configurations	503
50.3 Show the Configuration of a Specified PP	503
50.4 Show the Configuration of a Specified Tunnel	504
50.5 List the Configuration Files	504
50.6 Show a List of File Information	504
50.7 Show the IPv6 Address Granted to the Interface	505
50.8 Show the SSH Server Public Key	505
50.9 Display the Filter Contents of the Specified Interface	505
50.10 Firmware File List	506
Chapter 51: Status Display	507
51.1 Show the ARP Table	507
51.2 Show the Interface Status	507
51.3 Show the Peer Status	507
51.4 Show DLCI	508
51.5 Show the IP Routing Information Table	508
51.6 Show Routing Information Obtained by RIP	509
51.7 Show IPv6 Routing Information	509
51.8 Show the IPv6 RIP Table	509
51.9 Show the Neighbor Cache	509
51.10 Show IPsec SA	510
51.11 Show the Certificate Information	510
51.12 Show the CRL File Information	511
51.13 Show VRRP Information	511
51.14 Show the Address Map of the Dynamic NAT Descriptor	511
51.15 Show the List of Active NAT Descriptor Applications	512
51.16 Show the Address Map of the NAT Descriptor of the LAN Interface	512
51.17 Show the Number of Ports Being Used by IP Masquerading	513
51.18 Show the L2TP Status	513
51.19 Show the PPTP Status	513
51.20 Show OSPF Information	513
51.21 Show the BGP Status	514
51.22 Show the DHCP Server Status	514
51.23 Show the DHCP Client Status	515
51.24 Show the DHCPv6 Status	515
51.25 Show the Backup Status	515
51.26 Show the Connections Managed by Dynamic Filters	515
51.27 Show the Connections Managed by IPv6 Dynamic Filters	516
51.28 Show the Status of the Network Monitor Function	517
51.29 Show the History of Intrusion Information	517
51.30 Show the Connection Time for Each Peer	517
51.31 Show Settings Related to the NetVolante DNS Service	518
51.32 Show the Switching Hub MAC Address Table	518
51.33 Show the UPnP Status Information	519
51.34 Show the Tunnel Interface Status	519
51.35 Show the VLAN Interface Status	519
51.36 Show Information Regarding the Triggered Mail Notification Function	519
51.37 Show Multicast Routing Information	520
51.38 Show IGMP Group Management Information	520

51.39 Show Information Managed by PIM-SM	521
51.40 Show MLD Group Management Information	521
51.41 Show IPv6 Multicast Routing Information	521
51.42 Show Information about the Logged in User	521
51.43 Show the Packet Buffer Status	522
51.44 Show the QoS Status	523
51.45 Show the Cooperation Status	523
51.46 Show OSPFv3 Information	524
51.47 Show the Input Cut-Off Filter Status	524
51.48 Show the Policy Filter Status	525
51.49 Show the Services Affected by the Policy Filter	525
51.50 Show the URL Filter Information	525
51.51 Show the Heartbeat Information	526
51.52 Show the USB Host Function Operation Status	526
51.53 Show Connection Information Related to the Remote Setup Function	526
51.54 Show Technical Info	527
51.55 Show the Operation Status of the microSD Slot	527
51.56 Show the Operation Status of the External Memory	527
51.57 Show the RTFS Status	527
51.58 Show the Startup Information	528
51.59 Show Detail of the Startup Information History	528
51.60 Show a List of the Startup Information History	528
51.61 Show a List of the Switches Controlled by the Router	529
51.62 Display the DNS Cache	529
Chapter 52: Logging	530
52.1 Show the Log	530
52.2 Show the Account	531
52.3 Show the PP Account	531
52.4 Show the Communication History	531

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.
- FOMA, mopera, and mopera U are registered trademarks of NTT DOCOMO 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.8.03.30, Rev.9.00.08, Rev.10.01.40.
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.rtpro.yamaha.co.jp>

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 Bold face
	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 RTX1200, 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, ..., lan1/8
LAN with LAN division function	lan1.1, lan1.2, lan1.3, lan1.4
LAN with enhanced VLAN division function	vlan1,vlan2, ..., vlan8
BRI on the main module	bri1
First LAN module	lan2
First 8BRI module	bri2.1, bri2.2, ..., bri2.8
Second 8BRI module	bri3.1, bri3.2, ..., bri3.8

Interface Type	Interface Name
First PRI module	pri1

In firmware Rev. 8.03 and later, 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
RTX3000	1-150
RTX1200	1-100
RTX1100/RTX800/RT107e	1-30

1.7 About the Factory Default Settings

The RTX1200, RT107e, and RTX800 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.

```
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
```

In addition, the initial login and administrator passwords on the RTX800 are both “doremi”.

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.

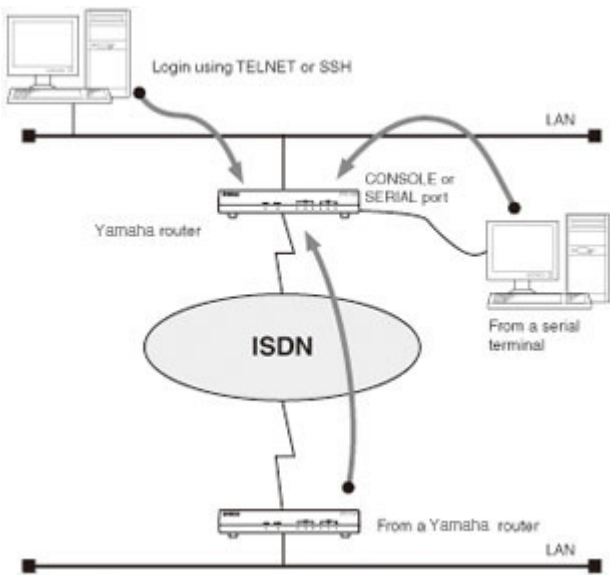
2.1 Console

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. The factory default login and administrator passwords on the RTX800 are both “doremi”.

- 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 Using TELNET

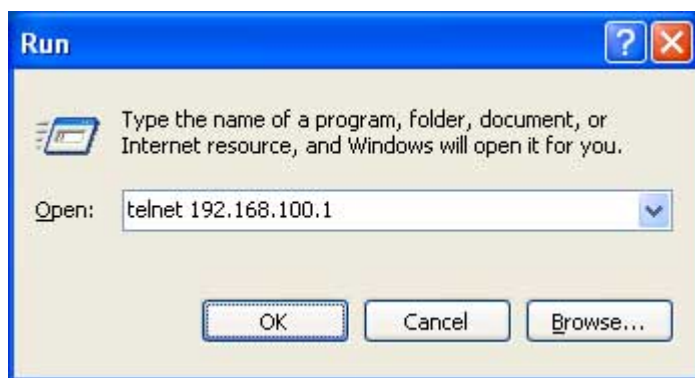
This section gives a configuration example using TELNET on Windows XP. The IP address of the Yamaha router is 192.168.100.1 in this example.

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



2. Type “telnet 192.168.100.1” and click OK.

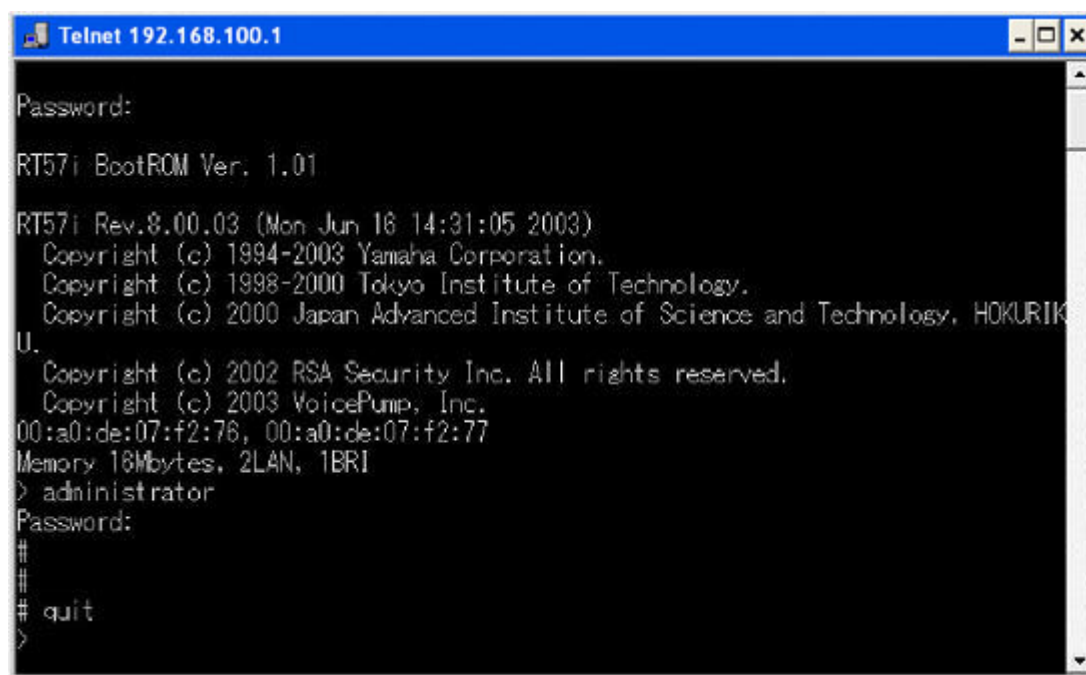
If you are using another IP address for the router, type that address in place of “192.168.100.1”.



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.



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.

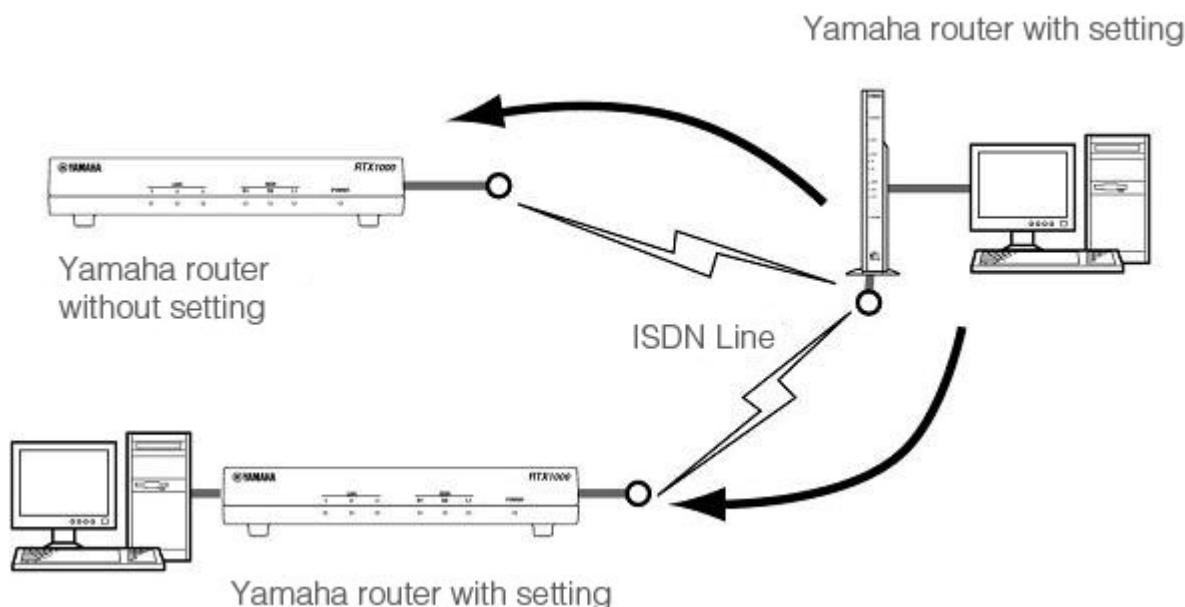
6. Type console commands to configure the router.
7. When you are done, type **save** and press the Enter key.

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.

2.1.3 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 SSH Server

On models that support the SSH server function, users can access the router from a host on the LAN by logging in using SSH. The SSH client used on the host comes standard on Mac OS X (Terminal) and UNIX platforms. It does not come standard on Windows OS platforms. On platforms that do not come with an SSH client, obtain an application such as freeware that has a 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. Note that only firmware Rev.10.01.11 and later can handle encrypted configuration files.



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.

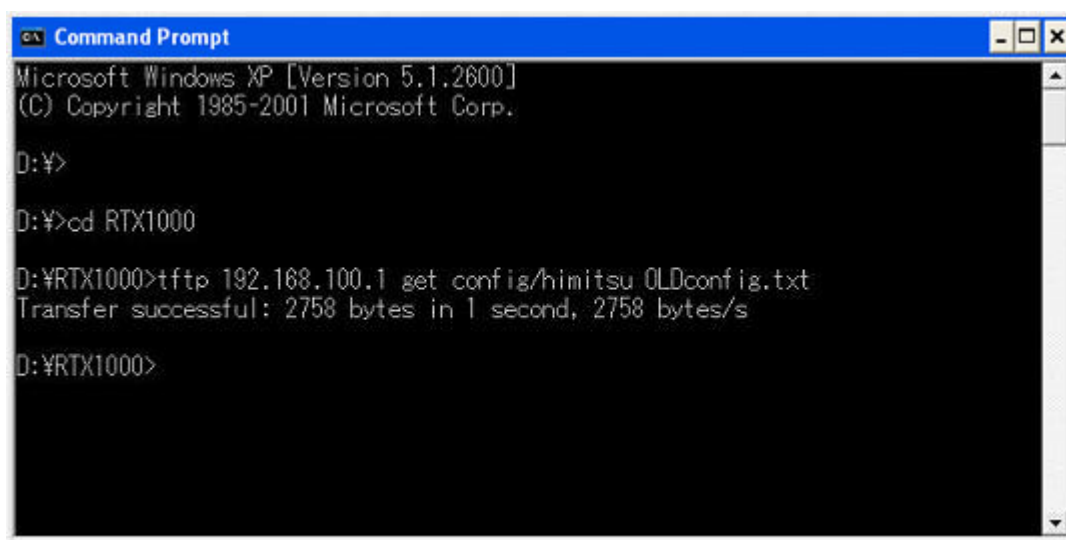
2.3.2 Reading the Configuration File

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



```
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>
```

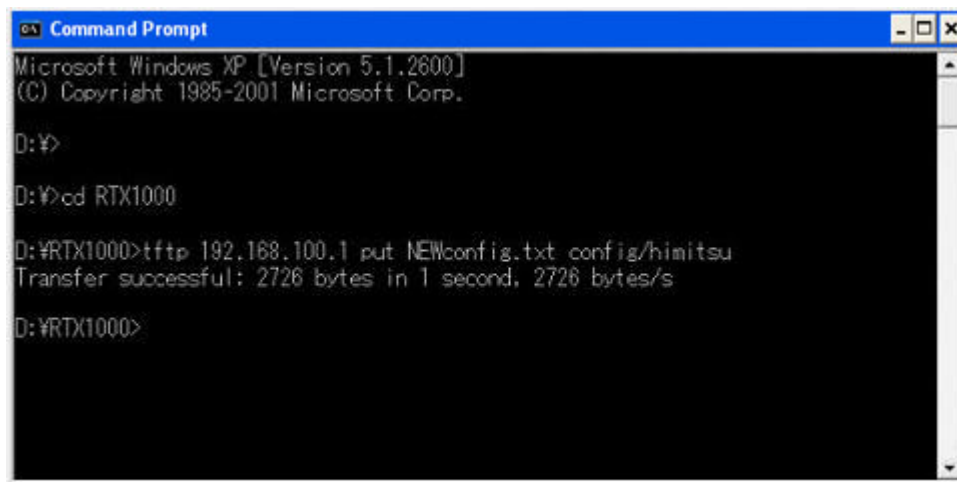
2.3.3 Writing the Configuration File

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



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
RETURN	
q	Quit
Ctrl-C	

To show the contents of **show config**, **show config list**, **show config pp**, **show config tunnel**, **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 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	
{n} Ctrl-J	Advance {n} lines
{n} Ctrl-E	
{n} Ctrl-M	
{n} ENTER	
{n} RETURN	
{n} k	Go back {n} lines
{n} Ctrl-K	

Keyboard Operation	Description and Notes
{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
\	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.

In firmware Rev.10.01.11 and later revisions, 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

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 grep command.
?	Searches the search pattern entered after the command character toward the back. The search pattern is the same as with the grep command.
n	Searches the same search pattern as the previous / or ? command in the same direction.
N	Searches the same search pattern as the previous / or ? command in the reverse direction.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

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
```

In firmware Rev.10.01.11 and later, 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 '>>' is available in firmware Rev.10.01.11 and later.

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.

On RTX1200 loading firmware Rev.10.01.32 and later, *filename* must be 99 characters or less.

For other models, *filename* must be 64 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]

RTX1200

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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

3.2 Showing a List of Commands

[Syntax]

show command

[Description]

Lists the command names and their simple explanations.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.6 Set 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]

RTX1200, RTX800

4.7 Set Whether to Use RADIUS for Password Authentication When Switching to Administrator**[Syntax]****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** command is compared. When 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 specified:

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

[Models]

RTX1200, RTX800

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 administrator 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 administrator 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
<ul style="list-style-type: none"> • 120..21474836 (RTX1200, RTX800) • 30..21474836 (RTX3000, RTX1100, RT107e) 	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]

In firmware Rev.10 and later, you can limit connections to the administrator pages GUI by setting off the administrator attribute.

http can be specified for the connection attribute in firmware Rev. 10 and later. Sftp can be specified in firmware Rev 10.01.22 later.

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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

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.

http can be specified in firmware Rev.10 and later.
 sftp can be specified in firmware Rev.10.01.22 and later.

[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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

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 telnet command as a TELNET client.
off	Not allow the use of the telnet 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

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] : cct

[Description]

Sets the time zone.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

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)

Setting	Description
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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

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 **rddate** 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.

IPv6 address can be specified for the *ntp_server* in RTX1200/RTX800 loading firmware Rev.10.01.36 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

4.17 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.18 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.

In firmware Rev.10 and later, the setting specified by this command is applied to the configuration shown by the **show config** command even when the **save** command is not executed.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.19 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.

In firmware Rev.10 and later, the setting specified by this command is applied to the configuration shown by the **show config** command even when the **save** command is not executed.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.20 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.

In firmware Rev.10 and later, the setting specified by this command is applied to the configuration shown by the **show config** command even when the **save** command is not executed.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.21 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.22 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.23 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.24 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.25 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.26 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.27 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]

RTX3000, RTX1200, RT107e, RTX800

4.28 Set the Source Port Number for SYSLOG Packets

[Syntax]

syslog srcport *port*

no syslog srcport [*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]

RTX1200, RTX800

4.29 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]

RTX1200, RTX800

4.30 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

Setting	Description
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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.31 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.32 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

- [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.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.33 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.34 Set the Monitored Temperature Threshold

[Syntax]**system temperature threshold** *t1 t2***no system temperature threshold** *t1 t2***[Setting and Initial value]**

- *t1*
 - [Setting] : Temperature at which an alarm is generated (°C)
 - [Initial value] :
 - 65(RTX3000)
 - 75(RTX1200)
- *t2*
 - [Setting] : Temperature at which the alarm is released (°C)
 - [Initial value] :
 - 60(RTX3000)
 - 70(RTX1200)

[Description]

The internal temperature is monitored, and an alarm is indicated through SYSLOG or the ALM lamp when the temperature exceeds *t1*. Once an alarm is generated, the ALM lamp stays on until the temperature falls below *t2*.

[Models]

RTX3000, RTX1200

4.35 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.
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]

RTX1200, RTX1100, RT107e, RTX800

4.36 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.37 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.

RTX1200 loading firmware Rev.10.01.11 and later can use this function.

[Models]

RTX1200, RTX800

4.38 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]

RTX1200, RTX1100, RTX800

4.39 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

Setting	Description
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
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
off	Disable the LAN division function and port division function

- speed-downshift
 - Speed-downshift function

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

- energy-saving
 - Energy-saving function

Setting	Description
on	Enable the energy-saving function
off	Disable the energy-saving function

- [Initial value] :
 - mtu=1500
 - auto-crossover=on
 - macaddress-aging=on (model not allowing setting of the number of seconds)

- `macaddress-aging=300` (model allowing setting of the number of seconds)
- `port-based-ks8995m/port-based-option=off`
- `speed-downshift=on`
- `energy-saving=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.

To set “port-based-ks8995m/port-based-option” on firmware versions earlier than Rev.10.01, type “port-basedks8995m”. To set it on firmware versions Rev.10.01, type “port-based-option”.

You can type “port-based-ks8995m” on firmware versions Rev.10.01, but the output of the **show config** command will be “port-based-option”.

○*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 range of data length that can be specified varies depending on the LAN interface. The range is 64 to 1500 for LAN interfaces that do not support jumbo frames. For LAN interfaces that support jumbo frames, the range is as follows:

Model	Interface	Selectable Range
RTX3000	LAN1, LAN2	64 to 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. If the setting of the **ip mtu** command or the **ipv6 mtu** command is specified, this setting is used regardless of whether the *mtu* setting of the interface is specified. If all settings are not 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, not only the MAC addresses that the switching hub stores are not cleared automatically, but also the entries are not cleared even if the **clear switching-hub macaddress** command is issued. The entries are cleared only when this function is turned back on.

You can specify the number of seconds for the following models. However, a margin of error may be generated between the command setting value and actual time spent for deletion.

Model	Selectable Range
RTX1200	1 to 86400

When on is entered for a model allowing setting of the number of seconds, a value is converted to the initial value, “300”.

The size of the MAC address table is indicated below.

Model	Maximum Number of Entries
RTX1200	8192
RTX1100, RT107e, RTX800	1024

○LAN division function

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

This option is not available on RT107e.

There are two LAN division functions: normal and enhanced. The enhanced function can be used on firmware Rev.10.01.

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 also becomes possible.

For example, the RTX1100 normally has three LAN interfaces, but using the LAN division function allows six 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 for the normal and enhanced functions.

The name of the LAN interfaces created with the normal function is represented by the original LAN interface name, period, and the port number.

For example, lan1 of the RTX1100 is a LAN interface with a switching hub consisting of four ports, 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 set 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
RTX1200	vlan1-vlan8

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

The LAN interface MAC addresses used in LAN division are the same as the original LAN interface MAC addresses. Therefore, the lan1.1-lan1.4 and vlan1-vlan8 MAC addresses discussed above are all the same as lan1.

○Port division function

This function can be used on firmware Rev.8.03.24 and later, and also LAN interfaces with a switching hub.

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

The normal function divides the ports into groups and allows communication within the group and other routers, but can prohibit communication with ports of 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.

When the number of switching hub ports is 4.

split_pattern	Po rt				Description
	1	2	3	4	
1 : 234	←→	← — — — →			Port 1 and other ports
1 : 2 : 34	←→	←→	← — — — →		Port 1, port 2, and other ports
1 : 2 : 3 : 4	←→	←→	←→	←→	Divide all ports

With RTX1200, you can omit the last group. In the table below, patterns with the last group omitted are indicated in parenthesis.

split_pattern	Port								Description
	1	2	3	4	5	6	7	8	
123:45678 (123)	← — — →			← — — — — →					Ports 1 to 3 and other ports
1:234:5678 (1:234)	↔	← — — — →			← — — — — →				Port 1, ports 2 to 4, and other ports
12:34:56:78 (12:34:56)	← — — →		← — — →		← — — →		← — — — — →		Ports 1 and 2, 3 and 4, 5 and 6, and other ports
1:2:3:4:5:6:7:8 (1:2:3:4:5:6:7)	↔	↔	↔	↔	↔	↔	↔	↔	Divide all ports

Even if you omit the end when you specify a pattern, the pattern will be output in full when you execute the **show config** command.

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.

When “-” is specified, packets received in the port are not routed. Also, devices connected to that port cannot communicate with the router.

For example, when the following setting is activated, a packet received in the port 1 to 3 is transferred to the port 4 and the router, and a packet received in the port 4 is transferred to the port 1 to 3, but not to the router. In other words, the ports are divided into three groups such as the port 1 and 4, the port 2 and 4, and the port 3 and 4, and the port 1 to 3 cannot communicate with each other, but only with the port 4. Also, although the port 1 to 3 can communicate with the router, the port 4 cannot communicate in the same way and also no packet received is routed.

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

○Speed-downshift function

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

It is available on RTX1200.

○Energy-saving function

When on is set, this function allows reduction of power consumption on LAN ports that are not used.

It is available on RTX1200.

[Note]

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

[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.

- On firmware versions earlier than Rev.10.01

```
# lan type lan1 100-fdx 1 port-based-ks8995m=divide-network
```

- On firmware Rev.10.01

```
# 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 switching hub that has four ports and a firmware version earlier than Rev.10.01 installed

```
# lan type lan1 port-based-ks8995m=split-into-12:34
```

- Dividing ports 1, 2, and 3, 4, 5, and 6, and the other ports on a switching hub that has eight ports and firmware Rev. 10.01 installed

```
# lan type lan1 port-based-option=split-into-123:456:78
```

- Abbreviating the division pattern

```
# lan type lan1 port-based-option=split-into-123:456
```

- Allow jumbo frames (9000 bytes) to be used on LAN1.

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

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.40 Set the Size of the Buffer for Packets Received through the LAN Interface

[Syntax]

lan receive-buffer-size *interface size*

no lan receive-buffer-size *interface*

[Setting and Initial value]

- interface*
 - [Setting] : LAN interface name
 - [Initial value] : -
- size*
 - [Setting] : Receive buffer size (1..1000)
 - [Initial value] :
 - 128 (20 for the whole LAN interface when QoS is specified)

[Description]

Sets the size of the buffer for packets received through the LAN interface (received queue length) with the number of packets.

[Models]

RTX800

4.41 Set the Login Timer

[Syntax]

login timer *time*

no login timer [*time*]

[Setting and Initial value]

- time*
 - [Setting] :

Setting	Description
120..21474836 (RTX1200/RTX800)	The Number of seconds for automatically logging out when there is no key input
30..21474836 (other models)	
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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.42 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.43 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]

RTX3000, RTX1200, RTX1100, RTX800

4.44 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]

IDs can be used in firmware Rev.8.03.68, Rev.9.00.31 and later.
The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.45 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

Setting	Description
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

- 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.46 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]

RTX1200, RTX1100, RT107e, RTX800

4.47 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

[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]

RTX1200, RTX1100, RT107e, RTX800

4.48 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]

RTX1200, RTX1100, RT107e, RTX800

4.49 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]

RTX1200, RTX1100, RT107e, RTX800

4.50 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]

RTX1200, RTX1100, RT107e, RTX800

4.51 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]

RTX1200, RT107e, RTX800

4.52 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.

[Note]

RTX1200 loading firmware Rev.10.01.11 and later can use this function.

[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]

RTX1200, RTX800

4.53 Turn the SSH Server Function ON/OFF

[Syntax]

```
ssh service service
no ssh 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.54 Set the Listen Port of the SSH Server Function

[Syntax]

ssh listen *port*

no ssh 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.55 Set the IP Address of the Host Allowed to Access the SSH Server

[Syntax]

ssh host *ip_range* [*ip_range* ...]

no ssh 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

- [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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.56 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.57 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.58 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

Setting	Description
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.

[Note]

If the client does not support the list of algorithms that you specify for *algorithm*, you will not be able to connect to that client through SSH.

RTX1200 loading firmware Rev.10.01.11 and later can use this function.

[Models]

RTX1200, RTX800

4.59 Check Whether the SSH Client Is Alive

[Syntax]

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

no sshd 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.60 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

Setting	Description
none	Prohibit access from all hosts
LAN interface name	LAN interface name allowed to access to the 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.

RTX1200 and RTX800 loading firmware Rev. 10.01.22 and later can use this function.

[Models]

RTX1200, RTX800

4.61 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] :

RTX1100, RT107e, RTX800

group	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
small	500	187	12	125	1
middle	1332	499	33	333	1
large	2000	562	12	125	4
huge	20	0	0	1	0

RTX1200

group	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
small	2500	937	62	625	1
middle	6664	2499	166	1666	1
large	10000	2812	62	625	4

group	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
huge	20	0	0	1	0

RTX3000

group	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
small	2500	937	62	625	1
middle	6664	2499	166	1666	1
large	10000	2812	62	625	4
jumbo	10000	2812	62	625	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]

The jumbo group can be used only on models that support the 1000BASE-T LAN interface and the transmission of jumbo packets.

[Example]

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

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

4.62 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]

RTX1200, RTX800

4.63 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]

RTX1200, RTX800

4.64 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]

RTX1200, RTX800

4.65 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.

[Note]

RTX1200 loading firmware Rev.10.01.11 and later can use this function.

[Models]

RTX1200

4.66 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]

RTX1200, RTX800

4.67 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]

RTX1200, RTX800

4.68 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]

RTX1200

4.69 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

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.

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

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.

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

Chapter 6

ISDN Configuration

6.1 Common Configuration

6.1.1 Specify the BRI Line Type

[Syntax]

line type *interface line* [*channels*]

no line type *interface line* [*channels*]

[Setting and Initial value]

- *interface*
 - [Setting] : BRI interface name
 - [Initial value] : -
- *line*
 - [Setting] :

Setting	Description
isdn, isdn-ntt	ISDN circuit switch
164	Digital exclusive line, 64 kbit/s
1128	Digital exclusive line, 128 kbit/s

- [Initial value] : isdn
- *channels* : Can be specified only when the line parameter is set to isdn or isdn-ntt.
- [Setting] :

Setting	Description
1b	Use only one B channel
2b	Use both B channels

- [Initial value] : 2b

[Description]

Sets the BRI line type. The change in the setting is applied by restarting the router or executing the **interface reset** command for the corresponding interface.

[Note]

If you wish to allocate one B channel for establishing or receiving calls on the separate communication device, set the *channels* parameter to 1b.

[Models]

RTX1100

6.1.2 Set the Local ISDN Number

[Syntax]

isdn local address *interface isdn_num*[/*sub_address*]

isdn local address *interface* /*sub_address*

noisdn local address *interface*

[Setting and Initial value]

- *interface*
 - [Setting] :
 - BRI interface name
 - PRI interface name
 - [Initial value] : -
- *isdn_num*
 - [Setting] : ISDN number
 - [Initial value] : -
- *sub_address*

- [Setting] : ISDN sub address (Text string consisting of ASCII characters from 0x21 to 0x7e)
- [Initial value] : -

[Description]

Sets the local ISDN number and sub address. It is recommended that the ISDN number and sub address be set completely. Specify the ISDN number including the area code.

[Note]

It may be necessary to use only numbers in the ISDN sub address for mutual connection with other devices.

[Models]

RTX1100

6.1.3 Set the Terminator

[Syntax]

isdn terminator *interface terminator*

no isdn terminator *interface* [*terminator*]

[Setting and Initial value]

- *interface*
 - [Setting] : BRI interface name
 - [Initial value] : -
- *terminator*
 - [Setting] :

Setting	Description
on	Turn the terminator ON
off	Turn the terminator OFF

- [Initial value] : on

[Description]

Turns the terminator of the specified BRI interface ON or OFF.

[Note]

When directly connecting the router to an external DSU, be sure to turn ON the router terminator. When connecting with a bus wiring from the DSU, turn OFF the router terminator because the bus wiring normally has a terminator. However, if the router is located at the end of the bus wiring, and the bus wiring has no terminator, you must turn ON the router terminator.

[Models]

RTX1100

6.1.4 Set the Interface Used for PP

[Syntax]

pp bind *interface* [*interface*]

no pp bind [*interface*]

[Setting and Initial value]

- *interface*
 - [Setting] : A BRI interface name followed by a BRI interface name
 - [Initial value] : -

[Description]

Set the interface that is actually used for the selected destination.

[Models]

RTX1100

6.1.5 Set Transmission Restriction According to Charging Amount

[Syntax]

account threshold [*interface*] *yen*

account threshold pp *yen*

no account threshold *interface* [*yen*]

no account threshold [*yen*]

no account threshold pp [*yen*]

[Setting and Initial value]

- *interface*
 - [Setting] :
 - BRI interface name
 - PRI interface name
 - [Initial value] : -
- *yen*
 - [Setting] :

Setting	Description
Yen (1..2147483647)	Charging amount
off	Not use the transmission restriction function

- [Initial value] : off

[Description]

Stops transmission when a total charging amount notified from the network (you can display the amount with the **show account** command) reaches a specified amount.

The **account threshold** command is for setting a total amount of the whole router. When the *interface* parameter is specified, a total amount of each interface is used for control. With the **account threshold pp** command, a total amount of transmission to a selected communication partner is used for control.

Since a charging amount is notified from the network at the time of disconnection, you cannot restrict long time connection because disconnection is not allowed. In this case, you must configure the setting allowing monitoring during communication and forceful disconnection with the **isdn forced disconnect time** command. Also, a total charging amount can be reset to zero (0) with the **clear account** command. With the **schedule at** command, configure the system so that the **clear account** command is executed periodically, and you can automatically restrict the charging amount constantly every month.

[Note]

Keep in mind that all charging amount information is cleared when the router is turned OFF or restarted. A charging amount is based on charging information notified from NTT via ISDN. Therefore, when you are using a discount service, the charging amount may be different from the amount claimed by NTT. Also, when you communicate by using a carrier other than NTT, no charging information is sent.

[Models]

RTX1200

6.1.6 Set Whether to Permit Incoming PIAFS

[Syntax]

isdn piafs arrive *arrive*

no isdn piafs arrive [*arrive*]

[Setting and Initial value]

- *arrive*
 - [Setting] :

Setting	Description
on	Permit
off	Reject

- [Initial value] : on

[Description]

Sets whether to permit incoming PIAFS. When incoming PIAFS is permitted, all PIAFS methods can be received.

[Note]

A PHS terminal must be set to send a caller ID.

[Models]

RTX1100

6.1.7 Specify an Activation Side at PIAFS Connection

[Syntax]

isdn piafs control *switch*

no isdn piafs control

[Setting and Initial value]

- *switch*
- [Setting] :

Setting	Description
call	Be a PIAFS activation side when you are a sender
both	Be a PIAFS activation side when you are a sender or receiver
arrive	Be a PIAFS activation side when you are a receiver

- [Initial value] : call

[Description]

Selects a side that controls PIAFS.

[Note]

A combination of this command settings and call establishing/receiving decides whether the router is an activation side or activated side as follows:

set the <i>switch</i> parameter	call	both	arrive
When establishing a call	Time of activation	Activation side	Activated side
When receiving a call	Activated side	Activation side	Activation side

[Example]

```
# pp select 2
# isdn piafs control call
# pp enable 2
```

[Models]

RTX1100

6.1.8 Set the PIAFS Transmission Method**[Syntax]**

```
isdn piafs call speed [64kmode]
no isdn piafs call [speed [64kmode]]
```

[Setting and Initial value]

- *speed*
- [Setting] :

Setting	Description
off	Synchronous PPP transmission
32k	PIAFS 32k transmission
64k	PIAFS 64k transmission

- [Initial value] : off
- *64kmode*
- [Setting] :

Setting	Description
guarantee	The guarantee method is used for PIAFS 64k transmission
best-effort	The best-effort method is used for PIAFS 64k transmission

- [Initial value] : -

[Description]

Sets whether to enable the PIAFS mode transmission.

Selects the PIAFS mode speed also.

When *speed* is set to be off, the synchronous PPP transmission is activated. When *speed* is set to be 32k, the PIAFS 32k transmission is activated. When *speed* is set to be 64k, the PIAFS 64k transmission is activated and the *64kmode* setting is enabled.

When *64kmode* is not set, or *guarantee* is set, PIAFS 64k transmission based on the guarantee method is activated.
 When *64kmode* is set to be best-effort, transmission based on the best-effort method is activated.

[Note]

Since a special sub address is used for PIAFS 64k, an originating sub address that a user set with the command is ignored.

[Models]

RTX1100

6.2 Set the Peer Side

6.2.1 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]

RTX1200, RTX1100, RT107e, RTX800

6.2.2 Set the Remote ISDN Number

[Syntax]

isdn remote address *call_arrive* *isdn_num* [/*sub_address*] [*isdn_num_list*]

isdn remote address *call_arrive* *isdn_num* [*isdn_num_list*]

no isdn remote address *call_arrive* [*isdn_num* [/*sub_address*] [*isdn_num_list*]]

[Setting and Initial value]

- *call_arrive*

- [Setting] :

Setting	Description
call	For establishing and receiving
arrive	Receive only

- [Initial value] : -

- *isdn_num*

- [Setting] : ISDN number

- [Initial value] : -

- *sub_address*
 - [Setting] : ISDN sub address (String consisting of ASCII characters from 0x21 to 0x7e)
 - [Initial value] : -
- *isdn_num_list*
 - [Setting] : Series of ISDN numbers or combination of ISDN number and sub address delimited by a space
 - [Initial value] : -

[Description]

Sets the selected remote ISDN number and sub address. Specify the ISDN number including the area code.

This command takes no meaning if the selected remote is anonymous.

If multiple ISDN numbers are specified, a connection is made to the first ISDN number. If the connection fails, the second ISDN number is used. Likewise, the operation of using the next ISDN number when the previous number fails is repeated.

The order in which connections are attempted on multiple channels on the remote device such as with MP is specified using the **isdn remote call order** command.

[Models]

RTX1100

6.2.3 Set the Auto Connection

[Syntax]

isdn auto connect *auto*

no isdn auto connect [*auto*]

[Setting and Initial value]

- *auto*
 - [Setting] :

Setting	Description
on	Enable auto connection
off	Disable auto connection

- [Initial value] : on

[Description]

Sets whether to auto connect to the selected destination.

[Models]

RTX1100

6.2.4 Set the Order in Which Calls are Made to the Remote Device

[Syntax]

isdn remote call order *order*

no isdn remote call order [*order*]

[Setting and Initial value]

- *order*
 - [Setting] :

Setting	Description
round	Round robin method
serial	Sequential search method

- [Initial value] : serial

[Description]

This command is valid when multiple ISDN numbers are specified by the **isdn remote address call** command. When connecting to multiple channels simultaneously on the remote device such as when using MP, this command sets the order in which the ISDN numbers are selected.

If round is specified, the next ISDN number specified by this command is used on the next call after the first call to the ISDN number specified by the **isdn remote address call** command. The numbers are shifted in this manner. When a call is made to the last specified number, the next call is made to the first specified ISDN number. This operation is repeated.

If serial is specified, a call is always made to the first specified ISDN number. If the connection fails for some reason, the next ISDN number is used.

For both round and serial, if no connection is established to any destination or all channels are disconnected from the destination, the first ISDN number is used to establish a call.

[Note]

When using MP, it is more efficient to use round.

[Models]

RTX1100

6.2.5 Permit Incoming Calls

[Syntax]

isdn arrive permit *arrive* [*vrrp interface vrid*[slave]]

no isdn arrive permit [*arrive*]

[Setting and Initial value]

- *arrive*

- [Setting] :

Setting	Description
on	Permit
off	Prohibit

- [Initial value] : on

- *interface*

- [Setting] : LAN interface name

- [Initial value] : -

- *vrid*

- [Setting] : VRRP group ID (1..255)

- [Initial value] : -

[Description]

Sets whether to permit calls received from the selected destination.

It is possible to dynamically change the operation of permitting or prohibiting received calls depending on the VRRP condition by specifying on and specifying the VRRP group.

In this case, if the slave parameter is omitted, reception is permitted only when the specified VRRP group is operating as the master. If the slave parameter is specified, reception is permitted only when the specified VRRP group is operating as a slave.

[Note]

If both **isdn arrive permit** and **isdn call permit** command are set to off, communication is not possible via the ISDN line.

[Models]

RTX1100

6.2.6 Permit Outgoing Calls

[Syntax]

isdn call permit *permit*

no isdn call permit [*permit*]

[Setting and Initial value]

- *permit*

- [Setting] :

Setting	Description
on	Permit
off	Prohibit

- [Initial value] : on

[Description]

Sets whether to permit calls to the selected destination.

[Note]

If both **isdn arrive permit** and **isdn call permit** command are set to off, communication is not possible.

[Models]

RTX1100

6.2.7 Set the Call Block Timer

[Syntax]

isdn call block time *time*
no isdn call block time [*time*]

[Setting and Initial value]

- *time*
 - [Setting] : Number of seconds (0..15.0)
 - [Initial value] : 0

[Description]

Sets the time for prohibiting a call to the same destination after the communication with the selected destination is disconnected. The number of seconds can be set in unit of 0.1 seconds.

The timer specified by the **isdn call prohibit time** command applies only to the case when communication is disconnected due to an error. However, the timer specified by this command also applies to normal disconnection.

[Note]

An appropriate value should be specified in a condition in which the operation of making a call immediately after disconnection is repeated.

It is a good ideal to use this command in combination with the **isdn forced disconnect time** command.

[Models]

RTX1100

6.2.8 Set the Call Prohibit Timer after an Erroneous Disconnection

[Syntax]

isdn call prohibit time *time*
no isdn call prohibit time [*time*]

[Setting and Initial value]

- *time*
 - [Setting] : Number of seconds (60..21474836.0)
 - [Initial value] : 60

[Description]

Sets the time for prohibiting a call to the same destination when an attempt is made to call the selected destination fails. The number of seconds can be set in unit of 0.1 seconds.

The timer specified by the **isdn call block time** command is always applied after a disconnection. However the timer specified by this command applies only to the case when communication is disconnected due to an error.

[Models]

RTX1100

6.2.9 Set Whether to Make a Callback Request to the Peer

[Syntax]

isdn callback request *callback_request*
no isdn callback request [*callback_request*]

[Setting and Initial value]

- *callback_request*
 - [Setting] :

Setting	Description
on	Make a request
off	Not make a request

- [Initial value] : off

[Description]

Sets whether to make a callback request to the selected destination.

[Models]

RTX1100

6.2.10 Set Whether to Answer Callback Requests from the Destination

[Syntax]

```
isdn callback permit callback_permit
no isdn callback permit [callback_permit]
```

[Setting and Initial value]

- *callback_permit*
 - [Setting] :

Setting	Description
on	Answer
off	Not answer

- [Initial value] : off

[Description]

Sets whether to call back in response to a callback request from the selected destination.

[Models]

RTX1100

6.2.11 Set the Callback Request Type

[Syntax]

```
isdn callback request type type
no isdn callback request type [type]
```

[Setting and Initial value]

- *type*
 - [Setting] :

Setting	Description
yamaha	Yamaha type
mscbcp	MS callback

- [Initial value] : yamaha

[Description]

Sets the callback type used when making a callback request.

[Models]

RTX1100

6.2.12 Sets the Callback Permit Type

[Syntax]

```
isdn callback permit type type1 [type2]
no isdn callback permit type [type1 [type2]]
```

[Setting and Initial value]

- *type1,type2*
 - [Setting] :

Setting	Description
yamaha	Yamaha type
mscbcp	MS callback

- [Initial value] :
 - type1=yamaha
 - type2=mscbcp

[Description]

Sets the callback type that is permitted.

[Models]

RTX1100

6.2.13 Set Whether to Permit Number Designation from the User in MS Callback

[Syntax]

isdn callback msbcp user-specify *specify*
no isdn callback msbcp user-specify [*specify*]

[Setting and Initial value]

- *specify*
 - [Setting] :

Setting	Description
on	Permit
off	Reject

- [Initial value] : off

[Description]

When operating as a server, if any phone number is available for calling back, only that number is called back. However, if a call is received at a PP interface set to anonymous, no calling line identification is available, and no phone number exists for calling back, you can specify whether to call back by a number designation from the callback request side (user).

[Note]

If the setting is off and call back is not possible, a connection is established directly without calling back.

[Models]

RTX1100

6.2.14 Set the Callback Timer

[Syntax]

isdn callback response time *type time*

[Setting and Initial value]

- *type*
 - [Setting] :

Setting	Description
1b	Call back on 1B.

- [Initial value] : -
- *time*
 - [Setting] : Number of seconds (0..15.0)
 - [Initial value] : 0

[Description]

Sets the time from when a callback request is received from the selected destination until actually calling the destination. The number of seconds can be set in unit of 0.1 seconds. Sets the time from when a callback request is received from the selected destination until actually calling the destination. The number of seconds can be set in unit of 0.1 seconds.

[Models]

RTX1100

6.2.15 Set the Callback Wait Timer

[Syntax]

isdn callback wait time *time*
no isdn callback wait time [*time*]

[Setting and Initial value]

- *time*
 - [Setting] : Number of seconds (1..60.0)
 - [Initial value] : 60

[Description]

After a callback is requested to the selected destination, the request is accepted, and the line is disconnected, if a callback is not received from the destination before this timer runs out, the connection fails. The number of seconds can be set in unit of 0.1 seconds.

[Models]
RTX1100

6.2.16 Specify the Timer Type for Disconnecting the ISDN Line

[Syntax]

isdn disconnect policy *type*
no isdn disconnect policy [*type*]

[Setting and Initial value]

- type*
 - [Setting] :

Setting	Description
1	Simple traffic monitor type
2	Charging unit time type

- [Initial value] : 1

[Description]

The simple traffic monitor type is a conventional type in which the traffic is monitored by three timer commands, **isdn disconnect time**, **isdn disconnect input time**, and **isdn disconnect output time**. The line is disconnected when no packets flow for a given time.

In the charging unit time type, the charging unit time and monitor time is set using the **isdn disconnect interval time** command. If no packets flow within the monitor time, the line is disconnected at an integer multiple of the charge unit time. You can expect a reduction in the communication charge.

[Example]

```
# isdn disconnect policy 2
# isdn disconnect interval time 240 6 2
```

[Models]
RTX1100

6.2.17 Set the Disconnection Timer (Normal)

[Syntax]

isdn disconnect time *time*
no isdn disconnect time [*time*]

[Setting and Initial value]

- time*
 - [Setting] :

Setting	Description
1..21474836.0	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 destination. The number of seconds can be set in unit of 0.1 seconds.

[Note]

We denote the value set by this command as X seconds, the value specified by the **isdn disconnect input time** command as IN seconds, and the value specified by the **isdn disconnect output time** command as OUT seconds.

If the times are set as X>IN or X>OUT, the line is disconnected after X seconds when no packet input/output is observed.

[Models]
RTX1100

6.2.18 Set the Disconnection Timer (Fast)

[Syntax]

isdn fast disconnect time *time*

no no isdn fast disconnect time [*time*]

[Setting and Initial value]

- *time*
- [Setting] :

Setting	Description
1..21474836.0	Number of seconds
off	Disable the timer

- [Initial value] : 20

[Description]

When a packet is routed to a given destination and an attempt is made to call that destination, but the ISDN line is in use by another destination and the call cannot be made, this timer starts for the destination that is using the ISDN line. If no packets flow for the time specified by this timer, the destination is disconnected, and the destination waiting to be called is connected. The number of seconds can be set in unit of 0.1 seconds.

If the **isdn auto connect** is off, this timer is discarded.

[Note]

If the other device connected to the same ISDN line is using the B channel, this command may not function. In addition, if the router PP Anonymous connection is using all B channels, this command does not function when a new PP Anonymous connection is started.

[Models]

RTX1100

6.2.19 Set the Disconnection Timer (Forced)

[Syntax]

isdn forced disconnect time *time*

no isdn forced disconnect time [*time*]

[Setting and Initial value]

- *time*
- [Setting] :

Setting	Description
1..21474836.0	Number of seconds
off	Disable the timer

- [Initial value] : off

[Description]

Sets the maximum time for connecting to the selected destination. The number of seconds can be set in unit of 0.1 seconds.

If the time specified by this command elapses, the line is forcibly disconnected even if packets are being exchanged.

This timer is effective when a line cannot be automatically disconnected due to invalid packets (ping attack and so on) received from the Internet side in a dial-up connection. It is a good ideal to use this command in combination with the **isdn call block time** command.

[Models]

RTX1100

6.2.20 Set the Input Disconnection Timer (Normal)

[Syntax]

isdn disconnect input time *time*

no isdn disconnect input time [*time*]

[Setting and Initial value]

- *time*
- [Setting] :

Setting	Description
1..21474836.0	Number of seconds

Setting	Description
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 destination. The number of seconds can be set in unit of 0.1 seconds.

[Note]

For example, if a program that periodically outputs UDP packets goes into an infinite loop, the line can be disconnected by setting this timer.

See the note in 5.2.17 Set the Disconnection Timer (Normal).

[Models]

RTX1100

6.2.21 Set the Output Disconnection Timer (Normal)

[Syntax]

isdn disconnect output time *time*

no isdn disconnect output time [*time*]

[Setting and Initial value]

- *time*
 - [Setting] :

Setting	Description
1..21474836.0	Number of 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 destination. The number of seconds can be set in unit of 0.1 seconds.

[Note]

For example, if a program that periodically outputs UDP packets goes into an infinite loop, the line can be disconnected by setting this timer.

See the note in 5.2.17 Set the Disconnection Timer (Normal).

[Models]

RTX1100

6.2.22 Set the Charging Unit Time and Monitor Time for the Charging Unit Time Type

[Syntax]

isdn disconnect interval time *unit watch spare*

no isdn disconnect interval time [*unit watch spare*]

[Setting and Initial value]

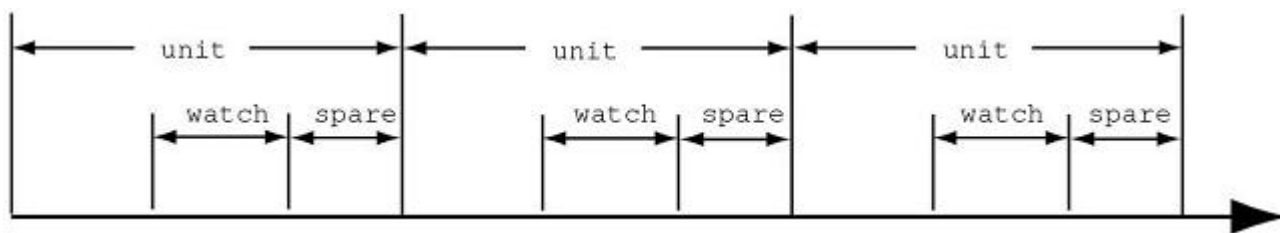
- *unit* : Charging unit time
 - [Setting] :
 - Number of seconds (1..21474836.0)
 - off
 - [Initial value] : 180
- *watch* : Monitor time
 - [Setting] :
 - Number of seconds (1..21474836.0)
 - off
 - [Initial value] : 6
- *spare* : Disconnect margin time
 - [Setting] :
 - Number of seconds (1..21474836.0)

- off
- [Initial value] : 2

[Description]

Sets the charging unit time and monitor time used in the charging unit time type. The number of seconds can be set in unit of 0.1 seconds.

See the figure below for an illustration of the different times.



The router monitors the traffic for the time specified by *watch*. If no packets flow during this time, the router disconnects the line. The parameter *spare* is used to provide a margin to prevent the actual disconnection from exceeding the unit time due to a slow disconnection procedure.

Because the time over which the line is connected is a multiple of *unit*, you can expect to reduce the communication charge as compared to using the simple traffic monitor type.

[Example]

```
# isdn disconnect policy 2
# isdn disconnect interval time 240 6 2
```

[Models]

RTX1100

Chapter 7

IP Configuration

7.1 Common Interface Settings

7.1.1 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]

RTX1200, RTX800

7.1.2 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]*
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]*]

[Setting and Initial value]

- interface*
 - [Setting] : LAN interface name, WAN interface name
 - [Initial value] : -
- loopback*
 - [Setting] : Loopback 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.

You can specify the WAN interface on RTX1200 and RTX800 loading firmware Rev.10.01.32 and later.

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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.4 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 (64..1500. 64..9578 for LAN1 and LAN2 on the RTX3000)
 - [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.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.5 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.

[Note]

Firmware Rev.10.01.22 and later can use this function.

[Models]

RTX1200, RTX800

7.1.6 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.7 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
 - anonymous
- 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"> • <i>number</i> <ul style="list-style-type: none"> • Filter number (1..21474836) (multiple numbers can be specified by delimiting each number with a space)
metric <i>metric</i>	Specify the metric <ul style="list-style-type: none"> • <i>metric</i> <ul style="list-style-type: none"> • Metric value (1..15) • 1 when omitted.
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"> • <i>weight</i> <ul style="list-style-type: none"> • Weight on the route (0..2147483647) • 1 when omitted.
keepalive	Valid only when there is reachability to <i>gateway</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.

You can specify the keepalive option on RT107e loading firmware Rev.8.03.42 and later.

You can specify the WAN interface on RTX1200 and RTX800 loading firmware Rev.10.01.32 and later.

[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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.8 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] :
 - xxx.xxx.xxx.xxx where xxx is a decimal number
 - * (the 8 bits corresponding to the net mask are zeroes. 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] : IP Destination IP address of the IP packet (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] :
 - xxx.xxx.xxx.xxx where xxx is a decimal number
 - 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=value/mask	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!=value/mask	
*	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
gopher	70
finger	79
www	80
pop3	110

Mnemonic	Port Number
sunrpc	111
ident	113
ntp	123
nntp	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540

- 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.

You can specify 'tcpsyn' for *protocol* on firmware Rev.10.00 and later.

You can specify a type and code of ICMP for the following firmware revisions:

- RTX1100 and RT107e loading Rev.8.03.68 and later
- RTX3000 loading Rev.9.00.31 and later

[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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.9 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 100)
 - [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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.10 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.11 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.12 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] : -
- *protocol* : Protocol mnemonic
 - [Setting] :
 - tcp/udp/ftp/tftp/domain/www/smtp/pop3/telnet/netmeeting

The following settings are available on firmware Rev.10.01 and later:

- 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/netmeeting/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]

RTX3000, RTX1100, RT107e

7.1.13 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]

RTX3000, RTX1100, RT107e

7.1.14 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.

The *type* option can be specified on firmware Rev.8.03.46, Rev.9.00.15, and later, and each parameter on the following firmware revisions:

Parameter	Revision
winny, default	Rev.8.03.46, Rev.9.00.15, and later
Parameters excluding the parameters above	Rev.10.01

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

Also, firmware revisions supporting this function are Rev.8.03.46, Rev.9.00.15, and later.

Concerning Share, the version 1.0 EX2 (Share TCP version) can be detected, but no other previous versions are covered.

Also, firmware revisions supporting this function are Rev.10.01.

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.15 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX800

7.1.16 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX800

7.1.17 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX800

7.1.18 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX800

7.1.19 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. The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.20 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] :
 - 400 (RTX1200 and RTX800 loading firmware versions earlier than Rev.10.01.22)
 - 1000 (other models)

[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.

RTX1200 loading firmware Rev.10.01.16 can use this function.

[Models]

RTX1200, RTX800

7.1.21 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.22 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] : Series of filter numbers delimited by spaces (Total of static filters and dynamic filters: Up to 300 for RTX3000 loading firmware Rev.9.00.47 and later, and up to 128 for the 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.

The dynamic keyword cannot be used on the RTX1200 or RTX800. For dynamic filtering, use the **ip policy filter** command.

Dynamic filtering cannot be used with a loopback or null interface.

You cannot set *direction* to 'in' for a null interface.

You can specify the WAN interface on RTX1200 and RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.23 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 ip filter 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.24 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..100)
 - [Initial value] : -
- *filter_num_list*
 - [Setting] : List of statistic filter numbers (1..100)
 - [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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.25 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 interface name
 - [Initial value] : -
- *proxyarp*
 - [Setting] :

Setting	Description
on	Enable Proxy ARP
off	Disable Proxy ARP

- [Initial value] : off
- *vrid*
 - [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.

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.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.26 Set the ARP Entry Lifetime

[Syntax]

ip arp timer timer

no ip arp timer [*timer*]

[Setting and Initial value]

- *timer*
 - [Setting] : Number of seconds of the ARP entry lifetime (30..32767)
 - [Initial value] : 1200

[Description]

Sets the ARP entry lifetime. The combination of the IP address and MAC address obtained by the ARP procedure is stored as an ARP entry. When the time specified by this command elapses, the entry is cleared. However, for models loading firmware Rev.8.02 and later and equipped with a fast path, the ARP procedure is executed again, and the entry is cleared if there is no response to the ARP.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.27 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 the MTU value of the interface
discovery	Set the value using the MTU discovery function
64..9578 (Case of LAN1 and LAN2 of RTX3000)	MTU value
64..1500 (other models)	

- [Initial value] : -

[Description]

Sets an ARP entry statically. An ARP entry set by this command is always valid. The TTL is shown as ‘permanent’ when the **show arp** command is executed. The entry is not cleared even if the **clear arp** command is executed.

If the *mtu* option is set to discovery, MTU discovery by ARP is enabled.

If the *mtu* option is omitted, the MTU of the interface is fixed.

[Note]

The *mtu* option can be specified on the RTX3000.

If the *mtu* option is set to discovery, the communication with the target host must be possible when the search is performed. If communication is not possible such as when a connection is not established with the target host, the MTU discovery fails, and the default value of 1500 bytes is used for the MTU.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.28 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 (models that support 1000BASE-T)
 - 40 (models that support the fast path function)
 - 200 (models that do not support the fast path function)

[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.

[Note]

In the previous versions released before introduction of this command, there was no upper limit for the number of transmissions that are held, and therefore, all transmissions could be held without limit.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.1.29 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.

RTX1200 loading firmware Rev.10.01.11 and later can use this function.

[Models]

RTX1200, RTX800

7.2 Setting the Remote PP Interface

7.2.1 Set the IP Address on the Remote PP Interface

[Syntax]

ip pp remote address ip_address

ip pp remote address dhcp [*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] : -

- dhcp : 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.

The number of ISDN B channels that can be used on the installed BRI/PRI interface can be specified.

This command is valid only when the PP is set to anonymous.

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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.2.2 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.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.2.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.2.4 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)

<i>option</i>	<i>value</i>	Description
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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.2.5 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.2.6 Set the Operation When Disconnection of the Exclusive Line is Detected

[Syntax]

leased keepalive down *action*

no leased keepalive down [*action*]

[Setting and Initial value]

- *action*
 - [Setting] :

Setting	Description
silent	No action
reset	Restarts the router

- [Initial value] : silent

[Description]

Sets the operation of the router when the keepalive function detects disconnection of the exclusive line.

[Models]

RTX1200

7.3 RIP Configuration

7.3.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.3.2 Set the RIP Trusted Gateway

[Syntax]

ip interface rip trust gateway [except] *gateway_list*

ip pp rip trust gateway [except] *gateway_list*

ip tunnel rip trust gateway [except] *gateway_list*

no ip interface rip trust gateway [[except] *gateway_list*]

no ip pp rip trust gateway [[except] *gateway_list*]

no ip tunnel rip trust gateway [[except] *gateway_list*]

[Setting and Initial value]

- *interface*
 - [Setting] : LAN interface name
 - [Initial value] : -
- *gateway_list*
 - [Setting] : Series of IP addresses (up to 10)
 - [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.

[Note]

Trusted and untrusted gateways are not set, and RIP from all hosts are handled as if it can be trusted.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.3.3 Set the RIP Routing Preference

[Syntax]**rip preference** *preference***no rip preference** [*preference*]**[Setting and Initial value]**

- *preference*
 - [Setting] : A value greater than or equal to 1
 - [Initial value] : 1000

[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.

[Note]

The level of preference of static routes is fixed to 10000.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.3.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.3.5 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.3.6 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.3.7 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.3.8 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]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.3.9 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]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.3.10 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]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.3.11 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 ip pp rip connect interval 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.3.12 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.3.13 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 ip pp rip disconnect interval 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.3.14 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.3.15 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]

RTX3000, RTX1200, RTX1100, RTX800

7.3.16 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]

RTX1200, RTX800

7.3.17 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]

RTX1200, RTX800

7.3.18 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 rip timer 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]
RTX1200, RTX800

7.4 VRRP Configuration

7.4.1 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] :
 - on
 - off
 - [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]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.4.2 Set the Shutdown Trigger

[Syntax]

```
ip interface vrrp shutdown trigger vrid interface
```

```

ip interface vrrp shutdown trigger vrid pp peer_num [dlci=dlci]
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] : -
- *dlci*
 - [Setting] : DLCI 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 lan keepalive .
pp type	<p>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.</p> <ul style="list-style-type: none"> • When a call is not established if the line is an ISDN line. • When the router decides by the LCP keepalive function that the peer goes down if the line is an exclusive line • When the router decides by the PVC status confirmation procedure that the specified DLCI number cannot communicate if the line is a frame relay and also “<i>dlci=dlci</i>” is specified • When the router detects that the peer is down through the pp keepalive use setting.
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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.5 Backup Configuration

7.5.1 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 uselcp-echo** command, instead of **pp always-on** command.

RT107e loading firmware Rev.8.03.42 and later can use this function.

[Models]

RTX3000, RTX1200, RTX1100, RT107e

7.5.2 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. Also, it applies to exclusive line backup and FR backup.

[Models]

RTX3000, RTX1200, RTX1100

7.5.3 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]

RTX3000, RTX1200, RTX1100

7.5.4 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]

RTX3000, RTX1200, RTX1100

7.5.5 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>	Description
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]

RTX3000, RTX1200, RTX1100

7.5.6 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]

RTX3000, RTX1200, RTX1100

7.5.7 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]

RTX3000, RTX1200, RTX1100

7.5.8 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. 1..1000 for the RTX3000.)
 - [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*
 - Can be specified on the RTX1200, RTX800, and RT107e

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] :

<i>option</i>	<i>value</i>	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.

The local-address parameter can be specified on firmware Rev.9.00.47 and later, Rev.10.01.16 and later, and Rev.8.03.87 and later.

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.

The ipsec-refresh, ipsec-refresh-up, and ipsec-refresh-down parameters can be specified on firmware Rev.8.03.68 and later.

These parameters can be specified on RTX3000 loading firmware Rev.9.00.31 and later.

The gateway-selection-rule parameter can be specified on firmware Rev.8.03.68 and later.

These parameters can be specified on RTX3000 loading firmware Rev.9.00.24 and later.

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

7.6 IGMP Configuration

7.6.1 Set IGMP for Each Interface

[Syntax]

```
ip interface igmp type [option ...]
ip pp igmp type [option...]
ip tunnel igmp type [option...]
no ip interface igmp type [option...]
no ip pp igmp type [option...]
no ip tunnel igmp type [option...]
```

[Setting and Initial value]

- *interface*
 - [Setting] : LAN interface name
 - [Initial value] : -
- *type* : IGMP operation mode
 - [Setting] :

Setting	Description
off	Disable IGMP
router	Operate as an IGMP router
host	Operate as an IGMP host

- [Initial value] : off
- *option*
 - [Setting] :
 - version=*version*
 - IGMP version

Setting	Description
2	IGMPv2
3	IGMPv3
2,3	Support both IGMPv2 and IGMPv3 (IGMPv2 compatible mode)

- `syslog=switch`
 - Whether to output detailed information to syslog

Setting	Description
on	Show
off	Not show

- `robust-variable=value`
 - Set the robust variable value specified by IGMP (1..10)
- `delay-timer=SW`
 - Timing of the forwarding of the IGMP report message

Setting	Description
on	Forward after a random delay
off	Forward immediately

- [Initial value] :
 - `version=2,3`
 - `syslog=off`
 - `robust-variable=2`
 - `delay-timer=on`

[Description]

Sets the IGMP operation of the interface.

[Note]

All revisions after firmware Rev.8.03 can use this function.

[Models]

RTX3000

7.6.2 Static IGMP Settings

[Syntax]

```
ip interface igmp static group [filter_mode [source ...]]
ip pp igmp static group [filter_mode [source...]]
ip tunnel igmp static group [filter_mode [source...]]
no ip interface igmp static group [filter_mode source...]
no ip pp igmp static group [filter_mode source...]
no ip tunnel igmp 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	INCLUDE mode of IGMP
exclude	EXCLUDE mode of IGMP

- [Initial value] : -

- *source*
- [Setting] :

Setting	Description
IPv4 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 a listener that does not support IGMP. *filter_mode* and *source* are used to limit the transmission source of multicast packets.

filter_mode and *source* are used to limit the transmission source of multicast packets. If *filter_mode* is set to include, list the transmission sources from which to receive the packets in *source*. When *source* is omitted, no request from any transmission source is received.

If *filter_mode* is set to exclude, list the transmission *source* from which to not receive the packets in *source*. When *source* is omitted, requests from all transmission sources are received.

[Note]

All revisions after firmware Rev.8.03 can use this function.

[Models]

RTX3000

7.7 PIM-SM Configuration

7.7.1 Set PIM-SM for Each Interface

[Syntax]

```
ip interface pim sparse switch [option ...]
ip pp pim sparse switch [option...]
ip tunnel pim sparse switch [option...]
no ip interface pim sparse [switch [option...]]
no ip pp pim sparse [switch [option...]]
no ip tunnel pim sparse [switch [option...]]
```

[Setting and Initial value]

- *interface*
 - [Setting] : LAN interface name
 - [Initial value] : -
- *switch* : Whether to enable PIM-SM
 - [Setting] :

Setting	Description
off	Disable
on	Enable

- [Initial value] : off

- *option*

- [Setting] :
 - *dr-priority=priority*
 - DR priority

Setting	Description
off	Not send DR priority
1..255	Priority

- *hold-time=value*
 - Hold time value (20..600)
- *register-checksum*
 - Range for calculating the register checksum

Setting	Description
all	Entire data including the multicast packets to be encapsulated
header	Only the eight bytes of the PIM header

- [Initial value] :
 - dr-priority=1
 - register-checksum=header
 - holdtime=60

[Description]

Sets the PIM-SM operation of the interface.

[Note]

All revisions after firmware Rev.8.03 can use this function.

[Models]

RTX3000

7.7.2 Specify the Static Relationship between the Group and RP

[Syntax]

```
ip pim sparse rendezvous-point static group rendezvous_point [priority=priority]
no ip pim sparse rendezvous-point static group rendezvous_point
```

[Setting and Initial value]

- *group*
 - [Setting] : IP address/mask length (the mask length can be omitted)
 - [Initial value] : -
- *rendezvous_point*
 - [Setting] : RP IP address
 - [Initial value] : -
- *priority*
 - [Setting] : Priority (1-200)
 - [Initial value] : -

[Description]

Defines statically the relationship of the RP group.

[Note]

All revisions after firmware Rev.8.03 can use this function.

[Models]

RTX3000

7.7.3 Set the Detailed Log Output Related to PIM-SM

[Syntax]

```
ip pim sparse log [option ...]
no ip pim sparse log [option ...]
```

[Setting and Initial value]

- *option* : Specify the type of detailed log type to be output
 - [Setting] :

Setting	Description
message-info	Log related to the transmission/reception of PIM messages
timer-info	Log related to the various internal timers
state-info	Log related to various status changes
data-info	Log related to the transmission/reception of DATA packets

- [Initial value] : -

[Description]

Sets the detailed log output related to PIM-SM. Multiple *option* can be selected by separating each option with a space. The log that is output by setting this command is designed to be used for detailed debugging. Basic information is output according to the rules below even if this command is not set.

If **syslog info** on is set (default setting), a log at the lowest level that can be used to check whether PIM-SM is enabled is output. If **syslog debug** on is set, a detailed operation log is output.

[Note]

All revisions after firmware Rev.8.03 can use this function.

[Models]

RTX3000

7.7.4 Set the Checksum Calculation Method of the Register

[Syntax]

ip pim sparse register-checksum *size*

no ip pim sparse register-checksum [*size*]

[Setting and Initial value]

- *size* : Checksum calculation range of the register packet
 - [Setting] :

Setting	Description
header	First eight bytes of the PIM header
all	Entire packet including IP packets that are encapsulated in the register packet

- [Initial value] : header

[Description]

Specifies the checksum calculation range of the register packet. The checksum calculation range of the register packet may vary depending on the router that is connected as the RP. Specify the calculation method to match the RP setting.

[Note]

All revisions after firmware Rev.8.03 can use this function.

[Models]

RTX3000

7.7.5 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]

RTX1200, RTX800

7.7.6 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
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]

RTX1200, RTX800

7.8 Set Packet Transfer Filters

7.8.1 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

Setting	Description
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]

The WAN interface can be specified on firmware Rev.10.01.32 and later.

[Models]

RTX1200

7.8.2 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]

The WAN interface can be specified on firmware Rev.10.01.32 and later.

[Models]
RTX1200

Chapter 8

Ethernet Filter Configuration

8.1 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)

When the source IP address of the Ethernet frame falls within the lease range of the specified DHCP scope and the source MAC address of the frame is not reserved in the scope, the frame passes through 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

8.2 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. On firmware Rev.10.01, you can specify the VLAN interface for the interface used for the LAN division function.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

8.3 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]

RTX1200, RTX800

Chapter 9

Input Cut-Off Filter Configuration

9.1 Set the Filter Definition

[Syntax]

```
ip inbound filter id action src_address[/mask] [dst_address[/mask] [protocol [src_port [dst_port]]]]
ipv6 inbound filter id action src_address[/mask] [dst_address[/mask] [protocol [src_port [dst_port]]]]
no ip inbound filter id [action [src_address[/mask] [dst_address[/mask] [protocol [src_port [dst_port]]]]]
no ipv6 inbound filter id [action [src_address[/mask] [dst_address[/mask] [protocol [src_port [dst_port]]]]]
```

[Setting and Initial value]

- *id*
 - [Setting] : Filter ID (1..65535)
 - [Initial value] : -
- *action* : Action
 - [Setting] :

Setting	Description
pass-log	Pass and log
pass-nolog	Pass without logging
reject-log	Reject and log
reject-nolog	Reject without logging
 - [Initial value] : -
- *src_address* : Source address
 - [Setting] :
 - IP address
 - * (all IP addresses)
 - 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] : -
- *dst_address* : Destination address
 - [Setting] :
 - Same format as *src_address*
 - Same as one * when omitted
 - [Initial value] : -
- *mask* : IP address bit mask (can be specified only when *src_address* and *dst_address* are network addresses)
 - [Setting] :
 - xxx.xxx.xxx.xxx where xxx is a decimal number (only valid for IPv4)
 - Hexadecimal number following 0x (only valid for IPv4)
 - Number of mask bits
 - When omitted, the maximum mask length
 - [Initial value] : -
- *protocol* : Protocol
 - [Setting] :
 - Decimal number indicating the protocol (0..255)
 - Mnemonic indicating the protocol

Mnemonic	A decimal number	Description
icmp	1	ICMP packet
icmp-error	-	icmp packet with a certain TYPE code

Mnemonic	A decimal number	Description
icmp-info	-	icmp packet with a certain TYPE code
tcp	6	TCP packet
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
udp	17	UDP packet
gre	47	gre packet of PPTP
esp	50	esp packet of IPsec
ah	51	ah packet of IPsec

- Series of above items delimited by commas (up to 5 items)
- tcpflag=flag_value/flag_mask or tcpflag!=flag_value/flag_mask

flag_value	hexadecimal value following 0x 0x0000 .. 0xffff
flag_mask	hexadecimal value following 0x 0x0000 .. 0xffff

- * (All protocols)
- Same as * when omitted.
- [Initial value] : -
- *src_port* : 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

Mnemonic	Port Number
route	520
uucpn	540

- 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)
- Same as * when omitted.
- [Initial value] : -
- *dst_port* : Destination port number
 - [Setting] :
 - Same format as *src_port*.
 - [Initial value] : -

[Description]

Defines the conditions under which packets are discarded or accepted at the entrance to the interface. You can check the settings of this command using the **ip/ipv6 interface inbound filter list** command.

[Models]

RTX1200, RTX800

9.2 Setting the Filter Application

[Syntax]

```

ip interface inbound filter list id...
ipv6 interface inbound filter list id...
ip pp inbound filter list id ...
ipv6 pp inbound filter list id ...
ip tunnel inbound filter list id ..
ipv6 tunnel inbound filter list id ..
no ip interface inbound filter list [id ...]
no ipv6 interface inbound filter list [id ...]
no ip pp inbound filter list [id ...]
no ipv6 pp inbound filter list[id ...]
no ip tunnel inbound filter list [id ...]
no ipv6 tunnel inbound filter list [id ...]
```

[Setting and Initial value]

- *interface*
 - [Setting] : LAN or WAN interface name
 - [Initial value] : -
- *id*
 - [Setting] : The ID of a filter defined by the **ip/ipv6 inbound filter** command
 - [Initial value] : -

[Description]

Limits the type of packets that the interface receives by combining packet filters specified by the **ip/ipv6 inbound filter** command.

When you specify multiple IDs, the router checks, in order, whether packets match the conditions of the **ip/ipv6 inbound filter** commands that correspond to the IDs.

[Note]

You cannot specify the WAN interface with the **ipv6 inbound filter** command.

[Models]

RTX1200, RTX800

Chapter 10

Policy Filter Configuration

10.1 Define a Service

[Syntax]

```
ip policy service id service_name protocol [source_port destination_port]
ipv6 policy service id service_name protocol [source_port destination_port]
no ip policy service id [service_name [protocol [source_port destination_port]]]
no ipv6 policy service id [service_name [protocol [source_port destination_port]]]
```

[Setting and Initial value]

- *id*
 - [Setting] : Service ID (1..65535)
 - [Initial value] : -
- *service_name*
 - [Setting] : Service name (up to 16 characters)
 - [Initial value] : -
- *protocol*
 - [Setting] : Protocol (tcp,udp,icmp,ipv6,rsvp,gre,esp,ah,icmp6,icmpv6,ospf,pim)
 - [Initial value] : -
- *source_port* : Source port number (can only be specified when the protocol is tcp or upd)
 - [Setting] :

Setting	Description
*	All
0..65535	Number
examples: 6000-, 6000-6010, -6010	Range of numbers

- [Initial value] : -
- *destination_port* : Destination port number (can only be specified when the protocol is tcp or upd)
 - [Setting] :
 - Same format as source_port.
 - [Initial value] : -

[Description]

Defines a service. You can specify the services that you define with this command using the **ip/ipv6 policy filter** and **ip/ipv6 policyservice group** commands.

[Note]

You cannot enter an integer for the service_name.

[Models]

RTX1200, RTX800

10.2 Define an Interface Group

[Syntax]

```
ip policy interface group id [name=name] [interface ...] [group group_id ...]
ipv6 policy interface group id [name=name] [interface ...] [group group_id ...]
no ip policy interface group id [name=name] [interface ...] [group group_id ...]
no ipv6 policy interface group id [name=name] [interface ...] [group group_id ...]
```

[Setting and Initial value]

- *id*
 - [Setting] : Interface group ID (1..65535)
 - [Initial value] : -
- *name*
 - [Setting] : Name (up to 32 characters)
 - [Initial value] : -

- *interface* : Interface

- [Setting] :

Setting	Description
*	All
lan*	All LAN interfaces
pp*	All PP interfaces
tunnel*	All TUNNEL interfaces
lanN-lanM	Range of LAN interfaces (example: lan1-lan3)
ppN-ppM	Range of PP interfaces (example: pp1-pp30)
tunnelN-tunnelM	Range of TUNNEL interfaces (example: tunnel1-tunnel10)
lanN	LAN interface
ppN	PP interface
tunnelN	TUNNEL interface
local	The router itself

- [Initial value] : -

- *group_id*

- [Setting] : The ID of an interface group specified by another **ip/ipv6 policy interface group** command (1 .. 65535)
- [Initial value] : -

[Description]

Defines an interface group. By entering a value for *group_id* after the group keyword, you can insert other interface groups into the current one. However, groups beyond the specified group are not referred to. You can specify the groups that you define with this command using the **ip/ipv6 policy filter** command.

[Models]

RTX1200, RTX800

10.3 Define an Address Group

[Syntax]

```

ip policy address group id [name=name] [address ...] [group group_id ...]
ipv6 policy address group id [name=name] [address ...] [group group_id ...]
no ip policy address group id [name=name] [address ...] [group group_id ...]
no ipv6 policy address group id [name=name] [address ...] [group group_id ...]

```

[Setting and Initial value]

- *id*
 - [Setting] : Address group ID (1..65535)
 - [Initial value] : -
- *name*
 - [Setting] : Name (up to 32 characters)
 - [Initial value] : -
- *address* : Addresses
 - [Setting] :

Setting	Description
*	All
IP address	Single IP address
IP address/netmasklength	Single network
IP address-IP address	IP address range

- [Initial value] : -

- *group_id*

- [Setting] : The ID of an address group specified by another **ip/ipv6 policy address group** command (1 .. 65535)
- [Initial value] : -

[Description]

Defines an address group. By entering a value for *group_id* after the group keyword, you can insert other address groups into the current one. However, groups beyond the specified group are not referred to. You can specify the groups that you define with this command using the **ip/ipv6 policy filter** command.

[Models]

RTX1200, RTX800

10.4 Define a Service Group

[Syntax]

```
ip policy service group id [name=name] [service ...] [group group_id ...]
ipv6 policy service group id [name=name] [service...] [group group_id ...]
no ip policy service group id [name=name] [service ...] [group group_id ...]
no ipv6 policy service group id [name=name] [service ...] [group group_id ...]
```

[Setting and Initial value]

- *id*
 - [Setting] : Service group ID (1..65535)
 - [Initial value] : -
- *name*
 - [Setting] : Name (up to 32 characters)
 - [Initial value] : -
- *service* : Service
 - [Setting] :

Setting	Description
*	All
Pre-defined service	http, ftp, dns, etc. The mnemonics of the ip filter command port setting can be used.
User-defined service	Names defined by the ip/ipv6 policy service command
Protocol and port numbers	tcp/port number or udp/port number

- [Initial value] : -
- *group_id*
 - [Setting] : The ID of a service group specified by another **ip/ipv6 policy service group** command (1..65535)
 - [Initial value] : -

[Description]

Defines a service group. By entering a value for *group_id* after the group keyword, you can insert other service groups into the current one. However, groups beyond the specified group are not referred to. You can specify the groups that you define with this command using the **ip/ipv6 policy filter** command.

[Models]

RTX1200, RTX800

10.5 Define a Policy Filter

[Syntax]

```
ip policy filter id action source_interface [dest_interface [source_address [dest_address [service]]]]
ipv6 policy filter id action source_interface [dest_interface [source_address [dest_address [service]]]]
no ip policy filter id [action [source_interface [dest_interface [source_address [dest_address [service]]]]]]
no ipv6 policy filter id [action [source_interface [dest_interface [source_address [dest_address [service]]]]]]
```

[Setting and Initial value]

- *id*
 - [Setting] : Policy filter ID (1 .. 65535)
 - [Initial value] : -
- *action* : Action
 - [Setting] :

Setting	Description
pass-log	Pass and log
pass-nolog	Pass without logging
reject-log	Reject and log
reject-nolog	Reject without logging
restrict-log	Pass and log only when the line is open
restrict-nolog	Pass without logging only when the line is open
static-pass-log	Pass and log without using stateful inspection
static-pass-nolog	Pass without logging and without using stateful inspection

- [Initial value] : -
- *source_interface* : Source interface
- [Setting] :

Setting	Description
*	All
lan*	All LAN interfaces
pp*	All PP interfaces
tunnel*	All TUNNEL interfaces
lanN-lanM	Range of LAN interfaces (example: lan1-lan3)
ppN-ppM	Range of PP interfaces (example: pp1-pp30)
tunnelN-tunnelM	Range of TUNNEL interfaces (example: tunnel1-tunnel10)
lanN	LAN interface
wan1	WAN interface
ppN	PP interface
tunnelN	TUNNEL interface
local	The router itself
Group number	Numbers defined by the ip/ipv6 policy interface group command

- [Initial value] : -
- *dest_interface* : Destination interface
- [Setting] :
 - The format is the same as the format for the source interface.
- [Initial value] : -
- *source_address* : Source address
- [Setting] :

Setting	Description
*	All
IP address	Single IP address
IP address/netmasklength	Single network
IP address-IP address	IP address range
Group number	Numbers defined by the ip/ipv6 policy address group command

- [Initial value] : -
- *dest_address* : Destination address
- [Setting] :
 - The format is the same as the format for the source address.
- [Initial value] : -
- *service* : Service
- [Setting] :

Setting	Description
*	All
User-defined service	Names defined by the ip/ipv6 policy service command
Protocol and port numbers	tcp/port number or udp/port number
Group number	Numbers defined by the ip/ipv6 policy service group command

- [Initial value] : -

[Description]

Defines a policy filter. “*” is used for omitted parameters.

You cannot set the interface to anonymous.

Definitions made using this command are not valid unless settings have been made using the **ip/ipv6 policy filter set** and **ip/ipv6 policy filter set enable** commands.

[Note]

The WAN interface can be specified on firmware Rev.10.01.

[Example]

Allow a PC on LAN1 to access a Web server on LAN2.

```
# ip policy filter 1 pass-log lan1 lan2 * * http
```

[Models]

RTX1200, RTX800

10.6 Define a Policy Set

[Syntax]

```
ip policy filter set id [name=name] filter_set ...
ipv6 policy filter set id [name=name] filter_set ...
no ip policy filter set id [name=name] [filter_set ...]
no ipv6 policy filter set id [name=name] [filter_set ...]
```

[Setting and Initial value]

- *id*
 - [Setting] : Policy set ID (1..65535)
 - [Initial value] : -
- *name*
 - [Setting] : Name (up to 32 characters)
 - [Initial value] : -
- *filter_set*
 - [Setting] :
 - Series of policy numbers delimited by spaces (up to 128)
 - You can express hierarchies by using square brackets.
 - [Initial value] : -

[Description]

Defines a policy set. When a new connection is established, the router determines, in order, whether the new connection matches the conditions in the policy set.

In hierarchical structures, higher-level policy filters are applied first, followed by lower-level policy filters.

You can express hierarchies using square brackets. An opening square bracket indicates movement to the next lower level, and a closing square bracket indicates movement to the next higher level.

Enter opening square brackets before numbers and closing square brackets after them.

You can enter a hyphen after a policy filter number to disable that policy filter.

You cannot use the same policy filter repeatedly.

[Example]

Only allow access from a LAN to PP interface for Website viewing.

```
#ip policy filter 1 reject-nolog lan1 pp1 * * *
#ip policy filter 2 pass-nolog * * * * www
```

```
#ip policy filter set 1 name="WWW Access" 1 [2]
```

```
#ip policy filter set enable 1
```

[Models]

RTX1200, RTX800

10.7 Enabling a Policy Set

[Syntax]

ip policy filter set enable *id*

ipv6 policy filter set enable *id*

no ip policy filter set enable [*id*]

no ipv6 policy filter set enable [*id*]

[Setting and Initial value]

- *id*
 - [Setting] : Policy set ID (1..65535)
 - [Initial value] : -

[Description]

Specifies a policy set. Only the policy set that you specify with this command is enabled. You can only enable one policy set at a time.

[Note]

Always perform this command after the contents of the currently enabled policy set have changed.

[Models]

RTX1200, RTX800

10.8 Automatically Switch Policy Sets

[Syntax]

ip policy filter set switch *original backup* trigger *trigger* ... [count=*count*] [interval=*interval*] [recoverytime=*time*]

ipv6 policy filter set switch *original backup* trigger *trigger* ... [count=*count*] [interval=*interval*] [recoverytime=*time*]

no ip policy filter set switch *original backup* [trigger *trigger* ... [count=*count*] [interval=*interval*] [recovery-time=*time*]]

no ipv6 policy filter set switch *original backup* [trigger *trigger* ... [count=*count*] [interval=*interval*] [recovery-time=*time*]]

[Setting and Initial value]

- *original*
 - [Setting] : Original policy set number (1..65535)
 - [Initial value] : -
- *backup*
 - [Setting] : Backup policy set number (1..65535)
 - [Initial value] : -
- *trigger* : Trigger for switching
 - [Setting] :

Setting	Description
winny	Detection of Winny by the unauthorized access detection function
share2	Detection of Share by the unauthorized access detection function
ethernet-filter	Discarding of an IP packet by the Ethernet filter
qos-class-control	Detection of bandwidth use by DCC (Dynamic Class Control)

- [Initial value] : -
- *count* : The number of triggers that have to be received for the policy set to be changed. The policy set is switched when the number of triggers specified by *count* are received within the time specified by *interval*.
 - [Setting] :
 - 1..10
 - [Initial value] : 1 [time]
- *interval* : The period of time over which triggers are counted. The policy set is switched when the number of triggers specified by *count* are received within the time specified by *interval*.
 - [Setting] :
 - Number of seconds (2..600)
 - [Initial value] : 5 [seconds]

- *time* : The time after the last trigger occurs until the router returns to the original policy set
- [Setting] :

Setting	Description
60..604800	Number of seconds
infinity	Never switch back to the original policy

- [Initial value] : 3600 [seconds]

[Description]

Automatically switches the policy set according to the occurrence of the event specified by the *trigger* parameter.

For the *original* and *backup* parameters, specify policy set IDs that have been defined by the **ip/ipv6 policy filter set** command.

You can change policy sets according to different events by using multiple commands as shown below.

- **ip policy filter set switch 1 2** trigger winny
- **ip policy filter set switch 1 3** trigger ethernet-filter
- **ip policy filter set switch 1 4** trigger qos-class-control

The *count* and *interval* parameters set the timing at which policy sets are switched in response to events.

The policy set is switched when the number of triggers specified by *count* are received within the time specified by *interval*.

When *count* is set to one, the policy set is switched upon the occurrence of the first event, so the setting of *interval* is irrelevant.

Use the *time* parameter to set the time after the last trigger occurs until the router returns to the original policy set.

If you set time to infinity, the router never switches back to the original policy set.

You can switch back to the original policy set by executing the **ip/ipv6 policy filter set enable** command.

After the policy set has been switched, if the settings of the **ip/ipv6 policy filter set** or **ip/ipv6 policy filter set enable** command are changed, the policy set switch is cancelled and the router switches back to the original policy.

You cannot specify the same the same policy set for both *original* and *backup*.

Also, if the policy set that you specify with *original* or *backup* is undefined, policy set switching does not take place.

[Example]

Change the policy set from 1 to 2 upon the detection of Winny or upon the discarding of an IP packet by the Ethernet filter.

```
ip policy filter set 1 name="main" 101 102 103 104 105 106
ip policy filter set 2 name="backup" 201 202 203 204 205 206
ip policy filter set switch 1 2 trigger winny ethernet-filter
```

[Models]

RTX1200, RTX800

10.9 Set the Timer

[Syntax]

```
ip policy filter timer [option=timeout ...]  
no ip policy filter timer
```

[Setting and Initial value]

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

Setting	Description
tcp-syn-timeout	Drop the session if no data flows within the specified time after receiving SYN
tcp-fin-timeout	Release the session if the specified time elapses after receiving FIN
tcp-idle-time	Drop the session if no TCP session data flows within the specified time
udp-idle-time	Drop the session if no UDP session data flows within the specified time
dns-timeout	Drop the session if no data flows within the specified time after receiving a DNS query
icmp-timeout	Drop the session if no ICMP session data flows within the specified time (applies to ping)

- [Initial value] :

- tcp-syn-timeout=30
- tcp-fin-timeout=5
- tcp-idle-time=3600
- udp-idle-time=30
- dns-timeout=5
- icmp-timeout=10
- *timeout*
 - [Setting] : Timeout value (s)
 - [Initial value] : -

[Description]

Sets the value of the timer used by the policy filter. The settings of this command are the same for both IPv4 and IPv6.

[Models]

RTX1200, RTX800

Chapter 11

URL Filter Configuration

11.1 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]

RTX1200, RTX800

11.2 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... RTX3000, up to 128 items...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 for RTX3000, and up to 128 for other models. The number entered within the command line character string length (4095 characters) is also acceptable.

Packets that do not meet any of the specified filters are discarded.

[Note]

The WAN interface can be specified on firmware Rev.10.01.32 and later.

[Models]

RTX1200, RTX800

11.3 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]

RTX1200, RTX800

11.4 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]

RTX1200, RTX800

11.5 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 (case of models other than RTX3000)
- off : Do not return an HTTP response. Use TCP RST to close the TCP session
 - [Initial value] : off (case of RTX3000)
- *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]

RTX1200, RTX800

11.6 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, pass-nolog, or reject-nolog by the **url filter** command.

[Models]

RTX1200, RTX800

Chapter 12

PPP Configuration

12.1 Set the Peer Name and Password

[Syntax]

```
pp auth username username password [myname myname mypass] [isdn1] [clid [isdn2]] [mscbcp] [ip_address]
[ip6_prefix]
pp auth username username password [myname myname mypass] [ip_address] [ip6_prefix]
no pp auth username username [password...]
```

[Setting 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] : -
- *isdn1*
 - [Setting] : Peer ISDN address
 - [Initial value] : -
- *clid* : Keyword indicating that originating number authentication is to be used
 - [Initial value] : -
- *isdn2*
 - [Setting] : ISDN address used in the originating number authentication
 - [Initial value] : -
- *mscbcp* : Keyword indicating that MS callback is permitted
 - [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.

Use the second syntax on models that do not have a BRI interface.

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.

An ISDN number can be set as an option enabling a call to be made to a routing or remote IP address associated with the name. *isdn1* is an ISDN address for calling. If *isdn1* is omitted, calls are no longer made to this peer.

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.

The `clid` keyword indicates that the originating number authentication is to be used. If this keyword is not present, originating number authentication is not carried out. The originating number authentication uses *isdn2*, if it exists or *isdn1* if it does not.

The `mscbcp` keyword indicates that MS callback is permitted. If **isdn callback permit** is set to on for calls received from this user, MS callback operation is carried out.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.2 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
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.

[Note]

On models without PPTP, only pap and chap can be specified.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.3 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.

[Note]

On models without PPTP, only pap, chap, and chap-pap can be specified.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.5 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.6 LCP Configuration

12.6.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.6.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.6.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.6.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.6.5 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.6.6 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.6.7 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.6.8 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.6.9 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.7 PAP Configuration

12.7.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.7.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.8 CHAP Configuration

12.8.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.8.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.9 IPCP Configuration

12.9.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.9.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.9.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.9.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.9.5 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.9.6 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.9.7 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.9.8 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.9.9 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]

RTX1200, RTX800

12.10 MSCBCP Configuration

12.10.1 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]

RTX3000, RTX1200, RTX1100, RTX800

12.10.2 Set the mscbcpx-maxretry Parameter

[Syntax]**ppp mscbcpx maxretry** *count***no ppp mscbcpx 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]

RTX3000, RTX1200, RTX1100, RTX800

12.11 CCP Configuration

12.11.1 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] :
 - none(RT107e)
 - stac (models other than those listed above)

[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.

On RTX3000, stac0, stac, cstac, and none can be specified.
 On RT107e, only none can be specified.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.11.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.11.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.11.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.11.5 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]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.12 IPV6CP Configuration

12.12.1 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]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.13 MP Configuration

12.13.1 Set Whether to Use MP

[Syntax]
ppp mp use *use*
no ppp mp use [*use*]

[Setting and Initial value]

- use*
 - [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : off

[Description]

Sets whether to use MP for the selected peer.
Even if on is specified, communication is established without using MP if the negotiation with the peer at the LCP step fails.

[Models]
RTX1200, RTX1100, RTX800

12.13.2 Set the MP Control Method

[Syntax]
ppp mp control *type*
no ppp mp control [*type*]

[Setting and Initial value]

- type*
 - [Setting] :

Setting	Description
arrive	Control MP if itself is the receiving end of the first B channel

Setting	Description
both	Control MP if itself is either the originating or receiving end of the first B channel
call	Control MP if itself is the originating end of the first B channel

- [Initial value] : call

[Description]

Sets the conditions for connecting/disconnecting the second B channel by controlling MP for the selected peer. Normally, the MP is controlled when itself is the originating end of the first B channel (default value).

[Models]

RTX1200, RTX1100, RTX800

12.13.3 Set the Load Threshold for MP

[Syntax]

ppp mp load threshold *call load call_count disc_load disc_count*

no ppp mp load threshold [*call_load call_count disc_load disc_count*]

[Setting and Initial value]

- *call_load*
 - [Setting] : Call load threshold percentage (1..100)
 - [Initial value] : 70
- *call_count*
 - [Setting] : Count (1..100)
 - [Initial value] : 1
- *disc_load*
 - [Setting] : Disconnect load threshold percentage (0..50)
 - [Initial value] : 30
- *disc_count*
 - [Setting] : Count (1..100)
 - [Initial value] : 2

[Description]

Sets the threshold level of the data transmission load used to call or disconnect the second B channel of [PPP, MP] for the selected peer.

The load is evaluated as a percentage of the line speed, and the larger of the two values of transmission and reception is used. If a load exceeding *call_load* is repeated the number of times specified by *call_count*, the second B channel is called. On the contrary, if a load that falls short of *disc_load* is repeated the number of times specified by *disc_count*, the second B channel is disconnected.

[Models]

RTX1200, RTX1100, RTX800

12.13.4 Set the Maximum Number of MP Links

[Syntax]

ppp mp maxlink *number*

no ppp mp maxlink [*number*]

[Setting and Initial value]

- *number*
 - [Setting] : Number of links
 - [Initial value] : 2

[Description]

Sets the minimum number of links of [PPP, MP] for the selected peer.

[Models]

RTX1200, RTX1100, RTX800

12.13.5 Set the Minimum Number of MP Links

[Syntax]

ppp mp minlink *number*

no ppp mp minlink [*number*]

[Setting and Initial value]

- *number*
 - [Setting] : Number of links
 - [Initial value] : 1

[Description]

Sets the minimum number of links of [PPP, MP] for the selected peer.

[Models]

RTX1200, RTX1100, RTX800

12.13.6 Set the Load Measurement Interval for MP

[Syntax]

ppp mp timer *time*

no ppp mp timer [*time*]

[Setting and Initial value]

- *time*
 - [Setting] : Number of seconds (1..21474836)
 - [Initial value] : 10

[Description]

Sets the load measurement interval for [PPP, MP] for the selected peer.

The unit is seconds. All MP operations are carried out at the interval specified by this command, not just the load measurement.

[Models]

RTX1200, RTX1100, RTX800

12.13.7 Set Whether to Divide MP Packets

[Syntax]

ppp mp divide *divide*

no ppp mp divide [*divide*]

[Setting and Initial value]

- *divide*
 - [Setting] :

Setting	Description
on	Divide
off	Not divide

- [Initial value] : on

[Description]

Sets whether to divide the packet when sending MP packets for [PPP, MP] for the selected peer.

Specify off only for peers that fail to connect when the packet is divided.

If the router is configured not to divide the packets, it may cause adverse effects particularly on the transmission efficiency of TCP.

Packets less than 64 bytes in length are not divided regardless of the setting of this command.

[Models]

RTX1200, RTX1100, RTX800

12.14 BACP Configuration

12.14.1 Set the bacp-restart Parameter

[Syntax]

ppp bacp restart *time*

no ppp bacp 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, BACP] for the selected peer.

[Models]

RTX1100

12.14.2 Set the bacp-max-terminate Parameter

[Syntax]

```
ppp bacp maxterminate count
no ppp bacp maxterminate [count]
```

[Setting and Initial value]

- *count*
 - [Setting] : Count (1..10)
 - [Initial value] : 2

[Description]

Sets the transmission count of terminate-request of [PPP, BACP] for the selected peer.

[Models]

RTX1100

12.14.3 Set the bacp-max-configure Parameter

[Syntax]

```
ppp bacp maxconfigure count
no ppp bacp maxconfigure [count]
```

[Setting and Initial value]

- *count*
 - [Setting] : Count (1..10)
 - [Initial value] : 10

[Description]

Sets the transmission count of configure-request of [PPP, BACP] for the selected peer.

[Models]

RTX1100

12.14.4 Set the bacp-max-failure Parameter

[Syntax]

```
ppp bacp maxfailure count
no ppp bacp maxfailure [count]
```

[Setting and Initial value]

- *count*
 - [Setting] : Count (1..10)
 - [Initial value] : 10

[Description]

Sets the transmission count of configure-nak of [PPP, BACP] for the selected peer.

[Models]

RTX1100

12.15 BAP Configuration

12.15.1 Set the bap-restart Parameter

[Syntax]

```
ppp bap restart time
no ppp bap restart [time]
```

[Setting and Initial value]

- *time*

- [Setting] : Milliseconds (20..10000)
- [Initial value] : 1000

[Description]

Sets the retransmission time of configure-request and terminate-request of [PPP, BAP] for the selected peer.

[Models]

RTX1100

12.15.2 Set the bap-max-retry Parameter

[Syntax]

ppp bap maxretry *count*
no ppp bap maxretry [*count*]

[Setting and Initial value]

- *count*
 - [Setting] : Retry count (1..30)
 - [Initial value] : 30

[Description]

Sets the maximum retry count of [PPP, BAP] for the selected peer.

[Models]

RTX1100

12.16 PPPoE Configuration

12.16.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.16.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.16.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.16.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.16.5 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.16.6 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.16.7 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.16.8 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.16.9 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.16.10 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.16.11 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

12.16.12 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]

RTX1200, RTX800

Chapter 13

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)

13.1 DHCP Server and Relay Agent Function

13.1.1 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 “1.7About the Factory Default Settings”.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.1.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.1.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.1.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.1.5 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.

On firmware Rev.8.03 and later, 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** or **dhcp delete 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

Designation using dhcp scope bind	A. B. C.	D.
Information used for client identification	Client-Identifier option	<i>chaddr</i> (*1)

*1 Limited to the case when the Client-Identifier option is not present. If the Client-Identifier option is present, this setting is discarded.

When leasing the address with **dhcp server rfc2131 compliant** on or with the *use-clientid* function enabled, the DHCP server uses the Client-Identifier option in preference to *chaddr*. Therefore, it is possible to check whether the client is using the Client-Identifier option by executing the **show status dhcp** command and checking the client identifier.

In other words, if the leased client is displayed with a MAC address, the Client-Identifier option is not used. If the client is displayed with a hexadecimal string or text string, the Client-Identifier option is used.

2. When **dhcp server rfc2131 compliant** off is specified or the use-clientid function is disabled

Designation using dhcp scope bind	(*2)	D.
Information used for client identification	(*3)	chaddr

*2 Other designation methods cannot be used.

*3 The Client-Identifier option is discarded.

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.
- When the lease information is cleared as a result of restarting the router or reconfiguring the scope, the IP address that the client uses may change when an extension for the address is requested or when the client is restarted within the lease period.
 - 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.1.6 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.

- Clients with reserved IP addresses within the scope get those addresses assigned to them.
- 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.
- 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.
 - 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.1.7 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 show status dhcp summary 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.1.8 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(RTX1200/RTX800 Rev.10.01.36 and later)
 - 1..49,64..76,85..87,128..254 (other models)
 - 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 hexadecimal 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.1.9 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.1.10 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.1.11 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.1.12 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 **dhcprelay 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.1.13 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.2 DHCP Client Function

13.2.1 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

- [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]

You can specify the WAN interface on RTX1200 and RTX800 loading firmware Rev.10.01.32 and later.
When the WAN interface is set, you cannot specify *secondary*.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.2.2 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
 - [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.
You can specify the WAN interface on RTX1200 and RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.2.3 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
 - [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. You can specify the WAN interface on RTX1200 and RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.2.4 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
 - [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]

You can specify the WAN interface on RTX1200 and RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.2.5 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
 - [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 hexadecimal
- [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] : -

[Description]

Sets the type field and ID of the DHCP client ID option.

[Note]

You can specify the WAN interface on RTX1200 and RTX800 loading firmware Rev.10.01.32 and later.
When the WAN interface is set, you cannot specify *secondary*.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.2.6 Set the Options to Be Stored in the Message That the DHCP Client Sends to the DHCP Server

[Syntax]

```
dhcp client option interface primary option=value
dhcp client option interface secondary option=value
dhcp client option pp peer_num option=value
dhcp client option pool pool_num option=value
no dhcp client option interface primary [option=value]
no dhcp client option interface secondary [option=value]
no dhcp client option pp peer_num [option=value]
no dhcp client option pool pool_num [option=value]
```

[Setting and Initial value]

- *interface*
 - [Setting] : LAN or WAN 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 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] : -

[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.
 You can specify the WAN interface on RTX1200 and RTX800 loading firmware Rev.10.01.32 and later.
 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

13.2.7 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]

RTX1200, RTX800

Chapter 14

ICMP Configuration

14.1 IPv4 Configuration

14.1.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.1.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.1.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.1.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.1.5 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.1.6 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.1.7 Set Whether to Send ICMP Time Exceeded

[Syntax]

ip icmp time-exceeded send *send*

no ip icmp time-exceeded send [*send*]

[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.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.1.8 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.1.9 Set Whether to Send ICMP Destination Unreachable

[Syntax]

ip icmp unreachable send *send*

no ip icmp unreachable send [*send*]

[Setting and Initial value]

- *send*
- [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : on

[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.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.1.10 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.1.11 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	Log
off	Not log

- [Initial value] : off

[Description]

Sets whether to record received ICMP to a debug type log.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.1.12 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.

You can specify the WAN interface on RTX1200 and RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.1.13 Set Whether to Perform MTU Discovery Using 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	Perform MTU discovery using ARP
off	Not perform MTU discovery using ARP

- [Initial value] : on
- **min_mtu**
 - [Setting] : Minimum MTU of the discovery range
 - [Initial value] : 4000

[Description]

Sets whether to perform MTU discovery using ARP.

If this command is set to on when the use of jumbo frames is enabled with the **lan type** command and the **ip mtu** command on the specified interface, the MTU of the peer is searched by repetitively sending ARP of large size to the peer that has been resolved by ARP.

[Models]

RTX3000

14.1.14 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	Not send

- [Initial value] : on

[Description]

Sets whether to send ICMP Destination Unreachable (TOO BIG) for packets that have been truncated because the length exceeded the MTU of that interface.

[Note]

On a LAN that uses jumbo frames, the maximum size of jumbo frames varies depending on the host or switching hub. Therefore, the size of jumbo frames must be aligned on all devices existing on the LAN to maintain communication.

If there is a host that has been configured to send packets that are larger than the frame size of the router by mistake, the router normally simply rejects such packets. However, by setting this command to on, the router sends ICMP error when such packets are received. However, by setting this command to on, the router sends ICMP error when such frames are received. This causes the path MTU discovery to work effectively and you can expect the host to quickly truncate the frame size.

[Models]

RTX3000

14.2 IPv6 Configuration

14.2.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.2.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.2.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.2.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.2.5 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.2.6 Set Whether to Send ICMP Time Exceeded

[Syntax]

ipv6 icmp time-exceeded send *send*
no ipv6 icmp time-exceeded send [*send*]

[Setting and Initial value]

- *send*
- [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : on

[Description]

Sets whether to send ICMP Time Exceeded.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.2.7 Set Whether to Send ICMP Destination Unreachable

[Syntax]

ipv6 icmp unreachable send *send*
no ipv6 icmp unreachable send [*send*]

[Setting and Initial value]

- *send*
- [Setting] :

Setting	Description
on	Send
off	Not send

- [Initial value] : on

[Description]

Sets whether to send ICMP Destination Unreachable.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.2.8 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	Log
off	Not log

- [Initial value] : off

[Description]

Sets whether to record received ICMP to a debug type log.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.2.9 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.2.10 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.2.11 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.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

14.2.12 Set Whether to Send ICMP Error (Packet Too Big) for Frames Truncated due to 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	Send
off	Not send

- [Initial value] : on

[Description]

Sets whether to send ICMP Packet Too Big for frames that have been truncated because the length exceeded the MTU of that interface.

[Note]

On a LAN that uses jumbo frames, the maximum size of jumbo frames varies depending on the host or switching hub. Therefore, the size of jumbo frames must be aligned on all devices existing on the LAN to maintain communication.

If there is a host that has been configured to send frames that are larger than the frame size of the router by mistake, the router normally simply rejects such frames. However, by setting this command to on, the router sends ICMP error when such frames are received. This causes the path MTU discovery to work effectively and you can expect the host to quickly truncate the frame size.

[Models]

RTX3000

Chapter 15

Tunneling

15.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

15.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

15.3 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
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.

On models without PPTP, the pptp keyword cannot be specified.

On models without L2TP/IPsec, the l2tp keyword cannot be specified.

IPUDP tunnel can be specified only for the data connect connection.

On models without the data connect connection, the ipudp keyword cannot be specified.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

15.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

15.5 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

15.6 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

Chapter 16

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"> pp enable pp disable pp select 	<==>	<ul style="list-style-type: none"> tunnel enable tunnel disable tunnel select

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
RTX3000	1-1000	1-1000
RTX1200	1-100	1-100
RTX1100	1-30	1-30
RT107e	1-6	1-6
RTX800	1-20	1-20

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.

16.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.2 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.
 RTX1200 loading firmware Rev.10.01.22 and later can use this function.

[Models]

RTX1200

16.3 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

Setting	Description
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.
RTX1200 loading firmware Rev.10.01.22 and later can use this function.

[Models]

RTX1200

16.4 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 (Rev.10.01.22 and later: up to 128 bytes/other revisions: up to 32 bytes)
 - [Initial value] : -
- *text*
 - [Setting] : Key expressed using ASCII text characters (Rev.10.01.22 and later: up to 128 characters/other revisions: up to 32 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.5 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's certificate.

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.
RTX1200 loading firmware Rev.10.01.22 and later can use this function.

[Models]

RTX1200

16.6 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.
RTX1200 loading firmware Rev.10.01.22 and later can use this function.

[Models]

RTX1200

16.7 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.
RTX1200 loading firmware Rev.10.01.22 and later can use this function.

[Models]

RTX1200

16.8 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

Setting	Description
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.
RTX1200 loading Rev.10.01.36 and later can use this function.

[Models]

RTX1200

16.9 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.10 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	ipsec ike encryption
Group	ipsec ike group
Hash algorithm	ipsec ike hash
PFS	ipsec ike pfs
Phase 1 mode	ipsec ike local name etc.

[Note]

This command does not affect operation of IKEv2.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.11 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.12 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.13 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 (RTX1200Rev.10.01.22 and later: up to 256 characters/other revisions: up to 32 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
tel	NGN telephone number(ID_IPV6_ADDR)
tel-key	NGN telephone number(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 'tel': the peer IPv6 address (ID_IPV6_ADDR) is used for determining a remote security gateway.

When the *type* parameter is 'tel-key': The setting value "ID_KEY_ID" is used for determining the remote security gateway.

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.

[Note]

The *type* parameter is available on RTX1200 loading firmware Rev.10.01.22 and later.

Models without the data connect connection function cannot use tel and tel-key for the *type* parameter.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.14 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.15 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.16 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 (RTX1200Rev.10.01.22 and later: up to 256 characters/other revisions: up to 32 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
tel	NGN telephone number(ID_IPV6_ADDR)
tel-key	NGN telephone number(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', 'tel', or 'tel-key', the router operation is similar to the case where 'key-id' is specified. When the version of IKE is IKE v2 and the *type* parameter is 'tel', the IPv6 address for its own (ID_IPV6_ADDR) is used for key exchange. When the version of IKE is IKE v2 and the *type* parameter is 'tel-key', the setting value ID_KEY_ID is used for key exchange.

[Note]

Models without the data connect connection function cannot use tel and tel-key for the *type* parameter.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.17 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. This is available on firmware Rev.8.03 and later.

[Note]

If this command is not specified, IKE is started using an IP address of an interface close to the remote security gateway.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.18 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.19 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.

RTX1200 loading firmware Rev.10.01.22 and later can use RFC4306.

The down option can be used on firmware versions Rev.10.01.16 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.20 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.21 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 (RTX3000, RTX1200, RTX800)
 - des-cbc (Other models)

[Description]

Sets the encryption algorithm used for operation of IKEv1.

If the router is to function as an initiator, the router proposes the algorithm specified by this command. If the router is to function 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]

aes256-cbc can be specified on RTX3000 loading firmware Rev.9.00.50 and later, and RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

When the router negotiates an encryption algorithm in IKEv2, it is determined dynamically regardless of this command configuration. In precise, if the router is to function as an initiator, it proposes all algorithms it supports simultaneously, and let a remote security gateway select one. Also if it is to function as a responder, it selects the safest algorithm among the proposed ones.

AES256-CBC > AES192-CBC > AES128-CBC > 3DES-CBC > DES-CBC

* Only IKEv2 supports AES192-CBC.

[Example]

```
# ipsec ike encryption 1 aes-cbc
```

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.22 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
1000...2000	RTX3000

Setting	Model
100....200	RTX1200
10...20	RTX800
8...64	Other models

- [Initial value] :
 - 2000 (RTX3000)
 - 200 (RTX1200)
 - 20 (RTX800)
 - 8 (Other models)

[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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.23 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] :
 - modp768 (RTX1100, RT107e)
 - modp1024 (Other models)

[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.

[Note]

The following models can specify only modp768 and modp1024 for the group identifier.

- RTX1100, RT107e

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.24 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 (RTX3000, RTX1200, RTX800)
 - md5 (Other models)

[Description]

Sets the hash algorithm for the IKEv1 operation.

If the router is to function as an initiator, the router proposes the algorithm specified by this command. If the router is to function 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]

sha256 can be specified on RTX1200 loading firmware 10.01.32 and later.

IKEv2 has two negotiation parameters corresponding to the IKEv1 hash algorithm, Integrity Algorithm and PRF (Pseudo-Random Function). However, when these parameters are negotiated, it is determined dynamically regardless of this command configuration. In precise, if the router is to function as an initiator, it proposes all algorithms it supports simultaneously, and let a remote security gateway select one. Also if it is to function 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
* HMAC-SHA2-256-128 is supported on RTX1200 loading firmware Rev.10.01.32 and later.
```

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
* HMAC-SHA2-256 is supported on RTX1200 loading firmware Rev.10.01.32 and later.
```

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.25 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.26 Set the IKE Payload Type

[Syntax]

```
ipsec ike payload type gateway_id type
no ipsec ike payload type gateway_id [type]
```

[Setting and Initial value]

- *gateway_id*
 - [Setting] : Security Gateway ID
 - [Initial value] : -
- *type* : Message format
 - [Setting] :

Setting	Description
1	Maintain the compatibility with release 2 of Yamaha router
2	Match release 3 of Yamaha router
3	Match the generation method of the initial vector (IV) to some implementations.

- [Initial value] : 2

[Description]

Sets the IKEv1 payload type. To connect to a Yamaha router of an old revision, the type must be set to 1.

[Note]

This command does not affect operation of IKEv2.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.27 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.28 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.29 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.30 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 (1..500)
 - [Initial value] : -
- *username*
 - [Setting] : User name (RTX1200/RTX800 loading firmware Rev.10.01.22 and later: up to 256 characters/other revisions: up to 32 characters)(between 3 and 32 characters)
 - [Initial value] : -
- *password*
 - [Setting] : Password (RTX1200/RTX800 loading firmware Rev.10.01.22 and later: up to 64 characters/other revisions: up to 32 characters)(between 3 and 32 characters)
 - [Initial value] : -

[Description]

Sets the user ID to use in IKEv1 XAUTH authentication or IKEv2 EAP-MD5 authentication.

[Models]

RTX1200, RTX800

16.31 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 (1..500)
 - [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]

RTX1200, RTX800

16.32 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 (1..500)
 - [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]

RTX1200, RTX800

16.33 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 (1..500)
 - [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>	Description
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]

RTX1200, RTX800

16.34 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]

RTX1200, RTX800

16.35 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]

RTX1200, RTX800

16.36 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.

[Note]

You cannot connect through XAUTH if *option* is specified and you use a Yamaha router or an YMS-VPN1 as the caller in a dial-up VPN.

RTX1200 loading firmware Rev.10.01.11 and later can use this function.

[Models]

RTX1200, RTX800

16.37 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.

[Note]

When the router uses YMS-VPN1 as a VPN client, it can only perform XAUTH authentication if it is configured to assign internal IP addresses.

[Models]

RTX1200, RTX800

16.38 Register the Simultaneous Connection Limit License of the VPN Client

[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 number (1..500)
 - [Initial value] : -
- *key*
 - [Setting] : Router key (up to 64 characters)
 - [Initial value] : -

[Description]

Sets a router key (license key) to accept the VPN connection from the VPN client software (YMS-VPN1-CP).

Each router key has the number of simultaneous connections granted uniquely. By registering multiple different router keys, you can reserve the number of the maximum simultaneous connections corresponding to the total of the router keys. In this case, the VPN client software can use any client key that corresponds to the router keys registered with this command.

Regardless of the client key that the VPN client software uses, connections are restricted according to the registered number of the maximum simultaneous connections corresponding to the total of the router keys.

[Note]

RTX1200 loading firmware Rev.10.01.22 and later can use this function.

[Example]

```
# tunnel select 1
# tunnel template 2-20
# ipsec tunnel 1
# ipsec sa policy 1 1 esp aes-cbc sha-hmac
# ipsec ike log 1 payload-info
# ipsec ike license-key use 1 on
# ipsec ike remote address 1 any
# ipsec ike xauth request 1 on 11
# ipsec ike mode-cfg address 1 1
# tunnel enable 1
# ipsec ike license-key 1 abcdefg-10-hijklmno
# ipsec ike license-key 2 pqrstuv-10-wxyz0123
# ipsec ike mode-cfg address pool 1 172.16.0.1-172.16.0.20/32
# auth user 1 user1 pass1
# auth user 2 user2 pass2
:
# auth user 20 user20 pass20
# auth user group 11 1-20
# auth user group attribute 11 xauth=on xauth-dns=10.10.10.1
```

[Models]

RTX1200

16.39 Apply the Simultaneous Connection Limit License of the VPN Client

[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 ID
 - [Initial value] : -
- sw
 - [Setting] :

Setting	Description
on	Permit the router key application
off	Prohibit the router key application

- [Initial value] : off

[Description]

Sets whether to permit application of the router key (license key) to accept VPN connection from the VPN client software (YMS-VPN1-CP).

When the gateway of which application of the router key is permitted is to function as a responder in the aggressive mode, the **ipsec ike remote name** command and the **ipsec ike pre-shared-key** command configurations are ignored, and a unique parameter extracted from the router key is used respectively instead. Therefore, only the VPN client software that has a corresponding client key can operate VPN connection with the relevant gateway.

[Note]

RTX1200 loading firmware Rev.10.01.22 and later can use this function.

[Models]

RTX1200

16.40 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.41 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.42 SA Configuration

Keep in mind that all SAs are cleared when the router is restarted.

16.42.1 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	IPsec SA
isakmp-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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.42.2 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] : -
- *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] : -
- *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 capsule 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.

If the router is to function as IKEv2, the *ah_algorithm* and *esp_algorithm* parameters has no effect, and these algorithms are determined dynamically at the time of negotiation.
In precise, if the router is to function as an initiator, it proposes all algorithms it supports simultaneously, and let a remote security gateway select one. Also if it is to function 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
* HMAC-SHA2-256 is supported on RTX1200 loading firmware Rev.10.01.32 and later.
- Encryption algorithm
AES256-CBC > AES192-CBC > AES128-CBC > 3DES-CBC > DES-CBC

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.
sha256-hmac and aes256-cbc can be specified on RTX1200 loading firmware Rev.10.01.32 and later.

[Example]

```
# ipsec sa policy 101 1 esp aes-cbc sha-hmac
```

[Models]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.42.3 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]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.42.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.42.5 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
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. The *force* option is available on RTX1200 loading firmware Rev.10.01.22 and later.

[Models]

RTX1200, RTX800

16.42.6 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.43 Tunnel Interface Configuration

16.43.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.43.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.43.3 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]

RTX3000, RTX1200, RTX1100

16.43.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.43.5 Set a Tunnel Template

[Syntax]

```
tunnel template tunnel_num [tunnel_num ...]
no tunnel template
```

[Setting and Initial value]

- tunnel_num
 - [Setting] : A tunnel interface number or range of tunnel interface numbers to use as a template (you can specify multiple numbers and ranges)
 - [Initial value] : -

[Description]

Set whether or not to apply the settings of selected tunnel interfaces to other tunnel interfaces as a template.

When the following parameters are the same as the tunnel interface numbers, this command converts these parameters to the numbers of the selected tunnel interfaces and applies them to the tunnel interfaces.

- The policy IDs set by the **ipsec sa policy** command
- The security gateway IDs set by commands that start with **ipsec**

When the **ipsec ike remote name** command is applied, the tunnel interface number is appended to the end of the security gateway name of the peer.

If a command has already been set for a selected interface that has been set for the template, the settings of the selected interface are given priority and applied.

The commands that are applied to other tunnel interfaces when they are set for the template interfaces are listed below.

- Commands that begin with **ipsec ike** and have a security gateway ID parameter
- **ipsec auto refresh** command (only when the security gateway ID parameter is not omitted)
- **ipsec tunnel** command
- **ipsec sa policy** command
- **tunnel enable** command

You can check how the template settings are affecting the actual settings by executing the following command.

show config tunnel *tunnel_num* expand

[Note]

This command is available on firmware Rev.8.03 and later. You can only use this command when a tunnel interface is selected.

[Example]

- About the **ipsec sa policy** Command

```
tunnel select 1
tunnel template 2-3
ipsec sa policy 1 1 esp aes-cbc sha-hmac
When the above commands are executed, the following commands are automatically enabled.
ipsec sa policy 2 2 esp aes-cbc sha-hmac
ipsec sa policy 3 3 esp aes-cbc sha-hmac
```

- About the **ipsec ike ...** Command

```
tunnel select 1
tunnel template 2-3
ipsec ike local address 1 192.168.0.1
When the above commands are executed, the following commands are automatically enabled.
ipsec ike local address 2 192.168.0.1
ipsec ike local address 3 192.168.0.1
```

- About the **ipsec ike remote name** Command

```
tunnel select 1
tunnel template 2-3
ipsec ike remote name 1 pc
When the above commands are executed, the following commands are automatically enabled.
ipsec ike remote name 2 pc2
ipsec ike remote name 3 pc3
```

- About Tunnel Interface Number Specification

You can specify individual numbers and ranges to apply the command to at the same time.

```
# tunnel template 2 4-100
# tunnel template 100 200-300 400
```

- The settings are the same in the following examples.
 - (Example 1)

```
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

```

- (Example 2)

```

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

```

[Models]

RTX1200, RTX800

16.44 Transport Mode Configuration

16.44.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

16.45 PKI Configuration

16.45.1 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.

[Note]

RTX1200 loading firmware Rev.10.01.22 and later can use this function.

[Models]

RTX1200

16.45.2 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*.

[Note]

RTX1200 loading firmware Rev.10.01.22 and later can use this function.

[Models]

RTX1200

Chapter 17

Set the 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.

17.1 Set Whether to Run L2TP/IPsec

[Syntax]

l2tp service *service*

no l2tp service [*service*]

[Setting and Initial value]

- *service*
 - [Setting] :

Setting	Description
on	L2TP/IPsec is activated.
off	L2TP/IPsec is not activated.

- [Initial value] : off

[Description]

Sets whether to run L2TP/IPsec.

When L2TP/IPsec is valid, opens the UDP port number 1701 and waits for L2TP connection.

When L2TP/IPsec is invalid, closes the UDP port number 1701 and disconnects all activated L2TP connections.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

17.2 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 31 characters)
 - [Initial value] : -

[Description]

Sets whether to carry out the L2TP tunnel authentication.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

17.3 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.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

17.4 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.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

17.5 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.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

17.6 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.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

Chapter 18

PPTP Configuration

You can only use PPTP to connect to a PC if the PC has the Microsoft Windows VPN.

18.1 Common Configuration

Refer also to the **tunnel encapsulation**, **tunnel endpoint address**, and **ppp ccp type** commands.

18.1.1 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.

RTX800 loading firmware Rev.10.01.40 and later can use this function.

[Models]

RTX1200, RTX800

18.1.2 Set the Tunnel Interfaces That Are Bound to the Peer Information Number

[Syntax]

```
pp bind 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.

Use the second syntax to bind multiple connected tunnel interfaces to use an anonymous interface to register multiple connections.

[Note]

Set PPTP 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 ptp.

RTX800 loading firmware Rev.10.01.40 and later can use this function.

[Models]

RTX1200, RTX800

18.1.3 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.

RTX800 loading firmware Rev.10.01.40 and later can use this function.

[Models]

RTX1200, RTX800

18.1.4 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.

RTX800 loading firmware Rev.10.01.40 and later can use this function.

[Models]

RTX1200, RTX800

18.1.5 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.

RTX800 loading firmware Rev.10.01.40 and later can use this function.

[Models]

RTX1200, RTX800

18.1.6 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.

RTX800 loading firmware Rev.10.01.40 and later can use this function.

[Models]

RTX1200, RTX800

18.1.7 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.

RTX800 loading firmware Rev.10.01.40 and later can use this function.

[Models]

RTX1200, RTX800

18.1.8 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.

RTX800 loading firmware Rev.10.01.40 and later can use this function.

[Models]

RTX1200, RTX800

18.2 Remote Access VPN Function

18.2.1 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.

RTX800 loading firmware Rev.10.01.40 and later can use this function.

[Models]

RTX1200, RTX800

18.2.2 Set the Tunnel Endpoint Name

[Syntax]

tunnel endpoint name [*local_name*] *remote_name* [*type*]
no tunnel endpoint name [*local_name*] *remote_name* [*type*]

[Setting and Initial value]

- *local_name*
 - [Setting] : Local name
 - [Initial value] : -
- *remote_name*
 - [Setting] : Remote name
 - [Initial value] : -
- *type* : Name type

- [Setting] :

Setting	Description
fqdn	FQDN
tel	NGN telephone number

- [Initial value] : -

[Description]

Sets the tunnel endpoint name.

[Note]

The **tunnel endpoint address** command has priority over this command.

For PPTP tunnel, set the name to a domain name (FQDN).

On models without data connect connection function, the *type* parameter cannot be specified.

[Models]

RTX1200, RTX800

18.2.3 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.

RTX800 loading firmware Rev.10.01.40 and later can use this function.

[Models]

RTX1200, RTX800

18.2.4 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.

RTX800 loading firmware Rev.10.01.40 and later can use this function.

[Models]
RTX1200, RTX800

18.2.5 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.

RTX800 loading firmware Rev.10.01.40 and later can use this function.

[Models]
RTX1200, RTX800

18.2.6 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]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

Chapter 19

Set the SIP Function

19.1 Common Configuration

19.1.1 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]

RTX1200

19.1.2 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]

RTX1200

19.1.3 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]

RTX1200

19.1.4 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]

RTX1200

19.1.5 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.
 RTX1200 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200

19.1.6 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]

RTX1200

19.1.7 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]

RTX1200

Chapter 20

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.rtpro.yamaha.co.jp/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.

20.1 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>	IP address (IPv4/IPv6)
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, 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.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

20.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

20.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

20.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

20.5 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]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

20.6 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>	IP address (IPv4/IPv6)
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, 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.

[Models]
RTX1200

20.7 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]
RTX1200

20.8 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]
RTX1200

20.9 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]
RTX1200

20.10 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]
RTX1200

20.11 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]
RTX1200

20.12 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]
RTX1200

20.13 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.

[Note]

The group option can be specified for RTX1200 loading firmware Rev.10.01.29 and later.

[Models]

RTX1200

20.14 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>	IP address (IPv4/IPv6)
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.

[Models]

RTX1200

20.15 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 used for management using VACM. The MIB view family is a group of objects 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.

[Note]

RTX1200 loading firmware Rev.10.01.29 and later can use this function.

[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]

RTX1200

20.16 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 objects that are not included in the MIB view family specified with this command is prohibited.

[Note]

RTX1200 loading firmware Rev.10.01.29 and later can use this function.

[Models]

RTX1200

20.17 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]

RTX1200

20.18 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

20.19 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

20.20 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

20.21 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 "RTX3000 with BRI module"
```

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

20.22 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

20.23 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
 - BRI 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.

[Note]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

20.24 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. To display similarly to the Rev.4 and previous revisions, set the MIB variable to “enabled(1)”. In other words, specify on with this command.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

20.25 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. To display similarly to the Rev.4 and previous revisions, set the MIB variable to “enabled(1)”. In other words, specify on with this command.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

20.26 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]

RTX1200

20.27 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

20.28 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]

RTX1200, RTX1100, RT107e, RTX800

20.29 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.

RTX1200 loading firmware Rev.10.01.29 and later can use this function.

[Models]

RTX1200, RTX800

20.30 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]

RTX1200

20.31 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]

RTX1200

20.32 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]

RTX1200

20.33 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]

RTX1200

Chapter 21

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.

21.1 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.rtpro.yamaha.co.jp>> in our WWW site.

[Models]

RTX3000, RTX1200, RTX1100, RTX800

21.2 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.rtpro.yamaha.co.jp>> in our WWW site.

[Models]

RTX3000, RTX1200, RTX1100, RTX800

21.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

21.4 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]

RTX3000, RTX1200, RTX1100, RTX800

21.5 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]

RTX3000, RTX1200, RTX1100, RTX800

21.6 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]

RTX3000, RTX1200, RTX1100, RTX800

21.7 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

21.8 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]

RTX3000, RTX1200, RTX1100, RTX800

21.9 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]

RTX3000, RTX1200, RTX1100, RTX800

Chapter 22

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.

22.1 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.

The reverse option can be specified on firmware versions Rev.8.03 and later.

You can specify the WAN interface on RTX1200 and RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

22.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

22.3 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 ip interface address command
secondary	IP address specified by the ip interface secondary address 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	○	×	×

Applied Interface	LAN	PP	Tunnel
IP address	○	○	○

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

22.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

22.5 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] : -

[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]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

22.6 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]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

22.7 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
tcp	TCP protocol
udp	UDP protocol

Setting	Description
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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

22.8 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.

[Note]

The third and sixth syntax can be specified on the following revisions:
Rev.8.03.75 and later, Rev.9.00.37 and later, and Rev.10.01

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

22.9 Set the TTL Synchronization Method of the IP Masquerade Table

[Syntax]**nat descriptor masquerade ttl hold** *type***no nat descriptor masquerade ttl hold****[Setting and Initial value]**

- *type*

- [Setting] :

Setting	Description
auto	Synchronize the TTL of the control channel and data channel of connections of applications that are auto detectable.
all	Applied to all TCP connections by the same host
ftp	Applied only to the control channels of FTP

- [Initial value] : auto

[Description]

Sets the method of synchronizing the TTL of both the control channel and data channel of both IP masquerade tables for applications that are comprised of a control channel and a data channel in order to prevent data communication failure caused by the corresponding control channel terminating while data is being transferred on the data channel.

If auto is specified, the router synchronizes the TTL of the table corresponding to the connection of an auto detectable application.

If all is specified, the router synchronizes the TTL of the table corresponding to all connections by the same host.

If ftp is specified, the router synchronizes the TTL of the table corresponding to an FTP connection.

[Note]

If all is specified, the TTLs of many tables are synchronized. Consequently the inner resource may be used up, because many tables reside in the memory.

If there is an application that does not run correctly when auto is specified, you must specify all.

[Models]

RTX1100, RT107e

22.10 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

22.11 Set the Range of Ports Used for IP Masquerade

[Syntax]

```
nat descriptor masquerade port range nat_descriptor port_range1 [port_range2 [port_range3]]
no nat descriptor masquerade port range nat_descriptor [port_range1 [port_range2 [port_range3]]]
```

[Setting and Initial value]

- *nat_descriptor*
 - [Setting] : NAT descriptor number (1..2147483647)
 - [Initial value] : -
- *port_range1, port_range2, port_range3*
 - [Setting] : Range of port numbers indicated by two port numbers with a hyphen between them
 - [Initial value] :
According to the number of simultaneous NAT sessions, the range 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

[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 of *port_range1* are in use, the port numbers in the *port_range2* range are used. When all the port numbers of *port_range1* and *port_range2* are in use, the port numbers in the *port_range3* range are used.

[Note]

On models on which the number of simultaneous NAT sessions is set to 4096, only *port_range1* can be specified. *port_range2* and 3 cannot be set or used. Likewise, on models on which the number of simultaneous NAT sessions is set to 10000, *port_range1,2* can be specified. However, *port_range3* cannot be set or used. *port_range2* and 3 can be used on the following models.

Model	Number of Simultaneous NAT Sessions
RTX3000	40000
RTX1200	20000

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

22.12 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]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

22.13 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]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

22.14 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]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

22.15 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 sip use command setting value

- [Initial value] :
 - auto (models and revisions that can specify auto)
 - on (other models)

[Description]

Sets whether to overwrite the IP address included in SIP messages using static NAT or static IP masquerade.

[Note]

auto can be specified in RTX1200 loading firmware Rev.10.01.24 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

22.16 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

22.17 Set the Number of Sessions 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..20000)(RTX1200)
 - Limit (1..4096)(other models)
 - [Initial value] :
 - 20000(RTX1200)
 - 4096(other models)

[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]

RTX1200, RTX800

Chapter 23

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**, **tracert**, **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 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 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.

23.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

23.2 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.

[Note]

To use the DNS server notified by the DHCP server, use the **dns server dhcp** command.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

23.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

23.4 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 a DNS server is specified explicitly by the **dns server** command, that setting takes precedence. If there is no response from the server specified by the **dns server** command, the router connects to the peer and receives DNS server notification.

[Note]

To use this function, the **ppp ipcp msextn** on setting is required in the peer information specified by the **dns server pp** command.

To use the DNS server notified by the DHCP server, use the **dns server dhcp** command.

[Example]

```
# pp select 2
pp2# ppp ipcp msextn on
pp2# dns server pp 2
```

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

23.5 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 dns server 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

23.6 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

23.7 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

23.8 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
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, 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</i> [/ <i>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.
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

Setting	Description
	end. In other words, if you search for matches at the beginning by specifying “NetVolante.*”, the query will return NetVolante.jp, NetVolante.rtp.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]

Multiple combinations of the contents of the DNS query, DNS query sender, peer number for checking the line connection status, and DNS server are registered as DNS servers for requesting the resolution of the DNS query so that an appropriate DNS server can be selected from the combinations according to the DNS query. The table is searched in order from the smallest number. When *query* matches the contents of the DNS query, the router attempts to resolve the DNS query using that DNS server. Once a match is found, subsequent tables are not searched. If no match is found after searching through all the tables, the DNS server specified by the **dns server** command is used.

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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

23.9 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

Setting	Description
ns	Name server
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] : -
- *ttd*
 - [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 *ttd* parameter. When the *ttd* 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.rtpo.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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

23.10 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] :
 - 53 (Firmware versions earlier than Rev.10.01)
 - 10000-10999 (Rev.10.01 and later)

[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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

23.11 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]

RTX1200, RTX800

23.12 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]
RTX1200, RTX800

23.13 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]
RTX1200, RTX800

23.14 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 commend 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.

RTX1200 and RTX800 loading firmware Rev.10.01.36 and later can use this function.

[Models]

RTX1200, RTX800

Chapter 24

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. Classes are identified by a number between 1 and 100 on the RTX3000 and 1 and 16 on 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
RTX3000	1 to 16	1 to 100
Other models	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.

On the RTX3000, the class structure can be hierarchized, and the priority control class can be placed on the secondary class. In other words, bandwidth control or priority control can be set on the primary class, and priority control can be set on the secondary class.

24.1 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.

The speed pp command cannot be used on the RTX800 or RT107e.

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

24.2 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 (RTX3000)	Class
1..16 (other models)	
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 (can be specified only on the RTX3000, RTX1100, RTX1200, and RTX800)
dscp	Classify (into class 1-9) according to the PHB that is 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 or Dynamic Traffic Control (can be specified only on the RTX3000, RTX1200, and RTX800)

- [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] :
 - IPDestination IP address of the IP packet
 - Same as one * when omitted
 - [Initial value] : -
- *dest_addr*
 - [Setting] :
 - IPDestination 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

- 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. This can be specified on the RTX3000, RTX1100, RTX800, and RTX1200.

If *class1* is set to dscp, packets that match the filter are classified according to the PHB that is defined by the DSCP value of the IP header of that packet. This can be specified on the RTX3000, RTX800, and RTX1200.

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. The *cos* parameter can be specified on RTX3000, RTX1200, RTX1100, and RTX800.

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.

The *class1* and *class2* parameters can be concatenated using a slash. The *class2* parameter can be specified on the RTX3000.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.29 can specify the dscp parameter.

[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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

24.3 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 cbq is specified, the router carries out bandwidth control on the BRI and PRI interfaces. The **queue interface class property** command is used to set the bandwidth to be allotted to each class in advance, and the router controls the transmission of the packets classified by the **queue class filter** and **queue interface class filter list** commands so that they are sent within the specified bandwidth. It can be specified only for the PP interface.

wfq is a queuing algorithm that groups the packets waiting to be sent by their source/destination IP address, protocol, and port number as flows and controls the balance of the bandwidth used by each flow. By using wfq, the degradation of the TELNET response time can be reduced as compared to when fifo is used, when a protocol that requires small bandwidth but requires fast response time such as TELNET and a protocol that requires wide bandwidth more than the response time such as FTP are used simultaneously. Another characteristic of wfq is that it does not require configuration. Because there are no parameters to be configured, detailed adjustments cannot be made as compared to priority control and bandwidth control. However, it can be easily applied to control the bandwidth balance between the flows. It can be specified only for the PP interface.

If shaping is specified, the router carries out bandwidth control on the LAN interface. It can be specified only for the LAN interface.

[Note]

RT107e	The <i>type</i> parameter can be set to fifo or priority.
RTX800	The <i>type</i> parameter can be set to fifo, priorit or shaping.

Other models	The <i>type</i> parameter can be set to fifo, priorit, cbq, wfq or shaping.
--------------	---

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

24.4 Set the MP Interleave

[Syntax]

```
ppp mp interleave [delay] switch
no ppp mp interleave [[delay] switch]
```

[Setting and Initial value]

- delay*
 - [Setting] : Delay (milliseconds)
 - [Initial value] : 30
- switch*
 - [Setting] :

Setting	Description
on	Enable MP interleave
off	Disable MP interleave

- [Initial value] : off

[Description]

Sets whether to use MP interleave. The *delay* parameter specifies the maximum delay that is allowed by the protocol that has priority. The size in which the packets are divided is determined by the *delay* value and the line speed.

[Note]

The delay specified by *delay* is not assured.
The effect can be exerted only if the same setting is made on the receiving end.
This function cannot be used simultaneously with compression. If compression is enabled, this function is ignored. Therefore, compression must be disabled as follows:

```
ppp ccp type none
```

[Example]

```
# queue class filter 1 4 ip VOIP-GATEWAY * * * *
# queue class filter 2 3 ip * * icmp * *
# queue class filter 3 1 ip * * * * *
# pp select 1
pp1# pp bind bri2.1
pp1# queue pp type priority
pp1# queue class filter list 1 2 3
pp1# isdn remote address call 03-123-4567
pp1# ppp mp use on
pp1# ppp mp interleave on
pp1# ppp mp maxlink 1
pp1# ppp ccp type none
pp1# pp enable 1
```

[Models]

RTX3000, RTX1200, RTX1100, RTX800

24.5 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

24.6 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 from class 1 to class 16 (1..10000)
 - Queue length from class 1 to class 100 for the RTX3000 (1..10000)
 - [Initial value] :
 - 200 (RTX3000, RTX1200)
 - 40 (other models)
- *len1..len16*
 - [Setting] : Queue length from class 1 to class 16 (1..10000)
 - [Initial value] : 20
- *dthreshold-mid*
 - [Setting] : Threshold value of the queue size for the middle drop preference of AF PHB (1%..100%)
 - [Initial value] : 75%
- *dthreshold-high*
 - [Setting] : Threshold value of the queue size for the high drop preference of AF PHB (1%..100%)
 - [Initial value] : 50%

[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.

For DiffServ based QoS, the values specified by the *dthreshold-mid* and *dthreshold-high* parameters become the threshold values for stacking in the queues corresponding to high and middle drop preference of AF PHB. The threshold value is expressed as a percentage of the queue length of the class.

If *dthreshold-high* is omitted, the value takes on the same value as *dthreshold-mid*. The threshold value corresponding to low drop preference is always 100%. The *dthreshold-mid* and *dthreshold-high* parameters can be specified on RTX3000 and RTX1200.

[Note]

The *dthreshold-mid* and *dthreshold-high* parameters can be specified on RTX3000 and RTX1200 loading Rev.10.01.29 and

later.

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

If the queue length of the secondary class is specified on the RTX3000 with the **queue interface length secondary** command, this queue length takes precedence.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

24.7 Set the Queue Length of the Secondary Class

[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)
 - If omitted, the queue lengths of the secondary classes belonging to all primary classes are collectively specified.
 - [Initial value] : -
- *len1...len4*
 - [Setting] : Queue length from class 1 to class 4 (1..10000)
 - [Initial value] : 200

[Description]

Specifies the number of packets that can enter the queue of the secondary class belonging to the specified primary class for the interface. For classes of which the queue length is not specified, the queue length specified last is applied.

[Models]

RTX3000

24.8 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 (1..16. 1..100 for the RTX3000)
 - [Initial value] : 2

[Description]

Specifies the class in which the packets that do not match the filters are grouped for the interface.

[Note]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

24.9 Set the Default Secondary 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)
 - If omitted, the default classes of the secondary classes belonging to all primary classes are collectively specified.
 - [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 in the secondary class belonging to the specified primary class.

[Models]

RTX3000

24.10 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 [bandwidth=bandwidth...]
no queue pp class property class [bandwidth=bandwidth...]
```

[Setting and Initial value]

- *interface*
 - [Setting] : LAN or WAN interface name
 - [Initial value] : -
- *class*
 - [Setting] : Class (1..16. 1..100 for the RTX3000)
 - [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] : -
- *parent*
 - [Setting] : Parent class number (0..16)
 - [Initial value] : 0
- *borrow* : Whether to borrow bandwidth from the parent class when the bandwidth falls short
 - [Setting] :

Setting	Description
on	Borrow
off	Not borrow

- [Initial value] : on
- *maxburst*
 - [Setting] : Maximum number of bytes that can be sent consecutively (1..10000)
 - [Initial value] : 20
- *minburst*
 - [Setting] : Maximum number of bytes that can be sent consecutively during stable transmission (1..10000)
 - [Initial value] : maxburst/10
- *packetize*
 - [Setting] : Average length of packets flowing in the class (1..10000)

- [Initial value] : 512
- *type*
 - [Setting] :

Setting	Description
priority	Specify that the class is used as a priority control class.

- [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. Dynamic Traffic Control can be used on the RTX1100, RTX3000, and RTX800.

The *parent/borrow/maxburst/minburst/packetsize* parameter is valid only when cbq is specified by the **queue interface type** command.

Class number 0 represents the root class for cbq. The root class is a virtual class with 100% bandwidth and is a parent class of other classes by default. Packets cannot be allotted directly to the root class, and the bandwidth is allotted only for the purpose of lending it to other classes.

If a class is configured to borrow bandwidth from the parent class when the bandwidth falls short (borrow = on), the maximum speed of this class can increase up to the maximum speed of the parent class. Normally, the root class having 100% of the bandwidth is the parent class. Thus, the class bandwidth can be widened to the entire line speed. In this case, the *bandwidth* setting is used as a guideline for determining the ratio by which the bandwidth is divided with other classes when the line is congested.

If a class is configured not to borrow bandwidth (borrow =off), the maximum speed of the class is set to the *bandwidth* value, and this bandwidth is never exceeded. This is effective when you wish to limit the bandwidth of a certain traffic.

The *type* parameter is valid only when shaping is specified by the **queue interface type** command. By setting the *type* parameter to priority, the class becomes a priority control class, and the packet transfer of this class takes precedence over that of the bandwidth control class even when speed allocation by bandwidth control is specified for the interface. If there are multiple classes for which the *type* parameter is set to priority, higher priority is given to classes with higher class numbers. The *type* parameter can be specified on the RTX3000.

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.

The **queue pp class property** command is not available on the RTX800.

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RTX800

24.11 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 (1..16)
 - [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 mode parameter is available on Rev.10.01.

The trigger parameter specifies the internal router event that triggers the start of control. You can specify multiple triggers delimited by commas. The trigger parameter is available on Rev.10.01.

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 is available on Rev.10.01.

[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.

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX1200, RTX800

Chapter 25

Cooperation Function

25.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

25.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

25.3 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=100000000
 - 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.

The local-address option is available on Rev.8.03.60 and later.

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

25.4 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.

Setting	Description
	Multiple numbers can be specified by separating each number with a comma. Can be specified only when the peer operation is set to client.
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. The control option can be used 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.

The local-address option is available on Rev.8.03.60 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

25.5 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.

<i>interface</i>	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.

<i>interface</i>	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.

<i>interface</i>	Interface name (LAN,TUNNEL)
<i>class</i>	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
interval	Watch interval (1-65535)[sec]. 10[sec] if omitted.
syslog	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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

25.6 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] : -
- *interval*
 - [Setting] : Interval at which the bandwidth is increased (1-65535) [sec]. 10[sec] if omitted.
 - [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*.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

25.7 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

Chapter 26

OSPF

OSPF is a type of interior gateway protocol. It is a dynamic link-state routing protocol based on a graph-theoretic model.

26.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

26.2 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]

OSPF cannot be used if a secondary address has been assigned to one of the interfaces.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

26.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

26.4 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]

Searches the LAN interface from the smallest interface number and uses the IP address of the interface that is assigned the primary IP address as the router ID.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

26.5 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

26.6 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]

Up to 100 filter numbers can be set.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

26.7 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

26.8 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)

Setting	Description
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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

26.9 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

26.10 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
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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

26.11 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

26.12 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

26.13 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
	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.

NAME	VALUE	Description
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"> COST=100000/S 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
	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.

The LOOPBACK interface can be specified on Rev.8.03 and later revisions.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

26.14 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

26.15 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

26.16 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

Chapter 27

BGP

27.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

27.2 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] :

Setting	Description
<i>ip_address/mask</i>	IP address/netmask
all	All networks

- [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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

27.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

27.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

27.5 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

27.6 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

27.7 Apply the Filter to the Route Received with BGP

[Syntax]

```
bgp export remote_as filter filter_num ...
bgp export aspath seq "aspath_regexp" filter filter_num ...
no bgp export remote_as [filter filter_num ...]
no bgp export aspath seq ["aspath_regexp" [filter filter_num ...]]
```

[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_regexp*
 - [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
```

aspath can be used on the RTX1200 and RTX800.

If this command is not specified, all routes received by BGP are discarded.

Up to 100 filter numbers can be set.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

27.8 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
ip_address/mask	IP address/netmask

Setting	Description
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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

27.9 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

27.10 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

27.11 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
ip_address/mask	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)

- [Initial value] : 1

[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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

27.12 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

- [Initial value] :
 - hold-time=180
 - metric is not sent.
 - passive=off
 - gateway not specified.
 - local-address not specified.

[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.

After the following revision and later, you can specify up to 32 routers.

- RTX1200/RTX800 : Rev.10.01.36

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

27.13 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

Chapter 28

IPv6

28.1 Common Configuration

28.1.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.1.2 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 (1280..1500. 1280..9578 for LAN1 and LAN2 on the RTX3000)
 - [Initial value] : 1500

[Description]

Sets the link MTU of the IPv6 interface.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.1.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.1.4 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]

RTX1200, RTX800

28.1.5 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.

On Rev.8.03.37 and later, the **ipv6 multicast routing process** command has been removed and incorporated into this command. Thus, when you specify fast, IPv6 multicast packets are also processed using the fast path function.

[Models]

RTX1200, RTX800

28.2 IPv6 Address Management

28.2.1 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*.

dhcp can be specified on RTX1200/RTX800 loading firmware Rev.10.01.24 and later.

address_type can be specified on RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

dhcp-prefix can be specified on RTX1200/RTX800 loading firmware Rev.10.01.24 and 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.2.2 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
 - [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*.

dhcp-prefix can be specified on RTX1200/RTX800 loading firmware 10.01.24 and later.

[Example]

Grant an RA prefix received on LAN2 to LAN1

```
# ipv6 lan1 prefix ra-prefix@lan2::/64
```

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.2.3 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
off	When operating as a client, send Solicit

- [Initial value] : off

[Description]

Sets the DHCPv6 operation at each interface.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.24 and later can use this function.

The *ir=value* option is available on RTX1200/RTX800 loading firmware Rev.10.01.36 and later.

[Models]

RTX1200, RTX800

28.2.4 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
 - [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.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.2.5 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]

RTX1200, RTX800

28.2.6 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
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]

RTX1200, RTX800

28.3 Neighbor Discovery

28.3.1 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] :
 -
- [Initial value] : 2592000
- *preferred_lifetime* : Preferred prefix lifetime
 - [Setting] :
 -

Setting	Description
0..4294967295	Rev.10.01.32 and later
60..15552000	other models

Setting	Description
0..4294967295	Rev.10.01.32 and later
60..15552000	other models

- [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 (Rev.10.01.32 and later: greater than or equal to 0 and less than or equal to 4294967295/other revisions: greater than or equal to 60 and less than or equal to 15552000) 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*.

dhcp-prefix can be specified on RTX1200/RTX800 loading firmware Rev.10.01.24 and 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.3.2 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

NAME	VALUE	Description
		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.

[Note]

On RT107e, the mtu= option cannot be specified.

The adv-retrans-time= option and the adv-cur-hop-limit= option can be specified on firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.4 Route Control

28.4.1 Add IPv6 Routing Information

[Syntax]

```

ipv6 route network gateway gateway [parameter] [gateway gateway [parameter]]
no ipv6 route network

```

[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* [*dlci=dlci*] : Route to the PP interface. When “*dlci=dlci*” is specified, a route to the frame relay DLCI.
 - *peer_num*
 - Peer number
 - anonymous
 - *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 operating as a DHCP client when using the default gateway provided by DHCP

- *tunnel tunnel_num* : Route to the tunnel interface
- [Initial value] : -
- *parameter* : Multiple parameters below can be specified by delimiting each parameter with a space
- [Setting] :

Setting	Description
<i>metric metric</i>	Specify the metric <ul style="list-style-type: none"> • <i>metric</i> <ul style="list-style-type: none"> • Metric value (1..15) • 1 when omitted.
<i>hide</i>	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]

On RT107e, the *dlci=* option of the PP interface cannot be specified.

dhcp can be specified for *gateway* on RTX1200/RTX800 loading firmware Rev.10.01.24 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.5 RIPng

28.5.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.5.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.5.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.5.4 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.5.5 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.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.5.6 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.5.7 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 ipv6 pp rip connect interval 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.5.8 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.5.9 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 ipv6 pp rip connect interval 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.5.10 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.5.11 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.5.12 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]

RTX3000, RTX1200, RTX800

28.6 Filter Configuration

28.6.1 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] : IPDestination 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

An ICMP type and code can be specified on the followings:

- RTX1100 and RT107e loading Rev.8.03.68 and later
- RTX3000 loading Rev.9.00.31 and later

icmp4 can be specified for the packet type to be filtered on the followings:

- RTX1100 and RT107e loading firmware Rev.8.03.87 and later
- RTX3000 loading firmware Rev.9.00.48 and later
- RTX1200/RTX800 loading firmware Rev.10.01.22 and later

[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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.6.2 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.

The dynamic keyword cannot be used on the RTX800. For dynamic filtering, use the `ip policy filter` command.

You cannot set *direction* to 'in' for a null interface.

The LOOPBACK interface and the NULL interface can be specified on firmware Rev.8.03 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

28.6.3 Define a Dynamic IPv6 Filter

[Syntax]

ipv6 filter dynamic *dyn_filter_num srcaddr dstaddr protocol* [*option ...*]

ipv6 filter dynamic *dyn_filter_num srcaddr dstaddr 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] : -
- *dstaddr*
 - [Setting] : Destination IPv6 address
 - [Initial value] : -
- *protocol* : Protocol mnemonic
 - [Setting] :
 - tcp/udp/ftp/tftp/domain/www/smtp/pop3/telnet

The following settings are available on firmware Rev.10.01 and later:

- 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/
- dhcpcv6c/dhpcv6s/ms-sql/netmeeting/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]

RTX3000, RTX1100, RT107e

28.7 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.

28.7.1 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]

RTX3000, RTX1200, RTX1100, RT107e

28.7.2 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 pv6 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]

RTX3000, RTX1200, RTX1100, RT107e

28.7.3 Set the IPv6 Multicast Packet Transmission Mode

[Syntax]

```

ipv6 multicast routing process mode
no ipv6 multicast routing process

```

[Setting and Initial value]

- *mode*
 - [Setting] :

Setting	Description
fast	Use fast path
normal	Use normal path

- [Initial value] : fast

[Description]

Sets the IPv6 multicast packet transmission mode.

[Note]

If the interface receiving and sending the packet is LAN or PPPoE, fast path can be used. Otherwise, normal path is used regardless of the setting of this command.
On firmware Rev.8.03.37 and later, this command was incorporated into the **ipv6 routing process** command.

[Models]

RTX1100, RT107e

28.8 Neighbor Solicitation

28.8.1 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] :

option	value	Description
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]

RTX1200, RTX800

Chapter 29

OSPFv3

29.1 Apply 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]

The OSPFv3 settings are not applied when the command is executed in the following cases.

- The router ID is not set.
- The area is not set.
- None of the interface belongs to an area.
- The area for the virtual link to traverse does not exist.
- The interface belonging to an area for the virtual link to traverse does not exist.

If this command is executed when the OSPFv3 settings are already in effect, the settings are loaded from the default condition. Routing information that the OSPFv3 holds at that point and routing information distributed to other protocols are cleared once, and operation starts from the default condition.

[Models]

RTX3000

29.2 Enable/Disable 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.

[Models]

RTX3000

29.3 Set 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]

If the router ID is not set with this command when the **ipv6 ospf configure refresh** command is executed, the LAN interface is searched in ascending order. The IPv4 address of the interface that is granted the primary IPv4 address is used as the router ID.

If there is no interface that is granted the primary IPv4 address, the router ID is not set.

[Models]

RTX3000

29.4 Set 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] : Cost of the default route (0 to 16777215)

- [Initial value] : 0

[Description]

Sets the OSPFv3 area.

If the stub keyword is specified, it indicates that the area is a stub area. The *cost* parameter is a value greater than or equal to zero. It is used as the cost of the default route for the area border router to advertise within the area. If the *cost* parameter is not specified, the default route advertisement is not carried out.

[Models]

RTX3000

29.5 Advertise 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] : No subnet range set

[Description]

The routes within the range of the subnet 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]
RTX3000

29.6 Set 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 or loopback 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 or tunnel 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), 1562 (when specifying tunnel), varies depending on the line speed for PP
 - priority=1
 - retransmit-interval=5 seconds
 - transmit-delay=1 seconds
 - 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 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 type
	point-to-point	Point-to-point type
passive		Not send OSPFv3 packets to the interface. Specify this parameter when other OSPFv3 routers are not present at the respective 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

NAME	VALUE	Description
		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. $\text{cost} = 100000/S$
priority	Priority (0...255)	Set the priority for selecting the designated router. The router with a large value is selected as the designated router. If set to 0, the router is not selected as the designated router.
retransmit-interval	Seconds (1...65535)	Specify the retransmission interval when sending LSAs consecutively.
transmit-delay	Seconds	Set the time when the LSA is sent after the link state changes in unit of seconds.
hello-interval	Seconds (1...65535)	Set the transmission interval of HELLO packets in unit of seconds.
dead-interval	Seconds (1...65535)	Set the time until the router decides that the neighbor is down when HELLO cannot be received from the neighbor.

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 can be set for the type keyword of the NAME parameter on a LAN interface. On a PP interface using PPP or tunnel interface, only point-to-point can be specified.

- Regarding passive

Specify the passive keyword when there are no other OSPFv3 routers in the link 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 link to which the interface is connected is not advertised to other OSPFv3 routers unless the **ipv6 interface ospf area** command is specified. Therefore, for a LAN interface that connects to a network that does not use OSPFv3, the **ipv6 interface ospf area** command with the passive keyword attached can be specified to advertise the route to the network to other OSPFv3 routers without using OSPFv3.

If the **ipv6 pp ospf area** command is not specified for a PP interface, the route to the link to which the interface connects 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 OSPFv3 routers.

- Regarding hello-interval/dead-interval

The hello-interval and dead-interval values must be the same among all neighbors to 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 of the router is always zero. When receiving OSPFv3 packets, the router only receives packets with the same value.

The LOOPBACK interface can be specified on Rev.8.03 and later revisions.

[Models]

RTX3000

29.7 Set 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 to be traversed
 - [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] : Series of NAME=VALUE
 - [Initial value] :
 - retransmit-interval=5 seconds
 - transmit-delay=1 seconds
 - 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	Seconds (1...65535)	Set the retransmission interval when sending LSAs consecutively in seconds.
transmit-delay	Seconds (1...65535)	Set the time when the LSA is sent after the link state changes in unit of seconds.
hello-interval	Seconds (1...65535)	Set the transmission interval of HELLO packets in unit of seconds.
dead-interval	Seconds (1...65535)	Set the time until the router decides that the peer is down when HELLO cannot be received from the peer.

[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 of the router is always zero. When receiving OSPFv3 packets, the router only receives packets with the same value.

- Regarding the output interface

If a virtual link is set, the virtual link can only be used when a global address is granted to the output interface to the area to be traversed.

[Models]
RTX3000

29.8 Set the Level of Precedence of the OSPFv3 Routing

[Syntax]

```
ipv6 ospf preference preference
no ipv6 ospf preference [preference]
```

[Setting and Initial value]

- *preference*
 - [Setting] : OSPFv3 routing preference (1...2147483647)
 - [Initial value] : 2000

[Description]

Sets the OSPFv3 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 RIPv3 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]
RTX3000

29.9 Set 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 import the route received through OSPFv3 to the routing table. The filter is evaluated in the specified order. Only the route that is determined to be imported by the first matching filter is imported in the routing table. Routes that are determined not to be imported or those that do not match any of the filters are not imported.

If this command is not specified, all routes are imported 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.

[Models]
RTX3000

29.10 Set 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 matching 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* term of the **ipv6 ospf export from** command.

The IPv6 prefix is specified using *ipv6_prefix/prefix_len*. Multiple prefixes can be specified, and they are interpreted in the method specified by *kind*.

include	Routes that match the IPv6 prefix and routes included in the IPv6 prefix are applicable.
refines	Routes included in the IPv6 prefix are applicable but not routes that match the IPv6 prefix.
equal	Only routes that match the IPv6 prefix are applicable.

If the *nr* parameter is omitted, it is assumed that the route received from OSPFv3 matches the filter when any IPv6 prefixes apply, and the route is imported. If not is specified, it is assumed that the route received from OSPFv3 matches the filter when none of the IPv6 prefixes do not apply, and the route is imported. If the reject parameter is omitted, it is assumed that the route received from OSPFv3 matches the filter when any IPv6 prefix applies, and the route is not imported.

[Note]

You must be careful when setting multiple filters with not designation using 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 IPv6 prefix is checked by the next filter specified by the **ipv6 ospf export from ospf** command. 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 matches routes other than fec0:12ab:34cd:1::/64, and the second filter matches routes other than fec0:12ab:34cd:2::/64. In other words, route fec0:12ab:34cd:1::/64 does not match the first filter but matches the second filter causing the route to be imported. On the other hand, route fec0:12ab:34cd:2::/64 matches the first filter causing the route to be imported regardless of the second filter. Therefore, all routes are imported.

If you want to not import routes fec0:12ab:34cd:1::/64 and fec0:12ab:34cd:2::/64, you must specify the commands 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
```

[Models]
RTX3000

29.11 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] : Filter number of the **ipv6 ospf import filter** command (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 filter_num of the **ipv6 ospf import filter** command. The route being imported from an external protocol is evaluated by filters in the specified order. Routes that are determined to be imported by the first matching filter are imported in OSPFv3. Routes that are determined not to be imported or those that do not match any of the filters are not imported. If the filter number after the filter keyword is omitted, all routes are imported into OSPFv3.

The parameters specified by the applicable **ipv6 ospf import filter** command are used for the metric value and metric type parameters that are used when the route is advertised. If the keywords after filter are omitted, the following parameters are used.

- metric=1
- type=2

[Models]
RTX3000

29.12 Define 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 do not 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 matching 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 to 16777215)
type = <i>type</i>	Metric type (1 or 2)

- [Initial value] : -

[Description]

Defines the filter to be applied when importing AS external routes into the OSPFv3 routing table. The filter defined by this command takes effect when it is specified by the filter term of the **ipv6 ospf import from** command.

The IPv6 prefix is specified using *ipv6_prefix/prefix_len*. Multiple prefixes can be specified, and they are interpreted in the method specified by *kind*.

include	Routes that match the IPv6 prefix and routes included in the IPv6 prefix are applicable.
refines	Routes included in the IPv6 prefix are applicable but not routes that match the IPv6 prefix.
equal	Only routes that match the IPv6 prefix are applicable.

If the *nr* parameter is omitted, it is assumed that the route received from OSPFv3 matches the filter when any IPv6 prefixes apply, and the route is imported. If not is specified, it is assumed that the route received from OSPFv3 matches the filter when none of the IPv6 prefixes do not apply, and the route is imported. If the reject parameter is omitted, it is assumed that the route received from OSPFv3 matches the filter when any IPv6 prefix applies, and the route is not imported.

The metric value and metric type can be specified by *metric* and *type* for the *parameters* when advertising the route to be imported as an AS external route of OSPFv3. If these keywords are omitted, the following values are used.

- metric=1
- type=2

[Note]

You must be careful when setting multiple filters with not designation using the **ipv6 ospf import from** command. Whether a route that matches a filter specified by not is imported is not determined by that filter, and the IPv6 prefix is checked by the next filter specified by the **ipv6 ospf import from** command. 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 matches routes other than fec0:12ab:34cd:1::/64, and the second filter matches routes other than fec0:12ab:34cd:2::/64. In other words, route fec0:12ab:34cd:1::/64 does not match the first filter but matches the second filter causing the route to be imported. On the other hand, route fec0:12ab:34cd:2::/64 matches the first filter causing the route to be imported regardless of the second filter. Therefore, all routes are imported.

If you want to not import routes fec0:12ab:34cd:1::/64 and fec0:12ab:34cd:2::/64, you must specify the commands 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
```

[Models]
RTX3000

29.13 Set the OSPFv3 Log Output

[Syntax]

```
ipv6 ospf log log ...
no ipv6 ospf log [log...]
```

[Setting and Initial value]

- log
- [Setting] :

Setting	Description
interface	Log related to the interface status or virtual link
neighbor	Log related to the status of the neighbor router
packet	Log related to OSPFv3 packets

- [Initial value] : Output none of the logs

[Description]

Sets the log output type related to OSPFv3.

[Models]
RTX3000

Chapter 30

Status Mail Notification Function

This function provides a scheme for sending information representing the router status collectively using mail. This function was originally added for the WWW browser setup function, but it can also be used from the console by setting the commands below.

30.1 Set the Operation of the Status Mail Notification Function

[Syntax]

mail-notify status use *use*
no mail-notify status use

[Setting and Initial value]

- *use*
- [Setting] :

Setting	Description
on	Enable
off	Disable

- [Initial value] : on

[Description]

Sets whether to use the status mail notification function.

[Models]

RTX3000, RTX1100

30.2 E-mail Server Settings

[Syntax]

mail-notify status server *server*
no mail-notify status server

[Setting and Initial value]

- *server*
- [Setting] : IP address or domain name of the SMTP server
- [Initial value] : -

[Description]

Sets the mail server to use on the status mail notification function.

[Models]

RTX3000, RTX1100

30.3 Set the Source Mail Address

[Syntax]

mail-notify status from *address*
no mail-notify status from

[Setting and Initial value]

- *address*
- [Setting] : Source mail address (From)
- [Initial value] : -

[Description]

Sets the source mail address to use on the status mail notification function.

[Models]

RTX3000, RTX1100

30.4 Set the Destination Mail Address

[Syntax]

mail-notify status to *id address* [*option*]

no mail-notify status to *id*

[Setting and Initial value]

- *id*
 - [Setting] : ID (1..4)
 - [Initial value] : -
- *address*
 - [Setting] : Destination mail address (To)
 - [Initial value] : -
- *option*
 - [Setting] :

Setting	Description
alert	Send only alarms

- [Initial value] : -

[Description]

Sets the destination mail address of the status mail notification function. To set multiple mail addresses, set multiple commands using different IDs.

[Models]

RTX3000, RTX1100

30.5 Set the Subject

[Syntax]

mail-notify status subject *subject*

no mail-notify status subject

[Setting and Initial value]

- *subject*
 - [Setting] : Mail subject
 - [Initial value] : -

[Description]

Sets the subject of the mail sent by the mail notification function.

[Models]

RTX3000, RTX1100

30.6 Set the Transmission Timeout

[Syntax]

mail-notify status timeout *timeout*

no mail-notify status timeout

[Setting and Initial value]

- *timeout*
 - [Setting] : Timeout value in seconds (1..180)
 - [Initial value] : 30

[Description]

Sets the time until the router decides that the mail transmission failed.

[Models]

RTX3000, RTX1100

30.7 Set the Notified Information

[Syntax]

mail-notify status type *info* [*info*...]

no mail-notify status type

[Setting and Initial value]

- *info* : Information to be notified
 - [Setting] :

Setting	Description
all	Notify all of the information
interface	Notify interface information
routing	Notify routing information
vpn	Notify the VPN information
nat	Notify NAT information
firewall	Notify the firewall information
config-log	Notify the configuration and log

- [Initial value] : all

[Description]

Sets the mail information sent by the mail notification function. If all is specified, all of the information is notified regardless of the other keywords.

[Models]

RTX3000, RTX1100

30.8 Execute the Status Mail Notification

[Syntax]

mail-notify status exec

[Description]

Sends a mail using the status mail notification function.

[Models]

RTX3000, RTX1100

Chapter 31

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.

31.1 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.

[Note]

All revisions after firmware Rev.8.03 can use this function.

[Models]

RTX3000, RTX1200, RTX1100, RTX800

31.2 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

Setting	Description
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.

[Note]

All revisions after firmware Rev.8.03 can use this function.

[Models]

RTX3000, RTX1200, RTX1100, RTX800

31.3 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.

[Note]

All revisions after firmware Rev.8.03 can use this function.

[Models]

RTX3000, RTX1200, RTX1100, RTX800

31.4 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.

[Note]

All revisions after firmware Rev.8.03 can use this function.

[Models]

RTX3000, RTX1200, RTX1100, RTX800

31.5 Set the Template Used to Send Mail

[Syntax]

mail template *template_id mailserver_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] : -
- *mailserver_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. All revisions after firmware Rev. 8.03 can use this function.

[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:RTX1500 test" "Date:Mon, 23 Feb 2004 09:54:20 +0900"
MIME-Version:1.0 "Content-Type:text/plain; charset=iso-2022-jp"
```

[Models]

RTX3000, RTX1200, RTX1100, RTX800

31.6 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 (available on firmware Rev.10.01)
 - [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 (available on firmware Rev.10.01)
 - lan(*,x)
 - pp,tunnel(*,x,xx-yy,zz etc)
 - [Initial value] : -

- *dir_i* : Unauthorized access detection setup direction (available on firmware Rev.10.01)
 - [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	pp backup command
LAN backup	lan backup command
TUNNEL backup	tunnel backup command
Route backup	ip route 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]

trigger status is available on firmware Rev.10.01.

trigger intrusion can be specified on the following revisions:

Firmware Rev.9.00.37 and later, and Rev.10.01

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[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]

RTX3000, RTX1200, RTX1100, RTX800

Chapter 32

HTTP Server Function

32.1 Common Configuration

32.1.1 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]

RTX1200, RTX1100, RT107e, RTX800

32.1.2 Set the IP Address of the Host Allowed to Access the HTTP Server

[Syntax]

```
httpd host ip_range
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
any	Allow access from all hosts
lan	Allow hosts in the network of the LAN port (LAN1) and hosts in the network of the WAN port (LAN2)
lan1	Allow hosts in the network of the LAN port (LAN1)
lan2	Allow hosts in the network of the WAN port (LAN2)
lan3	Allow hosts in the network of LAN3
wan1	Allow hosts in the network of WAN1
none	Prohibit access from all hosts

- [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.

The lan3 keyword cannot be specified on models that do not have a LAN3 interface.

You can specify the WAN interface on RTX1200 and RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX1200, RTX1100, RT107e, RTX800

32.1.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

32.1.4 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]

RTX1200, RTX1100, RT107e, RTX800

32.1.5 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 easy setup page (RT107e) and WWW browser setup assistance function (models other than the RT107e).

[Models]

RTX1200, RTX1100, RT107e, RTX800

32.2 Set the Easy Setup Page

The commands in this chapter are used to register provider connection information on the Easy Setup Page of the RT107e. The information is automatically set by clicking the Apply button. Because using the commands in this chapter changes the

information registered on the Easy Setup 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 Easy Setup 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 Easy Setup Page or by using the **show config** command.

32.2.1 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
isdn-network	PPPoE network connection
none	None

- [Initial value] : none

[Description]

Sets the provider connection type.

[Models]

RT107e

32.2.2 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]

RT107e

32.2.3 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 Easy Setup 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]

RT107e

32.2.4 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]

RT107e

32.2.5 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 Easy Setup Page.

[Models]

RT107e

32.2.6 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]

RT107e

32.2.7 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 Easy Setup.
connection	The active default route is selected only during auto connection when manual connection is made using Easy Setup. When the manual connection is disconnected, connection is made to the default destination.

- [Initial value] : off

[Description]

Command dedicated to Easy Setup. Sets the type of filter type routing that is selected on the Easy Setup Page.

[Note]

The operation is not guaranteed when specified on the console.

[Models]

RT107e

32.2.8 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] : -
- *type*
 - [Setting] : Provider information ID information (“PRV” for example)
 - [Initial value] : -
- *name*
 - [Setting] : Provider name that the user assigned, etc.
 - [Initial value] : -

[Description]

Command dedicated to Easy Setup. Sets the provider name or the like entered on the Easy Setup Page.

The *protocol* option can be omitted. If so, use a provider setting name using the IPv4 address.

[Models]

RT107e

32.2.9 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 Easy Setup.

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]

RT107e

32.2.10 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]

RT107e

32.2.11 Set Whether to Automatically Connect When the Disconnect Button Is Pressed on the Easy Setup 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 Easy Setup Page.

[Note]

If set to off, the **pp enable** command is automatically set after the manual disconnect button is pressed on the Easy Setup 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]

RT107e

32.2.12 Set Whether to Carry Out IPv6 Connection on the Easy Setup 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 Easy Setup Page.

[Note]

This command is automatically turned on when IPv6 connection is set on the Easy Setup Page.

[Models]

RT107e

Chapter 33

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.

33.1 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX1200, RTX800

33.2 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX1200, RTX800

33.3 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

33.4 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]

RTX1200, RTX800

33.5 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX1200, RTX800

33.6 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX1200, RTX800

33.7 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

33.8 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX1200, RTX800

33.9 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]

You cannot specify the subdomain.
RTX1200 loading firmware Rev.10.01.11 and later can use this function.
The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX1200, RTX800

33.10 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]

RTX1200, RTX800

33.11 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]

RTX1200, RTX800

33.12 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]
RTX1200, RTX800

33.13 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. The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

33.14 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]

RTX1200, RTX800

33.15 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]

RTX1200, RTX800

Chapter 34

UPnP Configuration

34.1 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]

RTX1200, RTX1100, RT107e, RTX800

34.2 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.

[Note]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX1200, RTX1100, RT107e, RTX800

34.3 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]

RTX1200, RTX1100, RT107e, RTX800

34.4 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]

RTX1200, RTX1100, RT107e, RTX800

34.5 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]

RTX1200, RTX1100, RT107e, RTX800

Chapter 35

USB Configuration

35.1 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]

RTX1200, RTX800

35.2 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]

RTX1200, RTX800

Chapter 36

Schedule

36.1 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...
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
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] : -
- *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 or third syntax is specified, the command operates as if the **pp select** / **tunnel select** command has been executed on the specified peer number or tunnel number 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**, **rtfs format**, **rtfs 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.

usb-attached can be specified on firmware Rev.10.01.

The *time* parameter can be used for specifying the number of seconds on firmware Rev.10.01.16 and later.

[Example]

- Allow connection only between 8:00 and 17:00 on a weekday

```
# schedule at 1 */mon-fri 8:00 pp 1 isdn auto connect on
# schedule at 2 */mon-fri 17:00 pp 1 isdn auto connect off
# schedule at 3 */mon-fri 17:05 * disconnect 1
```

- Allow connection only for 15 minutes from minute 0 of every hour

```
# schedule at 1 *:00 pp 1 isdn auto connect on
# schedule at 2 *:15 pp 1 isdn auto connect off
# schedule at 3 *:15 * disconnect 1
```

- Switch 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
```

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

Chapter 37

VLAN Configuration

37.1 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 (RTX3000, RTX1200), 1-8 (Other models)
 - [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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

37.2 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]

RTX1200

Chapter 38

Heartbeat Function

38.1 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]

RTX1200, RTX800

38.2 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]

RTX1200, RTX800

38.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

Chapter 39

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.

39.1 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

39.2 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

39.3 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

39.4 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

39.5 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

39.6 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

39.7 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

39.8 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

39.9 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

39.10 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 (64..10000 on the RTX3000. 64..1000 on other models.)
 - [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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

39.11 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

39.12 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

Chapter 40

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.

40.1 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]

RTX1200, RTX800

40.2 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
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
any	Allow access from all hosts
lan	Allow access from hosts in all LAN networks
lan1	Allow access from hosts in the LAN1 network
lan2	Allow access from hosts in the LAN2 network
lan3	Allow access from hosts in the LAN3 network (on devices that have a LAN3 interface)
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.
The lan3 keyword cannot be specified on models that do not have a LAN3 interface.

[Models]

RTX1200, RTX800

Chapter 41

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.

On firmware Rev.10.01 and later, the following operations are also possible.

- 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 ping 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.rtpro.yamaha.co.jp>

41.1 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]

RTX1200

41.2 Set the Prefix for Statistical Information Files Saved to the External Memory

[Syntax]

external-memory statistics filename prefix *prefix* [*term*] [*crypto password*]

no external-memory statistics filename prefix [*prefix* [*term*] [*crypto password*]]

[Setting and Initial value]

- *prefix* : The file name prefix (alphanumeric characters only)
 - [Setting] :

Setting	Description
usb1: <i>filename</i>	The file name prefix
sd1: <i>filename</i>	The file name prefix

- [Initial value] : -
- *term* : The period of data to include in a single file
 - [Setting] :

Setting	Description
monthly	A month's worth of data
daily	A day's worth of data

- [Initial value] : monthly
- *crypto* : Encryption algorithm (if you want to encrypt the file)
 - [Setting] :

Setting	Description
aes128	Encrypt using AES128.
aes256	Encrypt using AES256.

- [Initial value] : -
- *password*
 - [Setting] : Password for the encrypted file expressed using ASCII text characters (between 8 and 32 characters in length)
 - [Initial value] : -

[Description]

Sets the prefix for statistical information files.

The actual file name is determined automatically based on this prefix.

For example, if you set the prefix to “yamaha”, a file containing the traffic levels on the LAN2 interface will be named “yamaha_traffic_lan2_20080708.csv”.

If you do not want to encrypt files, you must not specify the *crypto* or *password* parameters.

[Note]*term*

If you set TERM to daily, a new file will be created each day. However, you must be careful, because the number of statistical information files is limited to 100, and if you do not limit the types of files that are created or delete files frequently, the number of files will reach the limit very quickly.

In the actual file name, strings indicating the type of file and the date follow the *prefix*.

The file name format is indicated below. *prefix_type[_id]_yyyymm[dd].ext*

- *prefix*
 - A string that you set using this command
- *type*
 - The statistical information type

cpu	CPU usage
memory	Memory usage
flow	Number of fast path flows
route	Number of routes
nat	Number of NAT table entries

filter	Number of sessions of dynamic filter
traffic	Traffic levels for each interface
qos	Traffic levels for each QoS class

- *id*
 - the meaning of the *id* parameter varies depending on the type of statistical information.
 - Traffic levels for each interface.....Indicates the interface
 - Traffic levels for each QoS class.....Indicates the interface and the class
 - The *id* is omitted for all other statistical information.
- *yyyy*
 - Year according to the Gregorian calendar (4 digits)
- *mm*
 - Month (2 digits)
- *dd*
 - Day (2 digits)
 - The *dd* parameter is omitted for files that are divided monthly.
- *ext*
 - Extension

csv	CSV
rtfg	Encrypted file

On Rev.10.01.32 and later, the number of characters that can be specified for *prefix* is up to 15 characters excluding a prefix such as “usb1:”

On the other revisions, the number of characters that can be specified for *prefix* is up to 15 characters including a prefix such as “usb1:”

[Models]

RTX1200, RTX800

41.3 Set the Name of the Syslog File to Save to the External Memory

[Syntax]

external-memory syslog filename *name* [*crypto password*] [*limit=size*] [*backup=num*]

no external-memory syslog filename [*name*]

[Setting and Initial value]

- *name* : Syslog filename
- [Setting] :

Setting	Description
usb1: <i>filename</i>	The name of a file in the USB memory (filename must be 64 characters or less. You cannot specify a filename that includes a .bak extension.)
sd1: <i>filename</i>	The name of a file in the microSD memory card (filename must be 64 characters or less. You cannot specify a filename that includes a .bak extension.)

- [Initial value] : -
- *crypto* : If you want to encrypt the syslog, specify 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] : -
- *size*
 - [Setting] : Maximum size of SYSLOG file (1 MB to 1024 MB)

- [Initial value] : 10
- *num*
 - [Setting] : Maximum number of backup files (1 - 100)
 - [Initial value] : 10

[Description]

Set the name of the syslog file to save to the external memory.

You cannot specify a file name containing the .bak extension in *name*. Also, when you don't perform encryption, you cannot specify a file name containing the .rtfg extension in *name*.

If you specify *crypto* and *password*, the syslog is encrypted before it is saved to the external memory. When you encrypt a file, you must specify a *name* whose extension is .rtfg or leave out the extension. If you leave out the extension, the .rtfg extension is automatically added to the filename.

When a SYSLOG file size reaches the maximum, the SYSLOG file backup starts. A name of the backup file created in this case varies according to firmware.

When the number of backup files reaches the maximum number specified in *num*, or when an external memory has no available memory, the oldest backup file is deleted and then, a new backup file is created.

On RTX1200, you cannot specify the optional *size* or *num* since each parameter is fixed. Individually, *size* is always 1,024 (MB), and *num* is always 1. Also, a name of the backup file is determined based on the following rules:

If *name* has an extension:

- Save without encryption ... The extension is changed to .bak
- Encrypt and save ... Add _bak before the extension

When *name* contains no extension: ... Add the .bak extension

If this command is not specified, SYSLOG is not written into the external memory.

[Note]

When you change the settings listed below, you must also change the *name*.

- When you switch from saving an unencrypted syslog to saving an encrypted syslog.
- When you switch from saving an encrypted syslog to saving an unencrypted syslog.
- When you change the encryption algorithm or the password.

On RTX1200/RTX800 loading firmware Rev.10.01.32 and later, the number of characters used for *name* is up to 99 characters. On the other revisions, the number of characters used for *name* is up to 64 characters.

[Models]

RTX1200, RTX800

41.4 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]
RTX1200, RTX800

41.5 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]
RTX1200

41.6 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
- 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.

On RTX1200/RTX800 loading firmware Rev.10.01.32 and later, the number of characters used for *filename* is up to 99 characters.

On the other revisions, the number of characters used for *filename* is up to 64 characters.

[Example]

- Search for the “rtx1200.bin” file on the microSD card and load it as the firmware file.

```
# external-memory exec filename sd1:rtx1200.bin
```

- Search for the “rtx1200.bin” file in the “test” directory of the microSD card and load it as the firmware file.

```
# external-memory exec filename sd1:/test/rtx1200.bin
```

[Models]

RTX1200, RTX800

41.7 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
- 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.

On RTX1200/RTX800 loading firmware Rev.10.01.32 and later, the number of characters used for *filename* is up to 99 characters.

On the other revisions, the number of characters used for *filename* is up to 64 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]

RTX1200, RTX800

41.8 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]

RTX1200, RTX800

41.9 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]
RTX1200, RTX800

41.10 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
usb1: <i>filename</i>	A batch file in the USB memory
sd1: <i>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
- 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]

On RTX1200 loading firmware Rev.10.01.32 and later, 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.
On the other revisions, the number of characters that can be specified for *batchfile* is up to 64 characters. The number of characters that can be specified for *filename* is up to 64 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]
RTX1200

41.11 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.

RTX1200 loading firmware Rev.10.01.11 and later can use this function.

[Models]

RTX1200, RTX800

41.12 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.

You can specify mobile signal-strength for the *function* parameter on firmware Rev.10.01.11 and later.
You can specify execute lua for the *function* parameter on firmware Rev.10.01.16 and later.

[Models]

RTX1200

41.13 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]

RTX1200

Chapter 42

HTTP Upload Function

You can use this function to upload Yamaha router information (a setup file or syslog) to the specified HTTP server. You can use this feature to centrally manage the setup files and logs of multiple access points.

For setup files, the results of executing the **show config** or **show config N** command are saved to a file. For syslogs, the results of executing the **show log** command are saved to a file.

The name of the command that was executed appears at the start of the file.

You can store files to specified directories. This is useful when you want to collect information from multiple Yamaha router on an HTTP server. To specify a directory, use the **http upload** command.

This function can only be used if it is supported by the HTTP server.

The HTTP server OS (Windows, UNIX, etc.) does not matter, but when you use a UNIX HTTP server, because the CGI script is executed with the privileges of the nobody user account, the files created also have the privileges of the nobody user account. The CGI execution directory permission must be set to -----rw-.

The following URL provides script files that must be activated on the HTTP server, and technical information of this function:

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

42.1 Set a File to Upload to the HTTP Server

[Syntax]

http upload *type* [*config_no*] [*directory/*] *filename*

no http upload *type* [...]

[Setting and Initial value]

- *type*
 - [Setting] : 'config' or 'log'
 - [Initial value] : -
- *config_no*
 - [Setting] : 0-4.2
 - [Initial value] : -
- *directory*
 - [Setting] : The name of the destination directory
 - [Initial value] : -
- *filename*
 - [Setting] : The name of the destination file
 - [Initial value] : -

[Description]

Sets the information to upload to the HTTP server and the destination directory and file name.

This command creates the specified file inside of the specified directory (example: dir1/dir2/config.txt).

On firmware Rev.10.01.16 and later, you can specify following characters for a directory name and file name:

Text string	Meaning
%y	Year (yyyy)
%d	Day (dd)
%H	Hour (hh)
%S	Minutes (mm)
%S	Seconds (ss)
%n	Serial number
%a	LAN1 MAC address (00a0deXXXXXX)

Text string	Meaning
%P	Model name

When specifying a text string containing ‘%’ for a directory name or file name, you must specify ‘%’ continuously. *config_no* is enabled only when ‘config’ is specified for *type*. If *config_no* is omitted, active config is a target of uploading. Note that *config_no* can only be specified on models that support multiple setup files.

[Example]

Upload the directory and file called “ (Model name)/(serial number)/00a0deXXXXXX/20100101/120000.txt”

```
# http upload config %P/%n/%a/%y%m%d/%H%M%S.txt
```

Upload the file called “%config.txt”

```
# http upload config %%config.txt
```

[Models]

RTX1200, RTX800

42.2 Set the HTTP Upload Destination URL

[Syntax]

http upload url *url*

no http upload url [*url*]

[Setting and Initial value]

- url*
 - [Setting] : Upload destination URL
 - [Initial value] : -

[Description]

Sets the URL of the HTTP server that the file will be uploaded to. CGI must be enabled on the HTTP server, and the server must execute the CGI script for receiving the uploaded file.

[Models]

RTX1200, RTX800

42.3 Set Whether to Allow HTTP Uploading

[Syntax]

http upload permit *switch*

no http upload permit [*switch*]

[Setting and Initial value]

- switch*
 - [Setting] :

Setting	Description
on	Allow HTTP uploading.
off	Do not allow HTTP uploading.

- [Initial value] : off

[Description]

Sets whether to allow HTTP uploading.

[Models]

RTX1200, RTX800

42.4 Set the HTTP Upload Timeout Time

[Syntax]

http upload timeout *time*

no http upload timeout [*time*]

[Setting and Initial value]

- *time*
 - [Setting] : 1-180[seconds]
 - [Initial value] : 30

[Description]

Sets the time until the HTTP upload times out.

[Models]

RTX1200, RTX800

42.5 Set the HTTP Upload Retry Count and Interval

[Syntax]

http upload retry interval *interval count*
no http upload retry interval [*..*]

[Setting and Initial value]

- *interval*
 - [Setting] : 1-60[seconds]
 - [Initial value] : 30
- *count*
 - [Setting] : 1-10
 - [Initial value] : 5

[Description]

Sets how many times and at what interval to retry after an HTTP upload attempt fails.

[Models]

RTX1200, RTX800

42.6 Set the Proxy Server to Use for HTTP Uploading

[Syntax]

http upload proxy *proxy* [*port*]
no http upload proxy [*..*]

[Setting and Initial value]

- *proxy*
 - [Setting] : Proxy server
 - [Initial value] : -
- *port*
 - [Setting] : 1-65535
 - [Initial value] : 80

[Description]

Sets the proxy server to use for HTTP uploading.

[Models]

RTX1200, RTX800

42.7 Upload to an HTTP Server

[Syntax]

http upload go

[Description]

Uploads to an HTTP server.

If the upload attempt fails, the router retries according to the settings of the **http upload retry interval** command.

[Note]

When the **alarm http upload** command is set to 'on', the router sounds an alarm according to whether the upload succeeded or failed.

This command can be specified by the **schedule at** command. When it is specified with the startup option, it is executed at startup.

If you specify startup, the connection with the HTTP server may not be established when the router starts up and the upload

may fail.
You can prepare for this kind of occurrence by using the **http upload retry interval** command to configure appropriate retry settings.

[Models]
RTX1200, RTX800

42.8 Set Whether to Sound Alarms for the HTTP Upload Function

[Syntax]

alarm http upload *switch*
no alarm http upload [*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 HTTP upload function.

[Models]
RTX1200

Chapter 43

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).

43.1 Set Whether to Use a Mobile Terminal

[Syntax]

mobile use *interface use*

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

[Description]

Specify whether to use the mobile terminal connected to the specified bus to connect to the Internet.

[Models]

RTX1200, RTX800

43.2 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]

RTX1200, RTX800

43.3 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]

RTX1200, RTX800

43.4 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.

[Note]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX1200, RTX800

43.5 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
off	Do not automatically transmit from the mobile terminal

- [Initial value] : off

[Description]

Sets whether to auto connect to the selected destination.

[Models]

RTX1200, RTX800

43.6 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]

RTX1200, RTX800

43.7 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]

RTX1200, RTX800

43.8 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]

RTX1200, RTX800

43.9 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. Note that if *pdp*=type is omitted, ppp is assigned when mopera.ne.jp is specified for *apn*, and ip is assigned in other cases.

[Example]

```
mobile access-point name mopera.ne.jp cid=1 (for mopera)
mobile access-point name mopera.net cid=3 (for mopera U)
```

[Models]

RTX1200, RTX800

43.10 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]

RTX1200, RTX800

43.11 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.

Firmware Rev.10.01.11 and later can use this function.

[Models]

RTX1200, RTX800

43.12 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.

Firmware Rev.10.01.11 and later can use this function.
The *unit* parameter is available on firmware Rev.10.01.16 and later.

[Models]

RTX1200, RTX800

43.13 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]

RTX1200, RTX800

43.14 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]

RTX1200, RTX800

43.15 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]

RTX1200, RTX800

43.16 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.
No event is logged when you perform remote setup through FOMA.
The **syslog debug** on command must also be executed.

[Models]

RTX1200, RTX800

43.17 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.

[Note]

A case where you perform remote setup through FOMA is not included.

[Models]

RTX1200, RTX800

43.18 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.

Firmware Rev.10.01.11 and later can use this function.

[Models]

RTX1200, RTX800

43.19 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.

[Note]

Firmware Rev.10.01.11 and later can use this function.

[Models]

RTX1200, RTX800

43.20 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.

[Note]

Firmware Rev.10.01.11 and later can use this function.

[Models]

RTX1200, RTX800

43.21 Acquire the Signal Reception Level

[Syntax]

mobile signal-strength go

[Description]

Acquires the signal reception level.

[Note]

Firmware Rev.10.01.11 and later can use this function.

[Models]

RTX1200, RTX800

43.22 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

- 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.

[Note]

The router cannot acquire the signal reception level while it is connected to a PP interface.

Firmware Rev.10.01.11 and later can use this function.

The number of times for the interval option can be specified on firmware Rev.10.01.16 and later.

[Models]

RTX1200, RTX800

43.23 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.

Firmware Rev.10.01.11 and later can use this function.

[Models]

RTX1200, RTX800

43.24 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]

RTX1200, RTX800

43.25 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] :
 - on (Revisions other than the following revision)
 - off (Rev.10.01.11 and later)

[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]

RTX1200, RTX800

43.26 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.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

43.27 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.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

43.28 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.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

43.29 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.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

43.30 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.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

43.31 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.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

43.32 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 a reconnection is requested (60..21474836)
 - [Initial value] : -

[Description]

Sets whether to connect permanently to the specified WAN interface. 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]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

43.33 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.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

43.34 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 × 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.

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

43.35 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.

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

43.36 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.

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

43.37 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.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

43.38 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.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

Chapter 44

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.

44.1 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

44.2 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.

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

44.3 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 “/”.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

44.4 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 forcibly

- 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

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

44.5 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	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.

[Note]

RTX1200 loading firmware Rev.10.01.16 can use this function.

[Models]

RTX1200, RTX800

44.6 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

Chapter 45

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.

45.1 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

45.2 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.

On the RTX1200, you cannot use the automatic search function with the external memory. Also, you cannot specify a name that includes a slash for *name*.

The users whose settings are configured by this command cannot access the normal internal router GUI.

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

45.3 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.

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

45.4 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.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

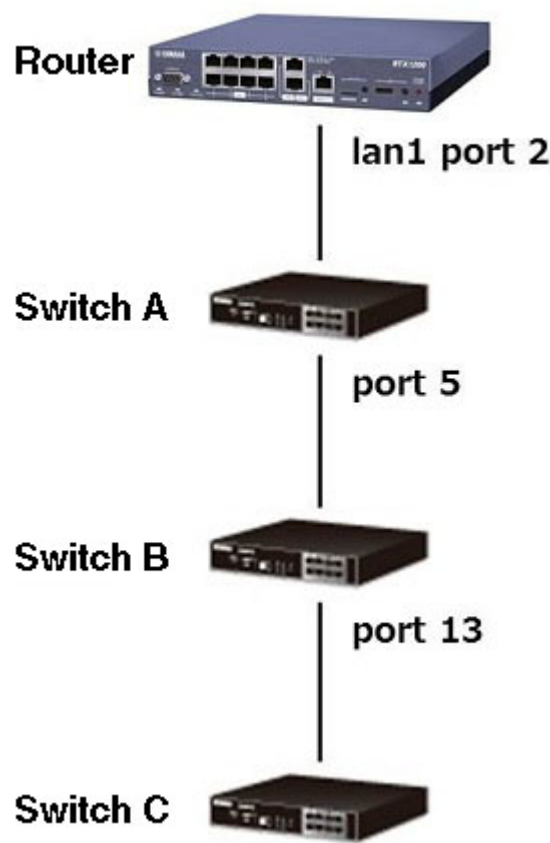
Chapter 46

Switch Control Function

The switch control function allows control of the Yamaha switches from the router.

You can specify a switch 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).

46.1 Set the Switch Control Function

46.1.1 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

Setting	Description
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]

RTX1200

46.1.2 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]

RTX1200

46.1.3 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]

RTX1200

46.1.4 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]

RTX1200

46.1.5 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]

RTX1200

46.1.6 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]

RTX1200

46.1.7 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]

RTX1200

46.1.8 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]

RTX1200

46.2 Switch Function

46.2.1 System

46.2.1.1 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]

RTX1200

46.2.1.2 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]

RTX1200

46.2.1.3 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]
RTX1200

46.2.1.4 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]
RTX1200

46.2.1.5 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]
RTX1200

46.2.1.6 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]
RTX1200

46.2.1.7 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]

RTX1200

46.2.1.8 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]

RTX1200

46.2.1.9 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"> Lighted on in green: The link is established Flashing in green: Data is being transferred Light-off: The link is lost
speed	Display the connection speed of each port. <ul style="list-style-type: none"> Lighted on in green: Connect to 1000BASE-T Lighted on in orange: Connect to 100BASE-TX Light-off: Connect to 10BASE-T
duplex	Display the connection state (full duplex / half duplex) of each port. <ul style="list-style-type: none"> Lighted on in green: Connect at full duplex Lighted on in orange: Connect at half duplex
status	Display the system state. <ul style="list-style-type: none"> Lighted on in orange: A loop is detected When a failure of the fan is detected in SWX2200-24G, the lower mode LED starts flashing in orange.

[Models]

RTX1200

46.2.1.10 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]

RTX1200

46.2.1.11 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]

RTX1200

46.2.1.12 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]

RTX1200

46.2.2 Port

46.2.2.1 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]

RTX1200

46.2.2.2 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]

RTX1200

46.2.2.3 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]

RTX1200

46.2.2.4 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]

RTX1200

46.2.2.5 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]

RTX1200

46.2.2.6 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]

RTX1200

46.2.3 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	

46.2.3.1 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]

RTX1200

46.2.3.2 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]

RTX1200

46.2.3.3 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]

RTX1200

46.2.3.4 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]

RTX1200

46.2.3.5 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]

RTX1200

46.2.4 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
```

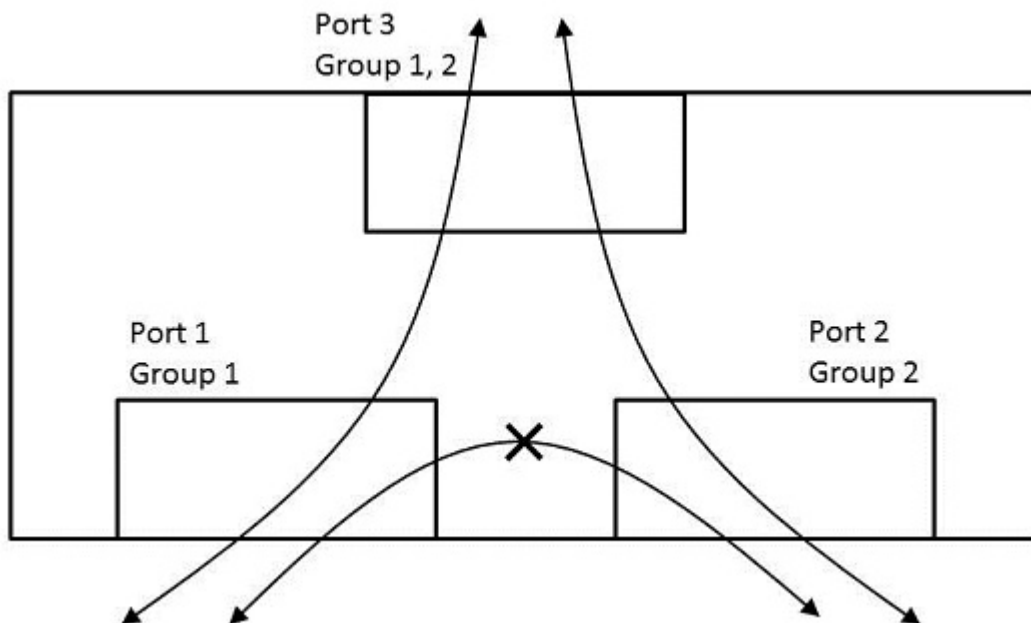
A packet the switch receives is grouped into any VLAN ID regardless of availability of VLAN tag, and transferred according to that information. The VLAN operation mode of the port is specified with the **vlan-port-mode** command.

vlan-port-mode	Receiving operation	Sending operation
access	Receive only a packet without a VLAN tag. The VLAN ID is grouped according to the vlan-access command setting.	At the time of receiving, send a packet grouped into the VLAN ID (vlan-access) 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 vlan-trunk 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 (vlan-trunk) 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 (vlan-access) of the destination port without a VLAN tag. Also, at the time of receiving, send a packet grouped into the VLAN ID (vlan-trunk) 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.

46.2.4.1 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]

RTX1200

46.2.4.2 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]

RTX1200

46.2.4.3 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]

RTX1200

46.2.4.4 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]

RTX1200

46.2.4.5 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]

RTX1200

46.2.4.6 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]

RTX1200

46.2.5 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	

46.2.5.1 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]

RTX1200

46.2.5.2 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]

RTX1200

46.2.5.3 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]

RTX1200

46.2.5.4 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]

RTX1200

46.2.5.5 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]

RTX1200

46.2.5.6 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]

RTX1200

46.2.5.7 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]

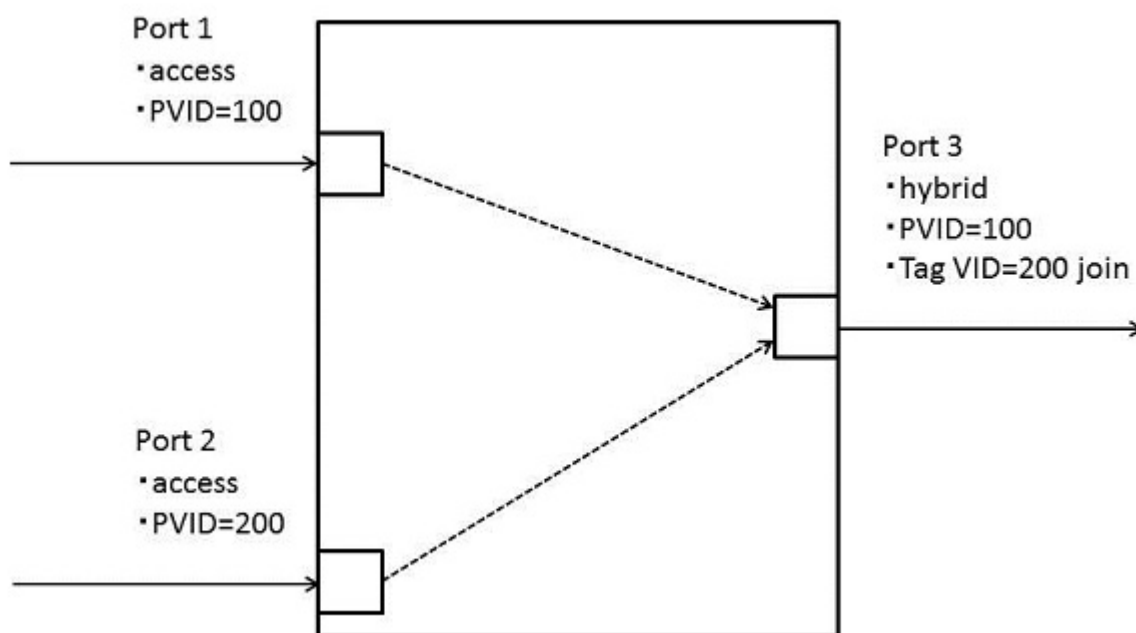
RTX1200

46.2.6 Mirroring

The mirroring function enables the communication on a certain port to be monitored on another port.

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.

46.2.6.1 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]

RTX1200

46.2.6.2 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]

RTX1200

46.2.6.3 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]

RTX1200

46.2.6.4 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]

RTX1200

46.2.7 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.

46.2.7.1 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

Setting	Description
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
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]

RTX1200

46.2.7.2 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

Setting	Description
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]

RTX1200

46.2.7.3 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]

RTX1200

46.2.7.4 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]

RTX1200

46.2.7.5 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]

RTX1200

46.2.7.6 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]

RTX1200

46.2.7.7 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]

RTX1200

46.2.8 Detect a Loop

The Yamaha switch detects a loop of the network by monitoring transfer of MAC address. Transfer of MAC address means that multiple ports learn one MAC address.

For a port for which the loop detection function is used, specify on for the **loopdetect-port-use** command.

The switch monitors the number of times that a MAC address transfers per second. When the number of times is over the threshold specified in the **loopdetect-count** command continuously for the time specified in the **loopdetect-time** command, the switch determines that a loop occurs. The LED of the port where the loop occurs lights up in orange.

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.

46.2.8.1 Set the Threshold for the Number of Times That a MAC Address Transfers 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 number of times that a MAC address transfers per second (3 .. 65535)
 - [Initial value] : 3
- *switch* : Switches
 - [Setting] :
 - MAC address
 - Route
 - [Initial value] : -

[Description]

Sets the threshold for the number of times that a MAC address transfers per second.

[Models]

RTX1200

46.2.8.2 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 until the number of times that a MAC address transfers per second is over the threshold specified in the **loopdetect-count** command continuously and the switch determines that a loop occurs.

[Models]

RTX1200

46.2.8.3 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]

RTX1200

46.2.8.4 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]

RTX1200

46.2.8.5 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]

RTX1200

46.2.8.6 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]

RTX1200

46.2.8.7 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]

RTX1200

46.2.8.8 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]

RTX1200

Chapter 47

Diagnosis

47.1 Port Availability Diagnosis

[Syntax]

diagnose config port map *interface protocol* [*src_addr* [*src_port*]] *dst_addr*

[Setting and Initial value]

- *interface*
 - [Setting] : LAN or PP interface name on the receiving side
 - [Initial value] : -
- *protocol*
 - [Setting] : Packet type to examine (you can specify multiple types by separating them with commas)
 - [Setting] :
 - Decimal number indicating the protocol (0..255)
 - Mnemonic indicating the protocol

Setting	Description
tcp	TCP packet
udp	UDP packet
icmp	ICMP packet
gre	gre packet of PPTP
esp	esp packet of IPsec
ah	ah packet of IPsec

- [Initial value] : -
- *src_addr*
 - [Setting] : Source IP address of the input packet
 - [Initial value] : -
- *src_port*
 - [Setting] : Source port number of the input packet
 - [Initial value] : -
- *dst_addr*
 - [Setting] : Destination IP address to examine (you can specify multiple types by separating them with commas)
 - [Initial value] : -

[Description]

Determines whether packets received from the interface specified by the *interface* parameter can pass through the router.

For tcp and udp packets, the router checks the well-known ports of the destination IP address specified by the *dst_addr* parameter and shows the ports that can pass through the router. For other packets, the router ignores the port settings and shows the packets that can reach the address specified by the *dst_addr* parameter.

If *src_addr* and *src_port* are omitted, the router automatically samples combinations of source IP addresses and source port numbers that are deemed necessary under the filter settings.

[Note]

This command only performs packet transfer processing virtually within the router; it does not actually send the examined packet type to the host specified by the *dst_addr* parameter. This means that even if a port is closed on the host, the port is considered open if it is possible for it to pass through the router. This applies even if *dst_addr* is set to the IP address of the router itself; the port availability of the router itself is not determined.

This command does not take the Ethernet filter into consideration.

[Models]

RTX1200, RTX800

47.2 Diagnosis of Access Ranges That Can Reach a Port

[Syntax]

diagnose config port access *interface* [*protocol*] *dst_addr dst_port*

[Setting and Initial value]

- *interface*
 - [Setting] : LAN or PP interface name on the receiving side
 - [Initial value] : -
- *protocol* : Packet type to examine (You can specify multiple types by separating them with commas. All types are examined if this parameter is omitted.)
 - [Setting] :

Setting	Description
tcp	TCP packet
udp	UDP packet

- [Initial value] : -
- *dst_addr*
 - [Setting] : Destination IP address to examine
 - [Initial value] : -
- *src_port*
 - [Setting] : Destination port number to examine
 - [Initial value] : -

[Description]

Displays the source IP addresses and source port numbers from which packets of the type specified by the *protocol* parameter can reach the host port number specified by the *dst_addr/dst_port* parameter.

[Note]

This command only performs packet transfer processing virtually within the router; it does not actually send the examined packet type to the host specified by the *dst_addr* parameter. This means that even if a port is closed to a packet on the host, if it is possible for the packet to pass through the router, the command determines that the packet can reach the host. This applies even if *dst_addr* is set to the IP address of the router itself; the port availability of the router itself does not affect the outcome.

This command does not take the Ethernet filter into consideration.

[Models]

RTX1200, RTX800

47.3 Set the Maximum Number of Passed Packets That Can Be Detected in the Port Availability Diagnosis

[Syntax]

diagnosis config port max-detect *num*

[Setting and Initial value]

- *num*
 - [Setting] : The maximum number of detectable passed packets (100..1000000)
 - [Initial value] : 2000

[Description]

Sets the maximum number of passed packets that can be detected in the port availability diagnosis and the diagnosis of access ranges that can reach a port. If the number of detected passed packets specified here is exceeded, the diagnosis is stopped.

[Note]

When the results of the port availability diagnosis are displayed, the router does its best to consolidate the source addresses and source port numbers from which successful transfer is possible. However, when the value specified by this setting is exceeded, the diagnosis is stopped before consolidation takes place, so the number of passed packets displayed in the diagnosis results may be less than the actual value specified here.

[Models]

RTX1200, RTX800

47.4 Set the Number of Port Availability Diagnosis Results to Store in the History

[Syntax]

diagnosis config port history-num *num*

[Setting and Initial value]

- *num*
 - [Setting] : The number of diagnosis results to store in the history (1..10)
 - [Initial value] : 3

[Description]

Sets the number of results to store from the port availability diagnosis and the diagnosis of access ranges that can reach a port.

[Note]

When you execute this command, if there are already more history entries than the specified number, the extra entries are deleted.

[Models]

RTX1200, RTX800

47.5 Display the Results of the Port Availability Diagnosis

[Syntax]

show diagnosis config port map

[Description]

Displays the results of the port availability diagnosis.

[Models]

RTX1200, RTX800

47.6 Display the Results of the Diagnosis of Access Ranges That Can Reach a Port

[Syntax]

show diagnosis config port access

[Description]

Displays the results of the diagnosis of access ranges that can reach a port.

[Models]

RTX1200, RTX800

47.7 Delete the Results of the Port Availability Diagnosis

[Syntax]

clear diagnosis config port

[Description]

Deletes all the results of the port availability diagnosis and the diagnosis of access ranges that can reach a port.

[Models]

RTX1200, RTX800

Chapter 48

Statistics

48.1 Set Whether to Enable the Statistics Function

[Syntax]

```
statistics type sw
no statistics type [sw]
```

[Setting and Initial value]

- type : Internal resource type
- [Setting] :

Setting	Description
cpu	CPU usage
memory	Memory usage
traffic	Traffic level
flow	Number of fast path flows
nat	Number of NAT entries
route	Number of routes
filter	Number of filter hits
qos	Amount of processing for each queue

- [Initial value] : -
- sw
- [Setting] :

Setting	Description
on	Enable the statistics function
off	Disable the statistics function

- [Initial value] : off

[Description]

Sets whether to enable each type of statistic.

[Note]

If you set this command to off, previous statistics are cleared.
Even if you access the relevant page, you will not be able to view statistics.

[Models]

RTX1200, RTX800

Chapter 49

Operation

49.1 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 a peer whose ISDN number is unknown

- [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(page 29).

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.2 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.(page 156).

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.3 Configuration Operation

49.3.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.3.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.3.3 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]

On RTX1200/RTX800 loading firmware Rev.10.01.32 and later, the number of characters used for *filename* is up to 99 characters.

For other models, *filename* must be 64 characters or less.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.3.4 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.
On firmware Rev.10.01, 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 on firmware Rev.10.01.
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.

On RTX1200/RTX800 loading firmware Rev.10.01.32 and later, the number of characters used for *filename* is up to 99 characters.
For other models, *filename* must be 64 characters or less.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.3.5 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 RTX800)
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 an executable firmware file on the internal flash ROM (only 0 on the RTX800; 0 or 1 on the RTX1200; only 1 on all other models)

- [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 on firmware Rev.10.01.

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.

On RTX1200/RTX800 loading firmware Rev.10.01.32 and later, the number of characters used for *filename* is up to 99 characters.

For other models, *filename* must be 64 characters or less.

[Models]

RTX3000, RTX1200, RTX1100, RTX800

49.3.6 Delete a Configuration File

[Syntax]

delete config *filename*

[Setting and Initial value]

- *filename* : Name of the file to be deleted
 - [Setting] :

Setting	Description
Number	Configuration file number of the internal Flash ROM (0..4.2)

- [Initial value] : -

[Description]

Deletes a saved configuration file.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.3.7 Delete an Executable Firmware File

[Syntax]

delete exec *filename*

[Setting and Initial value]

- *filename* : Name of the file to be deleted
 - [Setting] :

Setting	Description
Number	Executable firmware file number (only 1 can be specified)

- [Initial value] : -

[Description]

Deletes a saved executable firmware file.

[Models]

RTX3000, RTX1200, RTX1100

49.3.8 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.3.9 Set 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 be used at startup.

[Models]

RTX3000, RTX1200, RTX1100

49.3.10 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.3.11 Configure a Router at a Remote Location

[Syntax]

remote setup interface [*number* [/sub_address]] [*type*]

remote setup interface dlci=*dlci*

[Setting and Initial value]

- *interface* : Interface Name
 - [Setting] :
 - BRI interface name
 - PRI interface name
 - [Initial value] : -
- *number*
 - [Setting] : ISDN number
 - [Initial value] : -
- *sub_address*
 - [Setting] : ISDN sub address (Text string consisting of ASCII characters from 0x21 to 0x7e)
 - [Initial value] : -
- *dlci*
 - [Setting] : Frame relay DLCI number

- [Initial value] : -
- *type* : Remote setup method
- [Setting] :

Setting	Description
retransmission	This method can handle data loss.

- [Initial value] : -

[Description]

Configures a router at a remote location using the specified interface.

Both BRI and PRI are available, and also, can be specified for ISDN, exclusive line, and frame relay.

You must specify retransmission only when you perform remote setup through FOMA.

If you specify retransmission, the router uses a remote setup method that can recover lost data. This method is not compatible with the conventional remote setup function.

[Note]

For an exclusive line, the *number* and *sub_address* parameters are not necessary.

[Models]

RTX1200, RTX1100

49.3.12 Limit Configuration from a Router at a Remote Location

[Syntax]

remote setup accept *tel_num* [*tel_num_list*]

remote setup accept any

remote setup accept none

no remote setup accept

[Setting and Initial value]

- *tel_num*
 - [Setting] : Phone number
 - [Initial value] : -
- *tel_num_list*
 - [Setting] : List of phone numbers delimited by spaces
 - [Initial value] : -
- any : Keyword indicating that configuration from all remote routers is allowed
 - [Initial value] : any
- none : Keyword indicating that configuration from all remote routers is prohibited
 - [Initial value] : -

[Description]

Sets the peers to allow the configuration of the local router.

[Models]

RTX1200, RTX1100, RTX800

49.4 Clear Operation of Dynamic Information

49.4.1 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]

RTX3000, RTX1200, RTX1100

49.4.2 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]

RTX3000, RTX1200, RTX1100

49.4.3 Clear the ARP Table

[Syntax]**clear arp****[Description]**

Clears the ARP table.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.4.4 Clear the Dynamic Routing Information of IP

[Syntax]**clear ip dynamic routing****[Description]**

Clears the routing information of an IP configure dynamically.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.4.5 Clear the Log

[Syntax]**clear log****[Description]**

Clears the log.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.4.6 Clear the InARP

[Syntax]**clear inarp****[Description]**

Clears the peer IP address obtained by InARP for the selected peer. If InARP is on, restart InARP.

[Models]

RTX3000, RTX1200, RTX1100

49.4.7 Clear the DNS Cache

[Syntax]**clear dns cache****[Description]**

Clears the cache held by the DNS recursive server.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.4.8 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 interface name
 - [Initial value] : -
- *peer_num*
 - [Setting] : Peer number
 - [Initial value] : -
- *tunnel_num*
 - [Setting] : Tunnel interface number
 - [Initial value] : -

[Description]

Clears information of the counter of the specified interface.

[Note]

RTX1200 and RTX800 loading firmware Rev. 10.01.36 and later can use this function.

[Models]

RTX1200, RTX800

49.4.9 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.4.10 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.4.11 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.4.12 Clear the Neighbor Cache

[Syntax]

clear ipv6 neighbor cache

[Description]

Clears the neighbor cache.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.4.13 Delete the Startup Information History

[Syntax]

clear boot list

[Description]

Delete the startup information history.

[Models]

RTX1200

49.5 File and Directory Operation

49.5.1 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 “/”.

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

49.5.2 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.

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

49.5.3 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.

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

49.5.4 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.

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

49.6 Other Operations

49.6.1 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.6.2 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.6.3 Restart

[Syntax]

restart [*binary* [*config*]]

restart [*config*]

[Setting and Initial value]

- *binary*
 - [Setting] : Executable firmware file number (0..1)
 - [Initial value] : -
- *config*
 - [Setting] : Configuration file number of the internal Flash ROM (0..4.2)
 - [Initial value] : -

[Description]

Restarts the router.

You can specify the configuration file and executable firmware file used to start the router.

[Note]

The second syntax is supported on the RT107e and RTX800.

The first syntax is supported on the other models.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.6.4 Restart the Interface

[Syntax]

interface reset interface [*interface ...*]

[Setting and Initial value]

- *interface*
 - [Setting] :
 - LAN interface name
 - WAN interface name
 - BRI interface name
 - PRI interface name
 - [Initial value] : -

[Description]

Restarts the specified interface.

If auto negotiation is specified on a LAN interface, the auto negotiation procedure is started.

If the line type is changed using the **line type** command on a BRI or a PRI interface, this command must be executed to restart the interface.

Use the **interface reset pp** command for an interface using MP.

[Note]

If this command is executed on lan1 or lan2 on the RTX1100, RT107e, or RTX800, the lan1 and lan2 interfaces are reset

simultaneously.

On the RTX1200, when you execute this command on a single LAN interface, all the LAN interfaces are reset.

On models that only have LAN interfaces, you can only set the *interface* parameter to a LAN interface name.

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

Execute this command after adjusting all settings such as those specified by the **line type** and **pp bind** commands and the routing information. Execute this command with the communication to all peer numbers bound to the target interface stopped or with the line removed if the line type is being changed.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.6.5 Restart 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 selected peer number. Use this command for an interface using MP.

[Models]

RTX3000, RTX1200, RTX1100

49.6.6 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] : Tunnel number via NGN
 - [Initial value] : -

[Description]

Manually connects the line.

[Note]

The **connect tunnel** command is only available for the tunnel for connecting access points with the data connect function.

On models without data connect connection function, the **connect pp** and the **connect tunnel** command cannot be specified.

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.6.7 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] : Tunnel number via NGN
 - [Initial value] : -

[Description]

Manually disconnects the line.

[Note]

The **disconnect tunnel** command is only available for the tunnel for connecting access points with the data connect function. On models without data connect connection function, the **disconnect pp** and the **disconnect tunnel** command cannot be specified.

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.6.8 ping

[Syntax]

ping [-s *datalen*] [-c *count*] [-sa *ip_address*] [-w *wait*] *host*

[Setting and Initial value]

- *datalen*
 - [Setting] :

Setting	Description
1..65535 bytes	Rev.10.01.32 and later
64..65535 bytes	other models

- [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 (0.1..99.9)
 - [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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.6.9 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 (0.1..99.9)
 - [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.

The first syntax to the fifth syntax can be specified on firmware Rev.10.01.32 and later. On the other revisions, specify with the sixth syntax to tenth syntax.

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.

[Note]

The -s option, -c option, -sa option, and -w option are available on firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.6.10 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.

The *source* parameter is available on RTX1200 loading firmware Rev.10.01.16 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.6.11 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.6.12 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.6.13 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]

RTX3000, RTX1100, RT107e

49.6.14 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

49.6.15 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]

RTX3000, RTX1100, RT107e

49.6.16 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]

RTX1200, RTX1100, RT107e, RTX800

49.6.17 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]

RTX3000, RTX1200, RTX1100, RTX800

49.6.18 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. You can only specify prompt on the RTX1200, RTX1100 and RTX800.

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]

RTX1200, RTX1100, RT107e, RTX800

49.6.19 Clear the Input Cut-Off Filter Information

[Syntax]

```
clear ip inbound filter [interface [id]]
clear ipv6 inbound filter [interface [id]]
```

[Setting and Initial value]

- *interface* : Interface
 - [Setting] :
 - LAN interface (lan1, lan2, etc.)
 - WAN interface (wan1)
 - PP interface (pp 1, pp 2, etc.; you must insert a space between 'pp' and the number)
 - TUNNEL interface (tunnel 1, tunnel 2, etc.; you must insert a space between 'tunnel' and the number)
 - [Initial value] : -
- *id*
 - [Setting] : Filter ID (1 .. 65535)
 - [Initial value] : -

[Description]

Clears information, such as logs, about the specified input cut-off filter. If you do not specify an interface or ID, the information of all interfaces and IDs is cleared.

[Note]

The WAN interface can be specified on firmware Rev.10.01.

[Models]

RTX1200, RTX800

49.6.20 Clear the Policy Filter Information

[Syntax]

```
clear ip policy filter [id]
clear ipv6 policy filter [id]
```

[Setting and Initial value]

- *id*
 - [Setting] : Filter ID (1 .. 65535)
 - [Initial value] : -

[Description]

Clears information, such as logs, about the specified policy filter. If you do not specify an ID, all the policy filter information is cleared.

[Models]

RTX1200, RTX800

49.6.21 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX1200, RTX800

49.6.22 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]

RTX1200, RTX800

Chapter 50

Configuration Display

50.1 Show the Router Configuration

[Syntax]

show environment

[Description]

The following items are shown.

- Policy filtering module version (on models with the policy filter function)
- System revision
- CPU and memory usage (%)
- Firmware and configuration file that are running
- Firmware and configuration file used at startup
- Fan status (RTX3000)
- Internal temperature status (RTX3000, RTX1200)

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

50.2 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.

The second syntax is available on firmware Rev.8.02 and later. If a file is specified, you are prompted to enter the login password and administrator password.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

50.3 Show the Configuration of a Specified PP

[Syntax]

show config pp [*peer_num*]

less config 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 only the information related to the selected peer number among the items shown using the **show config** and **less config** commands.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

50.4 Show the Configuration of a Specified Tunnel

[Syntax]

```
show config tunnel [tunnel_num] [expand]
less config tunnel [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.

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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

50.5 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

50.6 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. The parameters that the user can specify for *location* are as follows by model:

Model	Parameter
RTX1200, RTX800	internal, Relative or absolute path
Other models	internal

all and file-only are available on RTX1200 and RTX800.

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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

50.7 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, or null 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.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

50.8 Show the SSH Server Public Key

[Syntax]

```
show sshd public key
```

[Description]

Shows the SSH server public key.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

50.9 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]

RTX1200, RTX800

50.10 Firmware File List

[Syntax]

show exec list

less exec list

[Description]

Displays information about the setup files stored in the internal flash ROM. The mark ‘*’ is displayed on the active setup file.

[Models]

RTX1200

Chapter 51

Status Display

51.1 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 (RTX3000), 1-8 (Other models)
 - [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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.2 Show the Interface Status

[Syntax]

show status *interface*

[Setting and Initial value]

- *interface*
 - [Setting] :
 - LAN interface name
 - WAN interface name
 - BRI interface name
 - PRI interface name
 - [Initial value] : -

[Description]

Shows the interface status.

[Note]

You can specify the WAN interface on RTX1200 and RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.3 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.4 Show DLCI

[Syntax]

show dlci [*peer_num*]

[Setting and Initial value]

- *peer_num*
 - [Setting] : Peer number
 - [Initial value] : -

[Description]

Shows the DLCI value and InARP status. If InARP is successful, the peer's IP address is also shown.

[Models]

RTX1200

51.5 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.6 Show Routing Information Obtained by RIP

[Syntax]**show ip rip table****[Description]**

Shows routing information obtained by RIP.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.7 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.

[Note]

The second and third syntaxes can be used on firmware Rev.9 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.8 Show the IPv6 RIP Table

[Syntax]**show ipv6 rip table****[Description]**

Shows the IPv6 RIP table.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.9 Show the Neighbor Cache

[Syntax]**show ipv6 neighbor cache**

[Description]

Shows the status of the neighbor cache.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.10 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.11 Show the Certificate Information

[Syntax]

show pki certificate summary [*cert_id*]

[Setting and Initial value]

- *cert_id*
 - [Setting] :

Setting	Description
1..2(RTX3000)	Certificate file identifier
1..8 (other than RTX3000)	

- [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.

[Note]

RTX1200 loading firmware Rev.10.01.22 and later can use this function.

[Models]

RTX1200

51.12 Show the CRL File Information

[Syntax]

show show pki crl [*crl_id*]

[Setting and Initial value]

- *crl_id*
 - [Setting] :

Setting	Description
1..2(RTX3000)	CRL file identifier
1..8 (other than RTX3000)	

- [Initial value] : -

[Description]

Shows the CRL file information.

The following information is shown:

- Version
- Issuer
- Update date and time
- Next update date and time

[Note]

RTX1200 loading firmware Rev.10.01.22 and later can use this function.

[Models]

RTX1200

51.13 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.14 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]

The detail option is available on firmware Rev.10.01.09 and later. On firmware Rev. 10.01.09 and later, 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 was added to the Rev. 10.01.09 as an option to display entries with the previous all entry display formats.

When IP masquerading is using a large number of ports, 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.

The **show nat descriptor masquerade port summary** command can be used in firmware Rev.10.01.01 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.15 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.16 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]

On firmware Rev. 10.01.09 and later, 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. The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.17 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]

RTX1200, RTX800

51.18 Show the L2TP Status

[Syntax]

show status l2tp

[Description]

Shows the L2TP status.

[Note]

RTX1200 and RTX800 loading firmware Rev.10.01.32 and later can use this function.

[Models]

RTX1200, RTX800

51.19 Show the PPTP Status

[Syntax]

show status pptp

[Description]

Shows the PPTP status and GRE statistical information.

[Models]

RTX1200, RTX1100, RTX800

51.20 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
virtual-link	Virtual link status

- [Initial value] : -

[Description]

Shows OSPF information.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.21 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.22 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.23 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.24 Show the DHCPv6 Status

[Syntax]

show status ipv6 dhcp

[Description]

Shows the status related to DHCPv6.

[Models]

RTX1200, RTX800

51.25 Show the Backup Status

[Syntax]

show status backup

[Description]

Shows the backup status of the interface set to backup.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.26 Show the Connections Managed by Dynamic Filters

[Syntax]

show ip connection

show ip connection [*interface* [*direction*]]

show ip connection pp [*peer_num* [*direction*]]

show ip connection tunnel [*tunnel_num* [*direction*]]

show ip connection summary

[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] : -
- *summary* : Show the number of managed connections for each interface and direction and the total.
 - [Initial value] : -

[Description]

Shows the connections managed by dynamic filters for the specified interface. If the interface is not specified, the information of all interfaces is shown.

[Note]

The **show ip connection** summary command is available on RTX3000 and RTX1200.
The WAN interface is available on RTX1200 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1100, RT107e

51.27 Show the Connections Managed by IPv6 Dynamic Filters

[Syntax]

show ipv6 connection
show ipv6 connection *interface* [*direction*]
show ipv6 connection pp [*peer_num* [*direction*]]
show ipv6 connection tunnel [*tunnel_num* [*direction*]]
show ipv6 connection summary

[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] : -
- *summary* : Show the number of managed connections for each interface and direction and the total.
 - [Initial value] : -

[Description]

Shows the connections managed by dynamic filters for the specified interface. If the interface is not specified, the information of all interfaces is shown.

[Note]

The **show ipv6 connection** summary command is available on RTX3000 and RTX1200.

[Models]

RTX3000, RTX1100, RT107e

51.28 Show the Status of the Network Monitor Function

[Syntax]

show status ip keepalive

[Description]

Shows the status of the network monitor function.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.29 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 on the RTX3000, RTX1200, and RTX800, and 50 on other models.

[Note]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.30 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]

RT107e

51.31 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]

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX1200, RTX800

51.32 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 (1..4 on models other than the RTX1200; 1..8 on the RTX1200)
 - [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.

[Note]

The *mac_address* parameter is available on firmware Rev.10.01.16 and later.

[Models]

RTX1200, RTX1100, RT107e, RTX800

51.33 Show the UPnP Status Information

[Syntax]

show status upnp

[Description]

Shows the UPnP status information.

[Models]

RTX1200, RTX1100, RT107e, RTX800

51.34 Show the Tunnel Interface Status

[Syntax]

show status tunnel [*tunnel_num*]

[Setting and Initial value]

- *tunnel_num*
 - [Setting] : Tunnel interface number
 - [Initial value] : -

[Description]

Shows the tunnel interface status.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.35 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 (RTX3000, RTX1200), 1-8 (Other models)
 - [Initial value] : -

[Description]

Shows the VLAN interface information. If a VLAN interface name is specified, only the information of that interface is shown.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.36 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]

RTX3000, RTX1200, RTX1100, RTX800

51.37 Show Multicast Routing Information

[Syntax]**show ip mroute** [*option*]**[Setting and Initial value]**

- *option* : Contents of the routing information to be output
 - [Setting] :

Setting	Description
summary	Show the minimum information focusing on the source, group, and output interface of the multicast
normal	Show basic status of each interface in addition to the information shown by summary
detail	Show detailed information taking into account various status management of PIM-SM
fib	Show information focusing on the transmission status of multicast packets. You can check from which interface the multicast packet was entered and which interface it is transmitted

- [Initial value] : normal

[Description]

Shows multicast routing information.

The contents of the displayed information can be specified using options.

Items output in the table

Item	Description
Inbound IF	Receive interface
Source	Source address of the transmitted packet
Group	Destination address of the transmitted packet
Outbound IF	Transmit interface
TTL	Time that the router holds the forwarding information when the condition in which no packet is received persists.
KAT	The remaining time of the keepalive timer when using PIM-SM
Flags	Operating status of each PIM parameter K (Keepalive), S (spt_bit)PIM

If an option is not specified, information corresponding to the normal option is shown.

[Models]

RTX3000

51.38 Show IGMP Group Management Information

[Syntax]**show status ip igmp****[Description]**

Shows a list of information managed by IGMP.

If an IGMP proxy is running, this command can be used to check the forwarding destination.

[Models]

RTX3000

51.39 Show Information Managed by PIM-SM

[Syntax]

show status ip pim sparse

[Description]

Shows a list of information managed by PIM-SM.

[Models]

RTX3000

51.40 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]

RTX3000, RTX1200, RTX1100, RT107e

51.41 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]

RTX3000, RTX1200

51.42 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

Mark	Condition
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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.43 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]

The jumbo group can be used only on models that support the 1000BASE-T LAN interface and the transmission of 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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.44 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
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 (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

[Note]

You can only set *info* to dcc on the RTX1200 and RTX800.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.45 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

Setting	Description
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]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.46 Show OSPFv3 Information

[Syntax]

show ipv6 ospf *info*

[Setting and Initial value]

- *info*
 - [Setting] :

Setting	Description
database	OSPFv3 database
neighbor	Neighbor router
interface	Status of each interface
virtual-link	Status of the virtual link

- [Initial value] : -

[Description]

Shows the OSPFv3 status.

[Models]

RTX3000

51.47 Show the Input Cut-Off Filter Status

[Syntax]

show status ip inbound filter [*type*]

show status ipv6 inbound filter [*type*]

[Setting and Initial value]

- *type* : Display type
 - [Setting] :

Setting	Description
summary	Only display a summary

- [Initial value] : -

[Description]

Shows the input cut-off filter status.

[Models]

RTX1200, RTX800

51.48 Show the Policy Filter Status

[Syntax]

show status ip policy filter [*id* [*type*]]

show status ipv6 policy filter [*id* [*type*]]

[Setting and Initial value]

- *id*
 - [Setting] : The ID of the filter whose information you want to display (1..65535) When omitted, the information for all filters is shown.
 - [Initial value] : -
- *type* : The display type
 - [Setting] :

Setting	Description
connection	The connection information related to the specified filter is displayed.

- [Initial value] : -

[Description]

Shows the policy filter status.

[Models]

RTX1200, RTX800

51.49 Show the Services Affected by the Policy Filter

[Syntax]

show status ip policy service

show status ipv6 policy service

[Description]

Shows the services that are affected by the policy filter.

[Models]

RTX1200, RTX800

51.50 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.

The WAN interface can be specified in RTX1200/RTX800 loading firmware Rev.10.01.32 and later.

[Models]

RTX1200, RTX800

51.51 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)

[Note]

RTX3000 loading firmware Rev.9.00.31 and later can use this function.

RTX1100 and RT107e loading firmware Rev.8.03.60 and later can use this function.

[Models]

RTX1200, RTX800

51.52 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]

RTX1200, RTX800

51.53 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]
RTX1200, RTX800

51.54 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]
RTX3000, RTX1200, RTX1100, RT107e, RTX800

51.55 Show the Operation Status of the microSD Slot

[Syntax]
show status sd

[Description]

Shows the operation status of the microSD slot.

[Models]
RTX1200

51.56 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]
RTX1200, RTX800

51.57 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
#
```

[Note]

RTX1200 loading firmware Rev.10.01.16 and later can use this function.

[Models]

RTX1200, RTX800

51.58 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.

[Note]

The *num* parameter can be specified on firmware Rev.10.01 and later.

[Models]

RTX1200, RTX800

51.59 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]

RTX1200

51.60 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]

RTX1200

51.61 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]

RTX1200

51.62 Display the DNS Cache

[Syntax]

show dns cache

[Description]

Displays the DNS cache content.

[Note]

RTX1200/RTX800 loading firmware Rev.10.01.36 can use this function.

[Models]

RTX1200, RTX800

Chapter 52

Logging

52.1 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.

The RTX1200 can log a maximum of 10,000 entries. Models other than RTX1200 can log a maximum of 500 entries. 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.

When the router is turned off, the log of models without the power-off log saving function is cleared.

When external-memory is specified, the SYSLOG file in the external memory is displayed.

When external-memory backup is specified, RTX1200 shows the contents of the SYSLOG backup file. To show the contents of the backup file, specify date and time data of the displayed file name (15-digit text string in the form of yyyymmdd_hhmmss) for *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.

The saved parameter is available on RTX1200/RTX800 loading firmware Rev.10.01.36 and later.

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.

The external-memory and backup parameters are available on firmware Rev.10.01.11 and later.

[Models]

RTX3000, RTX1200, RTX1100, RT107e, RTX800

52.2 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 ISDN fee

[Note]

All charging amount information is cleared when the router is turned OFF or restarted.

A charging amount is based on the sum of charging information notified from NTT via ISDN. Therefore, when you are using a discount service, the charging amount may be different from the amount claimed by NTT. Also, when you communicate by using a carrier other than NTT, no charging information is sent, and therefore, no account is made up.

[Models]

RTX3000, RTX1200, RTX1100

52.3 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]

RTX3000, RTX1200, RTX1100

52.4 Show the Communication History

[Syntax]

show history

[Description]

Shows the communication history.

[Models]

RT107e

Index

Symbols

> [35](#)
 >> [35](#)

A

account threshold [77](#)
 account threshold pp [77](#)
 administrator [482](#)
 administrator password [38](#)
 administrator password encrypted [38](#)
 administrator radius auth [40](#)
 alarm batch [72](#)
 alarm entire [71](#)
 alarm http revision-up [73](#)
 alarm http upload [416](#)
 alarm lua [441](#)
 alarm mobile [424](#)
 alarm sd [72](#)
 alarm startup [72](#)
 alarm usbhost [71](#)
 auth user [221](#)
 auth user attribute [221](#)
 auth user group [222](#)
 auth user group attribute [222](#)

B

bgp aggregate [321](#)
 bgp aggregate filter [321](#)
 bgp autonomous-system [322](#)
 bgp configure refresh [326](#)
 bgp export [323](#)
 bgp export aspath [323](#)
 bgp export filter [324](#)
 bgp import [325](#)
 bgp import filter [326](#)
 bgp log [328](#)
 bgp neighbor [327](#)
 bgp preference [323](#)
 bgp router id [322](#)
 bgp use [321](#)

C

clear account [487](#)
 clear account pp [488](#)
 clear arp [488](#)
 clear boot list [490](#)
 clear diagnosis config port [479](#)
 clear dns cache [488](#)
 clear heartbeat2 [400](#)
 clear heartbeat2 id [400](#)
 clear heartbeat2 name [400](#)
 clear inarp [488](#)
 clear ip dynamic routing [488](#)
 clear ip inbound filter [501](#)
 clear ip policy filter [501](#)
 clear ipv6 dynamic routing [490](#)
 clear ipv6 inbound filter [501](#)
 clear ipv6 neighbor cache [490](#)

clear ipv6 policy filter [501](#)
 clear log [488](#)
 clear mobile access limitation [418](#)
 clear mobile access limitation pp [418](#)
 clear nat descriptor dynamic [489](#)
 clear nat descriptor interface dynamic [489](#)
 clear nat descriptor interface dynamic pp [489](#)
 clear nat descriptor interface dynamic tunnel [489](#)
 clear status [489](#)
 clear switching-hub macaddress [499](#)
 clear url filter [501](#)
 clear url filter pp [501](#)
 clear url filter tunnel [501](#)
 cold start [486](#)
 connect [494](#)
 connect pp [494](#)
 connect tunnel [494](#)
 console character [46](#)
 console columns [46](#)
 console info [47](#)
 console lines [47](#)
 console prompt [46](#)
 cooperation [301](#)
 cooperation bandwidth-measuring remote [301](#)
 cooperation load-watch control [306](#)
 cooperation load-watch remote [303](#)
 cooperation load-watch trigger [304](#)
 cooperation port [301](#)
 cooperation type go [306](#)
 copy [491](#)
 copy config [483](#)
 copy exec [484](#)

D

date [44](#)
 delete [491](#)
 delete config [485](#)
 delete exec [485](#)
 description [61](#)
 dhcp client client-identifier [187](#)
 dhcp client client-identifier pool [187](#)
 dhcp client client-identifier pp [187](#)
 dhcp client hostname [185](#)
 dhcp client hostname pool [185](#)
 dhcp client hostname pp [185](#)
 dhcp client option [188](#)
 dhcp client option pool [188](#)
 dhcp client option pp [188](#)
 dhcp client release linkdown [189](#)
 dhcp convert lease to bind [182](#)
 dhcp duplicate check [178](#)
 dhcp manual lease [183](#)
 dhcp manual release [184](#)
 dhcp relay select [185](#)
 dhcp relay server [184](#)
 dhcp relay threshold [185](#)
 dhcp scope [178](#)
 dhcp scope bind [179](#)
 dhcp scope lease type [181](#)
 dhcp scope option [182](#)
 dhcp server rfc2131 compliant [177](#)

[dhcp service 176](#)
[diagnose config port access 477](#)
[diagnose config port map 477](#)
[diagnosis config port history-num 478](#)
[diagnosis config port max-detect 478](#)
[disconnect 494](#)
[disconnect ip connection 497](#)
[disconnect ipv6 connection 499](#)
[disconnect pp 494](#)
[disconnect tunnel 494](#)
[disconnect user 42](#)
[dns cache max entry 288](#)
[dns cache use 287](#)
[dns domain 281](#)
[dns host 287](#)
[dns notice order 282](#)
[dns private address spoof 283](#)
[dns server 281](#)
[dns server dhcp 186](#)
[dns server pp 282](#)
[dns server select 284](#)
[dns service 281](#)
[dns service fallback 288](#)
[dns srcport 286](#)
[dns static 285](#)
[dns syslog resolv 283](#)

E

[ethernet filter 138](#)
[ethernet interface filter 139](#)
[execute at-command 418](#)
[execute batch 409](#)
[exit 482](#)
[external-memory auto-search time 409](#)
[external-memory batch filename 410](#)
[external-memory boot permit 407](#)
[external-memory config filename 408](#)
[external-memory exec filename 407](#)
[external-memory performance-test go 410](#)
[external-memory statistics filename prefix 403](#)
[external-memory syslog filename 405](#)

G

[grep 33](#)

H

[heartbeat pre-shared-key 393](#)
[heartbeat receive 393](#)
[heartbeat send 394](#)
[heartbeat2 myname 395](#)
[heartbeat2 receive 397](#)
[heartbeat2 receive enable 398](#)
[heartbeat2 receive log 399](#)
[heartbeat2 receive monitor 398](#)
[heartbeat2 receive record limit 399](#)
[heartbeat2 transmit 395](#)
[heartbeat2 transmit enable 396](#)
[heartbeat2 transmit interval 396](#)
[heartbeat2 transmit log 397](#)
[help 37](#)
[http revision-down permit 65](#)
[http revision-up go 500](#)
[http revision-up permit 63](#)

[http revision-up proxy 64](#)
[http revision-up schedule 65](#)
[http revision-up timeout 64](#)
[http revision-up url 64](#)
[http upload 413](#)
[http upload go 415](#)
[http upload permit 414](#)
[http upload proxy 415](#)
[http upload retry interval 415](#)
[http upload timeout 414](#)
[http upload url 414](#)
[httpd custom-gui api password 443](#)
[httpd custom-gui api use 443](#)
[httpd custom-gui use 442](#)
[httpd custom-gui user 442](#)
[httpd host 370](#)
[httpd listen 371](#)
[httpd service 370](#)
[httpd timeout 371](#)

I

[interface reset 493](#)
[interface reset pp 494](#)
[ip arp timer 108](#)
[ip filter 95](#)
[ip filter directed-broadcast 98](#)
[ip filter dynamic 99](#)
[ip filter dynamic timer 100](#)
[ip filter set 98](#)
[ip filter source-route 98](#)
[ip flow timer 135](#)
[ip forward filter 135](#)
[ip fragment remove df-bit 107](#)
[ip host 285](#)
[ip icmp echo-reply send 190](#)
[ip icmp echo-reply send-only-linkup 190](#)
[ip icmp error-decrypted-ipsec send 193](#)
[ip icmp log 193](#)
[ip icmp mask-reply send 190](#)
[ip icmp parameter-problem send 191](#)
[ip icmp redirect receive 191](#)
[ip icmp redirect send 191](#)
[ip icmp time-exceeded send 192](#)
[ip icmp timestamp-reply send 192](#)
[ip icmp unreachable send 192](#)
[ip icmp unreachable-for-truncated send 194](#)
[ip implicit-route preference 134](#)
[ip inbound filter 141](#)
[ip interface address 90](#)
[ip interface arp log 110](#)
[ip interface arp mtu discovery 194](#)
[ip interface arp queue length 109](#)
[ip interface arp static 108](#)
[ip interface dhcp lease time 186](#)
[ip interface dhcp retry 187](#)
[ip interface dhcp retry 136](#)
[ip interface igmp 130](#)
[ip interface igmp static 131](#)
[ip interface inbound filter list 143](#)
[ip interface intrusion detection 101](#)
[ip interface intrusion detection notice-interval 102](#)
[ip interface intrusion detection repeat-control 102](#)
[ip interface intrusion detection report 103](#)
[ip interface intrusion detection threshold 103](#)
[ip interface mtu 92](#)

- ip interface nat descriptor [271](#)
- ip interface ospf area [315](#)
- ip interface ospf neighbor [318](#)
- ip interface pim sparse [132](#)
- ip interface proxyarp [108](#)
- ip interface proxyarp vrrp [108](#)
- ip interface rebound [92](#)
- ip interface rip auth key [118](#)
- ip interface rip auth key text [118](#)
- ip interface rip auth type [117](#)
- ip interface rip filter [116](#)
- ip interface rip force-to-advertise [121](#)
- ip interface rip hop [117](#)
- ip interface rip receive [116](#)
- ip interface rip send [115](#)
- ip interface rip trust gateway [114](#)
- ip interface secondary address [91](#)
- ip interface secure filter [105](#)
- ip interface secure filter name [105](#)
- ip interface tcp mss limit [104](#)
- ip interface vrrp [123](#)
- ip interface vrrp shutdown trigger [123](#)
- ip interface wol relay [60](#)
- ip keepalive [128](#)
- ip local forward filter [136](#)
- ip pim sparse log [133](#)
- ip pim sparse register-checksum [134](#)
- ip pim sparse rendezvous-point static [133](#)
- ip policy address group [145](#)
- ip policy filter [146](#)
- ip policy filter set [148](#)
- ip policy filter set enable [149](#)
- ip policy filter set switch [149](#)
- ip policy filter timer [150](#)
- ip policy interface group [144](#)
- ip policy service [144](#)
- ip policy service group [146](#)
- ip pp address [90](#)
- ip pp forward filter [136](#)
- ip pp igmp [130](#)
- ip pp igmp static [131](#)
- ip pp inbound filter list [143](#)
- ip pp intrusion detection [101](#)
- ip pp intrusion detection notice-interval [102](#)
- ip pp intrusion detection repeat-control [102](#)
- ip pp intrusion detection report [103](#)
- ip pp intrusion detection threshold [103](#)
- ip pp mtu [92](#)
- ip pp nat descriptor [271](#)
- ip pp ospf area [315](#)
- ip pp ospf neighbor [318](#)
- ip pp pim sparse [132](#)
- ip pp rebound [92](#)
- ip pp remote address [110](#)
- ip pp remote address pool [111](#)
- ip pp rip auth key [118](#)
- ip pp rip auth key text [118](#)
- ip pp rip auth type [117](#)
- ip pp rip backup interface [120](#)
- ip pp rip connect interval [119](#)
- ip pp rip connect send [119](#)
- ip pp rip disconnect interval [120](#)
- ip pp rip disconnect send [119](#)
- ip pp rip filter [116](#)
- ip pp rip force-to-advertise [121](#)
- ip pp rip hold routing [118](#)

- ip pp rip hop [117](#)
- ip pp rip receive [116](#)
- ip pp rip send [115](#)
- ip pp rip trust gateway [114](#)
- ip pp secure filter [105](#)
- ip pp secure filter name [105](#)
- ip pp tcp mss limit [104](#)
- ip route [93](#)
- ip route change log [105](#)
- ip routing [90](#)
- ip routing process [52](#)
- ip simple-service [93](#)
- ip stealth [193](#)
- ip tos supersede [107](#)
- ip tunnel address [201](#)
- ip tunnel forward filter [136](#)
- ip tunnel igmp [130](#)
- ip tunnel igmp static [131](#)
- ip tunnel inbound filter list [143](#)
- ip tunnel intrusion detection [101](#)
- ip tunnel intrusion detection notice-interval [102](#)
- ip tunnel intrusion detection repeat-control [102](#)
- ip tunnel intrusion detection report [103](#)
- ip tunnel intrusion detection threshold [103](#)
- ip tunnel mtu [92](#)
- ip tunnel nat descriptor [271](#)
- ip tunnel ospf area [315](#)
- ip tunnel ospf neighbor [318](#)
- ip tunnel pim sparse [132](#)
- ip tunnel rebound [92](#)
- ip tunnel remote address [201](#)
- ip tunnel rip auth key [118](#)
- ip tunnel rip auth key text [118](#)
- ip tunnel rip auth type [117](#)
- ip tunnel rip filter [116](#)
- ip tunnel rip force-to-advertise [121](#)
- ip tunnel rip hop [117](#)
- ip tunnel rip receive [116](#)
- ip tunnel rip send [115](#)
- ip tunnel rip trust gateway [114](#)
- ip tunnel secure filter [105](#)
- ip tunnel secure filter name [105](#)
- ip tunnel tcp mss limit [104](#)
- ipsec auto refresh [208](#)
- ipsec ike always-on [209](#)
- ipsec ike auth method [204](#)
- ipsec ike duration [227](#)
- ipsec ike eap myname [206](#)
- ipsec ike eap request [207](#)
- ipsec ike eap send certreq [207](#)
- ipsec ike encryption [216](#)
- ipsec ike esp-encapsulation [227](#)
- ipsec ike group [217](#)
- ipsec ike hash [218](#)
- ipsec ike keepalive log [215](#)
- ipsec ike keepalive use [214](#)
- ipsec ike license-key [225](#)
- ipsec ike license-key use [226](#)
- ipsec ike local address [213](#)
- ipsec ike local id [213](#)
- ipsec ike local name [212](#)
- ipsec ike log [226](#)
- ipsec ike mode-cfg address [225](#)
- ipsec ike mode-cfg address pool [224](#)
- ipsec ike mode-cfg method [224](#)
- ipsec ike nat-traversal [231](#)

- ipsec ike negotiate-strictly [208](#)
- ipsec ike payload type [219](#)
- ipsec ike pfs [220](#)
- ipsec ike pki file [206](#)
- ipsec ike pre-shared-key [205](#)
- ipsec ike queue length [216](#)
- ipsec ike remote address [211](#)
- ipsec ike remote id [211](#)
- ipsec ike remote name [210](#)
- ipsec ike restrict-dangling-sa [230](#)
- ipsec ike retry [209](#)
- ipsec ike send info [219](#)
- ipsec ike version [204](#)
- ipsec ike xauth myname [220](#)
- ipsec ike xauth request [223](#)
- ipsec ipcomp type [233](#)
- ipsec log illegal-spi [218](#)
- ipsec refresh sa [230](#)
- ipsec sa delete [232](#)
- ipsec sa policy [228](#)
- ipsec transport [236](#)
- ipsec tunnel [233](#)
- ipsec tunnel outer df-bit [232](#)
- ipsec use [203](#)
- ipv6 filter [344](#)
- ipv6 filter dynamic [346](#)
- ipv6 icmp echo-reply send [195](#)
- ipv6 icmp echo-reply send-only-linkup [195](#)
- ipv6 icmp error-decrypted-ipsec send [198](#)
- ipv6 icmp log [197](#)
- ipv6 icmp packet-too-big send [198](#)
- ipv6 icmp packet-too-big-for-truncated send [199](#)
- ipv6 icmp parameter-problem send [196](#)
- ipv6 icmp redirect receive [196](#)
- ipv6 icmp redirect send [196](#)
- ipv6 icmp time-exceeded send [197](#)
- ipv6 icmp unreachable send [197](#)
- ipv6 inbound filter [141](#)
- ipv6 interface address [331](#)
- ipv6 interface dad retry count [334](#)
- ipv6 interface dhcp service [334](#)
- ipv6 interface inbound filter list [143](#)
- ipv6 interface mld [348](#)
- ipv6 interface mld static [348](#)
- ipv6 interface mtu [329](#)
- ipv6 interface ospf area [353](#)
- ipv6 interface prefix [332](#)
- ipv6 interface rip filter [341](#)
- ipv6 interface rip hop [341](#)
- ipv6 interface rip receive [340](#)
- ipv6 interface rip send [340](#)
- ipv6 interface rip trust gateway [341](#)
- ipv6 interface rtadv send [337](#)
- ipv6 interface secure filter [345](#)
- ipv6 interface tcp mss limit [329](#)
- ipv6 max auto address [335](#)
- ipv6 multicast routing process [349](#)
- ipv6 nd ns-trigger-dad [350](#)
- ipv6 ospf area [352](#)
- ipv6 ospf area network [352](#)
- ipv6 ospf configure refresh [351](#)
- ipv6 ospf export [356](#)
- ipv6 ospf export from ospf [356](#)
- ipv6 ospf import [358](#)
- ipv6 ospf import from [358](#)
- ipv6 ospf log [360](#)
- ipv6 ospf preference [356](#)
- ipv6 ospf router id [351](#)
- ipv6 ospf use [351](#)
- ipv6 ospf virtual-link [355](#)
- ipv6 policy address group [145](#)
- ipv6 policy filter [146](#)
- ipv6 policy filter set [148](#)
- ipv6 policy filter set enable [149](#)
- ipv6 policy filter set switch [149](#)
- ipv6 policy interface group [144](#)
- ipv6 policy service [144](#)
- ipv6 policy service group [146](#)
- ipv6 pp address [331](#)
- ipv6 pp dad retry count [334](#)
- ipv6 pp dhcp service [334](#)
- ipv6 pp inbound filter list [143](#)
- ipv6 pp mld [348](#)
- ipv6 pp mld static [348](#)
- ipv6 pp mtu [329](#)
- ipv6 pp ospf area [353](#)
- ipv6 pp prefix [332](#)
- ipv6 pp rip connect interval [342](#)
- ipv6 pp rip connect send [342](#)
- ipv6 pp rip disconnect interval [343](#)
- ipv6 pp rip disconnect send [343](#)
- ipv6 pp rip filter [341](#)
- ipv6 pp rip hold routing [343](#)
- ipv6 pp rip hop [341](#)
- ipv6 pp rip receive [340](#)
- ipv6 pp rip send [340](#)
- ipv6 pp rip trust gateway [341](#)
- ipv6 pp rtadv send [337](#)
- ipv6 pp secure filter [345](#)
- ipv6 pp tcp mss limit [329](#)
- ipv6 prefix [335](#)
- ipv6 rh0 discard [330](#)
- ipv6 rip preference [344](#)
- ipv6 rip use [339](#)
- ipv6 route [338](#)
- ipv6 routing [329](#)
- ipv6 routing process [330](#)
- ipv6 source address selection rule [335](#)
- ipv6 stealth [198](#)
- ipv6 tunnel address [331](#)
- ipv6 tunnel dhcp service [334](#)
- ipv6 tunnel inbound filter list [143](#)
- ipv6 tunnel mld [348](#)
- ipv6 tunnel mld static [348](#)
- ipv6 tunnel ospf area [353](#)
- ipv6 tunnel prefix [332](#)
- ipv6 tunnel rip filter [341](#)
- ipv6 tunnel rip receive [340](#)
- ipv6 tunnel rip send [340](#)
- ipv6 tunnel secure filter [345](#)
- ipv6 tunnel tcp mss limit [329](#)
- isdn arrive permit [82](#)
- isdn auto connect [81](#)
- isdn call block time [83](#)
- isdn call permit [82](#)
- isdn call prohibit time [83](#)
- isdn callback mscbcu user-specify [85](#)
- isdn callback permit [84](#)
- isdn callback permit type [84](#)
- isdn callback request [83](#)
- isdn callback request type [84](#)
- isdn callback response time [85](#)

- isdn callback wait time [85](#)
- isdn disconnect input time [87](#)
- isdn disconnect interval time [88](#)
- isdn disconnect output time [88](#)
- isdn disconnect policy [86](#)
- isdn disconnect time [86](#)
- isdn fast disconnect time [86](#)
- isdn forced disconnect time [87](#)
- isdn local address [76](#)
- isdn piafs arrive [78](#)
- isdn piafs call [79](#)
- isdn piafs control [78](#)
- isdn remote address [80](#)
- isdn remote call order [81](#)
- isdn terminator [77](#)

L

- l2tp keepalive log [241](#)
- l2tp keepalive use [240](#)
- l2tp service [239](#)
- l2tp syslog [241](#)
- l2tp tunnel auth [239](#)
- l2tp tunnel disconnect time [240](#)
- lan backup [126](#)
- lan backup recovery time [126](#)
- lan keepalive interval [127](#)
- lan keepalive log [128](#)
- lan keepalive use [127](#)
- lan linkup send-wait-time [53](#)
- lan port-mirroring [53](#)
- lan receive-buffer-size [59](#)
- lan shutdown [53](#)
- lan type [54](#)
- leased keepalive down [113](#)
- less [34](#)
- less config [503](#)
- less config list [504](#)
- less config pp [503](#)
- less config tunnel [504](#)
- less exec list [506](#)
- less file list [504](#)
- less log [530](#)
- line type [76](#)
- login password [38](#)
- login password encrypted [38](#)
- login radius use [39](#)
- login timer [59](#)
- login user [39](#)
- lua [438](#)
- lua use [438](#)
- luac [439](#)

M

- mail notify [367](#)
- mail notify status exec [502](#)
- mail server name [364](#)
- mail server pop [365](#)
- mail server smtp [364](#)
- mail server timeout [366](#)
- mail template [366](#)
- mail-notify status exec [363](#)
- mail-notify status from [361](#)
- mail-notify status server [361](#)
- mail-notify status subject [362](#)

- mail-notify status timeout [362](#)
- mail-notify status to [361](#)
- mail-notify status type [362](#)
- mail-notify status use [361](#)
- make directory [490](#)
- mobile access limit connection length [425](#)
- mobile access limit connection time [425](#)
- mobile access limit duration [426](#)
- mobile access limit length [421](#)
- mobile access limit time [422](#)
- mobile access-point name [420](#)
- mobile auto connect [419](#)
- mobile call prohibit auth-error count [423](#)
- mobile dial number [421](#)
- mobile disconnect input time [419](#)
- mobile disconnect output time [420](#)
- mobile disconnect time [419](#)
- mobile display caller id [424](#)
- mobile pin code [417](#)
- mobile signal-strength [426](#)
- mobile signal-strength go [426](#)
- mobile syslog [424](#)
- mobile use [417](#)

N

- nat descriptor address inner [273](#)
- nat descriptor address outer [272](#)
- nat descriptor ftp port [277](#)
- nat descriptor log [278](#)
- nat descriptor masquerade incoming [276](#)
- nat descriptor masquerade port range [277](#)
- nat descriptor masquerade remove df-bit [279](#)
- nat descriptor masquerade rlogin [274](#)
- nat descriptor masquerade session limit [279](#)
- nat descriptor masquerade static [274](#)
- nat descriptor masquerade ttl hold [276](#)
- nat descriptor masquerade unconvertible port [278](#)
- nat descriptor sip [278](#)
- nat descriptor static [273](#)
- nat descriptor timer [275](#)
- nat descriptor type [271](#)
- netvolante-dns auto hostname [379](#)
- netvolante-dns auto hostname pp [379](#)
- netvolante-dns auto save [383](#)
- netvolante-dns delete go [378](#)
- netvolante-dns delete go pp [378](#)
- netvolante-dns get hostname list [378](#)
- netvolante-dns get hostname list pp [378](#)
- netvolante-dns go [377](#)
- netvolante-dns go pp [377](#)
- netvolante-dns hostname host [379](#)
- netvolante-dns hostname host pp [379](#)
- netvolante-dns port [378](#)
- netvolante-dns register timer [382](#)
- netvolante-dns retry interval [382](#)
- netvolante-dns retry interval pp [382](#)
- netvolante-dns server [380](#)
- netvolante-dns server update address port [381](#)
- netvolante-dns server update address use [381](#)
- netvolante-dns set hostname [380](#)
- netvolante-dns timeout [379](#)
- netvolante-dns timeout pp [379](#)
- netvolante-dns use [377](#)
- netvolante-dns use pp [377](#)
- nslookup [497](#)

ntp local address [45](#)
 ntpdate [45](#)

O

operation button function download [411](#)
 operation execute batch permit [412](#)
 operation external-memory download permit [406](#)
 operation http revision-up permit [65](#)
 ospf area [313](#)
 ospf area network [313](#)
 ospf area stubhost [314](#)
 ospf configure refresh [308](#)
 ospf export filter [310](#)
 ospf export from ospf [309](#)
 ospf import filter [311](#)
 ospf import from [309](#)
 ospf log [319](#)
 ospf merge equal cost stub [319](#)
 ospf preference [308](#)
 ospf router id [308](#)
 ospf use [308](#)
 ospf virtual-link [314](#)

P

ping [495](#)
 ping6 [496](#)
 pki certificate file [237](#)
 pki crl file [238](#)
 pp always-on [80](#)
 pp auth accept [157](#), [245](#)
 pp auth multi connect prohibit [158](#)
 pp auth myname [158](#)
 pp auth request [157](#), [245](#)
 pp auth username [156](#)
 pp backup [125](#)
 pp backup pp [125](#)
 pp backup recovery time [125](#)
 pp backup tunnel [125](#)
 pp bind [77](#), [243](#)
 pp disable [492](#)
 pp enable [492](#)
 pp keepalive interval [111](#)
 pp keepalive log [113](#)
 pp keepalive use [112](#)
 pp name [371](#)
 pp select [481](#)
 ppp bacp maxconfigure [171](#)
 ppp bacp maxfailure [171](#)
 ppp bacp maxterminate [171](#)
 ppp bacp restart [170](#)
 ppp bap maxretry [172](#)
 ppp bap restart [171](#)
 ppp ccp maxconfigure [167](#)
 ppp ccp maxfailure [167](#)
 ppp ccp maxterminate [167](#)
 ppp ccp no-encryption [248](#)
 ppp ccp restart [167](#)
 ppp ccp type [166](#)
 ppp chap maxchallenge [162](#)
 ppp chap restart [162](#)
 ppp ipcp ipaddress [163](#)
 ppp ipcp maxconfigure [164](#)
 ppp ipcp maxfailure [164](#)
 ppp ipcp maxterminate [164](#)
 ppp ipcp msexp [165](#)
 ppp ipcp remote address check [165](#)
 ppp ipcp restart [163](#)
 ppp ipcp vjc [163](#)
 ppp ipv6cp use [168](#)
 ppp lcp accm [423](#)
 ppp lcp acfc [159](#)
 ppp lcp magicnumber [159](#)
 ppp lcp maxconfigure [161](#)
 ppp lcp maxfailure [161](#)
 ppp lcp maxterminate [160](#)
 ppp lcp mru [159](#)
 ppp lcp pfc [160](#)
 ppp lcp restart [160](#)
 ppp lcp silent [161](#)
 ppp mp control [168](#)
 ppp mp divide [170](#)
 ppp mp interleave [294](#)
 ppp mp load threshold [169](#)
 ppp mp maxlink [169](#)
 ppp mp minlink [169](#)
 ppp mp timer [170](#)
 ppp mp use [168](#)
 ppp msccp maxretry [166](#)
 ppp msccp restart [165](#)
 ppp pap maxauthreq [162](#)
 ppp pap restart [162](#)
 pppoe access concentrator [172](#)
 pppoe auto connect [172](#)
 pppoe auto disconnect [173](#)
 pppoe disconnect time [174](#)
 pppoe invalid-session forced close [175](#)
 pppoe padi maxretry [173](#)
 pppoe padi restart [173](#)
 pppoe padr maxretry [174](#)
 pppoe padr restart [174](#)
 pppoe service-name [174](#)
 pppoe tcp mss limit [175](#)
 pppoe use [172](#)
 pptp hostname [244](#)
 pptp keepalive interval [248](#)
 pptp keepalive log [247](#)
 pptp keepalive use [247](#)
 pptp service [243](#)
 pptp service type [244](#)
 pptp syslog [246](#)
 pptp tunnel disconnect time [246](#)
 pptp window size [244](#)
 provider auto connect forced disable [375](#)
 provider dns server [373](#)
 provider dns server pp [374](#)
 provider filter routing [374](#)
 provider interface dns server [373](#)
 provider interface name [374](#)
 provider ipv6 connect pp [376](#)
 provider ntp server [375](#)
 provider ntpdate [375](#)
 provider select [372](#)
 provider set [372](#)
 provider type [372](#)

Q

queue class filter [290](#)
 queue interface class control [298](#)
 queue interface class filter list [294](#)

- queue interface class property [297](#)
- queue interface default class [296](#)
- queue interface default class secondary [296](#)
- queue interface length [295](#)
- queue interface length secondary [296](#)
- queue interface type [293](#)
- queue pp class filter list [294](#)
- queue pp class property [297](#)
- queue pp default class [296](#)
- queue pp length [295](#)
- queue pp type [293](#)
- queue tunnel class filter list [294](#)
- quit [482](#)

R

- radius account [267](#)
- radius account port [269](#)
- radius account server [268](#)
- radius auth [267](#)
- radius auth port [269](#)
- radius auth server [268](#)
- radius retry [269](#)
- radius secret [269](#)
- radius server [267](#)
- rdate [44](#)
- remote setup [486](#)
- remote setup accept [487](#)
- rename [492](#)
- restart [493](#)
- rip filter rule [121](#)
- rip preference [115](#)
- rip timer [122](#)
- rip use [114](#)
- rtfs format [75](#)
- rtfs garbage-collect [75](#)

S

- save [482](#)
- schedule at [388](#)
- sd use [403](#)
- security class [43](#)
- set [74](#)
- set-default-config [486](#)
- set-default-exec [486](#)
- sftpd host [69](#)
- show account [531](#)
- show account pp [531](#)
- show arp [507](#)
- show command [37](#)
- show config [503](#)
- show config list [504](#)
- show config pp [503](#)
- show config tunnel [504](#)
- show diagnosis config port access [479](#)
- show diagnosis config port map [479](#)
- show dlci [508](#)
- show dns cache [529](#)
- show environment [503](#)
- show exec list [506](#)
- show file list [504](#)
- show history [531](#)
- show ip connection [515](#)
- show ip connection pp [515](#)
- show ip connection tunnel [515](#)

- show ip intrusion detection [517](#)
- show ip intrusion detection pp [517](#)
- show ip intrusion detection tunnel [517](#)
- show ip mroute [520](#)
- show ip rip table [509](#)
- show ip route [508](#)
- show ip secure filter [505](#)
- show ip secure filter pp [505](#)
- show ip secure filter tunnel [505](#)
- show ipsec sa [510](#)
- show ipsec sa gateway [510](#)
- show ipv6 address [505](#)
- show ipv6 address pp [505](#)
- show ipv6 address tunnel [505](#)
- show ipv6 connection [516](#)
- show ipv6 connection pp [516](#)
- show ipv6 connection tunnel [516](#)
- show ipv6 mroute fib [521](#)
- show ipv6 neighbor cache [509](#)
- show ipv6 ospf [524](#)
- show ipv6 rip table [509](#)
- show ipv6 route [509](#)
- show log [530](#)
- show nat descriptor address [511](#)
- show nat descriptor interface address [512](#)
- show nat descriptor interface address pp [512](#)
- show nat descriptor interface address tunnel [512](#)
- show nat descriptor interface bind [512](#)
- show nat descriptor interface bind pp [512](#)
- show nat descriptor interface bind tunnel [512](#)
- show nat descriptor masquerade port summary [513](#)
- show pki certificate summary [510](#)
- show pki crt [511](#)
- show pp connect time [517](#)
- show sshd public key [505](#)
- show status [507](#)
- show status backup [515](#)
- show status bgp neighbor [514](#)
- show status boot [528](#)
- show status boot all [528](#)
- show status boot list [528](#)
- show status cooperation [523](#)
- show status dhcp [514](#)
- show status dhcpc [515](#)
- show status ethernet filter [140](#)
- show status external-memory [527](#)
- show status heartbeat [526](#)
- show status heartbeat2 [400](#)
- show status heartbeat2 id [400](#)
- show status heartbeat2 name [400](#)
- show status ip igmp [520](#)
- show status ip inbound filter [524](#)
- show status ip keepalive [517](#)
- show status ip pim sparse [521](#)
- show status ip policy filter [525](#)
- show status ip policy service [525](#)
- show status ipv6 dhcp [515](#)
- show status ipv6 inbound filter [524](#)
- show status ipv6 mld [521](#)
- show status ipv6 policy filter [525](#)
- show status ipv6 policy service [525](#)
- show status l2tp [513](#)
- show status lua [439](#)
- show status mail service [519](#)
- show status mobile signal-strength [427](#)
- show status netvolante-dns [518](#)

[show status netvolante-dns pp 518](#)
[show status ospf 513](#)
[show status packet-buffer 522](#)
[show status pp 507](#)
[show status pptp 513](#)
[show status qos 523](#)
[show status remote setup 526](#)
[show status rtfis 527](#)
[show status sd 527](#)
[show status switch control 529](#)
[show status switching-hub macaddress 518](#)
[show status tunnel 519](#)
[show status upnp 519](#)
[show status usbhost 526](#)
[show status user 521](#)
[show status vlan 519](#)
[show status vrrp 511](#)
[show techinfo 527](#)
[show url filter 525](#)
[show url filter pp 525](#)
[show url filter tunnel 525](#)
[sip arrive address check 250](#)
[sip arrive session timer method 250](#)
[sip arrive session timer refresher 249](#)
[sip log 251](#)
[sip response code busy 251](#)
[sip use 249](#)
[sip user agent 249](#)
[snmp community read-only 252](#)
[snmp community read-write 253](#)
[snmp display ipcp force 263](#)
[snmp host 252](#)
[snmp ifindex switch static index 264](#)
[snmp local address 259](#)
[snmp syscontact 259](#)
[snmp syslocation 259](#)
[snmp sysname 260](#)
[snmp trap community 253](#)
[snmp trap enable snmp 260](#)
[snmp trap enable switch 265](#)
[snmp trap enable switch common 265](#)
[snmp trap host 253](#)
[snmp trap link-updown separate-l2switch-port 263](#)
[snmp trap mobile signal-strength 263](#)
[snmp trap send linkdown 261](#)
[snmp trap send linkdown pp 261](#)
[snmp trap send linkdown tunnel 261](#)
[snmp yrippedisplayatmib2 261](#)
[snmp yrifswitchdisplayatmib2 262](#)
[snmp yrifunneldisplayatmib2 262](#)
[snmp yrswindex switch static index 264](#)
[snmpv2c community read-only 254](#)
[snmpv2c community read-write 254](#)
[snmpv2c host 254](#)
[snmpv2c trap community 255](#)
[snmpv2c trap host 255](#)
[snmpv3 context name 256](#)
[snmpv3 engine id 255](#)
[snmpv3 host 257](#)
[snmpv3 trap host 258](#)
[snmpv3 usm user 256](#)
[snmpv3 vacm access 258](#)
[snmpv3 vacm view 257](#)
[sntpd host 401](#)
[sntpd service 401](#)
[speed 290](#)
[speed pp 290](#)
[sshd client alive 69](#)
[sshd encrypt algorithm 68](#)
[sshd host 67](#)
[sshd host key generate 68](#)
[sshd listen 67](#)
[sshd service 66](#)
[sshd session 67](#)
[statistics 480](#)
[switch control firmware upload go 447](#)
[switch control function default 447](#)
[switch control function execute 446](#)
[switch control function execute clear-counter 473](#)
[switch control function execute clear-macaddress-table 457](#)
[switch control function execute reset-loopdetect 476](#)
[switch control function execute restart 451](#)
[switch control function get 446](#)
[switch control function get boot-rom-version 448](#)
[switch control function get counter-frame-rx-type 468](#)
[switch control function get counter-frame-tx-type 470](#)
[switch control function get energy-saving 449](#)
[switch control function get firmware-revision 448](#)
[switch control function get led-brightness 450](#)
[switch control function get loopdetect-count 473](#)
[switch control function get loopdetect-linkdown 474](#)
[switch control function get loopdetect-port-use 475](#)
[switch control function get loopdetect-recovery-timer 474](#)
[switch control function get loopdetect-time 473](#)
[switch control function get macaddress-aging 455](#)
[switch control function get macaddress-aging-timer 456](#)
[switch control function get mirroring-dest 466](#)
[switch control function get mirroring-src-rx 467](#)
[switch control function get mirroring-src-tx 467](#)
[switch control function get mirroring-use 466](#)
[switch control function get model-name 449](#)
[switch control function get port-auto-crossover 453](#)
[switch control function get port-flow-control 454](#)
[switch control function get port-speed 452](#)
[switch control function get port-speed-downshift 453](#)
[switch control function get port-use 452](#)
[switch control function get qos-dscp-remark-class 462](#)
[switch control function get qos-dscp-remark-type 461](#)
[switch control function get qos-policing-speed 463](#)
[switch control function get qos-policing-use 463](#)
[switch control function get qos-shaping-speed 464](#)
[switch control function get qos-shaping-use 464](#)
[switch control function get qos-speed-unit 462](#)
[switch control function get serial-number 448](#)
[switch control function get status-counter-frame-rx 471](#)
[switch control function get status-counter-frame-tx 472](#)
[switch control function get status-counter-octet-rx 472](#)
[switch control function get status-counter-octet-tx 472](#)
[switch control function get status-fan 451](#)
[switch control function get status-led-mode 450](#)
[switch control function get status-loopdetect-port 475](#)
[switch control function get status-loopdetect-recovery-timer 476](#)
[switch control function get status-macaddress-addr 456](#)
[switch control function get status-macaddress-port 456](#)
[switch control function get status-port-speed 455](#)
[switch control function get system-macaddress 449](#)
[switch control function get system-name 449](#)
[switch control function get system-uptime 452](#)
[switch control function get vlan-access 459](#)
[switch control function get vlan-id 458](#)
[switch control function get vlan-multiple 460](#)
[switch control function get vlan-multiple-use 460](#)

switch control function get vlan-port-mode [458](#)
 switch control function get vlan-trunk [459](#)
 switch control function set [446](#)
 switch control function set counter-frame-rx-type [468](#)
 switch control function set counter-frame-tx-type [470](#)
 switch control function set energy-saving [449](#)
 switch control function set led-brightness [450](#)
 switch control function set loopdetect-count [473](#)
 switch control function set loopdetect-linkdown [474](#)
 switch control function set loopdetect-port-use [475](#)
 switch control function set loopdetect-recovery-timer [474](#)
 switch control function set loopdetect-time [473](#)
 switch control function set macaddress-aging [455](#)
 switch control function set macaddress-aging-timer [456](#)
 switch control function set mirroring-dest [466](#)
 switch control function set mirroring-src-rx [467](#)
 switch control function set mirroring-src-tx [467](#)
 switch control function set mirroring-use [466](#)
 switch control function set port-auto-crossover [453](#)
 switch control function set port-flow-control [454](#)
 switch control function set port-speed [452](#)
 switch control function set port-speed-downshift [453](#)
 switch control function set port-use [452](#)
 switch control function set qos-dscp-remark-class [462](#)
 switch control function set qos-dscp-remark-type [461](#)
 switch control function set qos-policing-speed [463](#)
 switch control function set qos-policing-use [463](#)
 switch control function set qos-shaping-speed [464](#)
 switch control function set qos-shaping-use [464](#)
 switch control function set qos-speed-unit [462](#)
 switch control function set system-name [449](#)
 switch control function set vlan-access [459](#)
 switch control function set vlan-id [458](#)
 switch control function set vlan-multiple [460](#)
 switch control function set vlan-multiple-use [460](#)
 switch control function set vlan-port-mode [458](#)
 switch control function set vlan-trunk [459](#)
 switch control use [444](#)
 switch control watch interval [445](#)
 switch select [445](#)
 syslog debug [49](#)
 syslog execute command [50](#)
 syslog facility [48](#)
 syslog host [48](#)
 syslog info [49](#)
 syslog local address [49](#)
 syslog notice [48](#)
 syslog srcport [50](#)
 system led brightness [73](#)
 system packet-buffer [70](#)
 system temperature threshold [52](#)

T

tcp log [61](#)
 tcp session limit [105](#)
 telnet [498](#)
 telnetd host [51](#)
 telnetd listen [51](#)
 telnetd service [50](#)
 telnetd session [51](#)
 terminate lua [440](#)

terminate lua file [440](#)
 tftp host [60](#)
 time [44](#)
 timezone [43](#)
 traceroute [497](#)
 traceroute6 [497](#)
 tunnel backup [234](#)
 tunnel backup pp [234](#)
 tunnel backup tunnel [234](#)
 tunnel disable [200](#)
 tunnel enable [200](#)
 tunnel encapsulation [200](#)
 tunnel endpoint address [202](#)
 tunnel endpoint name [246](#)
 tunnel name [371](#)
 tunnel select [481](#)
 tunnel template [234](#)

U

upnp external address refer [384](#)
 upnp external address refer pp [384](#)
 upnp port mapping timer [385](#)
 upnp port mapping timer type [384](#)
 upnp syslog [385](#)
 upnp use [384](#)
 url filter [152](#)
 url filter log [154](#)
 url filter port [153](#)
 url filter reject [154](#)
 url filter use [153](#)
 url interface filter [152](#)
 url pp filter [152](#)
 url tunnel filter [152](#)
 usbhost modem flow control [428](#)
 usbhost modem initialize [428](#)
 usbhost overcurrent duration [387](#)
 usbhost use [387](#)
 user attribute [40](#)

V

vlan interface 802.1q [391](#)
 vlan port mapping [391](#)

W

wan access limit connection length [435](#)
 wan access limit connection time [436](#)
 wan access limit duration [436](#)
 wan access limit length [433](#)
 wan access limit time [434](#)
 wan access-point name [432](#)
 wan always-on [432](#)
 wan auth myname [429](#)
 wan auto connect [430](#)
 wan bind [429](#)
 wan disconnect input time [431](#)
 wan disconnect output time [431](#)
 wan disconnect time [430](#)
 wins server [164](#)
 wol send [499](#)