

# Руководство пользователя

**QSR-2830**

## Оглавление

<b>1</b>	<b>CONFIGURING ACLS</b>	<b>17</b>
1.1	Overview	17
1.1.1	ACL Introduction	17
1.1.2	Why to Configure ACLs	17
1.1.3	When to Configure Access Lists	17
1.1.4	Input/Output ACL, Filtering Domain Template and Rule	18
1.2	Configuring IP Access List	19
1.2.1	Guide to Configuring IP ACLs	19
1.2.2	Configuring IP ACLs	21
1.2.3	Displaying IP ACLs	22
1.3	Configuring IPv6 Extended ACLs	22
1.3.1	Configuring IPv6 Extended ACLs	22
1.3.2	Displaying Configuration of IPv6 Extended ACLs	23
1.4	Configuring Extended Expert ACLs	23
1.4.1	Guide to Configuring Expert Extended ACLs	23
1.4.2	Configuring an Expert Extended ACL	23
1.4.3	Displaying Configuration of Expert Extended ACLs	24
1.5	Configuring MAC Extended ACLs	24
1.5.1	Guide to Configuring MAC Extended ACLs	24
1.5.2	Configuring a MAC Extended ACL	24
1.5.3	Displaying Configuration of MAC Extended ACLs	25
1.5.4	Other Related Configurations	25
1.5.5	Configuring ACEs by Priority	25
1.5.6	Configuring ACL Logging	26
1.5.7	Configuring ACL80	28
1.5.8	Configuring IP Options Filtering	29
1.5.9	Configuring ACLs Based on the Time Range	30
1.5.10	Configuring TCP Flag Filtering	31
1.5.11	Configuring Comments	32
1.5.12	Configuring SVI Router ACLs	33
1.6	Configuration Examples	33
1.6.1	IP ACL Example	33
1.6.2	IPv6 Extended ACL Configuration Example	35
1.6.3	Typical Application of Intranet ACL	36

1.6.3.1	Notes	36
1.6.4	Application of expert ACL & ACL 80	42
<b>2</b>	<b>CONFIGURING THE FIREWALL</b>	<b>45</b>
<b>2.1</b>	<b>Understanding IP-MAC Binding</b>	<b>45</b>
2.1.1.1	Overview	45
2.1.2	Configuring IP-MAC Binding	45
2.1.2.1	Enabling or Disabling the IP-MAC Binding Function	45
2.1.2.2	Configuring IP-MAC Binding	45
2.1.2.3	Viewing IP-MAC Binding Information	46
<b>2.2</b>	<b>Understanding URL Filtering</b>	<b>47</b>
2.2.1	Overview	47
2.2.2	Configuring URL Filtering	47
2.2.2.1	Registering URLs	47
2.2.2.2	Configuring URL Filtering Rules	48
2.2.2.3	Applying Rules to Interfaces	48
2.2.3	Viewing Configuration Information and Statistical Information of the URL Filtering Module	48
2.2.3.1	Configuration Information	48
2.2.3.2	Statistical Information	51
2.2.4	Problems Encountered in Use of this Function	51
<b>2.3</b>	<b>Understanding Network Ingress Filtering</b>	<b>53</b>
2.3.1	Overview	53
2.3.2	Configuring NIF	53
2.3.2.1	Enabling or Disabling Network Ingress Filtering	53
2.3.2.2	Viewing Network Ingress Filtering Information	53
<b>2.4</b>	<b>Understanding TCP SYN Proxy</b>	<b>53</b>
2.4.1	Overview	53
2.4.2	Configuring TCP SYN Proxy	54
2.4.2.1	Enabling or Disabling TCP SYN Proxy Function	54
2.4.2.2	Viewing TCP SYN Proxy Information	54
<b>2.5</b>	<b>Understanding Special Protocol</b>	<b>54</b>
2.5.1	Overview	54
2.5.2	Configuring a Special Protocol	54
<b>2.6</b>	<b>Understanding TCP Sequence Number Tracking</b>	<b>56</b>
2.6.1	Overview	56
2.6.2	Configuring TCP Sequence Number Tracking	56
2.6.2.1	Enabling or Disabling the TCP Sequence Number Tracking Function	56
2.6.2.2	Configuring TCP Sequence Number Tracking Rules	56
<b>2.7</b>	<b>Understanding Session Limit</b>	<b>56</b>

2.7.1	Overview	56
2.7.2	Configuring a Session Limit	56
2.7.3	Viewing Session Limit Information	56
<b>2.8</b>	<b>Understanding Flow Management</b>	<b>58</b>
2.8.1	Overview	58
2.8.2	Configuring Flow Management	58
<b>2.9</b>	<b>Understanding Others</b>	<b>58</b>
2.9.1	Enabling Session Log	58
2.9.2	Configuring Session Timeout	58
2.9.3	Configuring Abnormal Session Status Restriction	58
2.9.4	Enabling Strict Status Tracking	58
2.9.5	Enabling ICMP Reverse Flow Check	59
2.9.6	Configuring Connection Filtering	59
<b>3</b>	<b>NETWORK SECURITY PROTOCOL (IPSEC)</b>	<b>60</b>
<b>3.1</b>	<b>Overview of IPsec</b>	<b>60</b>
3.1.1	Purposes of Encryption	60
3.1.2	Supported Standards	60
3.1.3	Terms	60
<b>3.2</b>	<b>IPsec Configuration</b>	<b>61</b>
3.2.1	Overview of IPsec Working Process	61
3.2.2	IPsec Configuration Tasks	62
3.2.2.1	Configuring Default Lifetime	63
3.2.2.2	Configuring Automatic Disconnection for Idle Tunnels	63
3.2.2.3	DF bit Override Function of IPsec Tunnel	64
3.2.2.4	Creating Encryption Access Lists	65
3.2.2.5	Defining Transform Set	66
3.2.2.6	Configuring IPsec MIB	68
3.2.2.7	Configuring Multicast Policies	68
3.2.2.8	Creating Crypto Map Entry	68
3.2.2.9	Applying Crypto Map Entry to an Interface	75
3.2.2.10	Creating Profile Crypto Map Entries	75
3.2.2.11	Applying Profile Crypto Map Entries to a Tunnel Interface	77
3.2.2.12	Configuring Extended Authentication	77
3.2.2.13	Configuring Accounting Mode of Extensible Authentication	77
3.2.2.14	Configuring IPsec Packet Filtering	78
3.2.2.15	Monitoring and Maintaining IPsec	78
3.2.3	IPsec Configuration Example	78
<b>3.3</b>	<b>IKE Configuration</b>	<b>79</b>

3.3.1	IKE Working Process	79
3.3.2	IKE Configuration Task	80
3.3.2.1	Enabling or Disabling IKE	80
3.3.2.2	Ensuring Compatibility between Access List and IKE	81
3.3.2.3	Creating IKE Policies	81
3.3.2.4	Selecting Working Mode	83
3.3.2.5	Configuring Local Identity	83
3.3.2.6	Setting Automatic Mode Recognition	84
3.3.2.7	Configuring Digital Certificate	84
3.3.2.8	Configuring Digital Envelope	84
3.3.2.9	Configuring Pre-shared Key	84
3.3.2.10	Configuring DPD Detection	85
3.3.2.11	Configuring NAT Traversal Timeout	85
3.3.2.12	Excluding Qtech Vendor Information	86
3.3.2.13	Configuring IKE Session Limit	86
3.3.2.14	Configuring Qtech IKE Negotiation Mode	86
3.3.2.15	Configuring Extended Authentication Timeout	86
3.3.2.16	Configuring AAA Server Response Timeout	86
3.3.2.17	Configuring Client Policy Delivery	86
3.3.2.18	Configuring IP address pool	87
3.3.2.19	TRACK Correlation	88
3.3.2.20	Backup Linkage Detection	88
3.3.2.21	IKE Maintenance	88
3.3.3	IKE Configuration Example	89
3.3.4	Typical Application Cases	89
3.3.4.1	Statically Configuring Tunnels	89
3.3.4.2	Dynamically Configuring Tunnels	94
3.3.4.3	Initiating Negotiation with the Domain Name	97
3.3.4.4	Dynamically Configuring to Use Certificate Negotiation	99
3.3.4.5	Reverse Route Injection	105
3.3.4.6	Mutual Backup of Multiple Peers	106
3.3.4.7	IPSEC OVER MPLS	116
4	CONFIGURING THE DIGITAL CERTIFICATE	120
4.1	Overview	120
4.1.1	Terminology	120
4.2	Configuring CA Server and Applying for & Exporting a Certificate	121
4.2.1	Installing the Certificate Services on a Windows 2003 Server	121
4.2.2	Setting Up CA Server on IIS	121
4.2.3	Applying for and Exporting a Certificate	122

4.2.4	Configuring the URL of CRL	123
4.2.5	Installing SCEP Add-on	123
<b>4.3</b>	<b>Digital Certificate Configuration</b>	<b>125</b>
4.3.1	Digital Certificate Configuration Tasks	125
4.3.2	Importing a Certificate	126
4.3.3	Acquiring Router Certificate Through SCEP	129
4.3.4	Configuring SNC certificate	132
4.3.5	Configuring an Offline Certificate	132
4.3.6	Certificate Configuration Commands (Optional)	134
4.3.7	Configuring Certificate Revocation Check Policy (Optional)	135
4.3.8	Downloading a CRL (Optional)	136
4.3.9	Configuration Example	137
<b>4.4</b>	<b>Monitoring and Maintenance</b>	<b>139</b>
<b>5</b>	<b>CONFIGURING VPDN</b>	<b>143</b>
5.1	Overview of VPDN	143
<b>6</b>	<b>CONFIGURING PPTP</b>	<b>144</b>
6.1	Overview of PPTP	144
6.2	Configuring the PPTP Server	144
6.2.1	Configuration Tasks	144
6.2.2	Configuring a Local Address Pool (Optional)	144
6.2.3	Configuring User Information (Optional)	144
6.2.4	Configuring VPDN Globally	145
6.2.5	Enabling/Disabling the VPDN Function	145
6.2.5.1	Setting Source Address of VPDN	145
6.2.5.2	Setting Maximum Number of VPDN Sessions	145
6.2.5.3	Setting Domain Resolution	145
6.2.5.4	Enabling Domain Authentication	146
6.2.5.5	Setting VPDN Rate Limiting	146
6.2.6	Configuring a Virtual-Template Interface	146
6.2.6.1	Setting a Virtual-Template Interface	146
6.2.7	Configuring VPDN Group	146
6.2.7.1	Setting VPDN Group	146
6.2.7.2	Setting Tunneling Mode	146
6.2.7.3	Setting Tunneling Protocol	147
6.2.7.4	Setting Virtual Template to Be Used	147
6.2.7.5	Setting the Name of the Remote Peer	147
6.2.7.6	Setting Local Name	147

6.2.7.7	Setting Source Address of VPDN group	148
6.2.7.8	Setting PPTP Flow Control Parameters	148
6.2.7.9	Setting PPTP Tunnel Parameters	148
6.2.7.10	Setting the Supported Domain Name	148
6.2.7.11	Binding a Domain Name to an Address Pool	149
6.2.7.12	Setting the DNS Negotiation Address for Binding PPP to the Domain Name	149
6.2.8	Configuration Examples	149
<b>6.3</b>	<b>Monitoring and Maintaining PPTP</b>	<b>153</b>
6.3.1	Monitoring PPTP	153
6.3.2	Maintaining PPTP	153
6.3.3	FAQs	155
<b>7</b>	<b>CONFIGURING L2TP</b>	<b>157</b>
7.1	Overview	157
7.2	Initiation by the Local Client	157
7.2.1	Configuration Task List	157
7.2.2	Creating and Configuring an L2TP-class Interface	157
7.2.2.1	Setting an L2TP-class Unit	157
7.2.2.2	Setting Time for the L2TP Control Connection	158
7.2.2.3	Setting Authentication for the L2TP Control Connection	158
7.2.2.4	Setting Maintenance and Update for the L2TP Control Connection	158
7.2.3	Creating and Configuring a Pseudowire-class Interface	159
7.2.3.1	Setting a Pseudowire-class Unit	159
7.2.3.2	Setting the Encapsulation Mode for L2TP Data Transmission	159
7.2.3.3	Setting IP Parameters for L2TP Data Transmission	159
7.2.3.4	Setting the L2TP Control Connection	160
7.2.4	Creating and Configuring a Virtual-ppp Interface	160
7.2.4.1	Setting a Virtual-ppp Interface	160
7.2.4.2	Setting the Pseudowire Rule	160
7.2.4.3	Setting the VRF Attribute	161
7.2.5	Configuration Examples	161
7.2.5.1	Establishing a Tunnel with the Windows 2000 Server	161
7.2.5.2	Establishing a Tunnel with Cisco 2620	165
7.2.5.3	Establishing a Tunnel with the Windows 2000 PC by Using hostname	170
7.2.5.4	IPv6 over L2TP Configuration Example	170
<b>7.3</b>	<b>Initiation by the Remote Client</b>	<b>173</b>
7.3.1	Configuration Task List	173
7.3.2	Configuring a Local Address Pool	173
7.3.3	Configuring User Information	173

7.3.4	Setting VPDN Global Parameters	173
7.3.4.1	Enabling or Disabling the VPDN Function	173
7.3.4.2	Setting the VPDN Source Address	174
7.3.4.3	Setting the Maximum Number of VPDN Sessions	174
7.3.4.4	Setting the Domain Resolution Option	174
7.3.4.5	Enabling or Disabling Domain Authentication	174
7.3.4.6	Ignoring the Source Address Check of VPDN	175
7.3.4.7	Setting VPDN Rate Limit	175
7.3.4.8	Configuring Rate Limit Function for VPDN Transmission	175
7.3.5	Configuring a Virtual-Template Interface	175
7.3.5.1	Setting a Virtual-Template Interface	176
7.3.6	Configuring VPDN-group	176
7.3.6.1	Setting a VPDN-group Interface	176
7.3.6.2	Setting the Tunneling Mode	176
7.3.6.3	Setting the Tunneling Protocol	176
7.3.6.4	Setting a Virtual Template to Be Used	177
7.3.6.5	Setting the Peer Name	177
7.3.6.6	Setting the Local Name	177
7.3.6.7	Setting the VPDN-group Source Address	177
7.3.6.8	Setting the L2TP Control Connection	178
7.3.6.9	Setting L2TP Data Transmission Parameters	178
7.3.6.10	Setting the VRF Option	179
7.3.6.11	Setting the Supported Domain Name	179
7.3.6.12	Setting the Domain Name-Bound Address Pool	179
7.3.6.13	Setting the DNS Negotiation Address of PPP Bound to a Domain Name	180
7.3.6.14	Re-Performing PPP Authentication	180
7.3.6.15	Re-Performing PPP Negotiation	180
7.3.6.16	Ignoring Errors on Control Packets	180
7.3.6.17	Configuring the Function of Not Carrying Tunnel Authentication Response AVP in SCCRP Packets	181
7.3.7	Configuration Examples	181
7.3.7.1	Establishing a Tunnel with the Windows 2000 Server	181
7.3.7.2	Establishing a Tunnel with Cisco 3640	185
7.3.7.3	Establishing a Tunnel with Cisco 2620	189
7.3.7.4	Configuration Example of Domain Authentication	191
7.3.7.5	IPv6 over L2TP	193
7.4	Monitoring and Maintaining L2TP Tunnels	194
7.4.1	Monitoring L2TP Tunnels	194
7.4.1.1	Displaying Information About the Current L2TP Tunnel	195
7.4.1.2	Performing Overall VPDN Debugging	196
7.4.1.3	Performing L2TP Data Debugging	197



7.4.1.4	Performing L2TP Error Debugging	197
7.4.1.5	Performing L2TP Event Debugging	198
7.4.1.6	Performing L2TP Message Data Debugging	199
7.4.2	Maintaining L2TP Tunnels	203
7.4.3	FAQs	203
<b>8</b>	<b>CONFIGURING VPDN 2.0</b>	<b>205</b>
8.1	VPDN 2.0 Overview	205
8.2	Configuring L2TP	205
8.2.1	Configuring Large Capacity L2TP	205
8.2.1.1	Configuration Task List	205
8.2.1.2	Configuring VPDN Address Pool (Optional)	205
8.2.2	Configuring User Information	205
8.2.3	Setting VPDN Global Parameters	206
8.2.3.1	Enabling or Disabling the VPDN Function	206
8.2.3.2	Setting the VPDN Source Address	206
8.2.3.3	Setting the Maximum Number of VPDN Sessions	206
8.2.3.4	Setting the Domain Resolution Option	206
8.2.3.5	Enabling or Disabling Domain Authentication	207
8.2.3.6	Ignoring the Source Address Check of VPDN	207
8.2.3.7	Setting VPDN Rate Limit	207
8.2.4	Resolving Device Serial Number of VPDN	207
8.2.5	Transmitting Device Serial Number of VPDN	208
	Configuring a Virtual-Template Interface	208
8.2.5.1	Setting a Virtual-vpdn Interface	208
8.2.5.2	Setting VPDN Address Pool	208
8.2.6	Configuring VPDN-group	209
8.2.6.1	Setting a VPDN-group Interface	209
8.2.6.2	Setting the VPDN-group Source Address	209
8.2.6.3	Setting the Tunneling Mode	209
8.2.6.4	Setting the Tunneling Protocol	209
8.2.6.5	Setting a Logical Interface to Be Used	209
8.2.6.6	Setting the Peer Name	210
8.2.6.7	Setting the Local Name	210
8.2.6.8	Setting the L2TP Control Connection	210
8.2.6.9	Setting L2TP Data Transmission Parameters	211
8.2.6.10	Setting the VRF Option	212
8.2.6.11	Setting the Supported Domain Name	212
8.2.6.12	Re-Performing PPP Authentication	212
8.2.6.13	Re-Performing PPP Negotiation	212

8.2.6.14	Ignoring Errors on Control Packets	213
8.2.6.15	Setting the Domain Name's Delete on Time of Session	213
8.2.6.16	Setting No Sending of STOP Packet	213
8.2.6.17	Setting SCCRP Packet's No Carrying of Tunnel Authentication ResponseAVP	213
8.2.6.18	Setting Supported Flow-limit QOS by VPDN	214
8.2.7	Configuration Examples	214
8.2.7.1	Configuration Example of L2TP Large Capacity and Domain Authentication	214
8.2.7.2	Configuration Example of Virtual-vpdn and OSPF	215
8.2.7.3	Configuration Example of Irtual-vpdn and RIP	218
8.3	Monitoring and Maintaining VPDN 2.0	219
9	CONFIGURING THE TUNNEL INTERFACE	220
9.1	Understanding the Tunnel interface	220
9.1.1	Overview	220
9.1.2	Configuring the Tunnel Interface	221
9.1.2.1	Tunnel interface configuration tasks	221
9.1.2.2	Configuring the source address of a Tunnel interface	221
9.1.2.3	Configuring the destination address of a Tunnel interface	221
9.1.2.4	Configuring Tunnel mode	222
9.1.2.5	Configuring Tunnel checksum	222
9.1.2.6	Configuring the key of a tunnel interface	222
9.1.2.7	Configuring tunnel reception rules	223
9.1.2.8	Configuring TTL of a tunnel	223
9.1.2.9	Configuring TOS of a tunnel	223
9.1.2.10	Configuring PMTUD of a tunnel	223
9.1.2.11	Configuring the keepalive function of a tunnel	224
9.1.2.12	Configuring Tunnel nested encapsulation limit	225
9.1.2.13	Configuring Tunnel VRF	225
9.1.3	Example of Tunnel Interface Configuration	226
9.1.4	Monitoring and Maintaining Tunnel interfaces	227
9.1.5	Troubleshooting Faults on the Tunnel Interface	227
10	CONFIGURING THE AAA FUNCTION	229
10.1	Overview	229
10.1.1	Basic AAA Principles	229
10.1.2	Method List	229
10.2	AAA Configuration Steps	230
10.2.1	AAA Configuration Description	230
10.2.2	Enabling AAA	231
10.2.3	Disabling AAA	231

10.2.4	Follow-up Configuration	231
<b>10.3</b>	<b>Configuring Authentication</b>	<b>231</b>
10.3.1	Defining AAA Authentication Method List	231
10.3.2	Configuration Examples	232
10.3.3	Authentication Type	232
10.3.4	Configuring AAA Authentication	233
10.3.5	Configuring the AAA Login Authentication	233
10.3.5.1	Using the Local Database for Login Authentication	234
10.3.5.2	Using Radius for Login Authentication	234
10.3.6	Configuring the AAA Enable Authentication	235
10.3.6.1	Using the Local Username Database for Enable Authentication	235
10.3.6.2	Using RADIUS for Enable Authentication	236
10.3.7	Configuring the AAA Authentication for PPP Users	236
10.3.8	Configuring the AAA Authentication for 802.1x Users	236
10.3.9	Example of Authentication Configuration	237
10.3.10	Example of Terminal Service Application Configuration	237
<b>10.4</b>	<b>Configuring Authorization</b>	<b>238</b>
10.4.1	Authorization Types	238
10.4.2	Preparations for Authorization	238
10.4.3	Configuring Authorization List	239
10.4.4	Configuring AAA Exec Authorization	239
10.4.4.1	Using the Local Username Database for Exec Authorization	240
10.4.4.2	Using RADIUS for Exec Authorization	240
10.4.4.3	Example of Configuring Exec Authorization	240
10.4.5	Configuring AAA Network Authorization	241
10.4.5.1	Using RADIUS for Network Authorization	242
10.4.5.2	Example of Configuring Network Authorization	242
<b>10.5</b>	<b>Configuring Accounting</b>	<b>242</b>
10.5.1	Accounting Types	242
10.5.2	Preparations for Accounting	242
10.5.3	Configuring AAA Exec Accounting	243
10.5.3.1	Using the RADIUS for Exec Accounting	243
10.5.3.2	Example of Configuring Exec Accounting	244
10.5.4	Configuring AAA Network Accounting	244
10.5.4.1	Using RADIUS for Network Accounting	245
10.5.4.2	Example of Configuring Network Accounting	245
<b>10.6</b>	<b>Monitoring AAA users</b>	<b>245</b>
<b>10.7</b>	<b>Configuring VRF-supported AAA Group</b>	<b>245</b>

10.8	Configuring Login Lockout for Failed Authentication	246
10.9	Configuring Domain Name-based AAA Service	246
10.9.1	Overview	246
10.9.2	Domain name-based AAA Service Configuration Tasks	247
10.9.2.1	Enabling AAA	247
10.9.2.2	Defining the AAA Service Method List	247
10.9.2.3	Enabling the Domain Name-based AAA Service	247
10.9.2.4	Creating a Domain	248
10.9.2.5	Configuring the Domain Attribute Set	248
10.9.2.6	Querying the Domain configuration	249
10.9.3	Domain Name-based AAA Service Configuration Notes	249
10.9.4	Domain Name-based AAA Service Configuration Example	249
10.10	Typical AAA Configuration Example	250
10.10.1	Typical AAA Application	250
10.10.1.1	Network Topology	250
10.10.1.2	Network Requirements	250
10.10.1.3	Configuration Key-points	250
10.10.1.4	Configuration Steps	250
10.10.1.5	Configuration verification	252
10.10.2	AAA Multi-domain Authentication Application	254
10.10.2.1	Network Topology	254
10.10.2.2	Network Requirements	254
10.10.2.3	Configuration Key Points	254
10.10.2.4	Configuration Steps	254
10.10.2.5	Configuration Verification	256
11	CONFIGURING RADIUS	257
11.1	Overview of RADIUS	257
11.2	RADIUS Configuration Tasks	257
11.2.1	Configuring RADIUS Protocol Parameters	258
11.2.2	Specifying Radius Authentication	258
11.2.3	Specifying the Standard Radius Attribute Type	258
11.2.3.1	Configuring Calling-Station-ID Format	258
11.2.4	Specifying Private Radius Attribute Type	258
11.2.5	Configuring RADIUS Server Reachability Detection	260
11.3	Monitoring RADIUS	261
11.4	Radius Configuration Example	261
11.5	RADIUS IPv6 Configuration Example	262

<b>12</b>	<b>CONFIGURING TACACS+</b>	<b>264</b>
12.1	Overview of TACACS+	264
12.2	TACACS+ Application	264
12.3	TACACS+ Configuration Task	267
12.3.1	Configuring TACACS+ Parameters	267
12.4	Using TACACS+ for Implementing AAA Functions	268
12.4.1	Using TACACS+ for Login Authentication	268
12.4.2	Using TACACS+ for Enable Authentication	269
12.4.3	Using TACACS+ for Login Authorization	269
12.4.4	Using TACACS+ for Level 15 Command Audit	270
<b>13</b>	<b>CONFIGURING NAT</b>	<b>271</b>
13.1	NAT Overview	271
13.1.1	Configuring Static NAT for Internal Source Addresses	271
13.1.2	Configuring NAT for Internal Source Addresses	272
13.1.3	Configuring NAT Overlap	272
13.1.4	Configuring TCP Load Balancing	273
13.1.5	Configuring Special Protocol Gateway	274
13.1.6	Configuring NAT Static Port Range Mapping	274
13.1.7	Configuring ARP Response Function of NAT	274
13.1.8	Configuring NAT Keepalive Function	275
13.2	NAT Configuration Examples	275
13.2.1	Dynamic translation of internal source addresses	275
13.2.2	Reuse of internal global addresses	275
13.2.3	Static NAT for Internal Source Addresses	276
13.2.4	TCP Load Balancing	276
13.2.5	Load balancing among multiple outside interfaces	277
13.2.6	Configuring a local server	278
13.2.7	NAT Configuration in case of multiple VRF instances	280
13.2.8	VPN NAT configuration example	281
13.2.9	NAT Static Port Range Mapping	283
<b>14</b>	<b>CONFIGURING SSH TERMINAL SERVICE</b>	<b>285</b>
14.1	Overview of SSH	285
14.2	SSH Configuration	285
14.2.1	Default SSH Configurations	285
14.2.2	Configuring User Authentication	285
14.2.3	Enabling SSH Server	285

14.2.4	Shutting Down the SSH Server	286
14.2.5	Configuring the Supported SSH Server Version	286
14.2.6	Configuring SSH User Authentication Timeout Period	286
14.2.7	Configuring SSH Re-authentication Times	286
14.2.8	Configuring SSH Public Key Based Authentication	287
14.2.9	Configuring the SCP Server Function	287
14.3	Using SSH for Device Management	287
14.4	Enabling SSH public key based authentication	289
14.4.1	Operations on the SSH Client:	289
14.4.2	Operations on the SSH server	292
14.5	Transferring files through SSH	292
14.5.1	Operation on the SSH server:	292
14.5.2	Operation on the SSH server:	292
14.6	Typical SSH Configuration Examples	293
14.6.1	Configuring SSH Local Authentication	293
14.6.2	Application Requirements	293
14.6.3	Notes	293
14.6.4	Configuration Steps	294
14.6.5	Verifying the Configuration	296
14.7	Example of Configuring SSH AAA Authentication	296
14.7.1	Application Requirements	297
14.7.2	Notes	297
14.7.3	Configuration Steps	297
14.7.4	Verifying the Configuration	298
15	CONFIGURING IP ACCOUNTING	300
15.1	Understanding IP Accounting	300
15.2	Overview	300
15.3	Configuring IP Accounting	300
15.3.1	Enabling IP Accounting	300
15.3.2	Displaying IP Accounting Configuration	300
15.3.3	Displaying IP Accounting Statistics	301
15.3.4	Clearing IP Accounting Statistics	301
16	CONFIGURING SDG	302
16.1	Understanding SDG	302
16.1.1	Overview of SDG	302
16.1.2	Working Principle	302

16.1.3	Protocol Specification	303
16.2	Default Configurations	304
16.3	Configuring SDG	304
16.3.1	Configuring SDG Mode	304
16.3.2	Configuring the IP Address of the SMP Server	304
16.3.3	Configuring Aging Time for Offline Users	304
16.3.4	Configuring Keepalive Duration and Threshold of User Traffic	304
16.3.5	Configuring DNS Hijacking	305
16.3.6	Configure the Default User	305
16.3.7	Configuring SDG Classifiers	305
16.3.8	Configuring User Groups	305
16.3.9	Configuring Static Users	306
16.3.10	Clearing Users in a User Group	306
16.3.11	Configuring SDG Control Policies	306
16.3.12	Configuration Examples	306
16.3.12.1	Local mode	306
17	CONFIGURING ANTI-ATTACK FEATURES ON DEVICES	309
17.1	Overview of Device Anti-attack	309
17.2	Configuring Device Anti-attack	310
17.2.1	Device Anti-attack Configuration Tasks	310
17.2.2	Entering Control-plane Configuration Mode	310
17.2.3	Configuring SCPP	310
17.2.4	Configuring Glean-CAR	311
17.2.5	Configuring ARP-CAR	311
17.2.6	Configuring Port-Filter	312
17.2.7	Configuring MPP	312
17.2.8	Configuring ACPP	312
17.2.9	Enabling Device Anti-attack with Default Rules	312
17.3	Maintaining Device Anti-attack	312
17.3.1	Maintenance of device anti-attack	312
17.4	Typical Device Anti-Attack Configuration Example	313
18	CONFIGURING RPL	314
18.1	Understanding RPL	314
18.1.1	Overview	314
18.1.2	Basic Concept	314
18.1.3	Work Principle	314

18.1.4	Typical Application	314
18.2	Configuring RPL	314
18.2.1	Configuring RPL	314
18.3	Displaying Device Configurations	315
18.4	Configuration Examples	315
18.4.1	RPL Configuration Example	315



# 1 CONFIGURING ACLS

## 1.1 Overview

As part of Qtech's security solution, an access control list (ACL) is used to provide a powerful traffic filtering function. Currently, Qtech products support the following ACLs:

- Standard and extended IP ACLs
- IPv6 Extended ACLs

Depending on networks conditions, you can choose different ACLs to control data flows.

### 1.1.1 ACL Introduction

An ACL is also referred to as a firewall or packet filtering. ACLs permit or discard packets on interfaces of network devices by defining rules. According to application scopes, they can be divided into ACLs and QoS ACLs.

By filtering the data streams, you can restrict the communication data types in the network and restrict the users of the network and the device they can use. When data streams pass the switch, ACLs classify and filter them, that is, check the data streams input from the specified interface and determine whether to permit or deny them according to the matching conditions.

To sum up, the security ACL is used to control which data flow is allowed to pass through the network device. The QoS policy performs priority classification and processing for the data flow.

ACLs consist of a series of entries, known as Access Control Entry (ACE). Each entry has its matching condition and behavior.

ACL rules can be applied to the source addresses, destination addresses, upper layer protocols, time ranges or other information of data flows.

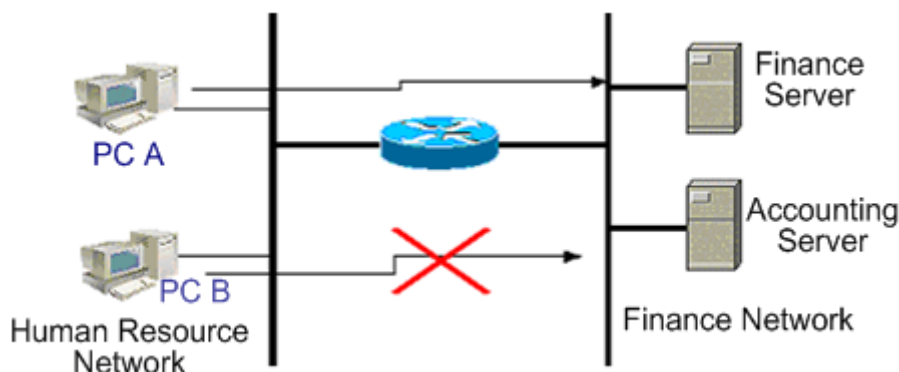
### 1.1.2 Why to Configure ACLs

There are many reasons why ACLs need to be configured. In most cases, ACLs are used to:

- Restrict route update: Control where the route update information is sent and received.
- Restrict network access: To ensure network security, provide users with access to desired services only (for example, if a user only needs webpage access and email services, other services such as Telnet are disabled), specify a time period in which access is permitted, or specify hosts which are allowed to access Internet.

In Figure 1, only host A is allowed to access Finance Network, while Host B is not.

Figure 1 Using ACLs to control network access



### 1.1.3 When to Configure Access Lists

Depending on your requirements, you can select the basic ACL or dynamic ACL. In general, the basic ACL can meet the security requirement. However, experienced hackers may use some software to forge source addresses and spoof the devices so as to gain access. Before the user can access the network, the dynamic ACL requires

authentication so that the hackers are difficult to invade the network. So, in some sensitive areas the dynamic ACL can be used to ensure the network security.

**Note**

An inherent problem of all ACLs is spoofing, the behavior of providing spoofed source addresses to deceive switches. This cannot be avoided even you use the dynamic ACL. During the effective access period of an authenticated user, a hacker may use a spoofed user address and accesses the network. There are two methods to resolve the problem. One method is to set free time for a user to access the network as little as possible, making it hard for a hacker to attack the network. The other method is to use IPSEC to encrypt network data, ensuring that all the data entering switches is encrypted.

ACLs are usually configured in the following positions of network devices:

- Devices between the internal network and external network (such as the Internet)
- Devices at the border of two parts in a network
- Devices on the access control port

The execution of the ACL statements must follow the order in the table strictly. Starting from the first statement, once the header of a packet matches a conditional judge statement in the table, the following statements are ignored.

### 1.1.4 Input/Output ACL, Filtering Domain Template and Rule

When a device interface receives a message, the input ACL checks whether the message matches an ACE of the ACL input on the interface. When a device interface is ready to output a message, the output ACL checks whether the message matches an ACE of the ACL output on the interface.

When detailed filtering rules are formulated, all or some of the preceding eight items may be used. As long as the message matches one ACE, the ACL processes the message as the ACE defined (permit or deny). The ACE of an ACL identifies Ethernet messages according to some fields of Ethernet messages. The fields include the following:

Layer-2 fields:

- 48-bit source MAC address (all the 48 bits must be declared)
- 48-bit destination MAC address (all the 48 bits must be declared)
- 16-bit layer-2 type field

Layer 3 fields:

- Source IP address field (you can specify all the 32 bits of the IP address, or specify a type of streams of the defined subnet)
- Destination IP address field (you can specify all the 32 bits of the IP address, or specify a type of streams of the defined subnet)
- Protocol type fields

Layer-4 fields:

- You can specify one UDP source port, destination port, or both
- You can specify one UDP source port, destination port, or both

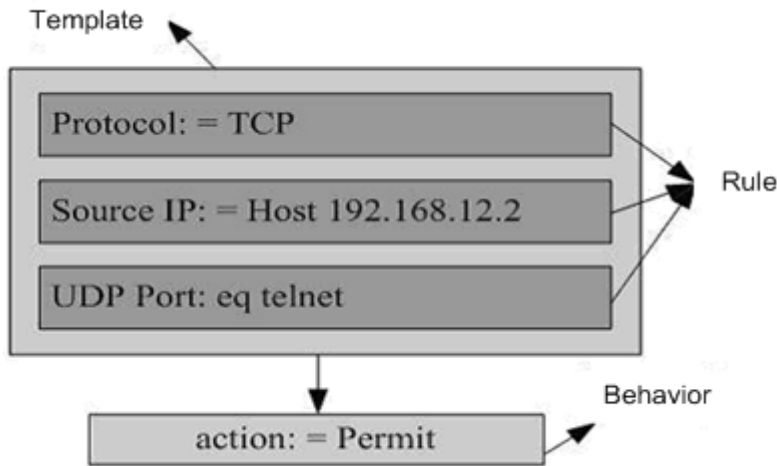
The filtering domain consists of the fields in the packets based on which the packets are identified and classified when you create an ACE. A filtering domain template is the definition formed by these fields. For example, when one ACE is generated, you want to identify and classify messages according to the destination IP field of a message. When another ACE is generated, you want to identify and classify messages according to the source IP address field of a message and the source port field of UDP. In this way, these two ACEs use different filtering domain templates.

Rules refer to the values of the ACE mask. For example, one ACE is:

```
permit tcp host 192.168.12.2 any eq telnet
```

In this ACE, the filtering domain template is a collection of the following fields: Source IP Address Fields, IP Protocol Fields and Destination TCP Port Fields. Corresponding values (rules) are respectively as follows: Source IP Address=Host 192.168.12.2; IP Protocol=TCP; TCP Destination Port=Telnet.

Figure 2 Analysis of the ACE: permit tcp host 192.168.12.2 any eq telnet



A filtering domain template can be the collection of L3 fields and L4 fields or the collection of multiple L2 fields. However, the filtering domain templates of a standard and extended ACL cannot be the collection of L2 and L3, L2 and 4, L2 and L3, or L4 fields.



**Note** 1. When associating SVI with the ACL at the outbound direction, you should note that:



**Caution** Standard IP ACL and extended IP ACL are supported. There are some limits on matching the destination IP address and the destination MAC address with an ACL. If you need to match the destination IP address not in the subnet IP range of the associated SVI in the standard IP ACL and extended IP ACL, this ACL will not take effect. For example, the IP address of VLAN 1 is 192.168.64.1 and subnet mask of VLAN 1 is 255.255.255.0. Now you create an ACL with the ACE of **deny udp any 192.168.65.1 0.0.0.255 eq 255** and apply this ACL to the egress of VLAN 1. This ACL will not function for the destination IP address is not in the subnet IP range of VLAN 1. If the ACE is **deny udp any 192.168.64.1 0.0.0.255 eq 255**, this ACL will take effect.



**Note** When applying an ACL, the labeled MPLS packet matching does not take effect if an ACE in the ACL (including the IP ACL) matches a non-L2 field (such as SIP and DIP).

## 1.2 Configuring IP Access List

To configure ACLs on a device, you must specify unique names or numbers for the ACLs of a protocol to uniquely identify each ACL within the protocol. The following table lists the protocols that can use numbers to specify ACLs and the number ranges of ACLs that can be used by each protocol.

Protocol	Number Range
Standard IP	1-99, 1300 - 1999
Extended IP	100-199, 2000 - 2699

### 1.2.1 Guide to Configuring IP ACLs

When you create an ACL, defined rules will be applied to all packets on a device. The device decides whether to forward or block a packet by judging whether the packet matches a rule.

Basic ACLs are classified into standard ACLs and extended ACLs. The typical rules defined in ACLs are as follows:

- Source address
- Destination address
- Upper layer protocol
- Time range

Standard IP ACLs (numbered from 1 to 99 and from 1300 to 1999) forward or block packets according to source addresses. Extended IP ACLs (numbered from 100 to 199 and from 2000 to 2699) use the above four combinations to forward or block packets. Other types of ACLs forward or block packets according to related codes.

A single ACL can use multiple separate ACL statements to define multiple rules. Where, all statements use the same number or name to bind these statements to the same ACL. However, the more the used statements are, the more difficult to read and understand an ACL.

### Statement containing an implicit deny statement for all packets

The end of the ACL contains an implicit deny statement for all packets that it did not find a match for before reaching the end, as shown in the following example:

```
access-list 1 permit host 192.168.4.12
```

This ACL allows only the messages destined for host 192.168.4.12. This is because the ACL contains the following rule statement at the end: **access-list 1 deny any**

Here is another example:

```
access-list 1 deny host 192.168.4.12
```

If the ACL contains the only preceding statement, the messages from any host will be denied on the port.



#### Note

It is required to consider the routing update message when defining the ACL. Since the end of the ACL contains an implicit deny statement for all packets, this may cause all routing update messages blocked.



If the inserted line cards do not include EA series, the ACEL associated with the outgoing direction of the AP port has no default deny ACE, which shall be configured manually as needed.

### Order to Input Rule Sentences

Each added rule is appended to the ACL. If a statement is created, then you cannot delete it separately but delete the whole ACL. Therefore, the order of ACL statements is very important. When deciding whether to forward or block packets, a device compares packets and statements in order of statement creation time until it finds a matching statement.

If you have created a statement that allows all packets to pass, then the following statements will not be checked, as shown in the following example:

```
access-list 101 deny ip any any
access-list 101 permit tcp 192.168.12.0 0.0.0.255 eq telnet any
```

Because the first rule statement denies all IP packets, the packets for accessing host 192.168.12.0/24 will be denied. Because the device discovers that the packets match the first rule statement, it will not check other rule statements.

### 1.2.2 Configuring IP ACLs

The configuration of the basic ACL includes the following steps:

- Define a basic ACL
- Apply the ACL to a specific interface.

There are two methods to configure a basic ACL.

Method 1: Run the following command in global configuration mode:

Command	Function
Qtech(config)# <b>access-list</b> id {deny   permit} {src src-wildcard   host src   any   interface idx} [time-range tm-rng-name]	Defines an ACL .
Qtech(config)# <b>interface</b> interface	Selects the interface to which the ACL is to be applied.
Qtech(config-if)# ip access-group id { in   out } [unreflect]	Applies the ACL to the specific interface

Method 2: Run the following command in ACL configuration mode:

Command	Function
Qtech(config)# <b>ip access-list</b> { standard   extended } { id / name }	Enters ACL configuration mode.
Qtech (config-xxx-nacl)# [sn] { permit   deny } {src src-wildcard   host src   any } [time-range tm-rng-name]	Adds ACEs to the ACL. For details about the command, see command reference.
Qtech(config-xxx-nacl)# <b>exit</b>	Exits ACL mode.
Qtech(config)# <b>interface</b> interface	Selects the interface to which the ACL is to be applied.
Qtech(config-if)# ip access-group id { in   out } [unreflect]	Applies the ACL to the specific interface.



#### Note

In method 1, an ACL can only be numbered. In method 2, an ACL can be numbered and named, and ACE priority can be specified if available. By default, the reflexive ACL is enabled on the IP ACL port. You can run the **unreflect** command to disable the reflexive ACL. (The operation principles of the reflexive ACL are described as follows:

- a. The router automatically generates a temporary ACL according to the L3 and L4 information of the originating traffic in the internal network based on the principles. That is, the protocol is constant, while the source and destination IP addresses, and the source and destination ports are rigidly exchanged.
- b. The router allows traffic to enter the internal network only when the L3 and L4 information of the returned traffic strictly matches the information in the temporary ACL previously created based on the outputting traffic. )

### 1.2.3 Displaying IP ACLs

To monitor ACLs, run the following command in privileged user mode:

Command	Function
Qtech# <b>show access-lists</b> [ id   name ]	Queries the basic ACLs.

## 1.3 Configuring IPv6 Extended ACLs

### 1.3.1 Configuring IPv6 Extended ACLs

The configuration of an IPv6 ACL includes the following steps:

- Define an IPv6 ACL
- Apply the ACL to a specific interface (application particular case)

To configure a basic ACL, run the following command in ACL configuration mode:

Command	Function
Qtech(config)# <b>ipv6 access-list</b> name	Enters ACL configuration mode.
Qtech (config-ipv6-nacl)# [sn] {permit   deny } prot {src-ipv6-prefix/prefix-len   host src-ipv6-addr   any} {dst-ipv6-pfix/pfix-len   any   host dst-ipv6-addr} [dscp dscp] [flow-label flow-label] [time-range tm-rng-name]	Adds ACEs to the ACL. For details about the command, see command reference.
Qtech(config-exp-nacl)# <b>exit</b>	Exits the access control list mode.
Qtech(config)# <b>interface</b> interface	Selects the interface to which the ACL is to be applied.
Qtech(config-if)# <b>ipv6 traffic-filter</b> name {in   out}	Applies the ACL to the specific interface.



### 1.3.2 Displaying Configuration of IPv6 Extended ACLs

To monitor ACLs, run the following command in privileged user mode:

Command	Function
show access-lists [name]	Queries the basic ACLs.

## 1.4 Configuring Extended Expert ACLs

To configure Expert extended ACLs on a device, you must specify unique names or numbers for the ACLs of a protocol to uniquely identify each ACL within the protocol. The following table lists the number range of the Expert ACLs.

Protocol	Number Range
Extended Expert ACL	2700-2899

### 1.4.1 Guide to Configuring Expert Extended ACLs

When you create an expert extended ACL, defined rules will be applied to all packets on a device. The device decides whether to forward or block a packet by judging whether the packet matches a rule.

The typical rules defined in Expert ACLs are as follows:

- All information in basic ACLs and MAC extended ACLs
- VLAN ID

Extended Expert ACLs (numbered from 2700 to 2899) are the syntheses of basic ACLs and MAC extended ACLs and can filter VLAN IDs.

A single expert ACL can use multiple separate ACL statements to define multiple rules. Where, all statements use the same number or name to bind these statements to the same ACL.

### 1.4.2 Configuring an Expert Extended ACL

The configuration of an expert ACL includes the following steps:

- Define an expert ACL
- Apply the ACL to a specific interface (application particular case)

There are two methods to configure an Expert ACL.

Method 1: Run the following command in global configuration mode:

Command	Function
Qtech (config)# <b>access-list</b> id {deny   permit} [prot   {[ethernet-type] [cos cos]]] [VID vid] {src src-wildcard   host src   interface idx} {host src-mac-addr   any} {dst dst-wildcard   host dst   any}{host src-mac-addr   any} [precedence precedence] [tos tos] [ dscp dscp] [fragment] [time-range tm-rng-name]	Defines an ACL. For details about the command, see command reference.
Qtech(config)# <b>interface</b> interface	Selects the interface to which the ACL is to be applied.
Qtech(config-if)# <b>expert access-group</b> id {in   out } [unreflect]	Applies the ACL to the specific interface.

Method 2: Run the following command in ACL configuration mode:

Command	Function
Qtech(config)# <b>expert access-list extended</b> {id name}	Enters ACL configuration mode.
Qtech (config-exp-nacl)# [sn]{ <b>permit</b>   <b>deny</b> }[prot   {[ethernet-type] [cos cos]]] [VID vid] {src src-wildcard   host src   interface idx}{host src-mac-addr   any} {dst dst-wildcard   host dst   any} {host dst-mac-addr   any}[[precedence precedence] [tos tos] [ dscp dscp] [fragment] [time-range tm-rng-name]	Adds ACEs to the ACL. For details about the command, see command reference.
Qtech(config-exp-nacl)# <b>exit</b>	Exit ACL mode.
Qtech(config)# <b>interface</b> interface	Selects the interface to which the ACL is to be applied.

Qtech(config-if)# <b>expert access-group</b> {id/name} {in out} [unreflect]	Applies the ACL to the specific interface.
---	--

**Note**

In method 1, an ACL can only be numbered. In method 2, an ACL can be numbered and named, and ACE priority can be specified if available. In a version supporting ACE priority, method 2 can also specify the priorities of ACEs (using the [sn] option in a command).

The router supports neither packet fragment filtering nor Expert ACLs.

### 1.4.3 Displaying Configuration of Expert Extended ACLs

To monitor ACLs, run the following command in privileged user mode:

Command	Function
show access-lists [ id   name ]	Queries the Expert ACLs.

## 1.5 Configuring MAC Extended ACLs

To configure MAC extended ACLs on a device, you must specify unique names or numbers for the ACLs of a protocol to uniquely identify each ACL within the protocol. The following table lists the range of the numbers that can be used to specify MAC ACLs.

Protocol	Number Range
MAC Extended Access List	700-799

### 1.5.1 Guide to Configuring MAC Extended ACLs

When a MAC ACL is created, the defined rules will be applied to all packets on a device. The device decides whether to forward or block a packet by judging whether the packet matches a rule.

The typical rules defined in MAC ACLs are as follows:

- Source MAC address
- Destination MAC address
- Ethernet protocol type
- Time-range

The MAC extended ACLs (numbered from 700 to 799) forward or block the packets based on the source and destination MAC addresses, and can also match Ethernet packets.

A single MAC ACL can use multiple separate ACL statements to define multiple rules. Where, all statements use the same number or name to bind these statements to the same ACL.

### 1.5.2 Configuring a MAC Extended ACL

The configuration of an MAC ACL includes the following steps:

- Define an MAC ACL
- Apply the ACL to a specific interface

There are two methods to configure an MAC ACL.

Method 1: Run the following command in global configuration mode:

Command	Function
Qtech(config)# <b>access-list</b> id {deny   permit}{any   host src-mac-addr} {any   host dst-mac-addr} [ethernet-type] [cos cos]	Defines an ACL. For details about the command, see command reference.



Qtech(config)# <b>interface</b> <i>interface</i>	Selects the interface to which the ACL is to be applied.
Qtech(config-if)# <b>mac access-group</b> <i>id</i> { <b>in</b>   <b>out</b> }	Applies the ACL to the specific interface.

Method 2: Run the following command in ACL configuration mode:

Command	Function
Qtech(config)# <b>mac access-list extended</b> { <i>id</i>   <i>name</i> }	Enters ACL configuration mode.
Qtech (config-mac-nacl)# [sn] { <b>permit</b>   <b>deny</b> }{ <b>any</b>   <b>host</b> <i>src-mac-addr</i> } { <b>any</b>   <b>host</b> <i>dst-mac-addr</i> } [ <i>ethernet-type</i> ] [ <b>cos</b> <i>cos</i> ]	Adds ACEs to the ACL. For details about the command, see command reference.
Qtech(config-mac-nacl)# <b>exit</b> Qtech(config)# <b>interface</b> <i>interface</i>	Exits ACL mode and selects the interface to which the ACL is to be applied.
Qtech(config-if)# <b>mac access-group</b> { <i>id</i>   <i>name</i> } { <b>in</b>   <b>out</b> }	Applies the ACL to the specific interface.



#### Note

Method 1 only configures the numerical value ACL. Method 2 can configure the names and numerical value ACL, and specify the table entry priorities (in the devices that support ACE priorities).

The route does not support MAC ACLs.

### 1.5.3 Displaying Configuration of MAC Extended ACLs

To monitor ACLs, run the following command in privileged EXEC mode:

Command	Function
show access-lists [ <i>id</i>   <i>name</i> ]	Queries the basic ACLs.

### 1.5.4 Other Related Configurations

#### 1.5.5 Configuring ACEs by Priority

To embody the ACE priority, criteria is set up for each ACL so that ACEs in an ACL are arranged in a standard manner: using an ACE sequence number as the start point and making the sequence number grows at an increment:

- ACEs are arranged by sequence number in ascending order in the chain table.
- ACE arrangement starts from a sequence number. If no number is specified, it increases at an increment on the basis of the previous ACE number.
- To specify the sequence number of an ACE, insert the ACE and ensure that a new ACE can be inserted between two adjacent ACEs.
- The ACL specifies the start number and the increment.

The **ip access-list resequence** {*acl-id*| *acl-name*} *sn-start* *sn-inc* command is available. For details, see command reference.

Whenever the preceding command is run, the ACEs in the ACL will be sorted. For example, the ACEs in the ACL named **tst\_acl** are numbered as follows:

In the beginning

```
ace1: 10
ace2: 20
ace3: 30
```

The ACEs are numbered as follows after “the **ip access-list resequence** *tst\_acl* 100 3” command is run:

```
Qtech(config)# ip access-list resequence tst_acl 100 3
ace1: 100
ace2: 103
ace3: 106
```

If you do not specify *sn-num* when adding ACE 4, ACE 4 is numbered as follows:

```
Qtech(config-std-nacl)# permit ...
ace1: 100
ace2: 103
ace3: 106
ace4: 109
```

If you set *seg-num* to **105** when adding ACE 5, ACE 5 is numbered as follows:

```
Qtech(config-std-nacl)# 105 permit ...
ace1: 100
ace2: 103
ace5: 105
ace3: 106
ace4: 109
```

The sequence number mechanism is designed to add ACEs by priority.

#### Delete ACEs

```
Qtech(config-std-nacl)# no 106
ace1: 100
ace2: 103
ace5: 105
ace4: 109
```

It is also convenient to delete ACEs with a sequence number.

### 1.5.6 Configuring ACL Logging

When ACL Logging is enabled, if a packet matches a logging-enabled ACE and the matching speed reaches or even exceeds the configured logging threshold, the system generates a log within one logging interval to determine whether to permit or deny this packet.



#### Note

This function applies only to standard and extended IP ACLs and is optional.

#### Default configuration

The ACL logging function is disabled by default.

ACL Options are configured as follows:

Configure the ACL logging speed threshold. This threshold means the maximum speed an ACE is matched. When it is exceeded, a log is generated.

Command	Function
Qtech(config)# <b>ip access-list log-update threshold</b> <i>threshold-value</i>	Configures the ACL logging threshold.

Configure the ACL logging interval, in milliseconds.

Command	Function
Qtech(config)# <b>ip ccess-list logging interval</b> <i>interval-value</i>	Configures the ACL logging interval.

Enable ACE logging so that packets matching an ACE can be counted.

Command	Function
Qtech(config)# <b>ip access-list extended</b> { <i>id</i>   <i>name</i> }	Enters ACL configuration mode.
Qtech(config-ext-nacl)# [ <i>sn</i> ] { <b>permit</b>   <b>deny</b> } <b>protocol</b> <b>source</b> <i>source-wildcard</i> <b>destination</b> <i>destination-wildcard</i> [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>fragment</b> ] [ <b>range</b> <i>lower upper</i> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>option</b> <i>option</i> ] [ <b>log</b> ]	Adds ACEs to the ACL. For details about the command, see command reference.

Command	Function
Qtech(config-exp-nacl)# exit	Exits ACL configuration mode and selects the interface to which the ACL is to be applied.

Configuration example:

- Configure the permission and password for enabling the ACL logging function.

```
Qtech> enable
Qtech#
```

- Enter global configuration mode.

```
Qtech# configure terminal
Qtech(config)#
```

- Configure the ACL logging threshold and interval.

```
Qtech(config)# ip access-list log-update threshold 1
Qtech(config)# ip access-list logging interval 1
```

- Enter ACL configuration mode and enable logging on the desired ACE.

```
Qtech(config-ext-nacl)# permit ip 99.9.9.0 0.0.0.255 any log
```

- Add a deny ACE and enable the logging function on the ACE.

```
Qtech(config-ext-nacl)# deny ip any any log
```

- end

```
Qtech(config-ext-nacl)# end
```

- The following log will be generated when the ACL logging threshold is reached or exceeded:

```
*Feb 20 14:10:48.747: %SEC-6-IPACCESSLOGNP: list s1 permitted 0 99.9.9.2 -> 99.9.9.1,
1 packet
*Feb 20 14:11:37.171: %SEC-6-IPACCESSLOGNP: list s1 permitted 0 99.9.9.2 -> 99.9.9.1,
2 packets
*Feb 20 14:42:51.207: %SEC-6-IPACCESSLOGNP: list s1 denied 0 90.9.9.2 -> 99.9.9.1, 1
packet
```

In privileged configuration mode, run the following commands to configure a global security tunnel:

Command	Function
Qtech# configure terminal	Enters global configuration mode.
Qtech(config)#security global access-group 1	Configures a global security tunnel.

In privileged configuration mode, execute the following commands to set an exception port:

Command	Function
Qtech# configure terminal	Enters global configuration mode.
Qtech(config)#interface <i>idx</i>	Enters interface configuration mode.
Qtech(config-if)# security uplink enable	Sets the interface as an exceptional port..

In privileged configuration mode, run the following commands to configure a security tunnel on the interface:

Command	Function
Qtech# configure terminal	Enters global configuration mode.
Qtech(config)#interface <i>idx</i>	Enters interface configuration mode.
Qtech(config-if)# security access-group 1	Configures a security tunnel on the interface.

The following example shows how to configure a security tunnel on a security port where IP/MAC binding is configured, so that IPX packets can pass:

Set port 4 as the security port and bind IP address and MAC address

```
Qtech(config)#interface FastEthernet 0/4
Qtech(config-if)#switchport port-security
Qtech(config-if)#switchport port-security binding 0000.0000.0011 vlan 1 192.168.6.3
```

Only the packets whose source IP address is 192.168.6.3 and MAC address is 0000.0000.0011 can pass the device through port 4. To receive IPX packets, set a security tunnel as follows:

```
Qtech#configure
Qtech(config)#expert access-list extended safe_channel
Qtech(config-exp-nacl)#permit ipx any any
Qtech(config-exp-nacl)#exit
Qtech(config)#security global access-group safe_channel
```

Or configure a security tunnel on the interface:

```
Qtech#configure
Qtech(config)#expert access-list extended safe_channel
Qtech(config-exp-nacl)#permit ipx any any
Qtech(config-exp-nacl)#exit
Qtech(config)#interface FastEthernet 0/4
```

```
Qtech(config-if)#security access-group safe_channel
```

IPX packets can pass through port 4 after a security channel is configured globally or on an interface.

### 1.5.7 Configuring ACL80

ACL 80 is also called the custom ACL, which is used to match the first 80 bytes of a packet. A packet consists of a series of byte flows. ACL 80 enables the user to filter packets according to the specified 16 bytes of the first 80 bytes in the packet.



**Note** The SMAC/DMAC/SIP/DIP/ETYPE field of the packets is not specified. In other words, a packet is filtered only when the specified 16 bytes match ACL 80 in addition to these fields.

For any 16-byte field, it is possible to compare or not the configured value by bits. In other words, it allows setting any bit of those 16 bytes as 0 or 1. There are two factors in filtering any byte: filtering rule and filter domain template. The bits of the both are one-to-one corresponding. The filtering rule specifies the value of the field to be filtered. The filter domain template specifies whether to filter the related fields in the filtering rule ("1" indicates matching the bit in the corresponding filtering rule, 0 for not). Therefore, when it is time to match a bit, it is required to set 1 for the corresponding bit in the filter domain template. If the filter domain template bit is set as 0, no match will be done no matter what the corresponding bit is in the filtering rule.

For example,

```
Qtech(config)# expert access-list advanced name
Qtech(config-exp-dacl)# permit 00d0f8123456 ffffffff 0
Qtech(config-exp-dacl)# deny 00d0f8654321 ffffffff 6
```

The user custom ACL matches any byte of the first 80 bytes in the layer-2 data frames according to the user definitions, and then performs corresponding processing for the packets. To use ACL 80 correctly, it is necessary to have in-depth knowledge about the structure of layer-2 data frames. The following illustrates the first 64 bytes in a layer-2 data frame (each letter indicates a hexadecimal number, and each two letters indicate a byte).

AA AA AA AA AA AA BB BB BB BB BB BB CC CC DD DD  
 DD DD EE FF GG HH HH HH II II JJ KK LL LL MM MM  
 NN NN OO PP QQ QQ RR RR RR RR SS SS SS SS TT TT  
 UU UU VV VV VV VV WW WW WW WW XY ZZ aa aa bb bb

The following table lists the meanings and offset values of each letter:

Letter	Meaning	Offset	Letter	Meaning	Offset
A	Destination MAC	0	O	TTL field	34
B	Source MAC	6	P	Protocol ID	35
C	VLAN tag field	12	Q	IP checksum	36
D	Data frame length field	14	R	Source IP address	38
E	DSAP field	18	S	Destination IP address	42

F	SSAP field	19	T	TCP source port	46
G	Ctrl field	20	U	TCP destination port	48
H	Org Code field	21	V	Sequence number	50
I	Encapsulated data type	24	W	Confirmation field	54
J	IP version No.	26	XY	IP header length and reservation bits	58
K	TOS field	27	Z	Reservation bit and flags bit	59
L	IP packet length	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

As shown in the preceding table, the offset of each field is the offset in the SNAP+tag 802.3 data frame. In ACL 80, the user can use two parameters, the rule mask and offset, to abstract any byte from the first 80 bytes of the data frame, and then compare it with the user defined rule to filter the matched data frame for corresponding processing. The user defined rule can be some fixed attributes of the data. For example, the user wants to filter all the TCP packets by defining the rule as "06", rule mask as "FF" and offset as 35. Here, the rule mask and offset work together to abstract the contents of the TCP protocol ID field in the received data frame, and compare it with the rule to filter all TCP packets.



**Caution**

ACL 80 can be used to match Ethernet packets, 803.3 SNAP packets, and 802.311c packets. If the value for matching DSAP to the cnt1 field is set to AAAA03, it indicates to match the 803.3 SNAP packets. If the value is set to E0E003, it indicates to match the 803.311c packets. This field cannot be set to match Ethernet packets.



**Caution**

ACL 80 only match only the 16 bytes of a packet. If the 16 bytes are used, no fields other than the 16 bytes can be matched. For example:

```
Qtech(config)# expert access-list advanced name
Qtech(config-exp-dacl)# permit 11223344556677889900aabbccd deeff
ffffffffffffffffffffffffffffffff 50
```

Add another ACE:

```
Qtech(config-exp-dacl)#permit 11223344556677889900aabbccd deeff
ffffffffffffffffffffffffffffffff 54
```

The configuration will fail because the 16 bytes are used by the first ACE. To match the second ACE, you must delete the first ACE.

### 1.5.8 Configuring IP Options Filtering

IP Options filtering is used to match options in the IP packet header by option value (0–255) or option name. If the IP options in a packet match all bits defined in ACEs, the packet is deemed to match the ACL. Users can set any values for IP options to filter packets with specified IP options.



**Note**

This feature applies only to named extended ACLs and is optional.

Configure IP Options filtering:

Command	Function
Qtech(config)# ip access-list extended { id   name }	Enters ACL configuration mode.

Command	Function
Qtech(config-ext-nacl)# [sn] { <b>permit</b>   <b>deny</b> } <b>protocol</b> <b>source</b> <b>source-wildcard</b> <b>destination</b> <b>destination-wildcard</b> [ <b>precedence</b> <b>precedence</b> ] [ <b>tos</b> <b>tos</b> ] [ <b>fragment</b> ] [ <b>range</b> <b>lower</b> <b>upper</b> ] [ <b>time-range</b> <b>time-range-name</b> ] [ <b>option</b> <b>option</b> ] [ <b>log</b> ]	Adds ACEs to the ACL. For details about the command, see command reference.
Qtech(config-exp-nacl)# <b>exit</b>	Exits ACL configuration mode and selects the interface to which the ACL is to be applied.
Or	
Qtech(config)# <b>interface</b> <i>interface</i>	Exits ACL configuration mode and selects the interface to which the ACL is to be applied.
Qtech(config-if)# <b>ip access-group</b> { <i>id</i>   <i>name</i> } { <b>in</b>   <b>out</b> }	Applies the ACL to the specific interface.

Configuration example:

- Configure the permission and password for enabling the IP Option feature.

```
Qtech> enable
Qtech#
```

- Enter global configuration mode.

```
Qtech# configure terminal
Qtech(config)#
```

- Enter ACL configuration mode.

```
Qtech(config)# ip access-list extended ip-options
Qtech(config-ext-nacl)#
```

- Add ACEs.

```
Qtech(config-ext-nacl)# permit ip any any option lsr
```

- Add deny ACEs.

```
Qtech(config-ext-nacl)# deny ip any any option any-options
```

- end

```
Qtech(config-ext-nacl)# end
```

- Display the configuration result.

```
Qtech# show access-list ip-options
ip access-lists extended ip-options
10 permit tcp any any option lsr
20 deny tcp any any option any-options
```

### 1.5.9 Configuring ACLs Based on the Time Range

You can make ACLs effective based on time, for example, ACLs take effect during certain periods in a week. For this purpose, you must first set a time range.

Time range implementation depends on the system clock. If you want to use this function, you must assure that the system has a reliable clock.

In privileged configuration mode, run the following commands:

Command	Function
Qtech# <b>configure terminal</b>	Enters global configuration mode.
Qtech(config)# <b>time-range</b> <i>time-range-name</i>	Identifies a time range by using a meaningful display character string as its name
Qtech(config-time-range)# <b>absolute</b> [ <b>start time</b> <i>date</i> ] <b>end</b> <b>time</b> <i>date</i>	Sets the absolute time range (optional). For details, see the time range configuration guide.
Qtech(config-time-range)# <b>periodic</b> <b>day-of-the-week</b> <b>time</b> <b>to</b> [ <i>day-of-the-week</i> ] <b>time</b>	Sets the periodic time range (optional).
Qtech# <b>show time-range</b>	Verifies the configuration.



Qtech# <b>copy running-config startup-config</b>	Saves the configuration.
Qtech(config)# <b>ip access-list extended 101</b>	Enters ACL configuration mode.
Qtech(config-ext-nacl)# <b>permit ip any any time-range time-range-name</b>	Configures a time range-based ACE.

**Note**

The length of the name should be 1-32 characters without any blank space. You can set one absolute time range at most. The application based on time-ranges will be effective only in this time range. You can set one or more intervals. If you have already set a running time range for **time-range**, the application takes effect at intervals in that time range.

The following example shows how to deny HTTP packets during the working hours in a week by using the time range-based ACLs:

```
Qtech(config)# time-range no-http
Qtech(config-time-range)# periodic weekdays 8:00 to 18:00
Qtech(config)# end
Qtech(config)# ip access-list extended limit-udp
Qtech(config-ext-nacl)# deny tcp any any eq www time-range no-http
Qtech(config-ext-nacl)# exit
Qtech(config)# interface gigabitEthernet 0/1
Qtech(config-if)# ip access-group no-http in
Qtech(config)# end
```

Example of time ranges:

```
Qtech# show time-range
time-range entry: no-http(inactive)
periodic Weekdays 8:00 to 18:00
time-range entry: no-udp
periodic Tuesday 15:30 to 16:30
```

### 1.5.10 Configuring TCP Flag Filtering

The TCP Flag filtering feature provides a flexible mechanism. At present, TCP Flag filtering control supports the match-all option. Namely, when the TCP Flags in a received packet exactly match those defined in the ACE, the packet will be checked by the ACL rule. A user can define any combination of TCP Flags to filter some packets with specific TCP Flags.

For example,

```
permit tcp any any match-all rst
```

Allow the packets to pass if the TCP Flag is reset and other fields are set to 0.

**Note**

This feature is optional when the protocol number is set to TCP in naming ACLs and numerical value ACLs. MAC extended and IP standard ACLs do not support this function.

To configure TCP Flag filtering, run the following commands:

Command	Function
Qtech(config)# <b>ip access-list extended { id   name }</b>	Enters ACL configuration mode
Qtech(config-ext-nacl)# [sn] { <b>permit   deny</b> } <b>tcp</b> source source-wildcard [ operator port ] destination destination-wildcard [operator port] [ <b>match-all</b> flag-name][ <b>precedence</b> precedence]	Adds ACEs to the ACL. For details about the command, see command reference.
Qtech(config-ext-nacl)# <b>exit</b>	Exits ACL configuration mode and selects the interface to which the ACL is to be applied.
Or	

Qtech(config)# <b>interface</b> <i>interface</i>	Exits ACL configuration mode and selects the interface to which the ACL is to be applied.
Qtech(config-if)# <b>ip access-group</b> { <i>id</i>   <i>name</i> } { <b>in</b>   <b>out</b> }	Applies the ACL to the specific interface

The following example explains how to configure TCP Flag filtering.

- Configure the permission and password for enabling the TCP Flag filtering function.

```
Qtech> enable
Qtech#
```

- Enter global configuration mode.

```
Qtech# configure terminal
Qtech(config)#
```

- Enter ACL configuration mode.

```
Qtech(config)# ip access-list extended test-tcp-flag
Qtech(config-ext-nacl)#
```

- Add an ACE.

```
Qtech(config-ext-nacl)# permit tcp any any match-all rst
Qtech(config-ext-nacl)# permit tcp host 1.1.1.1 any established
```

- Add a deny ACE.

```
Qtech(config-ext-nacl)# deny tcp any any match-all fin
Qtech(config-ext-nacl)#
```

- end

```
Qtech(config-ext-nacl)# end
```

- Show

```
Qtech# show access-list test-tcp-flag
ip access-lists extended test-tcp-flag
10 permit tcp any any match-all rst
20 deny tcp any any match-all fin
```

### 1.5.11 Configuring Comments

Comments on ACLs and ACEs are provided for easy query and understanding of ACL configuration.



#### Note

Up to one ACL comment and 2048 ACE comments can be configured in one ACL.



#### Caution

The length of each comment is 100 bytes.



The ACE comment is supported on the router only.

In privileged configuration mode, run the following commands to configure an ACL comment:

Command	Function
Qtech# <b>configure terminal</b>	Enters global configuration mode.
Qtech(config)# <b>ip access-list standard</b> <i>id</i>	Enters ACL configuration mode.
Qtech(config-std-nacl)# <b>list-remark</b> <i>comment</i>	Comments the ACL.

You can also run the following commands to set an ACL comment:

Command	Function
Qtech# <b>configure terminal</b>	Enters global configuration mode.
Qtech(config)# <b>access-list</b> <i>id</i> <b>list-remark</b> <i>comment</i>	Sets the ACL comment.

In privileged configuration mode, run the following commands to configure an ACE comment:

Command	Function
Qtech# <b>configure terminal</b>	Enters global configuration mode.
Qtech(config)# <b>ip access-list standard</b> <i>id</i>	Enters ACL configuration mode.
Qtech(config-std-nacl)# <b>remark</b> <i>comment</i>	Comment the ACE.



You can also run the following commands to set an ACE comment:

Command	Function
Qtech# <b>configure terminal</b>	Enters global configuration mode.
Qtech(config)# <b>access-list id list-remark comment</b>	Sets the ACE comment.

The following example shows how to configure the ACL comment and the ACE comment:

```
Qtech(config)#ip access-list standard 1
Qtech(config-std-nacl)#remark ace_remark_permit_62_start
Qtech(config-std-nacl)#permit 192.168.197.62 0.0.0.0
Qtech(config-std-nacl)#remark ace_remark_permit_62_end
Qtech(config-std-nacl)#list-remark acl_remark_foo
Qtech(config-std-nacl)#end
Qtech#write
Qtech#show access-lists 1
ip access-list standard 1
 remark ace_remark_permit_62_start
 10 permit host 192.168.197.62
 remark ace_remark_permit_62_end
list-remark acl_remark_foo
Qtech#
```

### 1.5.12 Configuring SVI Router ACLs

The ACLs applied to layer 3 interfaces are called Router ACLs, which apply only to the routing packets forwarded at layer 3.

To solve this problem, Qtech switches are configured with a command for enabling SVI Router ACLs. After this function is enabled, security ACLs on SVIs apply only to layer 3 forwarding packets between VLANs.

#### Default Configuration

By default, SVI Router ACLs are disabled. SVI ACLs apply to both inter-VLAN layer 3 packets and intra-VLAN bridge-forwarded packets.

#### Configuring SVI Router ACLs

Command	Function
Qtech# <b>configure terminal</b>	Enters global configuration mode.
Qtech# <b>[no] svi router-acls enable</b>	Enables/Disables the SVI Router ACLs.

This function is only supported on SS3000E, S5750, S8600 and S12000 series routers.

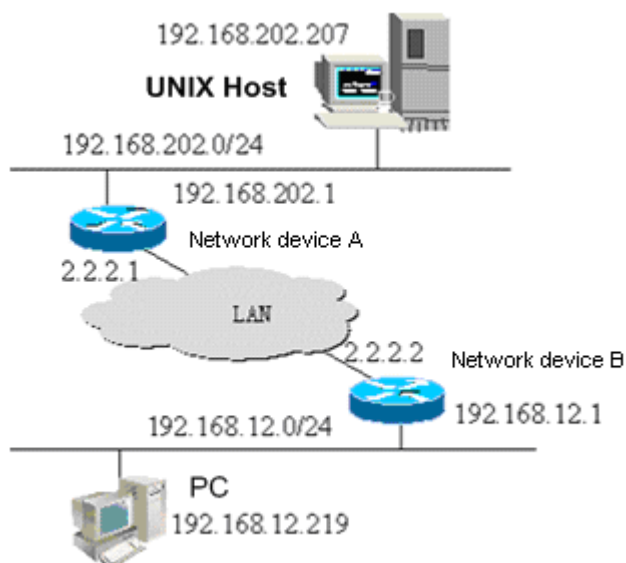
## 1.6 Configuration Examples

### 1.6.1 IP ACL Example

#### Configuration requirements:

There are two network devices A and B, as shown in Figure 1-3:

Figure 3 Basic ACL



It is required to implement the following security functions by configuring ACLs on device B.

Hosts on the 192.168.12.0/24 network segment can telnet the remote Unix host only in working hours and these host cannot ping the Unix server.

Device B is forbidden to access any services of hosts on the 192.168.202.0/24 network segment.



#### Note

This example shows a simplified topology of the banking system. Namely, only access from hosts on the LAN in a branch or outlet to the central host is allowed.

## Equipment Configuration

Device B configuration:

```
Qtech(config)# interface GigabitEthernet 0/1
Qtech(config-if)# ip address 192.168.12.1 255.255.255.0
Qtech(config-if)# exit
Qtech(config)# interface GigabitEthernet 0/2
Qtech(config-if)# ip address 2.2.2.2 255.255.255.0
Qtech(config-if)# ip access-group 101 in
Qtech(config-if)# ip access-group 101 out
```

According to requirements, configure an extended ACL numbered 101

```
access-list 101 permit tcp 192.168.12.0 0.0.0.255 any eq telnet time-range check
Qtech(config)# access-list 101 deny icmp 192.168.12.0 0.0.0.255 any
Qtech(config)# access-list 101 deny ip 2.2.2.0 0.0.0.255 any
Qtech(config)# access-list 101 deny ip any any
```

Configure the time range

```
Qtech(config)# time-range check
Qtech(config-time-range)# periodic weekdays 8:30 to 17:30
```

**Note**

For ACL 101, the last rule statement "access-list 101 deny ip any any" is not needed, because the end of the ACL contains an implicit deny statement for all packets.

Device A configuration:

```
Qtech(config)# hostname Qtech
Qtech(config)# interface GigabitEthernet 0/1
Qtech(config-if)# ip address 192.168.202.1 255.255.255.0
Qtech(config)# interface GigabitEthernet 0/2
Qtech(config-if)# ip address 2.2.2.1 255.255.255.0
```

### 1.6.2 IPv6 Extended ACL Configuration Example

It is required to implement the following security functions by configuring ACLs:

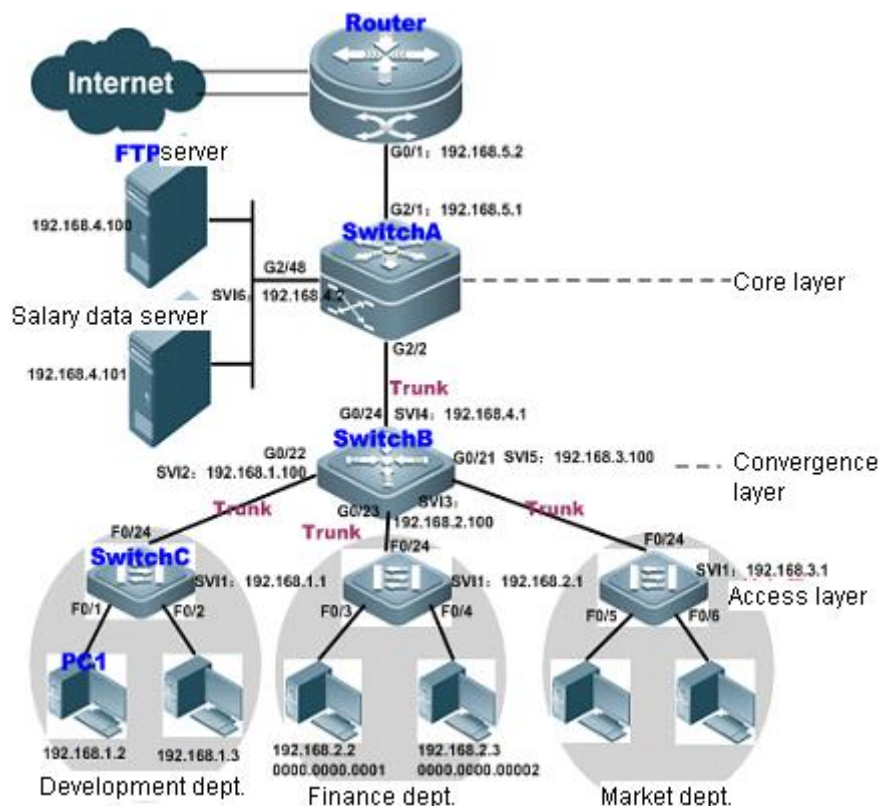
- The host whose IP address is 192.168.4.12 can access the gigabit 0/1 interface of a device.
- It cannot access other interfaces.

```
Qtech> enable
Qtech# config terminal
Qtech(config)# ipv6 access-list v6-list
Qtech(config-ipv6-nacl)# permit ipv6 ::192:68:4:12/24 any
Qtech(config-ipv6-nacl)# deny ipv6 any any
Qtech(config-ipv6-nacl)# exit
Qtech(config)# interface gigabitEthernet 0/1
Qtech(config-if)# ipv6 traffic-filter v6-list in
Qtech(config-if)# end
Qtech# show access-lists
ipv6 access-list extended v6-list
petmit ipv6 ::192.168.4.12 any
deny any any
```

- An ACL cannot match all the preceding areas. Besides, the IPv6 ACL does not apply to packet fragments. Besides, when **sip** and **dip** of a packet match an ACL, **type code** or source and destination ports of ICMP is ignored.

### 1.6.3 Typical Application of Intranet ACL

Figure 5 Networking Diagram



The preceding diagram shows the typical topology of an Intranet:

The access switch (Switch C) connecting PCs of respective departments is connected to the convergence switch through Gigabit optical cable (trunk mode).

The convergence switch (Switch B) assigns one VLAN for each department and is connected to the core switch through 10G optical fiber cable (trunk mode).

The core switch (Switch A) is connected with multiple servers, such as FTP, HTTP server and etc, and is connected to Internet through firewall.

#### Application Requirements

The ACL application in this network has the following requirements:

Ports that are susceptible to viruses must be disabled to guarantee Intranet security.

Only the internal PCs can access the servers.

Only PCs within a department can access each other.

R&D personnel are forbidden to use Instant messaging software such as QQ and MSN in working hours (namely from 09:00 to 18:00).

#### 1.6.3.1 Notes

- The viruses can be avoided by configuring extended ACLs on the router-connecting port (G2/1) of core switch (Switch A) to filter packets destined for relevant ports.
- As for the requirement that internal PCs can access the servers while external PCs are not allowed to access these servers, IP extended ACLs can be defined and applied to ports (G2/2, SVI2) of the core switch (Switch A) that connect with the convergence switch and server.
- As for the requirement that specific departments cannot access each other, IP extended ACLs can be applied to G0/22 and G0/23 of Switch B).

- Configuring time & IP based extended ACL can prevent R&D departments from suing QQ/MSN and other IM application during a specific period (applying time & IP based extended ACL to SVI2 of Switch B).

### Configuration Steps

- Configure the core switch: Switch A

Step 1: Define the virus-blocking ACL "Virus\_Defence".



#### Note

The worm viruses on the network will create a TFTP server on the local port of "udp/69" in order to transmit the binary virus program to other infected systems. While selecting the destination IP address, the worms will generally select the IP address of subnet to which the infected system belongs, and then randomly select the attack target on Internet as per certain algorithm. Once the connection is established, the worms will send attack data to TCP ports (135, 445, 593, 1025, 5554, 9995, and 9996), UDP ports (136, 445, 593, 1433, and 1434) and UDP/TCP ports (135, 137, 138, and 139) of targets. If the attack is successful, TCP/4444 port of target system will be used as the backdoor port. After that, worms will connect to this port and send **tftp** command in order to transmit virus file to the target system and run the file. The infected server will send substantive invalid data packets to the network, thus wasting network bandwidth and even causing failure of network devices and the network. In such a case, the extended ACL can be used to filter data packets destined for these ports.

```
A#configure terminal
A(config)#ip access-list extended Virus_Defence
```

! Deny packets destined for internal and external TCP ports which may have been used by viruses.

```
A(config-ext-nacl)#deny tcp any any eq 135
A(config-ext-nacl)#deny tcp any eq 135 any
A(config-ext-nacl)#deny tcp any any eq 136
A(config-ext-nacl)#deny tcp any eq 136 any
A(config-ext-nacl)#deny tcp any any eq 137
A(config-ext-nacl)#deny tcp any eq 137 any
```

.....! The configuration on other ports is similar.

```
A(config-ext-nacl)#deny tcp any any eq 9996
A(config-ext-nacl)#deny tcp any eq 9996 any
```

! Deny packets destined for internal and external UDP ports which may have been used by viruses.

```
A(config-ext-nacl)#deny udp any any eq 69
A(config-ext-nacl)#deny udp any eq 69 any
A(config-ext-nacl)#deny udp any any eq 135
A(config-ext-nacl)#deny udp any eq 135 any
A(config-ext-nacl)#deny udp any any eq 137
A(config-ext-nacl)#deny udp any eq 137 any
```

! The configuration on other ports is similar.

```
A(config-ext-nacl)#deny udp any any eq 1434
A(config-ext-nacl)#deny udp any eq 1434 any
```

! Deny ICMP packets.

```
A(config-ext-nacl)#deny icmp any any
```

! Permit all other IP packets.

```
A(config-ext-nacl)#permit ip any any
A(config-ext-nacl)#exit
```

Step 2: Apply the ACL *Virus\_Defence* to the router-connecting interface of the core device.

```
A(config)#interface gigabitEthernet 2/1
A(config-if)#no switchport
A(config-if)#ip address 192.168.5.1 255.255.255.0
```

! Apply the ACL *Virus\_Defence* in the inbound direction of G2/1 to deny virus infected packets from an external network.

```
A(config-if)#ip access-group Virus_Defence in
A(config-if)#exit
```

Step 3: Define the ACL *access\_server* that permits only Intranet PCs to access the server.

```
A(config)#ip access-list extended access_server
```

! Permit only specified Intranet PCs to access the server (IP address: 192.168.4.100).

```
A(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 host 192.168.4.100
A(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 host 192.168.4.100
A(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255 host 192.168.4.100
A(config-ext-nacl)#deny ip any any
```

Step 4: Apply the ACL *access\_server* to the interface connecting with convergence device and server.

```
A(config)#interface gigabitEthernet 2/2
A(config-if)#switch mode trunk
```

! Apply the ACL to the inbound direction of the convergence switch.

```
A(config-if)#ip access-group access_server in
A(config-if)#exit
```

! Create a VLAN.

```
A(config)#vlan 2
A(config-vlan)#exit
A(config)#interface gigabitEthernet 2/48
```

! The server-connecting interface of G2/48 belongs to VLAN 2.

```
A(config-if)#switch access vlan 2
A(config-if)#exit
```

! Apply the ACL to the inbound direction of the server-connecting interface.

```
A(config)#interface vlan 2
A(config-if-VLAN 2)# ip access-group access_server in
A(config-if-VLAN 2)# ip address 192.168.4.2 255.255.255.0
A(config-ext-nacl)#end
```

■ Configure the convergence switch: SwitchB

Step 1: Create VLAN 2, VLAN 3, and VLAN 4.

```
B#configure terminal
```

! Create VLAN 2, VLAN 3, and VLAN 4.

```
B(config)#vlan range 2-4
B(config-vlan-range)#exit
```

Step 2: Define ACLs.

! Define the IP extended ACLs *vlan\_access1* and *vlan\_access2*.

```
B(config)#ip access-list extended vlan_access1
```

! Prohibit PCs of the finance department and market department from accessing PCs of the R&D department.

```
B(config-ext-nacl)#deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
B(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
B(config-ext-nacl)#permit ip any any
B(config)#ip access-list extended vlan_access2
```

! Prohibit PCs of the R&D department and market department from accessing PCs of the finance department.

```
B(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
B(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
B(config-ext-nacl)#permit ip any any
B(config-ext-nacl)#exit
```



Step 3: Apply ACLs *vlan\_access1* and *vlan-access2* to the corresponding interfaces.

! Configure G0/22 as a trunk port and apply *vlan\_access1* to this port.

```
B(config)#interface GigabitEthernet 0/22
B(config-if)#switchport mode trunk
B(config-if)#ip access-group vlan_access1 in
```

! Configure G0/23 as a trunk port and apply *vlan\_access2* to this port.

```
B(config)# interface GigabitEthernet 0/23
B(config-if)# switchport mode trunk
B(config-if)# ip access-group vlan_access2 in
```

! Configure G0/24 as a trunk port.

```
B(config)#interface GigabitEthernet 0/24
B(config-if)#switchport mode trunk
```

! Configure the IP address of SVI 2.

```
B(config)#interface vlan 2
B(config-if)#ip address 192.168.1.100 255.255.255.0
```

! Configure the IP address of SVI 3.

```
B(config)#interface vlan 3
B(config-if)#ip address 192.168.2.100 255.255.255.0
```

! Configure the IP address of SVI 4.

```
B(config)#interface vlan 4
B(config-if)#ip address 192.168.4.1 255.255.255.0
```

Step 4: Define time range.

! Define the time range that starts from 09:00 to 18:00 in weekdays.

```
B#configure terminal
B(config)#time-range worktime
B(config-time-range)#periodic weekdays 9:00 to 18:00
```

Step 5: Define the traffic rule of R&D department.

```
B#configure terminal
```

! Create the extended ACL *yanfa* in configuration mode.

```
B(config)#ip access-list extended yanfa
```

! Prohibit all IM applications such as QQ and MSN on hosts of R&D department from 09:00 to 18:00 in weekdays.

```
B(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime
B(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 8001 any time-range worktime
B(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 443 any time-range worktime
B(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 1863 any time-range worktime
B(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 4000 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 1429 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6000 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6001 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6002 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6003 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6004 any time-range worktime
```

! Permit all other IP traffic.

```
B(config-ext-nacl)#permit ip any any
```

! Apply the ACL to the inbound direction of SVI 2.

```
B(config)#interface vlan 2
B(config-if)#ip access-group yanfa in
```

## Verification

Step 1: Verify whether ACEs are correct. The key is that whether the priorities of ACEs are correct and whether ACEs are effective.

```
SwitchA#show access-lists
ip access-list extended Virus_Defence
 10 deny tcp any any eq 135
 20 deny tcp any eq 135 any
 30 deny tcp any eq 4444 any
 40 deny tcp any any eq 5554
 50 deny tcp any eq 5554 any
 60 deny tcp any any eq 9995
 70 deny tcp any eq 9995 any
 80 deny tcp any any eq 9996
 90 deny tcp any eq 9996 any
100 deny udp any any eq tftp
110 deny udp any eq tftp any
120 deny udp any any eq 135
130 deny udp any eq 135 any
140 deny udp any any eq netbios-ns
150 deny udp any eq netbios-ns any
160 deny udp any any eq netbios-dgm
170 deny udp any eq netbios-dgm any
180 deny udp any any eq netbios-ss
190 deny udp any eq netbios-ss any
200 deny udp any any eq 445
210 deny udp any eq 445 any
220 deny udp any any eq 593
230 deny udp any eq 593 any
240 deny udp any any eq 1433
250 deny udp any eq 1433 any
260 deny udp any any eq 1434
270 deny udp any eq 1434 any
280 deny tcp any any eq 136
290 deny tcp any eq 136 any
300 deny tcp any any eq 137
310 deny tcp any eq 137 any
320 deny tcp any any eq 138
330 deny tcp any eq 138 any
340 deny tcp any any eq 139
350 deny tcp any eq 139 any
360 deny tcp any any eq 445
370 deny tcp any eq 445 any
380 deny tcp any any eq 593
390 deny tcp any eq 593 any
400 deny tcp any eq 1025 any
410 deny tcp any any eq 4444
420 deny icmp any any
430 permit tcp any any
440 permit udp any any
450 permit ip any any

ip access-list extended access_server
 10 permit ip 192.168.2.0 0.0.0.255 host 192.168.4.100
 20 permit ip 192.168.1.0 0.0.0.255 host 192.168.4.100
 30 permit ip 192.168.3.0 0.0.0.255 host 192.168.4.100
 40 deny ip any any
SwitchB#show access-lists
ip access-list extended vlan_access1
 10 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
 20 deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
 30 permit ip any any
```



```
ip access-list extended vlan_access2
 10 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
 20 deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
 30 permit ip any any

ip access-list extended yanfa
 10 deny tcp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime (active)
 20 deny tcp 192.168.1.0 0.0.0.255 eq 8001 any time-range worktime (active)
 30 deny tcp 192.168.1.0 0.0.0.255 eq 443 any time-range worktime (active)
 40 deny tcp 192.168.1.0 0.0.0.255 eq 1863 any time-range worktime (active)
 50 deny tcp 192.168.1.0 0.0.0.255 eq 4000 any time-range worktime (active)
 60 deny udp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime (active)
 70 deny udp 192.168.1.0 0.0.0.255 eq 1429 any time-range worktime (active)
 80 deny udp 192.168.1.0 0.0.0.255 eq 6000 any time-range worktime (active)
 90 deny udp 192.168.1.0 0.0.0.255 eq 6001 any time-range worktime (active)
100 deny udp 192.168.1.0 0.0.0.255 eq 6002 any time-range worktime (active)
110 deny udp 192.168.1.0 0.0.0.255 eq 6003 any time-range worktime (active)
120 deny udp 192.168.1.0 0.0.0.255 eq 6004 any time-range worktime (active)
```

Step 2: Verify whether ACL configuration is complete. The key is that whether the correct ACL has been applied to the specified interface.

Device A configuration:

```
A#show run
interface GigabitEthernet 2/1
 no switchport
 no ip proxy-arp
 ip access-group Virus_Defence in
 ip address 192.168.5.1 255.255.255.0
!
interface GigabitEthernet 2/2
 switchport mode trunk
 ip access-group access_server in
!
interface VLAN 2
 no ip proxy-arp
 ip access-group access_server in
 ip address 192.168.4.2 255.255.255.0
```

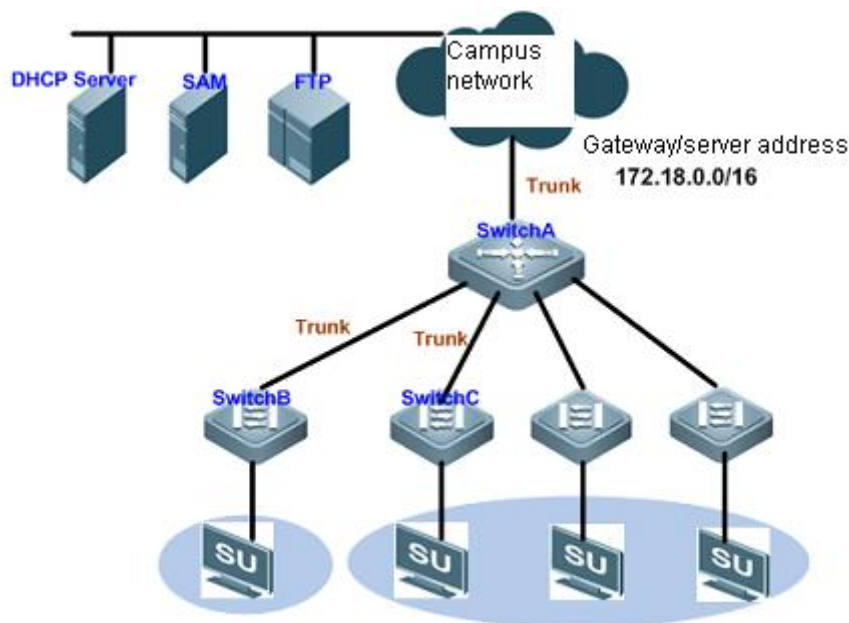
Device B configuration:

```
B#show run
!
interface GigabitEthernet 0/22
 switchport mode trunk
 ip access-group vlan_access1 in
!
interface GigabitEthernet 0/23
 switchport mode trunk
 ip access-group vlan_access2 in
!
interface VLAN 2
 no ip proxy-arp
 ip access-group yanfa in
 ip address 192.168.1.100 255.255.255.0
```

### 1.6.4 Application of expert ACL & ACL 80

#### Networking Diagram

Figure 6 Application topology diagram of the expert ACL&ACL 80



The preceding figure shows the simplified topology of a campus network:

Switch A is the convergence device assigning one VLAN for each faculty and is connected to the campus network through 10G optical cable (trunk mode).

Switch B and Switch C are access devices connecting PCs of respective faculties, and are connected to the convergence switch through Gigabit optical cable (trunk mode).

SU client must be installed on each PC so that a PC can access Internet after being authenticated.

#### Application Requirements

SU software is not embedded in Windows. You must download and install SU client on the PC. However, the PC cannot download software before 802.1x authentication. To solve this problem, the following requirements must be met:

- IP packets and ARP packets accessing the segment address of gateway/server (172.18.0.0/16) are allowed to pass through without authentication, so that the user PC can download software from the specified server or access gateway before authentication.
- DHCP packets (UDP port number being 67/68) are allowed to pass through without authentication, so that the user PC can acquire the IP address in order to proceed with authentication.

#### Notes

Configure ACL80 or expert ACL on the access device (Switch B/Switch C) and combine the feature of secure tunnel to permit certain packets without authentication.

In this case, ACL 80 is configured on Switch B and expert ACLs are configured on Switch C.

#### Configuration Steps

- Device B configuration

**Note**

ACL 80 allows the user to define 16 bytes out of the first 80 bytes of packets to perform per-bit matching and filtering. The user-defined string will be compared with the string extracted from packet (1 means match and 0 means mismatch), so as to determine further action.

Step 1: Configure the customized ACL.

```
B#configure terminal
```

! Create a customized ACL named "tongdao"

```
B(config)#expert access-list advanced tongdao
```

! Permit all ARP packets (protocol number being 0806, offset being 24) with source IP address(the offset in the source IP of ARP packets is 40) falling within the network segment of 172.18.0.0 (hexadecimal value being ac12)

```
B(config-exp-dacl)#permit 0806 ffff 24 ac12 ffff 40
```

! Permit all IP packets (protocol number being 0800, offset being 24) with source IP (the offset in the source IP of IP packets is 38) falling within the network segment of 172.18.0.0 (hexadecimal value being ac12)

```
B(config-exp-dacl)#permit 0800 ffff 24 ac12 ffff 38
```

! Permit DHCP packets with UDP port being 67 (Bootstrap Protocol Server) and 68 (Bootstrap Protocol Client) (offset in protocol number being 35; hexadecimal value of 11 to indicate UDP; offset in port being 46; hexadecimal value of 43/44 corresponding to 67 and 68).

```
B(config-exp-dacl)# permit 11 ff 35 00440043 ffffffff 46
```

```
B(config-exp-dacl)#exit
```

Step 2: Globally configure the ACL for secure tunnel application.

! Configure ACL "tongdao" for secure tunnel application

```
B(config)# security global access-group tongdao
```

■ Device C configuration:

Step 1: Configure an expert ACL.

```
C#configure terminal
```

! In configuration mode, create an expert ACL named "tongdao1"

```
C(config)#expert access-list extended tongdao1
```

! Permit all IP packets with source IP falling within the network segment of 172.18.0.0

```
C(config-exp-dacl)#permit ip 172.18.0.0 0.0.255.255 any any any
```

! Permit all packets with UDP port number being 67 (Bootstrap Protocol Server) and 68 (Bootstrap Protocol Client)

```
C(config-exp-dacl)# permit udp any any eq bootpc any any eq bootps
```

```
C(config-exp-dacl)#exit
```

Step 2: Globally configure the ACL for secure tunnel application.

! Configure ACL "tongdao1" for secure tunnel application

```
C(config)# security global access-group tongdao1
```

## Verifications

Step 1: Verify whether ACEs are correct. The key is that whether the priorities of ACEs are correct and whether ACEs are effective.

```
B# show access-lists
expert access-list advanced tongdao
 10 permit 0806 FFFF 24 AC12 FFFF 40
 20 permit 0800 FFFF 24 AC12 FFFF 38
 30 permit 11 FF 35 00440043 FFFFFFFF 46
```

```
C# show access-lists
expert access-list extended tongdao1
 10 permit ip 172.18.0.0 0.0.255.255 any any any
 20 permit udp any any eq bootpc any any eq bootps
```

Run the preceding command to verify whether the corresponding ACEs are correct.

Step 2: Verify whether ACL configuration is complete. The key is that whether the correct ACL has been applied in global configuration mode:

```
B#show run
!
expert access-list advanced tongdao
!
security global access-group tongdao
!
!
C#show run
!
expert access-list advanced tongdao1
!
security global access-group tongdao1
!
```

---

ACL configuration for different line cards:

---

The following description applies only to versions later than RGOS10.3.

This principle is also appropriate for hot pluggable line cards, which prompts the users to reset line cards.

If ACL out is implemented on the egress, then IP extended ACL and expert ACL will not support port matching. Besides, expert ACL only supports IP packet matching, not other L2 packets, IPV6 does not support flow\_label, DSCP and fragment matching.

If ACL out is processed in the original way, then associating ACL out with SVIs has lots of restrictions:

- Changes the priority of in and out direction; the ACL used in the outbound direction is higher than that used in the inbound direction.
- When you apply an ACL to the outbound direction of an SVI, there is no **deny any any** option by default. But there is **deny any any** option in other ACLs.
- Associating ACL with SVI in Out direction can support IP standard, IP extended, MAC extended, ACL application of expert extended ACLs.
- There are some restrictions for matching destination ip and destination mac in ACL when associating ACL with SVI in the outbound direction. If you want to match destination MAC in MAC extended and expert ACL and apply the ACL in the outbound direction of SVI, the entry will be set and not take effect.
- The set ACL will not take effect if you want to match destination IP address, which is not within the subnet IP range of associated SVI, in IP standard, IP extended and expert ACL. For example, the address of VLAN 1 is 192.168.64.1 255.255.255.0. And now, if you create an IP extended ACL with ACE deny udp any 192.168.65.1 0.0.0.255 eq 255, it will not take effect when applying this ACL to the egress of VLAN 1, for the destination IP address is not within the subnet IP range of VLAN 1; but it will take effect if the ACE is deny udp any 192.168.64.1 0.0.0.255 eq 255, for the destination IP address is up to specification.
- The priority of the ACL associated with an SVI in the outbound direction has the highest priority.
- ACL out does not support user-defined acl type.

## 2 CONFIGURING THE FIREWALL

### 2.1 Understanding IP-MAC Binding

#### 2.1.1 Overview

IP-MAC binding refers to that the IP address and MAC address of a host are bound on the router or firewall it directly connects to, so that an IP address can be used only by the host with the matching MAC address. This function is designed to prevent IP address spoofing. To deploy this function, two prerequisites must be met:

- 1) The MAC address is unique and genuine.
- 2) IP-MAC binding applies only to hosts that are directly connected to a router or firewall.

Furthermore, a host interface may be configured with multiple IP addresses, thus allowing multiple IP addresses to be bound to the same MAC address.

#### 2.1.2 Configuring IP-MAC Binding

##### 2.1.2.1 Enabling or Disabling the IP-MAC Binding Function

IP-MAC binding is disabled by default. To use this function, configure binding rules by using the **ipmacbind** command in global configuration mode. IP-MAC binding function will be disabled if all IP/MAC binding rules are deleted.

##### 2.1.2.2 Configuring IP-MAC Binding

The IP address of a host can be bound to its MAC address by using the **ipmacbind** command to prevent the IP address from being counterfeited by other hosts. Rebind the bound IP address if it already exists. Multiple IP addresses can be bound to the same MAC address. For example:

```
Qtech(config)# ipmacbind 192.168.52.69 032a.33ac.3f11 log
```

The preceding command binds the IP address 192.168.52.69 to the network card with MAC address 032a.33ac.3f11. Here, **log** indicates that the log function regarding IP-MAC binding is enabled. Besides, you can specify the format of any IP address and any MAC address. For example:

```
Qtech(config)# ipmacbind any any log
```

Meanwhile, the IP-MAC binding entries on a LAN can be detected and exported from the ARP table dynamically by using the **ipmacbind auto** command.

```
Qtech(config)# ipmacbind auto
```

You can configure an IP-MAC binding rule list as well as the rules in the list and apply the list to the interface. Besides, you can specify the default processing of packets not matching the IP-MAC binding rule on the current interface. For example:

```
Qtech(config)# ipmacbind list number
Qtech(config-ipmac-bind)#ipmacbind ip mac [log]
Qtech(config-if-GigabitEthernet 0/0)# ipmacbind list number [ default action {permit | deny [ log ] } ]
```

Configure the IP MAC binding rule list and the corresponding rules in the list, apply the list to the corresponding interface at the same time, and configure the default rule operation on the current interface.

```
Qtech(config)# ipmacbind list number
Qtech(config-ipmac-bind)#ipmacbind ip mac [log]
Qtech(config-if-GigabitEthernet 0/0)# ipmacbind list number [ default action {permit | deny [ log ] } ]
```

The **no** form of the **ipmacbind** command is used to delete IP-MAC binding entries. If an IP address is specified in this command, the IP address is deleted from an IP-MAC binding entry. Besides, you can use the **clear ipmacbind**

command to delete the IP-MAC binding entries dynamically exported from the ARP table or all IP-MAC binding entries. For example:

```
Qtech# clear ipmacbind dynamic
```

The preceding command clears all IP-MAC binding entries dynamically exported from the ARP table by using the **ipmacbind auto** command.

```
Qtech# clear ipmacbind all
```

The preceding command clears all IP-MAC binding entries including the information of the rule list.

By default, packets without IP MAC address binding rule are permitted to pass. Use the ipmacbind default action command to deny packets without IP MAC address.

```
Qtech(config)#ipmacbind default action deny
```

Rule description:

The IPMAC binding rule operation only permits or denies two situations. By default, the rule is permit, and the matching rule combinations and the results are as follows:

Deny:

IP Address	MAC Address	Result
False	Correct	Deny
Correct	False	Deny
False	False	Deny
Correct	Correct	Permit

Permit:

IP Address	MAC Address	Result
Correct	False	Deny
Correct	Correct	Permit
False	Correct	Permit
False	False	Permit

### 2.1.2.3 Viewing IP-MAC Binding Information

Run the **show ipmacbind** command to view records or statistics on current IP-MAC binding.

```
Qtech# show ipmacbind table
Total number of IPMAC-Bind rule: 2
IPMAC-Bind global rule:
No    Type      IP Address      MAC Address      Log
1     <static>  any             00d0.0011.0012  off

IPMAC-Bind list 1 rule:
No    Type      IP Address      MAC Address      Log
1     <static>  192.168.2.2    00d0.0011.0011  off
```

To view all IP-MAC binding entries and the IP-MAC binding rule information:

```
Qtech# show ipmacbind statistic
IPMAC-Bind global dropped 0 packets
IPMAC-Bind list 1 dropped 0 packets
```

To view the IP MAC function and the number of invalid packets intercepted by the IP MAC binding rule list;



```
Qtech# show ipmacbind hash
IPMAC-Bind global:
In MAC hash-list 211:
    1: ip-any, mac-00d0.0011.0012
IPMAC-Bind list 1:
In IP hash-list 616:
    1: ip-192.168.2.2, mac-00d0.0011.0011
```

To view the IP-MAC binding rule and the hash table corresponding to IP-MAC binding rule list:

## 2.2 Understanding URL Filtering

### 2.2.1 Overview

URL filtering is an extension of packet filtering, achieving in-depth access control. It is a means of content filtering and restricts intranet users from accessing certain illegal websites.

The process of URL filtering is as follows:

- 1) The firewall resolves the HTTP request from a client to obtain the requested URL;
- 2) The firewall uses the predefined URL filtering rules to match the requested URL;
- 3) If a match is detected, the firewall determines whether to permit or reject the access based on the matching result.
- 4) If no match is detected, the firewall sends the URL request to a third-party content filtering server (such as Websense or N2H2) and meanwhile suspends the HTTP session until a response is returned from the server. Then the firewall determines whether to permit or reject the HTTP request based on the response. All requests shall be denied and an alarm is reported if the server is unavailable.

Currently, only local URL filtering is supported. The linkage with a third-party content filtering server will be realized in future.

### 2.2.2 Configuring URL Filtering

URL filtering rules are configured as follows:

- 5) Specify the URLs to be filtered and add these URLs to a filtering category.
- 6) Configure filtering rules and add the filtering category to the rules.
- 7) Apply these rules to interfaces.

It should be noticed that you need to specify an ACL before applying the rules to the interfaces for advertising the URL filtering range.

#### 2.2.2.1 Registering URLs

To filter a URL, use a URL-related command in global configuration mode to register the URL and the filtering category the URL belongs to. To delete a registered URL, run the **no url** command.

It should be noticed that a URL always begins with a stop (.) in all cases.

For example:

```
Qtech(config)# ip urlfilter rule test .sina.com.cn
Qtech(config)# ip urlfilter rule test .*sina.com.cn
Qtech(config)# ip urlfilter rule test .sina*
Qtech(config)# ip urlfilter rule test .*sina*
```

In the example, the asterisk (\*) is used as the wildcard. The wildcard can be placed only at the end of a URL or after the first stop in a URL.

These URL formats are explained as follows:

- .sina.com.cn represents URLs such as www.sina.com.cn, blog.sina.com.cn, and new.sina.com.cn, instead of Qtech.blog.sina.com.cn, sports.news.sina.com.cn, and the like.
- .\*sina.com.cn represents all URLs ended with "sina.com.cn".
- .sina\* represents all URLs in which the first stop is followed by "sina". For example, blog.sina.com.cn matches this rule but Qtech.blog.sina.com.cn does not.

- \*sina\* represents all URLs containing "sina" such as Qtech.blog.sina.com.cn, blog.sina.com.cn, and www.adfsina.com.

### 2.2.2.2 Configuring URL Filtering Rules

Filtering rules should be configured after the URL category is configured.

URL filtering rules are configured in global configuration mode.

```
Qtech(config)# ip urlfilter category 1 test
```

The preceding command is to create a filtering rule numbered 1. Then, the predefined filtering category can be added to this rule. Each rule can accommodate 15 categories. That is, other predefined categories can also be added to this rule. For example:

- Qtech(config)# ip urlfilter category 1 test1
- Qtech(config)# ip urlfilter category 1 test2
- Qtech(config)# ip urlfilter category 1 test3

It should be noticed that Qtech products allow a category to be added to different rules.

```
Qtech(config)# ip urlfilter category 1 test
Qtech(config)# ip urlfilter category 2 test
Qtech(config)# ip urlfilter category 3 test
```

### 2.2.2.3 Applying Rules to Interfaces

After the preceding configuration is complete, you need to apply these rules to interfaces.

Before applying rules to interfaces, remember configuring an ACL rule in configuration mode.

The following example shows how to create a URL that filters all IP addresses and allows access to the URLs defined in rule 1. In this example, logs are recorded when access is denied.

```
Qtech(config)# access-list 1 permit any
Qtech(config)# interface gigabitEthernet 0/0
Qtech(config-if)# ip urlfilter exclusive-domain 1 1 permit in log
```

Now, URL filtering rule configuration is complete.

## 2.2.3 Viewing Configuration Information and Statistical Information of the URL Filtering Module

### 2.2.3.1 Configuration Information

Suppose that some URL filtering rules have been configured. The following describes how to query, configure, and delete these rules,

#### show ip urlfilter config address

Run the preceding command in configuration mode.

```
Qtech(config)# show ip urlfilter config address
===== [Url without wildcard] =====
cls_name          cls-id          url-address
=====
test1             2              .tianya.cn
-----
test2             3              .sohu.com
-----
test1             1              .sina.com.cn
-----
test1             2              .mop.com
===== [Url no-wildcard end] =====
===== [Url with pre-wildcard] =====
cls_name          cls-id          url-address
=====
```



```

test1          2          .*hong.com
-----
test2          3          .*263.net
-----
test1          2          .*163.com
=====
===== [Url pre-wildcard end] =====
===== [Url with post-wildcard] =====
cls_name      cls-id      url-address
=====
test2          3          .taob*
-----
test1          2          .google.com*
-----
test2          3          .ebay*
-----
test1          2          .baid*
=====
===== [Url post-wildcard end] =====
===== [Url with all-wildcard] =====
cls_name      cls-id      url-address
=====
test2          3          .*huawei*
-----
test1          2          .*cisco*
=====
===== [Url all-wildcard end] =====
===== [Relative CLI Command] =====
ip urlfilter rule test1 .tianya.cn
ip urlfilter rule test2 .sohu.com
ip urlfilter rule test .sina.com.cn
ip urlfilter rule test1 .mop.com
ip urlfilter rule test1 .*hong.com
ip urlfilter rule test2 .*263.net
ip urlfilter rule test1 .*163.com
ip urlfilter rule test2 .taob*
ip urlfilter rule test1 .google.com*
ip urlfilter rule test2 .ebay*
ip urlfilter rule test1 .baid*
ip urlfilter rule test2 .*huawei*
ip urlfilter rule test1 .*cisco*
=====
===== [Relative CLI Command To Del the Rules ] =====
no ip urlfilter rule test1 .tianya.cn
no ip urlfilter rule test2 .sohu.com
no ip urlfilter rule test .sina.com.cn
no ip urlfilter rule test1 .mop.com
no ip urlfilter rule test1 .*hong.com
no ip urlfilter rule test2 .*263.net
no ip urlfilter rule test1 .*163.com
no ip urlfilter rule test2 .taob*
no ip urlfilter rule test1 .google.com*
no ip urlfilter rule test2 .ebay*
no ip urlfilter rule test1 .baid*
no ip urlfilter rule test2 .*huawei*
no ip urlfilter rule test1 .*cisco*

```

Firstly, classify the addresses into four categories: addresses without a wildcard, addresses preceded by a wildcard, addresses followed by a wildcard and addresses with one wildcard at the beginning and one wildcard at the end. And we print out the classified addresses under the same category in a continuous manner.

Secondly, record all the commands you use to configure these addresses. As a result, even a green hand will be able to view the configuration process.

Lastly, provide you a cookie that shows you the commands for deleting configuration, so that you no longer need to run **show run** to query the command for deleting a configuration but copy the desired command and paste it in the CLI.

### show ip urlfilter config rule

The **show** command shows the addresses that have been configured in the current system. Now let's learn the configured rules.

```
Qtech(config)# show ip urlfilter config rule
===== [ Ip UrlFilter Rule configure ] =====
Id      Attribute          Details
-----
1      contain-class:      test
ref-interface:gigabitEthernet 0/0 gigabitEthernet 0/1
-----
2      contain-class:      test1
ref-interface:      gigabitEthernet 0/0
gigabitEthernet 0/1
gigabitEthernet 0/2
-----
3      contain-class:      test2
ref-interface:      gigabitEthernet 0/2
=====
===== [Relative CLI Command] =====
ip urlfilter category 1 test
ip urlfilter category 2 test1
ip urlfilter category 3 test2
===== [Relative CLI Command To Del the Rules ] =====
no ip urlfilter category 1 test
no ip urlfilter category 2 test1
no ip urlfilter category 3 test2
Using this command, you can view the address categories included in a rule and the
interface to which rules apply. Then you can determine the interface from which the
desired information can be obtained.
```

### show ip urlfilter config setting

Query information about gigabitEthernet 0/0.

```
Qtech(config-if)# show ip urlfilter config setting
===== [ Url Filter Rules On gigabitEthernet 0/0 ] =====
Rules On Input
=====
Id  Acl  Action  Class-name  Url-address
-----
1   1    permit  test       .sina.com.cn
-----
2   12   permit  test1      .tianya.cn
                    .mop.com
                    .*hong.com
                    .*163.com
                    .google.com*
                    .baid*
                    .*cisco*
-----
3   12   block   test2      .sohu.com
                    .*263.net
                    .taob*
                    .ebay*
                    .*huawei*
-----
2   13   permit  test1      .tianya.cn
                    .mop.com
```

```

.*hong.com
.*163.com
.google.com*
.baid*
.*cisco*
-----
3    13    block    test2    .sohu.com
                      .*263.net
                      .taob*
                      .ebay*
                      .*huawei*
=====
Relative CLI Command
=====
ip urlfilter exclusive-domain 1 1 permit in log
ip urlfilter exclusive-domain 2 12 permit in
ip urlfilter exclusive-domain 3 12 block in
ip urlfilter exclusive-domain 2 13 permit in
ip urlfilter exclusive-domain 3 13 block in
-----
Relative CLI Command to Del Rules
-----
no ip urlfilter exclusive-domain 1 1 permit in log
no ip urlfilter exclusive-domain 2 12 permit in
no ip urlfilter exclusive-domain 3 12 block in
no ip urlfilter exclusive-domain 2 13 permit in
no ip urlfilter exclusive-domain 3 13 block in
=====[ Url Filter Rules On gigabitEthernet 0/0 End]=====

```

In the command output, you can view rule IDs, effective scope of rules (ACL numbers), conform-action, inclusive categories, and URLs in these categories.

### 2.2.3.2 Statistical Information

Statistical information is also what administrators care much for.

```

Qtech(config)# show ip urlfilter statistics
url filter statistics
=====
the rule 1
    Total requests allowed: 0
    Total requests blocked: 0
the rule 2
    Total requests allowed: 0
    Total requests blocked: 0
the rule 3
    Total requests allowed: 0
    Total requests blocked: 0

```

### 2.2.4 Problems Encountered in Use of this Function

By now, you have seen that URL filtering function configuration is very flexible. But flexible things are always hard to command. Next, let's together have a look at some matters that require your attention.

One URL can only belong to one address category at one time.

Just as you have seen, one URL can only belong to one rule at one time according to our rules.

Only one rule applies to one interface.

Perhaps you have noticed that we provide only one action for each rule in regard to the rules for interfaces, i.e., the action we take when the website to access to matches our rules. What about the mismatch? Take opposite action, of course.

Different URLs have different priorities in the matching process.

Rules' priorities are arranged as follows in descending order:

- Rules without a wildcard.
- Rules with a wildcard at the beginning.
- Rules with a wildcard at the end
- Rules with one wildcard at the beginning and the other at the end.

Once matched by a rule with high priority, an address will not be matched by following rules.

```
ip urlfilter rule test .sina.com.cn
ip urlfilter rule test1 *.*

ip urlfilter category 0 test
ip urlfilter category 1 test1
!
!
ip access-list standard 1
10 permit any

interface gigabitEthernet 0/0
ip urlfilter exclusive-domain 1 1 block in log
ip ref
ip address 130.130.130.1 255.255.255.0
duplex auto
speed auto
!
interface gigabitEthernet 0/1
ip ref
ip address 192.168.52.141 255.255.255.0
duplex auto
speed auto

ip route 0.0.0.0 0.0.0.0 192.168.52.1
```

What is the function of this rule?

He has only configured two rules: one is for filtering .sina.com.cn, and the other is for filtering all websites with the character "." What did he do next? He added the two categories to the two rules, and apply the rule that filters all websites with the character "." to the ingress. It seems that he really wants to disable Internet access.

Well, guess whether the current rule can filter all websites or not? The answer is: of course not.

Take it easy. I will answer your question.

In order to save time and space, I will directly tell you that those websites with .sina.com.cn will not be filtered. Why?.

Let's analyze the process of searching, matching and filtering.

First of all, the website that users visit will match in the rule without wildcard. If they access www.sina.com.cn or news.sina.com.cn, the website will match the rule. Notice that once matched by any rule, the URL a user visits will no longer match following rules. This shall be emphasized. Then, as for our filtering program, the visited website falls into the category of "test" instead of "test 1".

When the category is found out, the filtering begins. Our filtering program on the interface will search in its own rule. When it finds that the category "test" is not included in its own rule, it will adopt the processing mode opposite to what is defined in its own rule to deal with this website. Since the guy defined the rule action is 'block', the action taken for the category "test" that is not in his rule will surely be "permit".

Now, let's have another look from the very beginning before we come to the conclusion why this guy has not filtered all rules. It is because he has not noticed the priority problem of website matching. Though the rule .\* can match all addresses, .sina.com.cn that has a higher priority will match in a better way.

Therefore, we can say that it is very important to configure rule priority.

Notice should be given to the website with lower level domain name(s) and URL redirection.

When we verified our own products, our filter device was always disabled for some websites. Later, we kept track of the visits to these websites. The result was really surprising. Let's see the example of [www.google.com](http://www.google.com).

Careful users may have found that when they access Google in China, they use [www.google.com](http://www.google.com), but they come to see [www.google.cn](http://www.google.cn) in the address bar of browser when the webpage is opened. This is called redirection.

However, under a real environment, the access process is more complicated. (Take our environment here for example).

First, we resolve the domain name of Google in DNS. Then, we will access the website of 210.70.14.147. Next, we will visit [www.google.cn](http://www.google.cn).

If you want to deal with such websites, you need to add the IP address and [google.cn](http://google.cn) into the rule.

Then, you can use tailored functions as you wish.

## 2.3 Understanding Network Ingress Filtering

### 2.3.1 Overview

A lot of DoS/DDoS attacks are carried out with forged source IP addresses. NIF (Network Ingress Filtering, RFC 2827) is aimed to defend against such attacks, or limit the scope and lower the risk of being attacked. It will check up whether the source IP address claimed by the data packet entering a network meets the network prefix advertised by route. If not, filter it. Such filtering mechanism implemented on the router at the network ingress will be very effective to prevent IP spoofing attacks. However, it will take no effect on the IP spoofing attacks with legitimate IP address prefix at all.

### 2.3.2 Configuring NIF

#### 2.3.2.1 Enabling or Disabling Network Ingress Filtering

NIF is disabled by default. To use this function, run the `ip ingress-filter` command in interface mode. For example:

```
Qtech(config-if)# ip ingress-filter log
```

The preceding command enables the NIF function on the interface and the log function of NIF at the same time.

The `no` form of `ip ingress-filter` disables the NIF function on the interface. For example:

```
Qtech(config-if)# no ip ingress-filter log
```

The preceding command disables the NIF function on the interface.

#### 2.3.2.2 Viewing Network Ingress Filtering Information

Run the `show ip ingress-filter` command to view current IP/MAC binding records or statistical information, e.g.,

```
Qtech(config)# show ip ingress-filter
Firewall Network-ingress-filter is enable, blocked 0 flows
Interface FastEthernet 1/0:
log is on, blocked 0 flows
```

Through the preceding command, you can view whether the NIF function is enabled and how much unauthorized information has been blocked.

## 2.4 Understanding TCP SYN Proxy

### 2.4.1 Overview

SYN proxy is an effective way to guard against SYN Flood attacks. SYN flood attacks occur at the stage of three-way handshakes of TCP. Attackers send a large number of TCP SYN packets to victims, who then open a lot of TCP links and respond attackers by sending TCP SYN ACK. However, attackers do not send TCP ACK packets to

complete three-way handshakes. In this case, thus victims' queues are filled with semi-connections and new connections cannot be established until these semi-connections time out. The basic process of TCP SYN proxy is that three-way handshakes between router/firewall proxy service terminal and client terminal are completed first, if the connection is legal, then connection with the service terminal will be established.

## 2.4.2 Configuring TCP SYN Proxy

### 2.4.2.1 Enabling or Disabling TCP SYN Proxy Function

TCP SYN proxy function is disabled by default. Before enabling this function, configure ACL rules to specify the streams to which TCP SYN proxy applies, e.g.,

```
Qtech(config)# access-list 100 permit ip 192.168.52.0 0.0.0.255 any
```

Then, run the **ip tcp-intercept list in|out** command in interface configuration mode to apply TCP SYN proxy to the streams that pass through the interface and match the ACL rules, e.g.,

```
Qtech(config)# interface gigabitEthernet 0/0
Qtech(config-if)# ip tcp-intercept list 100 in log
```

The preceding command indicates that TCP SYN proxy is applied to the inbound streams of gigabit0/0 complying with ACL 100 and the log function of TCP SYN proxy is enabled.

Use the **no** form of the **ip tcp-intercept list in|out** command to disable this function, e.g.,

```
Qtech(config)# interface gigabitEthernet 0/0
Qtech(config-if)# no ip tcp-intercept list 100 in log
```

### 2.4.2.2 Viewing TCP SYN Proxy Information

Use the **show ip tcp-intercept** command to view current TCP SYN proxy records or statistical information, e.g.,

```
Qtech(config-if)# show ip tcp-intercept
Intercepting new connections using access-list 100 at gigabitEthernet 0/0 in
20 incomplete, 1320 established connections (total 1340)
```

Through the preceding command, you can see that TCP SYN proxy has been enabled on gigabit 0/0 interface. In addition, 20 invalid TCP streams unfinished and 1,320 normal TCP streams have been monitored.

## 2.5 Understanding Special Protocol

### 2.5.1 Overview

Such protocols as FTP, MMS, H.323, etc have separate command control channels and data channels. And the data channels are port numbers, etc randomly specified through the control channels by both channels. If control channel port access is only allowed by configuring ACL and other packet filtering rules on network equipments, and provided that no special means is available for processing, data channels will be completely blocked. Therefore, a special way is needed to establish some temporary pass and access mechanisms for the data channels of these protocols.

### 2.5.2 Configuring a Special Protocol

Users need to configure rules in configuration mode, where they specify a name that consists of character strings and is easy to remember for a special protocol to access, e.g.,

You can add FTP to the rule library named "abc", to which the MMS protocol can also be added. These two protocols do not overlay or conflict with each other.

In the same way, a rule library named "123" may be defined.

```
Qtech(config)# ip inspect name abc ftp
Qtech(config)# ip inspect name abc mms
Qtech(config)# ip inspect name 123 mms
Qtech(config)# ip inspect name 123 h323

Qtech(config)# show ip inspect all
```

```
Inspection Rule Configuration
Inspection name abc
ftp
mms
Inspection name 123
mms
h323
```

Then, users need to enter the specified interface and add this rule. For example:

```
Qtech(config)# interface gigabitEthernet 0/0
Qtech(config-if)# ip inspect abc in
Qtech(config)# show ip inspect all
Inspection Rule Configuration
Inspection name abc
ftp
mms
Inspection name 123
mms
h323

Interface Configurationn
Interface gigabitEthernet 0/0
Inbound inspection rule is abc
ftp
mms
```

It should be noticed that one interface can only be applied with one special protocol rule library. If added with another, the newly added rule shall replace the original one. For example:

```
Qtech(config)# interface gigabitEthernet 0/0
Qtech(config-if)# ip inspect abc in
Qtech(config)# show ip inspect all
Inspection Rule Configuration
Inspection name abc
ftp
mms
Inspection name 123
mms
h323
Interface Configurationn
Interface gigabitEthernet 0/0
Inbound inspection rule is abc
ftp
mms
Qtech(config)# interface gigabitEthernet 0/0
Qtech(config-if)# ip inspect 123 in
Qtech(config)# show ip inspect all
Inspection Rule Configuration
Inspection name abc
ftp
mms
Inspection name 123
mms
h323
Interface Configurationn
Interface gigabitEthernet 0/0
Inbound inspection rule is 123
mms
h323
```



## 2.6 Understanding TCP Sequence Number Tracking

### 2.6.1 Overview

The purpose of TCP sequence number check is to guard against intrusion such as TCP session hijacking. It determines whether a data packet is valid by recording and tracking send sequence numbers, acknowledgement sequence numbers, and receive windows of both sides of a TCP connection.

### 2.6.2 Configuring TCP Sequence Number Tracking

#### 2.6.2.1 Enabling or Disabling the TCP Sequence Number Tracking Function

The TCP sequence number tracking function is disabled by default. To enable this function, run the **ip inspect** command in interface configuration mode; or you may use **no** form of this command to disable the function.

#### 2.6.2.2 Configuring TCP Sequence Number Tracking Rules

The TCP sequence number tracking function configuration basically agrees with the special protocol with the difference existing in that TCP protocol is added to **ip inspect name** rule library, e.g.,.

```
Qtech(config)# ip inspect name abc tcp
```

The preceding command indicates that TCP is added to the detection rule named "abc".

Then, it is still necessary to apply the configured ip inspect name detection rule to the interface, e.g.,.

```
Qtech(config)# interface gigabitEthernet 0/0
Qtech(config-if)# ip inspect abc in
```

The preceding command applies the detection rule named "abc" in the inbound direction of gigabit 0/0 interface.

## 2.7 Understanding Session Limit

### 2.7.1 Overview

This function is mainly designed to prevent flow flood attacks generated at certain IP address or IP network segment by limiting the speed of session establishment and total number of concurrent sessions.

### 2.7.2 Configuring a Session Limit

Before configuring the session limit function, users need to configure an ACL rule first to define the scope of the session limit function, e.g.,.

If users want to limit all sessions through ports whose sources and destination IP addresses are specified in the limit function, configure the following ACL first.

```
access-list 1 permit any
```

Then configure the rule in interface mode.

For example, now users want to configure a rule under gigabit 0/0 interface, and the rule takes effect in the inbound direction of this interface, the limit scope shall be ACL-defined scope, the speed of session establishment shall be 100 per second and concurrent sessions shall be 100,000 in total. Sessions that meet such requirements shall be allowed while others are blocked and the blocked session will be recorded in a log.

```
Qtech(config)# in gi 0/0
Qtech(config-if)# session-limit access-group 1 rate 100 concurrent 100000 in log
```

Use the **no** form of this command to delete configuration.

### 2.7.3 Viewing Session Limit Information

**show session-limit config**

```
Qtech(config-if)# show session-limit config
===== [ Show gigabitEthernet 0/0's config ] =====
Input
session-limit access-group 1 rate 12 concurrent 123 in log
session-limit access-group 12 rate 20 concurrent 100 in log
session-limit access-group 13 rate 20 concurrent 100 in log
session-limit access-group 14 rate 20 concurrent 100 in log
-----
Output
session-limit access-group 1 rate 12 concurrent 123 out log
===== [ Show gigabitEthernet 0/0's config end ] =====
```

### show session-limit del-rule

With this function, you may find the commands used to view and delete configuration.

```
Qtech(config-if)# show session-limit del-rule
===== [ Show Cmd to del the rule on the gigabitEthernet 0/0 ] =====
Input
no session-limit access-group 1 rate 12 concurrent 123
in log
no session-limit access-group 12 rate 20 concurrent 100
in log
no session-limit access-group 13 rate 20 concurrent 100
in log
no session-limit access-group 14 rate 20 concurrent 100
in log
-----
Output
no session-limit access-group 1 rate 12 concurrent 123
out log
== [ Show Cmd to del the rule on the gigabitEthernet 0/0's end ] =
```

### show session-limit statistics

```
Qtech(config-if)# show session-limit statistics
===== [ Show gigabitEthernet 0/0's Statistics ] =====
Input
matches access-group : 1
[Configure]: new_session_rate : 12 , concurren : 123
[Statistics]: conformed 2247 sessions, blocked 0 sessions
matches access-group : 12
[Configure]: new_session_rate : 20 , concurren : 100
[Statistics]: conformed 0 sessions, blocked 0 sessions
matches access-group : 13
[Configure]: new_session_rate : 20 , concurren : 100
[Statistics]: conformed 0 sessions, blocked 0 sessions
matches access-group : 14
[Configure]: new_session_rate : 20 , concurren : 100
[Statistics]: conformed 0 sessions, blocked 0 sessions
-----
Output
matches access-group : 1
[Configure]: new_session_rate : 12 , concurren : 123
[Statistics]: conformed 0 sessions, blocked 0 sessions
===== [ Show gigabitEthernet 0/0's Statistics End ] =====
```

## 2.8 Understanding Flow Management

### 2.8.1 Overview

The purpose of flow management is to prevent some users or applications from occupying excessive resources (e.g., bandwidth). Besides, flow limit is a simple and direct way to guard against ICMP flood and UDP flood attacks when other means of defense are void.

### 2.8.2 Configuring Flow Management

During flow management configuration, ACLs are used to control bandwidth quota of users, maximum number of concurrent connections, and number of new connections. Bandwidth is classified into uplink bandwidth and downlink bandwidth. If same bandwidth is specified on the uplink and downlink, the system automatically changes the keyword to **both**. The number of concurrent connections and speed of connection establishment are optional and can be left unspecified.

To configure this function, run the **ip rate-control** command in interface configuration mode.

You can use the **no** form of this command to disable this function.

It should be noticed that the command is effective only on the outbound interface.

## 2.9 Understanding Others

### 2.9.1 Enabling Session Log

At the end of a session, some information of the session, including source IP address, destination IP address, protocol, port, bytes sent and received, session duration, may need to be sent to the log server for future analysis. The session log function is disabled by default. To enable this function, run the **ip session log-on** command.

Sometimes a large number of session logs may be generated. In this case, some session logs may be lost due to limits on network transmission and processing capability of the log server.

### 2.9.2 Configuring Session Timeout

One session that remains inactive in a certain time will be considered completed. This period of time is called the timeout time of a session. Session timeout varies with session statuses. The system has different timeout settings for sessions in different statuses, which does not need to be changed in normal conditions. If you want to change timeout settings, run the **ip session timeout** command.

### 2.9.3 Configuring Abnormal Session Status Restriction

As for some abnormal session status, it is conducive to security enhancement to control the number of the packets sent from the source terminal. Generally, an appropriate threshold of different abnormal session status has been configured by the system and needs no change. When a change is needed, run the **ip session threshold** command.

### 2.9.4 Enabling Strict Status Tracking

Strict status tracking applies to TCP connection establishment and ICMP error packets. It interrupts connections in case of abnormal TCP connection (e.g., non-SYN packet) and reception of unreachable ICMP packets. Misreport may occur, therefore, strict status tracking is disabled by default. To enable this function, run the **ip session track-state-strictly** command. It is recommended that you enable this function when there is a high security requirement for better attack defense capability and disable it in internal networks or private networks to protect key services.



#### Note

When running the **ip session track-state-strictly** command to start the FW module for strict status tracking, the system will interrupt established TCP connections in order to trigger stream creation for effective tracking of the status. As a result, some established TCP services like telnet, ftp, etc will be interrupted when the command is used. Be cautious when using this command.

### 2.9.5 Enabling ICMP Reverse Flow Check

When ICMP reverse flow check is disabled, only the life time of ICMP reverse flows will be refreshed and flows are deleted and re-established by themselves in case of a ping failure. When the function is enabled, life time of both forward and reverse flows will be refreshed. This function is disabled by default. If there is a routing imbalance, packets are sent only in one direction and packets may be lost in a ping test. In this case, you can enable this function to avoid packet loss.

### 2.9.6 Configuring Connection Filtering

Invalid IP packets affect the transmission of normal packets. To prevent communication or attacks that hinge on invalid packets, you can enable connection filtering.

Before enabling this function, you need to know characteristics of invalid packets such as the source IP address, destination IP address, protocol, and port and then configure an ACL rule to define the range of forbidden packets. Finally, you can run the **ip session filter** *acl\_id* command.

This function takes effect globally. It checks and filters forward and reverse flows, and discards packets that meet the filter rule without creating flow entries on the platform.

The connection filtering function is not disabled or displayed by default.

## 3 NETWORK SECURITY PROTOCOL (IPSEC)

### 3.1 Overview of IPSec

#### 3.1.1 Purposes of Encryption

Data transmitted on a network without any protection measures is vulnerable to various kinds of attacks. When the data passes a device, any one who accesses this device can read, tamper or forge the data. For example, the protocol analyzer (such as sniffer) can be used to read packets and obtain confidential information. Inside an organization, the malicious users can tamper packets and perform destructive activities by interfering, reducing or blocking network traffic. Hence, it is extremely important to encrypt private, confidential and emergent data when it is transmitted.

Qtech Networks products support the IPSec and IKE protocols, ensuring that the data is transmitted securely in a network without any protection measures.

- The IPSec protocol is an open standard framework developed by IETF. It works in the network layer to provide encryption and authentication for the traffic between the devices that provide the IPSec protocol services. IPSec can protect all or part of the data above the IP layer. It provides the following optional security services: data confidentiality, data integrity, data origin authentication, and anti-replay. These functions prevent the data from being monitored, tampered and forged when being transmitted over the network.
- IKE is a key management protocol standard that should be used with IPSec. IKE works in the UDP layer to provide secure key exchange and management mechanism. Since IPSec can be used independently, IKE will make IPSec more flexible and easy to configure, strengthening the security.

#### 3.1.2 Supported Standards

Qtech Networks products implement the following encryption standards:

- IPSec: It specifies a set of security architectures and provides data confidentiality, integrity and data authentication services between IPSec entities. It can protect one or more data streams between hosts, between subnets, and between security gateways.
- AH: It provides the data authentication service and the anti-replay service.
- ESP: It provides the data encryption service, the optional data authentication service, and the anti-replay capability.
- DES: It is an encryption algorithm that uses a 64-bit key to encrypt the packet (there are 56 significant bits).
- 3DES: It is an encryption algorithm that uses a 192-bit key to encrypt packets (there are 168 significant bits).
- AES: It is a sub-key, 128-bit data input algorithm, key length is 128. As the next generation data encryption standard, AES boasts high security, high performance, high efficiency, easy-to-use and flexibility
- NULL: It is the null encryption algorithm that encapsulates, instead of encrypts, packets.
- MD5-HMAC: (Message Digest 5) It is a HASH algorithm used to verify packets and prevent them from being modified.
- SHA-HMAC: (secure HASH algorithm) It is a HASH algorithm used to verify packets and prevent them from being modified.
- IKE: This protocol implements the Oakley and Skeme key exchange protocols within the ISAKMP (Internet Security Association and Key Management Protocol) framework. It performs IPSec end-point authentication, IPSec parameter negotiation and key exchange.
- ISAKMP: It defines the format and parameters of the payload in data exchange, and the key negotiation mode.
- Diffie-Hellman: It is a public key encryption protocol that allows both parties involved in the exchange to establish shared secrecy on an insecure channel.

#### 3.1.3 Terms

**Anti-replay:** It is a security service that allows recipients to deny outdated packets or packet copies to avoid being attacked. It is a security association that is used for IKE negotiation and provides the authentication service.

**Note**

The manually created security association does not support the anti-replay function. Only the security associations that pass IKE negotiation support anti-replay.

**Data authentication:** It includes the following two concepts:

- Data integrity: Check whether the data has been modified.
- Data origin authentication: Check whether the data is really sent by the declared sender.

**Data confidentiality:** It protects the data from being snooped.

**Data stream:** It refers to the specific communication data that has a source address/mask, destination address/mask, the next protocol field of IP, and source and destination port IDs. The protocol and port fields can be specified using "any". All the traffic of a certain association that meets the above conditions is called a data stream. A data stream may represent a TCP connection between two hosts, or all the traffic between two subnets.

**Peer:** It refers to the device involved in IPSec or other devices.

**Security Association (SA):** It refers to a logical connection that provides the security service for a specific data stream. This security service has such parameters as specific security protocol, security algorithm, key, and data stream description. There are two types of security association: IPSec and IKE. The IPSec SA provides the IPSec protection function for data and allows users to establish a connection either manually or through IKE negotiation. The IKE SA is used to protect the negotiation data of IKE.

**Security Parameter Index (SPI):** SPI is a 32-bit integer, which is combined with a destination IP address and a security protocol type to form the unique ID of a SA. When a SA is established by using IKE, the SPI value of each SA is a pseudo-random inherited digit. If IKE is not used, specify an SPI value for each SA.

**Security association lifetime:** It refers to the validity period of a SA. The manually established security association has no lifetime, that is, it can be used permanently until a user deletes it manually. The lifetime of the SA established through IKE negotiated is negotiated with the remote IKE entity. The SA will be deleted once its lifetime expires, and IKE will negotiate about a new SA.

**Transform set:** The transform set describes the security suite that consists of a security protocol (AH or ESP) and an algorithm. For example, a transform set defines use of the ESP protocol and the DES encryption algorithm.

**Crypto map entry:** The crypto map entry associates the transform set with the data stream, and describes the peer address, and parameters necessary for communication. It fully describes the contents necessary for IPSec communication with the remote peer. An IPSec SA can be established only by using the crypto map entry.

At present, IPSec can be used to send IP packets in unicast manner only. Because the IPSec workgroup has not released the group key, now IPSec does not support IP packet multicast or broadcast.

If a device uses NAT, the static NAT should be configured, so that IPSec can work normally. NAT must be performed before IPSec encapsulation of the device, that is, IPSec should use the IP address of the public network.

## 3.2 IPSec Configuration

### 3.2.1 Overview of IPSec Working Process

IPSec provides a secure channel for two IPSec peers, such as two devices. You can define which sensitive data streams should be protected. These data streams will be transmitted along the secure channels. Moreover, you can define parameters to protect these sensitive packets by specifying parameters for these channels. When IPSec detects such a sensitive packet, it will establish a secure channel, through which this packet is sent to the remote peer.

The sensitive data streams can be defined by configuring the access list. Describe the sensitive data streams to be protected on the basis of the source/destination address, protocol and port in the access list. After configuring the access lists, use a crypto map set to apply these access lists to the interface, so that the interface protects the specific incoming and outgoing data streams.

One crypto map set can have multiple entries, each of which corresponds to a different access list. The device finds the entry that matches the current traffic by sequence (the device tries to match the packet with the access list specified by the entry). When a packet matches a permit entry in the specific access list, if the crypto map entry is labeled as ipsec-manual, IPSec is triggered directly to process the data stream securely; if the crypto map entry is



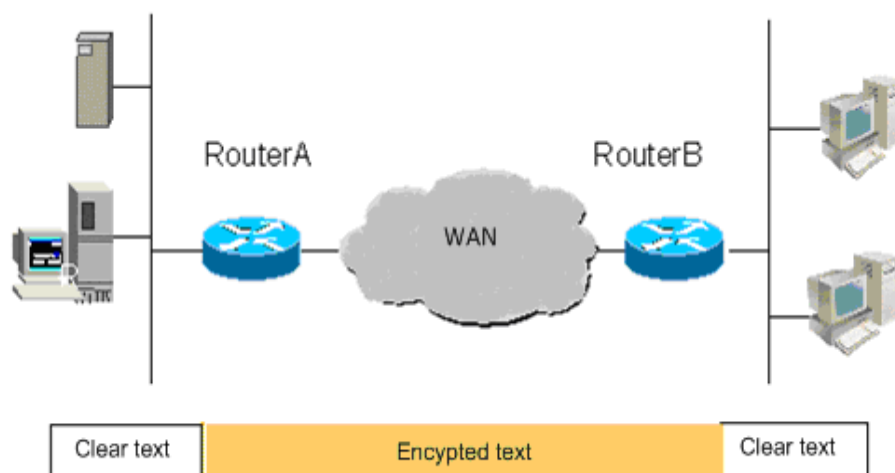
labeled as ipsec-isakmp, when an IPSec SA has been established, IPSec protection is provided to the data directly, otherwise IKE negotiation will be triggered automatically to create an IPSec SA. If the user does not configure IPSec or IKE parameters properly, it will be impossible to establish a SA, and the packets will be discarded.

Once a SA is established, the outgoing packet will be encrypted by IPSec and authentication information is filled in before it is sent to the peer. This packet is an incoming packet of the peer, which finds the related SA, and decrypts, authenticates and restores the packet.

The crypto map entry also specifies a transform set that defines the combination of the algorithm and protocol mode used by IPSec. Two IPSec peers must finally use the same transform set in order to communicate effectively.

The following figure shows an example of implementing IPSec protection between subnets:

Figure 7 Implementation of IPSec protection between subnets



### 3.2.2 IPSec Configuration Tasks

The ultimate purpose of IPSec configuration task is to establish an IPSec SA. An IPSec SA can be established manually or through negotiation by IKE. Manual configuration does not need IKE, but requires more parameters to be specified and has lower level of security. To establish a SA through IKE negotiation, you need to configure the IKE parameters besides configuring the IPSec parameters, so it has a higher level of security.

IPSec configuration tasks include:

- **Configure the default lifetime (optional):** This is an optional step. You can use this command to modify the default lifetime value of the system. If there is no special description, IKE will use this lifetime value for negotiation, so that the lifetime of IPSec is not longer than the default lifetime.
- **Create an encryption access list:** An encryption access list determines the data streams to be protected. IPSec needs to rely on the encryption access list to filter incoming/outgoing packets. It provides IPSec protection for the matched outgoing data, and checks the validity of the matched incoming packets.
- **Define a transform set:** A transform set describes how to protect data streams. The transform set is a combination of the specific security protocol and algorithm. It specifies an algorithm, a security protocol, and a data encapsulation mode. To specify the degree of and requirements for protection of the data, the user must define an appropriate transform set here in advance.
- **Create a crypto map entry:** To create a crypto map entry, associate the predefined access list with the transform set, and define the key and the peer address to form a complete IPSec scheme description.
- **Configure a multicast policy:** Disable IPSec encapsulation of multicast and broadcast packets.
- **Apply a crypto map entry to an interface:** This action activates IPSec scheme defining. It applies a crypto map entry to an interface to make the crypto map set start working on the interface.
- **Create a Profile crypto map entry:** Define IPSec encryption policies of dynamic multipoint VPN (DMVPN).
- **Apply a Profile crypto map entry to a tunnel interface:** Activate the IPSec functions of DMVPN.
- **Configure extended authentication mode:** This action is used for extended authentication.
- **Configure IPSec packet filter:** Decapsulated packets are no longer filtered.
- **Configure IPSec MIB:** It sends IPSec monitoring information to the SNMP server. This function is disabled by default and needs to be enabled using a command.



- **Monitor and maintain IPSec:** Monitor and maintain IPSec, view and adjust the IPSec parameters, and judge whether IPSec works normally.



**Note** IKE uses UDP port 500. The IPSec ESP and AH protocols are numbered 50 and 51 respectively. If access list (firewall) filtering data has been configured on the device, then before configuring IPSec, please make sure the traffic for protocols 50 and 51 and UDP port 500 on the interface used by IPSec is not blocked. If possible, add a statement to the access list to explicitly allow the traffic.

### 3.2.2.1 Configuring Default Lifetime

To configure the default lifetime, run the following command in global configuration mode or privileged user configuration mode:

Command	Function
Qtech(config)# <b>crypto ipsec security-association lifetime seconds</b> <i>seconds</i>	Changes the global lifetime limit of IPSec SA. This command will cause the SA timeout after the specified seconds elapse.
Qtech(config)# <b>crypto ipsec security-association lifetime kilobytes</b> <i>kilobytes</i>	Changes the global traffic lifetime of IPSec SA. This command will cause the SA timeout after the transmitted traffic (in KBs) protected by IPSec using this SA reaches a specified value.
Qtech# <b>clear crypto sa</b> or Qtech# <b>clear crypto sa peer</b> <i>{ip-address   peer-name}</i> or Qtech# <b>clear crypto sa map</b> <i>map-name</i>	Clears an existing SA. This will immediately interrupt all the existing SAs. The subsequent SAs will use a new lifetime. Otherwise, all the existing SAs will expire on the basis of the original lifetime.



**Note** Use the **clear crypto sa** command without parameters to clear the entire SA database. This will also clear the active encryption processes. You can use such keywords as peer and map to clear only one subnet from the SA database. For detailed information, refer to the command reference for **clear crypto sa**.

The default lifetime of the system is 1-hour communication (3600 seconds) or 4,608,000KB traffic (continuous communication for 1 hour at the rate of 10 MBit/s). If the user accepts the default value, skip this step. This default lifetime is used if there is no special description in the crypto map entry. When negotiating the lifetime of IPSec, IKE uses the smaller value of those of the local end and the peer. When the lifetime of the IPSec SA expires, IKE will negotiate again and replace a new set of parameters and key for IPSec to make it start working again.

The SA (and the related key) is timeout on the basis of the lifetime that expires earliest: Use the seconds (specified by the keyword seconds) or the kilobytes of transmitted traffic (specified by the keyword kilobytes). The manually established SA (established by the crypto map entry identified as ipsec-manual) has no lifetime limit.

In order to make sure that a new SA is available when the original SA expires, the new SA must be negotiated before the original SA expires. When there are 30 seconds left before the lifetime expires, or when there are 256 Kbytes left before the traffic that passes this channel reaches the lifetime (determined by the peer that reaches the lifetime first), a new SA is negotiated.

If no traffic takes this channel throughout the lifetime of a SA, this SA will be released but negotiation of a new SA will not be underway when the lifetime elapses. In this case, a new SA will be negotiated only when IPSec finds another packet that should be protected.

### 3.2.2.2 Configuring Automatic Disconnection for Idle Tunnels

To configure automatic disconnection for global idle tunnels, run the following command in global configuration mode or privileged EXEC mode:

Command	Function
Qtech(config)# <b>crypto ipsec security-association idle-time</b> sec	Specifies the disconnection period for global idle tunnels in seconds. The value range is 60–86400.

### 3.2.2.3 DF bit Override Function of IPSec Tunnel

The DF bit override function allows users to specify whether the device is reset, is set to 1, or copies the encapsulated header.

The DF bit on the IP header determines whether the device can fragment the packet. Value 1 indicates that this packet cannot be fragmented, and value 0 indicates that the packet can be fragmented. This function in IPSec tunnel mode allows the device to control whether the DF bit of the packet IP header encapsulated by IPSec is determined by the DF bit value of the original IP header. Only tunnel mode supports this feature.

To configure the DF bit value for all the interfaces, run the following command in global configuration mode:

Command	Function
Qtech(config)# <b>crypto ipsec df-bit</b> [clear   set   copy]	Sets the DF bit of the IP external header for all the interfaces in tunnel mode.

In the following example, the device is configured to clear the DF bit globally, and copy the DF bit on FastEthernet0/0. This way, all the interfaces other than FastEthernet0/0 allow packets larger than the MTU size to be sent (in fragments), while FastEthernet0/0 must determine whether to allow the device to fragment the packet according to the DF bit in the original IP header.

```
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key 0 DELaware address 192.168.10.66
crypto isakmp key 0 Key-What-Key address 192.168.11.19
!
!
crypto ipsec transform-set BearMama ah-md5-hmac esp-des
crypto ipsec df-bit clear
!
!
crypto map armadillo 1 ipsec-isakmp
set peer 192.168.10.66
set transform-set BearMama
match address 101
!
crypto map basilisk 1 ipsec-isakmp
set peer 192.168.11.19
set transform-set BearMama
match address 102
!
!
interface FastEthernet0/0
ip address 192.168.10.38 255.255.255.0
ip broadcast-address 0.0.0.0
crypto map armadillo
crypto ipsec df-bit copy
!
interface FastEthernet0/1
ip address 192.168.11.75 255.255.255.0
ip broadcast-address 0.0.0.0
crypto map basilisk
!
```

### 3.2.2.4 Creating Encryption Access Lists

The encryption access list is used to define which data streams should be encrypted, and which should not be encrypted. For example, you can create an encryption access list to protect all the IP traffic between Subnet A (192.168.202.0/24) and Subnet B (192.168.12.0/24) (access list 120), or the IP traffic between Host A and Host B (access list 101):

```
access-list 120 permit ip 192.168.12.0 0.0.0.255 192.168.202.0 0.0.0.255
access-list 101 permit ip host 2.2.2.2 host 2.2.2.1
```

The encryption access list specified by the IPSec crypto map entry has the following four major functions:

- Filter the outbound traffic that is encrypted by using IPSec (permit = protect).
- When starting to negotiate an IPSec SA, indicate which data streams are protected by the new SA (indicated by a single permit entry).
- Process the inbound traffic, so as to filter and discard those traffic that should have been protected by IPSec.
- When handling the IKE negotiation initiated by the IPSec peer, determine whether to accept the IPSec SA request that represents the requested data stream (only the crypto map entry ipsec-isakmp should be negotiated). You must make sure that the access lists of peers at both ends match. It is recommended that the access lists of peers at both ends are consistent.

To configure the encryption access list, run the following command in global configuration mode:

Command	Function
Qtech(config)# <b>access-list</b> <i>access-list-number {deny   permit}</i> <i>protocol source source-wildcard</i> <i>destination destination-wildcard</i> <b>[log]</b>	Describes the data stream in terms of its source/destination address and its wildcard, communication protocol and communication port. If the keyword <b>permit</b> is used, the policy described in the related crypto map entry will provide encryption protection for all the IP traffics that meet the specified conditions. The keyword <b>deny</b> can be used to prevent the traffic from being encrypted by the specific crypto map entry.
Or: Qtech(config)# <b>ipv6 access-list</b> ipv6-acl-name Qtech(config-ipv6-acl)# <b>{deny   permit}</b> <i>protocol source</i> <i>source-wildcard destination destination-wildcard</i>	
Qtech(config-exp-nacl)# <b>exit</b>	Exits ACL configuration mode.

If the keyword **permit** is used, the policy described in the related crypto map entry will provide encryption protection for all the IP traffic that meets the specified conditions. The keyword **deny** can be used to prevent the traffic from being encrypted by the specific crypto map entry.



#### Note

It is recommended that you define a mirrored encryption access list on the remote peer for each encryption access list defined on the local peer. Otherwise, some data is not protected or the SA cannot be established. Since the ACL has priority, the inclusion relation of ACEs should be noted during the configuration. In case of conflict, the ACE having a higher priority takes effect.

The keyword **any** should be used with great care because it will discard lots of broadcast information and make the device unable to work normally. The encryption access list is not specially designed for and used by IPSec. IPSec uses the extended IP access list, so the value of **access-list-number** ranges from 100 to 199]. If no port is defined, this encryption access list can be used for the data stream in either the inbound direction or the outbound direction.

For example, when you want to protect the IP traffic between Subnet A (192.168.12.0/24) and Subnet B (192.168.10.0/24), the following access list should be defined for the device:

```
access-list 101 permit ip 192.168.12.0 0.0.0.255 192.168.10.0 0.0.0.255
```

For example, if you want to protect the TCP traffic between Subnet A (192.168.12.0/24) and Host C (202.101.11.3), the following access list should be defined for the device:

```
access-list 120 permit tcp 192.168.12.0 0.0.0.255 202.101.11.3 0.0.0.0
```

If port filtering is defined, the destination address in the encryption access list provides the service for this port.

For example, if you need to protect the Telnet traffic between Host D (1.1.1.1) and Host E (2.2.2.2) that provides the Telnet service, define as follows on the device:

```
access-list 133 permit tcp 1.1.1.1 0.0.0.0 2.2.2.2 0.0.0.0 eq telnet
```



### Caution

In terms of permit ipv6 any any encryption access list, Qtech devices are not compatible with Cisco devices. Because Cisco devices will encrypt “neighbor request packet” and “neighbor advertisement packet” (Similar to ARP packets of IPv4), the IPSec data communication between two non-direct devices failed. To avoid the preceding issue, Qtech devices will not encrypt “neighbor request packet” and “neighbor advertisement packet”.

### 3.2.2.5 Defining Transform Set

Transform set is a combination of the specific security protocol and algorithm. During negotiation of the IPSec SA, the peer must use the same specific transform set to protect the specific data stream.

Because there is no anti-replay negotiation process between peers for the manually established SA, the same transform set must be specified for the two peers. Change to the definition of the transform set will apply to negotiation of the subsequently established SA, instead of the existing SA. If you want these new settings to take effect immediately, use the **clear crypto sa** command to clear all or part of the SA database.

To define a transform set, run the following command in global configuration mode:

Command	Function
Qtech(config)# <b>crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]</b>	The transform parameter is an algorithm supported by the system. Algorithms can be combined according to a certain rule.
Qtech(cfg-crypto-trans)# <b>mode {tunnel   transport}</b> (Optional)	Changes the mode associated with the transform set. Mode setting is useful only for the communication where both the source and the destination addresses and those of the IPSec peer, while not useful for other communications (all other communications are performed in the tunnel mode).
<b>exit</b>	Exits crypto transform configuration mode.
Qtech# <b>clear crypto sa</b> or Qtech# <b>clear crypto sa peer</b> {ip-address   peer-name} or Qtech# <b>clear crypto sa map</b> map-name	Clears the existing SAs, so as to make sure that any change to the transform set applies to the subsequently established SAs (the manually established SAs will be reestablished immediately)

Present below are all the transform sets supported by the system:

transform1 [transform2 ]	Description
ah-md5-hmac	AH protocol and MD5 HMAC algorithm
ah-sha-hmac	AH protocol and SHA HMAC algorithm
ah-sm3-hmac	AH protocol and SM3 HMAC algorithm
esp-des	ESP protocol and DES encryption algorithm
esp-3des	ESP protocol and 3DES encryption algorithm
esp-aes-128	ESP protocol and aes encryption algorithm with key length being 128.
esp-aes-192	ESP protocol and aes encryption algorithm with key length being 192.

transform1 [transform2 ]	Description
esp-aes-256	ESP protocol and aes encryption algorithm with key length being 256.
esp-sm4	ESP protocol and SM4 encryption algorithm with key length being 128.
ah-md5-hmac esp-des	The AH protocol is located outside, and the MD5 HMAC authentication algorithm is used. The ESP protocol is located inside, and the DES encryption algorithm is used
ah-sha-hmac esp-des	The AH protocol is located outside, and the SHA HMAC authentication algorithm is used. The ESP protocol is located inside, and the DES encryption algorithm is used
ah-md5-hmac esp-des esp-md5-hmac	The AH protocol is located outside, and the MD5 HMAC authentication algorithm is used. The ESP protocol is located inside, and the DES encryption algorithm and the MD5 HMAC authentication algorithm are used
ah-md5-hmac esp-null esp-md5-hmac	The AH protocol is located outside, and the MD5 HMAC authentication algorithm is used. The ESP protocol is located inside, and the null encryption algorithm and the MD5 HMAC authentication algorithm are used
ah-md5-hmac esp-des esp-sha-hmac	The AH protocol is located outside, and the MD5 HMAC authentication algorithm is used. The ESP protocol is located inside, and the DES encryption algorithm and the SHA HMAC authentication algorithm are used
ah-md5-hmac esp-null esp-sha-hmac	The AH protocol is located outside, and the MD5 HMAC authentication algorithm is used. The ESP protocol is located inside, and the null encryption algorithm and the SHA HMAC authentication algorithm are used
ah-sha-hmac esp-des esp-md5-hmac	The AH protocol is located outside, and the SHA HMAC authentication algorithm is used. The ESP protocol is located inside, and the DES encryption algorithm and the MD5 HMAC authentication algorithm are used
ah-sha-hmac esp-null esp-md5-hmac	The AH protocol is located outside, and the SHA HMAC authentication algorithm is used. The ESP protocol is located inside, and the null encryption algorithm and the MD5 HMAC authentication algorithm are used
ah-sha-hmac esp-des esp-sha-hmac	The AH protocol is located outside, and the SHA HMAC authentication algorithm is used. The ESP protocol is located inside, and the DES encryption algorithm and the SHA HMAC authentication algorithm are used
ah-sha-hmac esp-null sp-sha-hmac	The AH protocol is located outside, and the SHA HMAC authentication algorithm is used. The ESP protocol is located inside, and the null encryption algorithm and the SHA HMAC authentication algorithm are used
esp-des esp-md5-hmac	For the ESP protocol, the DES encryption algorithm and the MD5 HMAC authentication algorithm are used.
esp-null esp-md5-hmac	For the ESP protocol, the null encryption algorithm and the MD5 HMAC authentication algorithm are used.
esp-des esp-sha-hmac	For the ESP protocol, the DES encryption algorithm and the SHA HMAC authentication algorithm are used.
esp-null esp-sha-hmac	For the ESP protocol, the null encryption algorithm and the SHA HMAC authentication algorithm are used.
esp-3des	ESP protocol and 3DES encryption algorithm
esp-3des esp-sha	For the ESP protocol, the 3DES encryption algorithm and the SHA HMAC authentication algorithm are used.
esp-3des esp-md5	For the ESP protocol, the 3DES encryption algorithm and the MD5 HMAC authentication algorithm are used.
ah-md5-hmac esp-des	The AH protocol is located outside, and the MD5 HMAC authentication algorithm is used. The ESP protocol is located inside, and the 3DES encryption algorithm is used



transform1 [transform2 ]	Description
ah-sha-hmac esp-des	The AH protocol is located outside, and the SHA HMAC authentication algorithm is used. The ESP protocol is located inside, and the 3DES encryption algorithm is used
ah-md5-hmac esp-3des esp-sha	The AH protocol is located outside, and the MD5 HMAC authentication algorithm is used. The ESP protocol is located inside, and the 3DES encryption algorithm and the SHA HMAC authentication algorithm are used
ah-sha-hmac esp-3des esp-sha	The AH protocol is located outside, and the SHA HMAC authentication algorithm is used. The ESP protocol is located inside, and the 3DES encryption algorithm and the SHA HMAC authentication algorithm are used
ah-md5-hmac esp-3des esp-md5	The AH protocol is located outside, and the MD5 HMAC authentication algorithm is used. The ESP protocol is located inside, and the 3DES encryption algorithm and the MD5 HMAC authentication algorithm are used
ah-sha-hmac esp-3des esp-md5	The AH protocol is located outside, and the SHA HMAC authentication algorithm is used. The ESP protocol is located inside, and the 3DES encryption algorithm and the MD5 HMAC authentication algorithm are used

**Note**

Generally, the combination esp-des (without data authentication) will satisfy your requirement. If you want to verify data, you can choose esp-des esp-md5-hmac or esp-des esp-sha-hmac.

### 3.2.2.6 Configuring IPSec MIB

IPSec MIB management involves statistics of data streams and encrypted/decrypted data packets and it may affect performance of IPSec data communication in some certain. Therefore, the MIB statistical function is disabled by default. To access the MIB node of IPSec, you need to enable the IPSec MIB function using the CLI command.

Command	Function
Qtech(config)# <b>crypto mib enable</b>	Configures IPSec MIB statistics function.

### 3.2.2.7 Configuring Multicast Policies

If an ACL covers multicast and broadcast addresses, IPSec encapsulation will be applied to packets related to these addresses. To skip IPSec encapsulation, run the following command:

Command	Function
Qtech(config)# <b>crypto ipsec multicast disable</b>	Disables encapsulation of multicast and broadcast packets.

### 3.2.2.8 Creating Crypto Map Entry

The crypto map entry can be configured in the following aspects:

- Which traffic should be protected by IPSec: Associate the configured encryption ACL.
- Where the traffic protected by IPSec will be sent to: Which is the remote IPSec peer.
- Local address used for IPSec communication: Apply the crypto map set to the interface. IPSec uses the address of the communication interface as the address of the local peer.
- Which IPSec security policies should be applied to traffic: Choose from the list that consists of one or more transform sets.
- Lifetime of the SA.
- Whether the SA is established manually or through IKE negotiation.

The crypto map entries that have the same crypto map name (but with different map sequence numbers) constitute a crypto map set. Apply the crypto map set to the interface, so that all the IP traffic that passes this interface is judged according to the crypto map set applied to the interface. If a crypto map entry finds an outbound IP channel that should be protected, and the crypto map specifies use of IKE, the SA will be negotiated with the remote peer according to the parameters in this crypto map entry. If the crypto map entry specifies use of the manually established SA, then a SA must have been established during configuration. The data is encrypted for transmission once the SA is established successfully either manually or through IKE negotiation. If negotiation of SA fails, the data is discarded.

The policy described in the crypto map entry will be used during negotiation of SA. To carry out IPSec smoothly between two IPSec peers, the crypto map entries of the two peers must include mutually compatible configuration statements. When two peers try to establish a SA, both of them must have at least one crypto map entry that is compatible with the crypto map entry of the remote peer and at least meets the following conditions:

- The crypto map entry must include a compatible encryption access list (such as mirrored map access list).
- The crypto map entries at both sides must identify the address of the peer (unless the peer is using a dynamic crypto map).
- The crypto map entries must have at least one identical transform set.

Only one crypto map set is applied to a single interface. The crypto map set contains IPSec/IKE or combination of IPSec/manual entry. If you create multiple crypto map entries for a given interface, you have to use the *seq-num* parameter of the map entry to sort these map entries again. The smaller the value of *seq-num*, the higher the priority.

Multiple crypto map entries must be created for a single interface if one of the following situations exists.

- If different data streams on this interface will be processed by different IPSec peers.
- If you want to apply different IPSec securities to different types of traffic (destined for the same or different peers). For example, you want that the traffic among the subnets in a group is authenticated, while the traffic among other subnets is both authenticated and encrypted. In this case, different types of traffic should be defined in two different access lists, and a separate crypto map entry must be created for each encryption access list.

### Creating a SA manually

To create a SA manually, run the following commands in global configuration mode at the beginning:

Command	Function
Qtech(config)# <b>crypto map</b> <i>map-name</i> <i>seq-num ipsec-manual</i>	Specifies the crypto map entry to be created or modified. When using this command, you will enter crypto map configuration mode.
Qtech(config-crypto-map)# <b>match address</b> <i>access-list-id</i> or Qtech(config-crypto-map)# <b>match ipv6</b> <i>ipv6-acl-name</i>	Specifies an access list for the crypto map list. This access list determines which traffic should be protected by IPSec, and which traffic should not be protected by the IPSec security defined in this crypto map entry.
Qtech(config-crypto-map)# <b>match vrf</b> <i>vrf-name</i>	Specifies the crypto map list a VRF that are associated with the access list. Only when the packets under the VRF matching the access list can they be protected by IPSec.
Qtech(config-crypto-map)# <b>set peer</b> { <i>hostname</i>   <i>ip-address</i> }	Specifies a remote IPSec peer. The traffic protected by IPSec will be sent to this peer. If IKE is not used, only one peer can be configured.
Qtech(config-crypto-map)# <b>set transform-set</b> <i>transform-set-name</i>	Specifies which transform set to use. This transform set must be the same as the one specified in the corresponding crypto map entry of the remote peer. (If IKE is not used, only one transform set can be specified.)
Qtech(config-crypto-map)# <b>set vrf</b> <i>vrf-name</i>	Specifies the VRF that are associated with tunnel.



<pre>Qtech(config-crypto-map)# set session-key inbound ah spi hex-key-data or Qtech(config-crypto-map)# set session-key outbound ah spi hex-key-data</pre>	<p>If the specified transform set includes the AH protocol, you should use this command to set the AH Security Parameter Indexes (SPIs) and passwords for the protected outbound and inbound traffic. Here, the local inbound SPI, protocol and key must be the same as the outbound SPI, protocol and key of the remote peer, and vice versa.</p>
<pre>Qtech(config-crypto-map)# set session-key inbound esp spi cipher hex-key-data [authenticator hex-key-data] or Qtech(config-crypto-map)# set session-key outbound esp spi cipher hex-key-data [authenticator hex-key-data]</pre>	<p>If the specified transform set includes the ESP protocol, you should use this command to set the ESP security parameter indexes and passwords for the protected outbound and inbound traffics. If the transform set includes the ESP encryption algorithm, the encryption key must be provided. If the transform set includes the ESP authentication algorithm, the authentication key must be provided. Here, the local inbound SPI, protocol and key must be the same as the outbound SPI, protocol and key of the remote peer, and vice versa.</p>
<pre>Qtech(config-crypto-map)# set mtu length</pre>	<p>Sets the side of a fragment in tunnel mode.</p>
<pre>Qtech(config-crypto-map)# exit</pre>	<p>Exits the crypto map configuration mode and return to the global configuration mode.</p>

Repeat the preceding steps to create other necessary crypto map entries.

The following shows a configuration example:

#### Local peer (router A) configuration:

# Define a transform set named myset

```
crypto ipsec transform-set myset esp-des
```

# Define a manual map set named mymap

```
crypto map mymap 3 ipsec-manual
set peer 2.2.2.2
set session-key inbound esp 301 cipher abcdef1234567890
set session-key outbound esp 300 cipher abcdef1234567890
set transform-set myset
match address 101
!
access-list 101 permit ip 192.168.12.0 0.0.0.255 192.168.202.0 0.0.0.255
```

#### Remote peer (router B) configuration:

# Define a transform set named myset

```
crypto ipsec transform-set myset esp-des
```

# Define a manual map set named mymap

```
crypto map mymap 3 ipsec-manual
set peer 2.2.2.1
set session-key inbound esp 300 cipher abcdef1234567890
set session-key outbound esp 301 cipher abcdef1234567890
set transform-set myset
match address 101
!
access-list 101 permit ip 192.168.202.0 0.0.0.255 192.168.12.0 0.0.0.255
```



#### Caution

The keyword **hex-key-data** is a hexadecimal number. The length of **hex-key-data** following the keyword cipher in the configuration command in the sixth step and the length of **hex-key-data** in the configuration command in the fifth step are determined by the encryption algorithm in use (at present, IPSec supports the DES, 3DES and AES encryption algorithms). The length of **hex-key-data** following

the keyword authenticator in the configuration command in the sixth step is determined by the data authentication algorithms (including the SHA and MD5 algorithms) in use. In the above example, the encryption algorithm DES is used, and the length of 64 bits is required, so its value is set to abcdef1234567890 (equivalent to 0xabcdef1234567890). Because no data authentication algorithm is used in the above example, the key following authenticator is not configured. You can configure it simply by entering a string that contains digits from 1 to 9 and/or letters from a to f. It is unnecessary to identify it by 0x.

Table:

Name of Algorithm	Length of Key (bits)	Length of Entered Hexadecimal String (bytes)	Configuration Example
Des	64	8	Example: set session-key inbound esp 300 cipher abcdef1234567890
3Des	192	24	set session-key inbound esp 300 cipher abcdef1234567890 abcdef1234567890 abcdef1234567890
aes	128	16	set session-key inbound esp 300 cipher abcdef1234567890abcdef1234567890
Sm4	128	16	set session-key inbound esp 300 cipher abcdef1234567890abcdef1234567890
Md5	128	16	Example: set session-key inbound esp 302 cipher abcdef1234567890 authenticator abcdef1234567890abcdef1234567890
Sha	160	20	Example: set session-key inbound esp 302 cipher abcdef1234567890 authenticator abcdef1234567890abcdef1234567890abcd
Sm3	256	32	Example: set session-key inbound esp 302 cipher abcdef1234567890 authenticator abcdef1234567890abcdef1234567890abcdef1234567890abcdef1234567890



**Caution**

Generally, a full length of key should be configured. If the key is not complete, the device may append "0" (low security), or may not append "0" (this will cause negotiation of SA failed).

Use of the manual SA is the result prearranged by the local device and IPSec peer administrators. They may want to first use the manual SA for debugging, and then use the IKE-based SA or the remote peer does not support IKE.

**Configuring Anti-Replay Window**

The anti-replay window is the basic attack protection feature of IPSec. By default, when hash (MD5, SHA, etc) authentication mode is configured, the anti-reply feature will be enabled, yet you can still disable this feature through the following command:

Command	Function
Qtech(config)#crypto ipsec security-association replay disable	Disables the anti-replay window.



**Caution**

Since QoS will divert traffic into different queues, thus leading to the disorder of packet transmission, and if IPSec enables anti-replay window in such a context, IPSec will drop all packets exceeding the window. Therefore, you can disable the anti-replay window to avoid packet loss, but it will also increase the possibility of being attacked.

## Configuring Data Security Check

Data security check is the basic attack protection feature of IPSec. The criteria for attack judging is: if the packet which ought to be in encrypted text is received in plain text, such packet is considered unsafe and will be dropped. Under certain circumstances, data security check is not mandatory and can be disabled through the following command.

Command	Function
Qtech(config)# <b>crypto ipsec optional</b>	Disables IPSEC data security check.



### Caution

Data security check will result in significant resource overhead, and disabling this feature can save CPU resources. In the model of I2tp over ipsec, I2tp can force to enable IPSec, and thus only IPSec-encrypted packets are allowed. This feature can be used according to actual needs.

## Configuring to use IKE to create a crypto map entry for the SA

To configure to use IKE to create a crypto map entry for the SA, run the following commands in global configuration mode in the beginning:

Command	Function
Qtech(config)# <b>crypto map</b> <i>map-name seq-num ipsec-isakmp</i>	Specifies the crypto map entry to be created or modified. When using this command, you will enter crypto map configuration mode.
Qtech(config-crypto-map)# <b>match address</b> <i>access-list-id</i> or Qtech(config-crypto-map)# <b>match ipv6</b> <i>ipv6-acl-name</i>	Specifies an access list for the crypto map list. This access list determines which traffic should be protected by IPSec, and which traffic should not be protected by the IPSec security defined in this crypto map entry.
Qtech(config-crypto-map)# <b>match vrf</b> <i>vrf-name</i>	Specifies the crypto map list a VRF that are associated with the access list. Only when the packets under the VRF matching the access list can they be protected by IPSec.
Qtech(config-crypto-map)# <b>set peer</b> { <i>hostname</i>   <i>ip-address</i> }	Specifies a remote IPSec peer. The traffic protected by IPSec will be sent to this peer. You can configure multiple peers.
Qtech(config-crypto-map)# <b>set local</b> <i>ip-address</i>	Sets the IP address for local negotiation. If no IP address is specified, the primary address of the interface is used.
Qtech(config-crypto-map)# <b>set transform-set</b> <i>transform-set-name1</i> [ <i>transform-set-name2...transform-set-name6</i> ]	Specifies which transform set to use. List the transform set by priority (high priority first).
Qtech(config-crypto-map)# <b>set security-association lifetime seconds</b> <i>seconds</i> or Qtech(config-crypto-map)# <b>set security-association lifetime kilobytes</b> <i>kilobytes</i>	(Optional) Specifies a SA lifetime for the crypto map entry.
Qtech(config-crypto-map)# <b>set security-association idle-time</b> <i>seconds</i>	(Optional) Specify the idle time timeout for the crypto map entry.
Qtech(config-crypto-map)# <b>set exchange-mode</b> <i>main</i>   <i>aggressive</i>	Sets which mode is used to initiate negotiation using this static entry.
Qtech(config-crypto-map)# <b>set pfs</b> <i>group1</i>   <i>group2</i>	Specifies the Diffie-Hellman group identification.
Qtech(config-crypto-map)# <b>set mtu</b> <i>length</i>	Sets the fragment size in tunnel mode.

Command	Function
Qtech(config-crypto-map)# <b>set vrf vrf-name</b>	Specifies the VRF that are associated with tunnel.
Qtech(config-crypto-map)# <b>username name password {0 7} pass</b>	Configures the username and password used for extended authentication.
Qtech(config-crypto-map)# <b>reverse-route [remote-peer ip-address] [distance] [tag tagvalue] [track trackvalue] [bfd] [weight weightvalue]</b>	Configures Ipv4 reverse routing
Qtech(config-crypto-map)# <b>reverse-ipv6-route [remote-peer ip-address] [distance] [bfd] [weight weightvalue]</b>	Configures Ipv6 reverse routing
Qtech(config-crypto-map)# <b>exit</b>	Exits crypto map configuration mode and returns to global configuration mode.

Repeat the preceding steps to create other necessary crypto map entries.

The following example shows how to configure to establish a SA using IKE:

#### Local peer (router A) configuration:

# Define a transform set named myset

```
crypto ipsec transform-set myset esp-des
```

# Define a map set named mymap that establishes a SA using IKE

```
crypto map mymap 3 ipsec-isakmp
 set peer 2.2.2.2
 set transform-set myset
 match address 101
!
access-list 101 permit ip 192.168.12.0 0.0.0.255 192.168.202.0 0.0.0.255
```

#### Remote peer (router B) configuration:

# Define a transform set named myset

```
crypto ipsec transform-set myset esp-des
```

# Define a map set named mymap that establishes a SA using IKE

```
crypto map mymap 3 ipsec-isakmp
 set peer 2.2.2.1
 set transform-set myset
 match address 101
!
access-list 101 permit ip 192.168.202.0 0.0.0.255 192.168.12.0 0.0.0.255
```



#### Note

RGOS supports both the manual SA and the IKE-established SA. The two modes of establishing SAs can also be added to the same crypto map set.



#### Caution

Use IKE to establish a SA because IKE will negotiate again and use a new key when the lifetime expires, ensuring data security. However, because the content encrypted by using the DES encryption algorithm may be cracked maliciously within a certain time, the key must be modified regularly if the SA is established manually.

### Creating a dynamic crypto map

The dynamic crypto map (IKE is needed) requires less configuration. If the IP address of the remote peer is unknown during configuration, the dynamic crypto map function must be used. For example, a mobile subscriber is dynamically assigned an IP address. First, the mobile subscriber uses something other than the IP address, such as

the domain name, for the local IKE authentication. Once the authentication is complete, the SA request that meets the dynamic crypto map can be processed, and this dynamic crypto map can accept requests that meet the local policy.

### Understanding dynamic crypto map

Only IKE can use the dynamic crypto map. The dynamic crypto map entry acts as a policy template. The missing parameters can be obtained dynamically (IPSec negotiation) to meet requirement of the remote peer. It allows the remote peer and the device to exchange IPSec traffic even if the crypto map of the device does not fully satisfy the requirement of the remote peer.

The dynamic crypto map is used for the remote peer to initiate IPSec negotiation, not for the device to initiate new IPSec negotiation with the remote peer.

The dynamic crypto map set is referred to as a part of the crypto map. Any crypto map entry that refers to the dynamic map is the crypto map entry with the lowest priority in the crypto map set (namely it has the largest sequence number). This way, other crypto map entries will be evaluated first. The dynamic crypto map entry is checked when all the static crypto map entries do not match.

If the device accepts the request from the peer, it will create a new IPSec SA, and install a temporary crypto map entry, which is filled in with the negotiation result. At this point, the device uses a temporary crypto map entry as if it uses a normal crypto map entry. Once the SA expires, the temporary crypto map entry will be deleted.

For the static and dynamic crypto maps, if the incoming traffic not protected meets one permit statement in the access list, the traffic will be discarded because it is not protected by IPSec.

For the static crypto map entry, if the outgoing traffic meets the permit statement in the access list, and the corresponding SA has not been established, the device will initiate SA negotiation with the remote peer. For the dynamic crypto map entry, if a SA does not exist, the traffic is discarded directly (because the dynamic crypto map is not used to initiate a new SA negotiation).



**Caution** The **any** keyword should be used carefully in the **permit** entry in the dynamic crypto map. Because **permit** may cover multicast and broadcast, **deny** must be used to exclude the broadcast and multicast traffic, and other traffic that is not protected by IPSec must also be excluded.

The dynamic crypto map entries are grouped into a set like the normal crypto map entries. A set contains crypto map entries that are grouped together using the same crypto map name but have different sequence numbers.

To create a dynamic crypto map entry, use the following commands in global configuration mode:

Command	Function
Qtech(config)# <b>crypto dynamic-map</b> <i>dynamic-map-name dynamic-seq-num</i>	Creates a crypto map entry
Qtech(config-crypto-map)# <b>set transform-set</b> <i>transform-set-name1 [transform-set-name2...transform-set-name6]</i>	Specifies which transform set to use. List the transform set by priority (high priority first).
Qtech(config-crypto-map)# <b>match address</b> <i>access-list-id</i> or Qtech(config-crypto-map)# <b>match ipv6</b> <i>ipv6-acl-name</i>	(Optional) Specifies an access list for the crypto map list. This access list determines which traffic should be protected by IPSec, and which traffic should not be protected by the IPSec security defined in this crypto map entry. Note: Although the access list is optional to the dynamic crypto map, it is strongly recommended to configure it. If it is configured, the data stream ID suggested by the peer must match a permit entry in the crypto map access list. If it is not configured, the device accepts any data stream ID suggested by the peer.



Qtech(config-crypto-map)# <b>match vrf</b> <i>vrf-name</i>	Specifies the crypto map list a VRF that are associated with the access list. Only when the packets under the VRF matching the access list can they be protected by IPSec.
Qtech(config-crypto-map)# <b>set peer</b> { <i>hostname</i>   <i>ip-address</i> }	(Optional) Specifies a remote IPSec peer. You can configure multiple peers. This configuration is rare in the dynamic crypto map entry. The dynamic crypto map is often used when information about the peer is unknown.
Qtech(config-crypto-map)# <b>set local</b> <i>ip-address</i>	Sets the IP address of the local peer. If no IP address is specified, the primary address of the interface is used.
Qtech(config-crypto-map)# <b>set security-association lifetime seconds</b> <i>seconds</i> or Qtech(config-crypto-map)# <b>set security-association lifetime kilobytes</b> <i>kilobytes</i>	(Optional) Specifies a SA lifetime for the crypto map entry.
Qtech(config-crypto-map)# <b>set mtu</b> <i>length</i>	Sets the fragment size in tunnel mode.
Qtech(config-crypto-map)# <b>set vrf</b> <i>vrf-name</i>	Specifies the VRF that are associated with tunnel.
Qtech(config-crypto-map)# <b>username</b> <i>name</i> <b>password</b> <i>pass</i>	Configures the username and password used for extended authentication.
Qtech(config-crypto-map)# <b>exit</b>	Exits crypto map configuration mode and returns to the global configuration mode.

■ **Adding a dynamic crypto map set to the normal (static) crypto map set**

You can add one or more crypto map sets to a static crypto map set through reference of the crypto map entry to the dynamic map set. The crypto map entry that refers to the dynamic crypto map should be set as the entry with the lowest priority in the crypto map set.

To add a dynamic crypto map set to a static crypto map set, run the following command in global configuration mode:

Command	Function
Qtech (config)# <b>crypto map</b> <i>map-name</i> <i>seq-num</i> <b>ipsec-isakmp dynamic</b> <i>dynamic-map-name</i>	Adds a dynamic crypto map set to a static crypto map set

### 3.2.2.9 Applying Crypto Map Entry to an Interface

To apply a crypto map set to an interface, run the following command in interface configuration mode:

Command	Function
Qtech(config-if)# <b>crypto map</b> <i>map-name</i>	Applies a crypto map set to an interface.

A crypto map set should be configured for every interface that the IPSec traffic will pass. The device uses this crypto map set to judge all the traffic that passes this interface and apply a specific policy to filter the traffic.



**Note**

Only one crypto map set can be applied to an interface at one time, while the crypt map set can be applied to multiple interfaces at one time. When the IPSec traffic that passes this interface is processed, the IP address of this interface will be used as the address of the local device.

### 3.2.2.10 Creating Profile Crypto Map Entries

To create Profile crypto map entries for using IKE to establish SAs, run the following commands in global configuration mode in the beginning:



Command	Function
Qtech(config)# <b>crypto map</b> <i>map-name seq-num ipsec-isakmp</i>	Specifies the Profile crypto map entry to be created or modified. When using this command, you will enter crypto map configuration mode.
Qtech(config-crypto-map)# <b>match address</b> <i>access-list-id</i>	Specifies an access list for the crypto map list. This access list defines which communications are protected by the IPSec and which are not.
Qtech(config-crypto-map)# <b>set peer</b> { <i>hostname   ip-address</i> } [ <i>trustpoint1 [trustpoint2]</i> ]	Specifies remote IPSec peer. Communications protected by the IPSec are forwarding to this peer. Several peers can be configured.
Qtech(config-crypto-map)# <b>set local</b> <i>ip-address</i>	Sets the IP address of the negotiation. Use the primary IP address of the interface if it is not otherwise configured.
Qtech(config-crypto-map)# <b>set transform-set</b> <i>transform-set-name1</i> [ <i>transform-set-name2...transform-set-name6</i> ]	Specifies the transform set and lists the transform sets according to certain priority (set with higher priorities prevail).
Qtech(config-crypto-map)# <b>set security-association lifetime seconds</b> <i>seconds</i>	
Or: Qtech(config-crypto-map)# <b>set security-association lifetime kilobytes</b> <i>kilobytes</i>	
Qtech(config-crypto-map)# <b>set exchange-mode</b> <i>main   aggressive</i>	Sets the mode to initiate negotiations by this static entry.
Qtech(config-crypto-map)# <b>set pfs</b> <i>group1   group2</i>	Specifies the Diffie-Hellman group mark.
Qtech(config-crypto-map)# <b>set mtu</b> <i>length</i>	Sets the length of pre-fragment in tunnel mode.

Repeat the preceding steps to create other necessary crypto map entries.

The following example shows how to configure to establish a SA using IKE:

**Local peer (router A) configuration:**

# Define a transform set named myset

```
crypto ipsec transform-set myset esp-des
```

# Define a map set named *profile-name* that establishes a SA using IKE.

```
crypto ipsec profile profile-name
set transform-set myset
```

**Remote peer (router B) configuration:**

# Define a transform set named myset.

```
crypto ipsec transform-set myset esp-des
```

# Define a map set named *profile-name* that establishes a SA using IKE

```
crypto ipsec profile profile-name
set transform-set myset
```



#### Note

For the IPV6, IPSEC-IPV4, or IPSEC-IPV6 tunnels, the **match any** command must be configured in the map set *profile-name*. In addition, **Profile map** in this command can apply only to IPIP and IPv6 tunnels.

The dhcp over ipsec configuration takes effect only on the crypto map entry with the smallest value of *seq-num*.

### 3.2.2.11 Applying Profile Crypto Map Entries to a Tunnel Interface

To apply a Profile crypto map set to a tunnel interface, run the following command in interface configuration mode:

Command	Function
Qtech (config-if-Tunnel 1) # <b>tunnel protection ipsec profile profile-name</b>	Applies a crypto map set to a tunnel interface.

A crypto map set must be configured for every interface IPsec traffic passes through. Then the device can use the crypto map set to decrypt all packets through these interfaces.



#### Note

Profile crypto map entries can apply only to a tunnel interface. An attempt to apply a Profile crypto map entry to a non-tunnel interface may fail. In addition, only GRE, IPIP, and IPv6 tunnels are supported. If the **match any** command is configured in an entry, the entry applies only to IPIP and IPv6 tunnels.

### 3.2.2.12 Configuring Extended Authentication

Extended authentication uses AAA authentication items to verify the identities of users. To configure this function, run the following command in configuration mode:

Command	Function
Qtech (config) # <b>crypto map map-name client authentication list aaa-name</b>	Uses AAA authentication to verify identities of users.

### 3.2.2.13 Configuring Accounting Mode of Extensible Authentication

When the extensible authentication is implemented by using Authentication, Authorization and Accounting (AAA)/Remote Authentication Dial In User Service (RADIUS), some RADIUS servers require accounting packets for the keepalive purpose. In this case, the accounting mode of the extensible authentication needs to be configured. To do so, run the following command in configuration mode:

Command	Function
Qtech (config) # <b>crypto map map-name client accounting list aaa-name</b>	Applies the AAA accounting list.



#### Note

After this command is configured, accounting packets are used only for the keepalive purpose, and accounting data such as traffic will not be updated.

### 3.2.2.14 Configuring IPSec Packet Filtering

This function determines whether decrypted original IPSec packets need to be filtered. To configure this function, run the following command in configuration mode:

Command	Function
Qtech (config) # <b>crypto ipsec no-filter</b>	Decrypted packets are not filtered.

### 3.2.2.15 Monitoring and Maintaining IPSec

Some changes to the configuration only take effect when subsequent SAs are negotiated. If you want the new settings to take effect immediately, you must delete existing SAs, so that they will be established again using the new settings. The manually established SAs must be deleted and established again. Otherwise, changes will never take effect. If the device is processing the IPSec traffic, you may just want to clear the content that may be affected by the configuration change from the SA database (that is, only delete the SAs established by a given crypto map set). All the contents are only cleared from the SA database when the configuration is changed significantly, or the amount of the IPSec traffic that the device is processing is very small.

To delete and initiate the IPSec SA again, run the following commands in global configuration mode:

Command	Function
Qtech# <b>clear crypto sa</b>	Clears the entire SA database. This will also delete all the active security threads.
Qtech# <b>clear crypto sa peer</b> {ip-address   peer-name}	Clears the SAs with specific peer addresses.
Qtech# <b>clear crypto sa map</b> map-name	Clears the SAs of a specific crypto map set.
Qtech# <b>clear crypto sa spi</b> destination-address {ah   esp} spi	Clears the SAs with the specified destination address, protocol, or SPI.

To view configuration information of IPSec, run the following command in normal user mode:

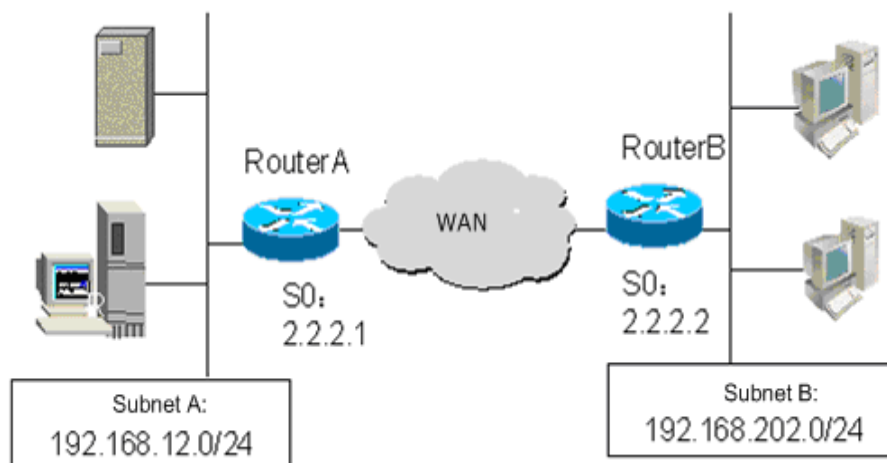
Command	Function
Qtech# <b>show crypto ipsec transform-set</b>	Views configuration of a transform set.
Qtech# <b>show crypto map</b> [map-name]	Views configuration of all or the specified crypto maps.
Qtech# <b>show crypto ipsec sa</b>	Views information about the IPSec SA.
Qtech# <b>show crypto dynamic-map</b> [tag map-name]	Views information about the dynamic crypto map.
Qtech# <b>debug crypto ipsec</b>	Displays debug messages about the IPSec event.

## 3.2.3 IPSec Configuration Example

### Configuration requirements

As shown in Figure 8, in order to protect the IP traffic from Subnet A (192.168.12.0/24) to Subnet B (192.168.202.0/24), use the Ethernet interface (192.168.12.1) of Router A and the Ethernet interface (192.168.202.1) of Router B as the security gateways at both ends, using the channel mode and the protection mode ESP-DES-SHA (the encryption and authentication services are available).

Figure 8 IPSec configuration example



### Router configuration

In order to protect the IP traffic between hosts in two subnets, you can use the manually established SA or the IKE-established SA. Because Router A and Router B have similar configurations, the following only shows the configuration of the manually established SA for Router A. For the configuration of the IKE-established SA, refer to the typical case in the "IKE Configuration Guide" chapter .

Configuration of Router A:

# Use an access list to define the traffic to be protected

```
access-list 101 permit ip 192.168.12.0 0.0.0.255 192.168.202.0 0.0.0.255
```

# Define a transform set:

```
crypto ipsec transform-set myset esp-des esp-sha-hmac
```

# The crypto map associates the IPsec access list with the transform set, and specifies the destination of the protected traffic

```
crypto map mymap 10 ipsec-manual
  match address 101
  set transform-set myset
  set session-key inbound esp 301 cipher 0123456789abcdef authenticator
0000111122223333444455556666777788889999
  set session-key outbound esp 300 cipher 0123456789abcdef authenticator
5555666677778888999900001111222233334444
  set peer 2.2.2.2
!
interface FastEthernet 0
  ip address 192.168.12.1 255.255.255.0
```

# Apply the crypto map to the interface

```
interface Serial 0
  ip address 2.2.2.1
  crypto map mymap
!
  ip route 0.0.0.0 0.0.0.0 2.2.2.2
```

## 3.3 IKE Configuration

### 3.3.1 IKE Working Process

IKE is a key management protocol standard that is used with the IPsec standard. IPsec is an IP security function that provides robust authentication and IP packet encryption. IPsec can be configured without using IKE. However, IKE enhances the IPsec function by providing additional functions and flexibility and making it easier to configure the IPsec standard. IKE is a hybrid protocol that implements the Oakley key exchange and the Skeme key exchange

(ISAKMP, Oakley and Skeme are security protocols implemented by IKE) within the Internet Security Association and Key Management Protocol (ISAKMP) framework.

IPSec must be configured (depending on IPSec of IKE) and applied to the interface before IKE can work. When an outgoing packet that meets requirements is detected on the interface, IPSec will trigger IKE to negotiate with the peer IKE. They establish a secure channel between the peers to transmit various supported IPSec parameters. Finally, a consistent SA is established at both ends to enable IPSec at both ends to work. If there are data that meets requirements to be transmitted when the lifetime of the IPSec SA expires over time, IKEs at both ends will start to negotiate IPSec again, and so on.

IKE can be used to eliminate the need to manually specify all the IPSec parameters and keys in the crypto map tables for the two parties in communication. It allows you to specify the lifetime of the IPSec SA. IKE makes IPSec change the key regularly and thus strengthen the security. IKE enables IPSec to provide the anti-replay service.

### 3.3.2 IKE Configuration Task

IKE configuration tasks including:

Enabling or Disabling IKE: make sure IKE is working.

Ensuring Compatibility between Access List and IKE: if an access list (firewall) is configured on the device, you must make sure that the UDP packets of IKE are not prohibited.

Creating IKE Policies: specify parameters in each IKE policy.

Selecting Working Mode: There are two working modes-main mode (default) and aggressive mode. (note: aggressive mode is also called violent mode).

Configuring Local Identity: specify local identity for IKE negotiation.

Setting Automatic Mode Recognition: specify whether the IKE negotiation responder automatically accept the negotiation in aggressive mode.

Configuring Digital Certificate: a digital certificate for IKE authentication.

Configuring Pre-shared Key: the pre-shared key is shared by the two peers participating in IKE negotiation.

Configuring DPD Detection: two mechanisms are used to implement DPD-- on-demand and periodic.

Configuring NAT Traversal Timeout: the UDC header is added to solve the NAT traversal problem. Use the keepalive packets to maintain the UDP linkage and to avoid the NAT connection timeout.

Exclude Qtech vendor information: Qtech vendor information is often delivered during IKE negotiation. If incompatibility is found in vendor information IKE Session limit, exclude Qtech vendor information

IKE SESSION LIMIT: set a limit on the number of IKE sessions. .

Qtech Networks' IKE session mode: except for Digital signature authentication, switch all IKE negotiation within the network to Qtech Networks' IKE session mode.

Extended Authentication Timeout: configure extended authentication timeout,

Configure domain authentication: configure extended domain authentication to associate IPSEC tunnel with VRF.

Configure cisco's compatible extended authentication: configure this command on devices that negotiate with cisco's devices.

Exclude designated IP addresses from extended Digital signature authentication.

TRACK Correlation: in a scenario where there the primary and backup linkage exist at the same time, the IPSec is used to monitor the status of primary linkage. When the primary link is UP, the IPSec channel in the backup link will be removed automatically. Currently, we can use TRACK and DLDP to monitor the primary linkage.

Backup Link Detection: when the backup linkage detection does not work, the negotiation process will be intervened.

IKE Maintenance (optional): maintain IKE, make sure IKE is working, check parameters.

#### 3.3.2.1 Enabling or Disabling IKE

IKE is enabled by default. If you do not want to use IKE with IPSec together, you can disable it with a command. However, only the manual IPSec SA can work.

To disable or enable IKE, run the following command in global configuration mode:

Command	Function
Qtech(config)# <b>no crypto isakmp enable</b>	Disables the IKE function.
Qtech(config)# <b>crypto isakmp enable</b>	Enables the IKE function.

If IKE is disabled, subsequent configuration will not take effect.



#### Caution

Disabling IKE will result in:

- During IPSec communication, the encryption key never changes, and you need to modify your key regularly.
- The anti-replay service is unavailable.
- You must establish all the SAs manually.

### 3.3.2.2 Ensuring Compatibility between Access List and IKE

IKE is an application running on the basis of UDP that transmits packets in the UDP format through port 500. If an access list (firewall) is configured on the device, and UDP packets are prohibited, IKE negotiation will fail. Therefore, you must make sure that the UDP packets of IKE are not prohibited.

### 3.3.2.3 Creating IKE Policies

Both parties participating in IKE negotiation must have at least one set of consistent IKE policies. This is mandatory for successful IKE negotiation. You must create multiple policies with priorities on each peer, so as to make sure at least one policy matches the policy of the remote peer.

Define the following five parameters in each IKE policy:

Parameter	Keyword	Value Range	Default Value
Encryption algorithm	Des	56-bit DES-CBC	56-bit DES-CBC
	3des	168-bit DES-CBC	
	aes	128-bit AES-CBC	
HASH algorithm	Sha	SHA-1 (HMAC variant)	SHA-1 (HMAC variant)
	md5	MD5 (HMAC variant)	
Authentication method	pre-share	Pre-shared key	Digital signature authentication
	rsa-sig	Digital signature authentication	
	digital-email	Digital envelope authentication	
Diffie-Hellman group ID	1	768-bit Diffie-Hellman group	768-bit Diffie-Hellman group
	2	1024-bit Diffie-Hellman group	
	5	3072-bit Diffie-Hellman group	
	14	2048-bit Diffie-Hellman group	
	15	3072-bit Diffie-Hellman group	



Parameter	Keyword	Value Range	Default Value
	16	4096-bit Diffie-Hellman group	
	17	6144-bit Diffie-Hellman group	
	18	8192-bit Diffie-Hellman group	
Lifetime of IKE SA	Void	1 minute to 1 day (in seconds)	1 day (86400 seconds)

When IKE negotiation starts, IKE tries to find a consistent policy on the two peers. The initiator of negotiation sends all the policies to the remote responder. The responder searches, by priority, the policies that match with the local policies in the policies received from the remote peer.

If both peers participating in negotiation have the same encryption, HASH, authentication and Diffie-Hellman parameters, and the lifetime specified by the policy of the remote peer is smaller than or equal to the lifetime specified by the compared policy, then they match (if no lifetime is specified, the shorter lifetime specified by the policy of the remote peer is used). If no acceptable matching policy is found, IKE refuses to negotiate and IPSec is not established. If a matching policy is found, IKE negotiates and establishes the IPSec SA.

You can select a value of each parameter by making a tradeoff between security and performance:

- Encryption algorithms: At present, 56-bit DES-CBC, 168-bit 3DES-CBC, and 128-bit AES-CBC are supported.
- Hash algorithms: SHA-1 and MD5. MD5 has less digest and is often considered a little faster than SHA-1. Attacks on MD5 are proved to be successful in one way, but extremely difficult. However, the HMAC variant (MD5) used by IKE can block this attack.
- Authentication method: Currently RGOS supports pre-shared key method and digital certificate authentication. To authenticate with the pre-shared key method, you need to configure a correct pre-shared key. To authenticate using a digital certificate, you need to configure a correct certificate for both parties (refer to the section regarding certificate configuration).
- There are two options for the Diffie-Hellman group ID: 768-bit or 1024-bit Diffie-Hellman. 1024-bit Diffie-Hellman is more difficult to crack, but occupies more CPU resources.
- The lifetime of the IKE SA, different from that of the IPSec SA, refers to the validity period of IKE negotiation. It can be set to any value. The following is a general rule: The shorter the lifetime (to a critical point), the securer the IKE negotiation is. If a longer lifetime is used, however, negotiation of IPSec SA will be faster.

You can create multiple IKE policies, each of which corresponds to a different combination of parameters. A unique priority (1-10000, where 1 represents the highest priority) should be assigned to each created policy.

You can configure multiple policies on each peer. However, you must make sure that one of these policies has exactly the same encryption, HASH, authentication and Diffie-Hellman parameters as the remote peer (they can have different lifetimes). If no policy is configured, the device uses the default policy, which is set to have the lowest priority and includes the default value of each parameter.

To configure a policy, run the following commands in global configuration mode in the beginning:

Command	Function
Qtech(config)# <b>crypto isakmp policy priority</b>	Identifies the policy to be created. Each policy is uniquely identified by the priority.
Qtech(config-isakmp)# <b>encryption des   3des   aes-128   aes-192   aes-256</b>	Specifies an encryption algorithm.
Qtech(config-isakmp)# <b>hash {sha   md5}</b>	Specifies a HASH algorithm.
Qtech(config-isakmp)# <b>authentication {pre-share   rsa-sig }</b>	Specifies an authentication method.
Qtech(config-isakmp)# <b>group {1   2  5}</b>	Specifies a Diffie-Hellman group ID.
Qtech(config-isakmp)# <b>lifetime seconds</b>	Specifies the lifetime of IKE SA.
Qtech(config-isakmp)# <b>exit</b>	Returns to global configuration mode.

If no value is specified for parameters, the default values are used.

To view the configured IKE policy, run the following command in privileged user mode:

Command	Function
Qtech# <b>show crypto isakmp policy</b>	Shows all the existing IKE policies.

**Note**

The configuration does not include the default policy and the default values of configured policies. To view these settings, use the **show crypto isakmp policy** command.

### 3.3.2.4 Selecting Working Mode

There are two working modes: main mode (default) and aggressive mode.

A working mode should be configured for the initiator. To do so, run the following commands at the crypto map entry where IKE is configured to establish a SA:

Command	Function
Qtech(config)# <b>crypto map map-name seq-num ipsec-isakmp</b>	Specifies the crypto map entry to be created or modified. When using this command, you will enter crypto map configuration mode.
Qtech(config-crypto-map)# <b>set exchange-mode {main   aggressive}</b>	Selects a working mode of IKE negotiation. The main mode is used by default.

By default, the responder negotiates in main mode. To use the aggressive mode, run the following command in global configuration mode.

Command	Function
Qtech(config)# <b>crypto ipsec-isakmp mode-detect</b>	Negotiates in the mode used by the initiator.

To view the working mode of IKE, run the following command in privileged user mode:

Command	Function
Qtech# <b>show crypto isakmp sa</b>	Browses all the current IKE SAs.

### 3.3.2.5 Configuring Local Identity

When selecting a working mode, you set the mode (main or aggressive mode) in which the initiator initiates the first negotiation message. If the main mode is selected, this configuration will not affect negotiation. If the aggressive mode is selected, this configuration specifies the identity type in the first negotiation message of the initiator, which directly affects negotiation in aggressive mode. Currently, you can set three forms: 1. Local address; 2. Domain name; 3. User name@domain name. You can set as necessary.

Command	Function
Qtech(config)# <b>self-identity address   fqdn   user-fqdn identity   dn</b>	Specifies the form of the negotiation identity in aggressive mode. Address: The primary IP address of the local interface through which negotiation is initiated. Fqdn: Specifies the domain name form for the local identity. User-fqdn: Specifies the user name@domain name form for the local identity. Dn: DN value of the certificate

### 3.3.2.6 Setting Automatic Mode Recognition

The device, as the center, needs to accept dial-in in multiple modes (main mode and aggressive mode). The device needs to respond to the two different types of initiation and negotiate. Therefore, this command is mainly used in this working environment. Configuration of this command for the initiator has no influence.

Command	Function
Qtech(config)# <b>crypto isakmp mode-detect</b>	Specifies that the responder negotiates by using automatic recognition.

### 3.3.2.7 Configuring Digital Certificate

By default, IKE authenticates by using a digital certificate. A digital certificate must be configured if this method is used. Refer to the "Digital Certificate Configuration" chapter.

### 3.3.2.8 Configuring Digital Envelope

The digital envelope authentication meets the need of IKE *IPSEC VPN Technology Specification*. The method is nearly the same with digital certificate. The different is when using digital envelope authentication, user should configure peer certificate first.

Here are key configurations, when configuring digital envelope:

Command	Function
Router(config)# <b>crypto pki certificate peer address</b>	Import peer certificate.
Qtech(config)# <b>crypto isakmp policy Priority</b>	Identifies the policy to be created. Each policy is uniquely identified by the priority.
Qtech(config-isakmp)# <b>authentication digital-email</b>	Specifies an authentication method.

Here are key configurations, when configuring new state code digital envelope authentication:

Command	Function
Router(config)# <b>crypto pki certificate peer address</b>	Import peer certificate.
Qtech(config)# <b>crypto isakmp policy Priority</b>	Identifies the policy to be created. Each policy is uniquely identified by the priority.
Qtech(config-isakmp)# <b>authentication digital-email asymmetric sm2</b>	Specifies new state code authentication mode.

### 3.3.2.9 Configuring Pre-shared Key

The pre-shared key is shared by the two peers participating in IKE negotiation. Therefore, each pre-shared key corresponds to a pair of IKE peers. On a given peer, you should specify a key that is the same as those of multiple pre-shared remote peers. For the purpose of security, you should configure different keys for different peer pairs.

To configure a pre-shared key, run the following commands in global configuration mode:

Command	Function
Router(config)# <b>ip host hostname address</b>	If hostname is used to identify the remote peer, specify the IP address corresponding to this hostname.
Qtech(config)# <b>crypto isakmp key 0 7 keystring { hostname peer-hostname   address peer-address } [no-xauth]</b>	Specifies a pre-shared key that is used with the remote IKE peer. Number 0 indicates the plain text is used. Number 7 indicates the cipher text is used.

Router(config)# <b>crypto isakmp key 0</b>  7 <i>keystring address peer-address [mask] [no-xauth]</i>	Specifies a pre-shared key used for the IKE peer of a certain network segment. Both <i>peer-address</i> and <i>mask</i> are 0.0.0.0. 0.0.0.0 is the default pre-shared key.
---	--

You must configure the same pre-shared key on each pair of peers.



#### Note

1. Like Cisco devices, versions later than RGOS 8.31 use the digital signature authentication in the IKE policy by default. If the pre-shared key is needed, IKE policy configuration must be added. See the following example:

```
crypto isakmp policy 1
 authentication pre-share
!
```

Earlier versions of RGOS only support authentication using the pre-shared key.

2. If the hostname of a remote IKE negotiation peer has been registered on DNS, the second step mentioned above can be omitted.

3. On Cisco devices, if the peer uses the hostname to identify the pre-shared key, the initiator will initiate negotiation in aggressive mode.

4. After the extended authentication command **crypto map map-name client authentication list aaa-name** is configured, use the command **no-xauth** to disable the extended authentication for devices with designated address.

### 3.3.2.10 Configuring DPD Detection

Currently, two mechanisms are used to implement DPD: 1. on-demand. This mechanism sends packets when a tunnel is idle in a time longer than what is configured. This will trigger sending of a DPD message. 2. periodic. This mechanism actively sends a DPD message when the idle time of the tunnel exceeds the configured time. The maximum number of retransmission times is 5. (For DPD configuration in earlier versions, refer to the version 8.2 configuration guide)

To configure DPD detection, run the the following commands:

Command	Function
Router(config)# <b>crypto isakmp keepalive seconds</b>	seconds - Idle time of the tunnel The default retransmission interval is 5 seconds, and the on-demand mechanism is used
Router(config)# <b>crypto isakmp keepalive seconds retries</b>	seconds - Idle time of the tunnel retries – Retransmission interval The on-demand mechanism is used by default.
Router(config)# <b>crypto isakmp keepalive seconds retries on-demand</b>	seconds - Idle time of the tunnel retries - Retransmission interval on-demand - The on-demand mechanism
Router(config)# <b>crypto isakmp keepalive seconds periodic</b>	seconds - Idle time of the tunnel periodic - periodic mechanism The default Retransmission interval is 5 seconds.
Router(config)# <b>crypto isakmp keepalive seconds retries periodic</b>	seconds - Idle time of the tunnel retries - Retransmission interval periodic - periodic mechanism

### 3.3.2.11 Configuring NAT Traversal Timeout

As the RFC3947 and IPSEC NAT-t are supported, the UDC header is added to solve the NAT traversal problem. To avoid the NAT connection timeout, the keepalive mode shall be used to send packets. The default time is 5 minutes.

Command	Function
---------	----------

Router(config)# <b>crypto isakmp nat keepalive</b> <i>seconds</i>	Seconds: the interval of sending the packets in keepalive mode. The default interval is 5 minutes.
---	--

### 3.3.2.12 Excluding Qtech Vendor Information

Qtech vendor information is often delivered during IKE negotiation. If incompatibility is found in vendor information, run the following command:

Command	Function
Router(config)# <b>crypto isakmp vendorid</b> <b>disable</b>	Excludes the vendor id information.

### 3.3.2.13 Configuring IKE Session Limit

To set a limit on the number of IKE sessions, run the following command:

Command	Function
Router(config)# <b>crypto isakmp session limit</b> <b>number</b>	Sets a limit on the number of IKE sessions.

### 3.3.2.14 Configuring Qtech IKE Negotiation Mode

To switch all IKE negotiation (except for Digital signature authentication ) within the network to Qtech Networks' IKE session mode, run the following command:

Command	Function
Router(config)# <b>crypto isakmp rg-sm1</b>	Switches all IKE negotiation (except for Digital signature authentication ) within the network to Qtech Networks' IKE session mode

### 3.3.2.15 Configuring Extended Authentication Timeout

To configure extended authentication timeout, run the following command:

Command	Function
Router(config)# <b>crypto isakmp xauth timeout</b> <i>seconds</i>	Configures the timeout time of extended authentication, with the value ranging from 5 to 90 seconds.

### 3.3.2.16 Configuring AAA Server Response Timeout

To configure AAA server response timeout, run the following command:

Command	Function
Router(config)# <b>crypto isakmp xauth timeout</b> <i>seconds</i>	Configures the timeout time of waiting AAA server response, with the value ranging from 5 to 10000 seconds.

### 3.3.2.17 Configuring Client Policy Delivery

When both Key ID authentication and extended authentication are used on a client, run the following commands in configuration mode to configure client policy delivery:

Command	Function
Qtech(config)# <b>crypto isakmp client configuration</b> <b>group</b> <i>name</i>	Creates or modifies a client configuration delivery entry. When using this command, you will enter client policy delivery configuration mode.



Router(config-isakmp-group)# <b>key 0</b> [7] <i>keystring</i>	Configures the shared key used for Key ID authentication. This configuration takes effect only in aggressive mode.
Router(config-isakmp-group)# <b>dns</b> pri-dns sec-dns	Configures the DNS from which a policy is delivered to a client.
Router(config-isakmp-group)# <b>netmask</b> mask	Configures the subnet mask from which a policy is delivered to a client.
Router(config-isakmp-group)# <b>pool</b> pool-name	Configures the address pool from which an IP address is selected for delivering a policy to a client.
Router(config-isakmp-group)# <b>network center</b> <i>net-addr/prefix</i>	(optional) open for the networks under the client's server. Only the packets forwarding to these networks can pass over the IPSec tunnel. Currently, the maximum number of these networks is 5.

### Configuring domain authentication

To enable domain authentication:

Command	Function
Router(config)# <b>crypto isakmp authorize</b> [ <b>split</b> ]	enables domain authentication:

To configure domain-delimiter:

Command	Function
Router(config)# <b>crypto isakmp domain-delimiter</b> <i>keyword</i> [ <b>prefix</b> <b>suffix</b> ]	Specifies domain-delimiter; by default, the <b>suffix</b> is domain.

To specify domain-name ,

Command	Function
Router(config-isakmp-group)# <b>domain</b> <i>domain-name</i> [ <b>vrf</b> ] <i>vrf-name</i>	Specifies the domain-name and associates domain-name with vrf-name

### Configuring cisco's compatible extended authentication:

To adopt cisco's compatible extended authentication for IKE negotiation. Run the following commands in configuration mode:

Command	Function
Router(config)# <b>crypto isakmp xauth cisco_comp</b>	Adopts Cisco's compatible extended authentication.



#### Note

After configured the command **crypto map** *map-name* **client authentication list** *aaa-name* on a crypto map, all clients need to be authenticated. However, some client with designated IP address do not need extended authentication. To exclude these designated IP addresses from extended Digital Signature Authentication, run the command mentioned in the above table.

#### 3.3.2.18 Configuring IP address pool

Use the following commands to issue an IP address for a XAUTH client:

Command	Function
Router(config)# <b>crypto isakmp ippool</b> <i>pool-name</i>	Creates an address pool
Qtech(config-isakmp-ippool)# <b>address</b> <i>low-ip high-ip</i>	Configures the range of the IP address pool.




### 3.3.2.19 TRACK Correlation

In a scenario where there is a backup linkage or multiple linkage, the IPSec is used to monitor the status of primary linkage. When the primary linkage is up, the IPSec channel in the backup linkage will be removed so as to clear the reverse routing. And then the normal data forwarding is guaranteed. Currently, TRACK and DLDP are used to monitor primary linkage. Refer to the corresponding files for the configuration of TRACK and DLDP.

Command	Function
Qtech(config)# <b>crypto isakmp link-redundancy backup</b> <i>backup_interface track track_id</i>	Monitors <i>track id</i> via the TRACK protocol. The IPSEC channel on <i>backup_interface</i> will be removed after <i>track id</i> is up.
Qtech(config)# <b>crypto isakmp link-redundancy backup</b> <i>backup_interface dldp master_interface</i>	Monitors <i>master_interface</i> via the DLDP protocol. The IPSEC channel on <i>backup_interface</i> will be removed after the <i>master_interface</i> is up.
Qtech(config)# <b>crypto isakmp link-redundancy backup</b> <i>backup_interface intf-down master_interface</i>	Monitors the DOWN event in <i>master_interface</i> . The IPSEC channel on <i>backup_interface</i> will be removed after it occurs.

### 3.3.2.20 Backup Linkage Detection

When the default backup linkage detection does not work, the negotiation process will be intervened

Command	Function
Qtech(config)# <b>crypto isakmp link-redundancy detect ike</b>	Only negotiate the first stage of IKE and ensure its basic function to be normal.
 <p><b>Caution</b> the command will only be configured when the default detection does not work. The default detection will detect the backup linkage in a better way.</p>	

### 3.3.2.21 IKE Maintenance

Clear an IKE connection

To clear an IKE connection, run the following commands in privileged user mode:

Command	Function
Qtech# <b>show crypto isakmp sa</b>	Shows the existing IKE connections, and note down the connection ID of the connection you want to clear.
Qtech# <b>clear crypto isakmp</b> [ <i>connection-id</i> ]	Clears an IKE connection. When <i>connection-id</i> is not used, all IKE connections are cleared.
Directly execute: Qtech# <b>clear crypto isakmp</b>	Clears all the local IKE connections.

IKE diagnosis

To obtain the IKE diagnostics information, run the following commands in privileged user mode:

Command	Function
Qtech# <b>show crypto isakmp policy</b>	Shows all the IKE policy parameters.
Qtech# <b>show crypto isakmp sa</b>	Shows all the current IKE SAs.
	Shows IKE address pool
Qtech# <b>debug crypto isakmp</b>	Shows debug messages about the IKE event.

Shows debug message about the IKE address pool event.

### 3.3.3 IKE Configuration Example

The following shows an IKE configuration example:

```
crypto isakmp enable
crypto isakmp policy 4
  group 1
  encryption 3des
crypto isakmp policy 5
  authen pre-share
  group 2
  lifetime 1000
crypto isakmp policy 6
  authen rsa-sig
  group 1
  lifetime 1000
```

For details, run the following command in privileged user mode:

```
Qtech # show crypto isakmp policy
```

Protection suite of priority 4

encryption algorithm: 3DES - Data Encryption Standard (56 bit keys).

hash algorithm: Secure Hash Standard

authentication method: Rsa-Sig

Diffie-Hellman group: #1 (1024 bit)

lifetime: 1000 seconds

Protection suite of priority 5

encryption algorithm: DES - Data Encryption Standard (56 bit keys).

hash algorithm: Secure Hash Standard

authentication method: Pre-shared key

Diffie-Hellman group: #2 (1024 bit)

lifetime: 1000 seconds

Protection suite of priority 6

encryption algorithm: DES - Data Encryption Standard (56 bit keys).

hash algorithm: Secure Hash Standard

authentication method: Rsa-Sig

Diffie-Hellman group: #1 (768 bit)

lifetime: 1000 seconds

Default protection suite

encryption algorithm: DES - Data Encryption Standard (56 bit keys).

hash algorithm: Secure Hash Standard

authentication method: Rsa-Sig

Diffie-Hellman group: #1 (768 bit)

lifetime: 86400 seconds

### 3.3.4 Typical Application Cases

#### 3.3.4.1 Statically Configuring Tunnels

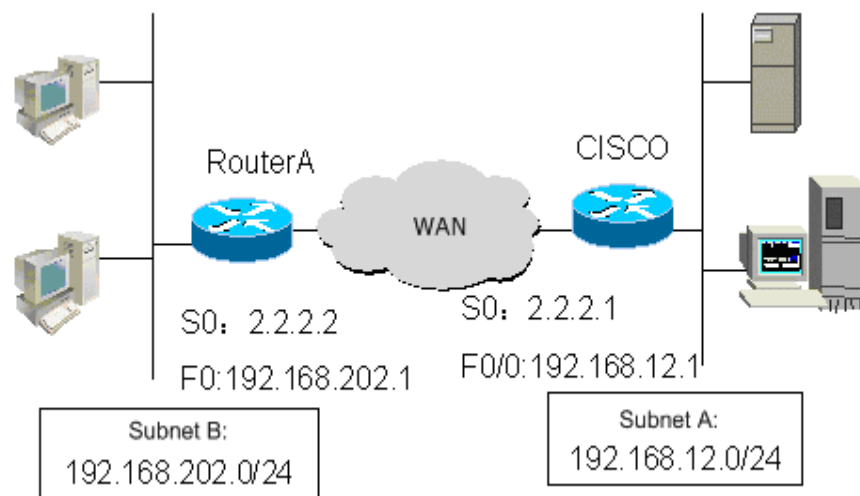
##### Analysis

In this case, the IP traffic between two subnets is protected by using a Cisco device connected to Subnet A as the gateway at one side, and using a Qtech device connected to Subnet B as the gateway at the other side. The following requirements should be met:

- The 3DES algorithm is used in phase 1.
- The tunnel mode is used.
- The protection method is ESP-DES-MD5 (the encryption and authentication services are available).

In the following application, a Cisco device is used as the center, and Qtech devices are used as remote branches. See Figure 9 :

Figure 9 Typical IPSec application



### Router configuration

This section describes how to manually establish a SA and establish a SA using IKE for Qtech router, namely Router A. Meanwhile, it also provides configurations of Cisco devices for your reference in actual work.

#### 8) Configuration for establishing a SA using IKE

Configuration of Router A:

```
!
hostname "RouterA"
```

#### # Enable IKE

```
crypto isakmp enable
crypto isakmp policy 1
authentication pre-share
encryption 3des
!
```

#### # Configure a pre-shared key and a transform set

```
crypto isakmp key 0 preword address 2.2.2.1
crypto ipsec transform-set myset esp-des esp-md5-hmac
```

#### # Define a crypto map set

```
crypto map mymap 5 ipsec-isakmp
 set peer 2.2.2.1
 set transform-set myset
 match address 101
!
interface FastEthernet0
 ip address 192.168.202.1 255.255.255.0
```

#### # Apply the crypto map to the interface

```
interface Serial0
 ip address 2.2.2.2 255.255.255.0
 encapsulation ppp
 crypto map mymap
!
ip route 0.0.0.0 0.0.0.0 Serial0
```

#### # Define an encryption access list to protect the IP traffic between the subnet 192.168.202.0/24 and the subnet 192.168.12.0/24

```
access-list 101 permit ip 192.168.202.0 0.0.0.255 192.168.12.0 0.0.0.255
!
```

```
end
```

Configuration of Cisco device:

```
!  
hostname Cisco  
  
# Define an IKE policy, using the pre-shared key for authentication, and using the default values for other  
parameters  
crypto isakmp policy 1  
  authentication pre-share  
  encryption 3des  
  
# Configure a pre-shared key  
crypto isakmp key 0 preword address 2.2.2.2  
  
# Define a transform set  
crypto ipsec transform-set myset esp-des esp-md5-hmac  
  
# Define a crypto map  
crypto map mymap 5 ipsec-isakmp  
  set peer 2.2.2.2  
  set transform-set myset  
  match address 101  
!  
interface FastEthernet0/0  
  ip address 192.168.12.1 255.255.255.0  
  
# Apply the crypto map to the interface  
interface Serial0  
  ip address 2.2.2.1 255.255.255.0  
  encapsulation ppp  
  crypto map mymap  
!  
ip route 192.168.202.0 255.255.255.0 Serial0  
  
# Define an encryption access list to protect the IP traffic between the subnet 192.168.12.0/24 and the subnet  
192.168.202.0/24  
access-list 101 permit ip 192.168.12.0 0.0.0.255 192.168.202.0 0.0.0.255  
!  
end
```

Configuration for establishing a SA manually

Configuration of Router A:

```
!  
hostname "RouterA"  
  
# Define a transform set  
crypto ipsec transform-set myset esp-des esp-md5-hmac  
  
# Define a crypto map set  
crypto map mymap 5 ipsec-manual  
  set peer 2.2.2.1  
  set session-key inbound esp 300 cipher abcdef1234567890  
  authenticator abcdef1234567890abcdef1234567890 //This is the same configuration  
statement as the previous line  
  set session-key outbound esp 301 cipher abcdef1234567890  
  authenticator abcdef1234567890abcdef1234567890 //This is the same configuration  
statement as the previous line  
  set transform-set myset  
  match address 101
```

```
!  
interface FastEthernet0  
ip address 192.168.202.1 255.255.255.0
```

# Apply the crypto map to the interface

```
interface Serial0  
ip address 2.2.2.2 255.255.255.0  
encapsulation ppp  
crypto map mymap  
!  
ip route 0.0.0.0 0.0.0.0 Serial0
```

# Define an encryption access list to protect the IP traffic between the subnet 192.168.202.0/24 and the subnet 192.168.12.0/24

```
access-list 101 permit ip 192.168.202.0 0.0.0.255 192.168.12.0 0.0.0.255  
!  
end
```

Configuration of Cisco device:

```
!  
hostname Cisco
```

# Define a transform set

```
crypto ipsec transform-set myset esp-des esp-md5-hmac
```

# Define a crypto map

```
crypto map mymap 5 ipsec-manual  
set peer 2.2.2.2  
set session-key inbound esp 301 cipher abcdef1234567890  
authenticator abcdef1234567890abcdef1234567890 //This is the same configuration  
statement as the previous line  
set session-key outbound esp 300 cipher abcdef1234567890  
authenticator abcdef1234567890abcdef1234567890 //This is the same configuration  
statement as the previous line  
set transform-set myset  
match address 101  
!  
interface FastEthernet0/0  
ip address 192.168.12.1 255.255.255.0  
# Apply the crypto map to the interface  
interface Serial0  
ip address 2.2.2.1 255.255.255.0  
encapsulation ppp  
crypto map mymap  
!  
ip route 192.168.202.0 255.255.255.0 Serial0
```

# Define an encryption access list to protect the IP traffic between the subnet 192.168.12.0/24 and the subnet 192.168.202.0/24

```
access-list 101 permit ip 192.168.12.0 0.0.0.255 192.168.202.0 0.0.0.255  
!  
end
```

Monitoring and debugging

9) Monitoring and debugging the IKE-based SA

On any host in Subnet B, send a packet to Subnet A. IKE negotiation is triggered and finally an IPSec SA is established successfully.

# Turn on the debugging switches of IKE and IPSec:

```
RouterA# debug crypto ipsec
```

```
IPSEC debugging is on
RouterA# debug crypto isakmp
ISAKMP debugging is on
```

# You can see the following debugging information during negotiation:

```
Get acquire: 192.168.202.0/0.0.0.255 -> 192.168.12.0/0.0.0.255 , prot 0, port 0/0
Acquire negotiate with 2.2.2.1
(36) Beginning Quick Mode exchange, M-ID of 4445127
(36) sending packet to 2.2.2.1 (I) QM_S11_WR1
ipsec_output:423, get item acclist 101
ipsec_output:429, match 3
(36) received packet from 2.2.2.1 (I) QM_S11_WR1
payload format: <Hdr>,<hash> <sa> <nonce> <id>
(36) processing SA payload. message ID = 4445127
(36) Creating IPsec SAs.
    inbound SA has spi 4445127
    protocol esp, DES_CBC
    auth MD5
    outbound SA has spi 275385850
    protocol esp, DES_CBC
    auth MD5
    lifetime of 3600 seconds, soft 3570 seconds
    lifetime of 4608000 kilobytes, soft 256 kilobytes
ipsec_output:423, get item acclist 101
ipsec_output:429, match 3
(36) sending packet to 2.2.2.1 (I) QM_IDLE
(36) Phase_2 negotiate complete!
```

# In order to view and confirm whether the SAs of IKE and IPsec have been established, use the following command:

```
RouterA# show crypto isakmp sa
destination      source          state           conn-id
lifetime(second)
 2.2.2.1         2.2.2.2        QM_IDLE        36
5013
```

# The preceding information shows that an IKE SA has been established successfully

```
RouterA# show crypto ipsec sa
Interface: Serial0
Crypto map tag:mymap, local addr 2.2.2.2 //The current crypto map set is named mymap
that uses the local address 2.2.2.2
  media mtu 1500
  local ident (addr/mask/prot/port): (192.168.202.0/0.0.0.255/0/0)
  remote ident (addr/mask/prot/port): (192.168.12.0/0.0.0.255/0/0)
PERMIT //Protect the traffic between 192.168.202.0/24 and
192.168.12.0/24
current_peer: 2.2.2.1 //The address of the remote peer is 2.2.2.1
  #pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
  #pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
  #send errors 0, #recv errors 0
//Statistical data in turn: number of encapsulation packets, number of encryption
packets, number of digest packets, number of de-capsulation packets, number of
decryption packets, number of verification packets, send errors, and receive errors.
  inbound esp sas: //Security association for the
inbound packet processing, with the protocol ESP
  spi:0x43D3C7 (4445127) //The SPI value is 4445127
  transform: esp-des esp-md5-hmac //The transform set is esp-des-md5
  in use settings={Tunnel,} //Tunnel mode
sa timing: remaining key lifetime (k/sec): (4607999/3578)
//There are 4607999 kbytes/3578 seconds left before expiry of the SA
  IV size: 8 bytes //The IV vector length is 8
  Replay detection support:Y //Anti-replay processing
```



```

outbound esp sas:                                     //Security association for
the outbound packet processing, with the protocol ESP
spi:0x106A0DFA (275385850)                           //The SPI value is 275385850
transform: esp-des esp-md5-hmac                     //The transform set is esp-des-md5
in use settings={Tunnel,}                           //Tunnel mode
sa timing: remaining key lifetime (k/sec): (4607999/3577)
//There are 4607999 kbytes/3577 seconds left before expiry of the SA
IV size: 8 bytes                                    //The IV vector length is 8
Replay detection support:Y                          //Anti-replay processing

```

The preceding statistical data shows that IPSec has been established and some packets are protected.

#### Monitoring and debugging the manually established SA

Because the manually established SA exists from the beginning, you needn't negotiate it and cannot view its debugging information. You can only view some statistical data:

```

RouterA# show crypto ipsec sa
Interface: Serial0
Crypto map tag:mymap, local addr 2.2.2.2           //The current crypto map set is named
mymap that uses the local address 2.2.2.2
media mtu 1500
local ident (addr/mask/prot/port): (192.168.202.0/0.0.0.255/0/0)
remote ident (addr/mask/prot/port): (192.168.12.0/0.0.0.255/0/0)
PERMIT                                             //Protect the traffic
between 192.168.202.0/24 and 192.168.12.0/24
current_peer: 2.2.2.1                             //The address of the remote peer is
2.2.2.1
#pkts encaps: 8, #pkts encrypt: 8, #pkts digest 8
#pkts decaps: 8, #pkts decrypt: 8, #pkts verify 8
#send errors 0, #recv errors 0
//Statistical data in turn: number of encapsulation packets, number of encrypted
packets, number of digest packets, number of decapsulated packets, number of
decryption packets, number of verification packets, send errors, and receive errors.
inbound esp sas:                                  //Security association for the inbound
packet processing, with the protocol ESP
spi: 0x12C (300)                                  //The SPI value is 300
transform: esp-des esp-md5-hmac                   //The transform set is esp-des-md5
in use settings={Tunnel,}                         //Tunnel mode
no sa timing                                       //Expired
IV size: 8 bytes                                  //The IV vector length is 8
Replay detection support:N                         //No anti-replay processing

outbound esp sas:                                 //Security association for the outbound
packet processing, with the protocol ESP
spi: 0x12D (301)                                  //The SPI value is 301
transform: esp-des esp-md5-hmac                   //The transform set is esp-des-md5
in use settings={Tunnel,}                         //Tunnel mode
no sa timing                                       //Expired
IV size: 8 bytes                                  //The IV vector length is 8
Replay detection support:N                         //No anti-replay processing

```

The preceding statistical data shows that IPSec has been established and some packets are protected.

### 3.3.4.2 Dynamically Configuring Tunnels

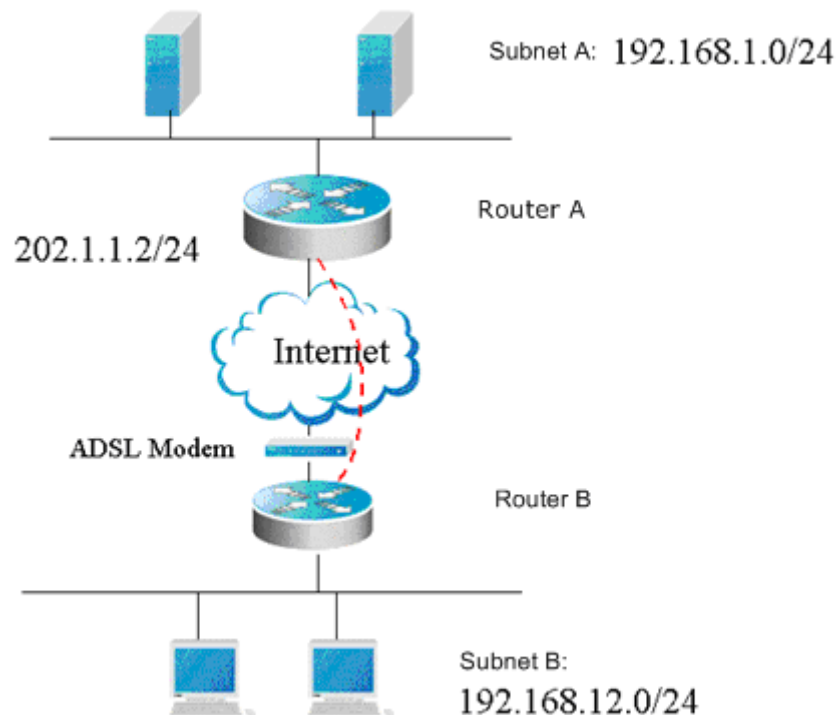
#### Case analysis

In this case, the IP traffic between two subnets is protected by using Qtech Router A connected to Subnet A as the gateway at one side, and using Qtech Router B connected to Subnet B as the branch gateway at the other side, as shown in Figure-4. The following requirements should be met:

- The tunnel mode is used.
- The protection method is ESP-DES-MD5 (the encryption and authentication services are available).

- The IP address of the WAN interface of Router A is fixed: 202.1.1.2/24. The router is connected to the Internet through a dedicated line.
- Router B is connected to the Internet through ADSL using the PPPOE protocol. Its IP address is allocated by the ISP dynamically.
- Use IKE to establish the SA.
- Use the pre-shared key.

Figure 10 IPSec typical case



### Router configuration

This section provides configuration for establishing a SA between Qtech routers, namely Router B and Router A.

Configuration of Router B:

```
!
hostname "RouterB"
```

# Enable IKE

```
crypto isakmp enable
```

# Configure a pre-shared key and a transform set

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key 0 preword address 202.1.1.2
crypto ipsec transform-set myset esp-des esp-md5-hmac
```

# Define a crypto map set

```
crypto map mymap 5 ipsec-isakmp
 set peer 202.1.1.2
 set transform-set myset
 match address 101
!
interface FastEthernet0
 ip address 192.168.12.1 255.255.255.0
interface FastEthernet1
 no ip address
```

```
pppoe enable
pppoe-client 1 dial-pool-number 1 dial-on-demand
```

# Apply the crypto map to the interface

```
interface Dialer0
  mtu 1488
ip address negotiate
  encapsulation ppp
  ppp pap sent-username xxx password xxx
  crypto map mymap
dialer idle-timeout 2400
  dialer pool 1
  dialer-group 1
!
dialer-list protocol ip permit
ip route 0.0.0.0 0.0.0.0 Dialer0 permanent
```

# Define an encryption access list to protect the IP traffic between the subnet 192.168.12.0/24 and the subnet 192.168.1.0/24

```
access-list 101 permit ip 192.168.12.0 0.0.0.255 192.168.1.0 0.0.0.255
!
end
```

Configuration of Router A:

```
!
hostname "RouterA"
```

# Define an IKE policy, using the pre-shared key for authentication, and using the default values for other parameters

```
crypto isakmp policy 1
  authentication pre-share
```

# Configure the default pre-shared key. Because the IP address of the remote end is dynamic, you couldn't know in advance it is necessary to configure the default pre-shared key

```
crypto isakmp key 0 preword address 0.0.0.0 0.0.0.0
```

# Define a transform set

```
crypto ipsec transform-set myset esp-des esp-md5-hmac
```

# Define a dynamic crypto map

```
crypto dynamic-map dymymap 5
  set transform-set myset
  match address 101
!
```

# Add a dynamic crypto map set to a static crypto map set

```
crypto map mymap 10 ipsec-isakmp dynamic dymymap
!
interface FastEthernet0/0
  ip address 192.168.1.1 255.255.255.0
```

# Apply the crypto map to the interface

```
interface Serial0
  ip address 202.1.1.2 255.255.255.0
  encapsulation ppp
  crypto map mymap
!
ip route 0.0.0.0 0.0.0.0 Serial0
```

# Define an encryption access list to protect the IP traffic between the subnet 192.168.1.0/24 and the subnet 192.168.12.0/24

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.12.0 0.0.0.255
!
end
```

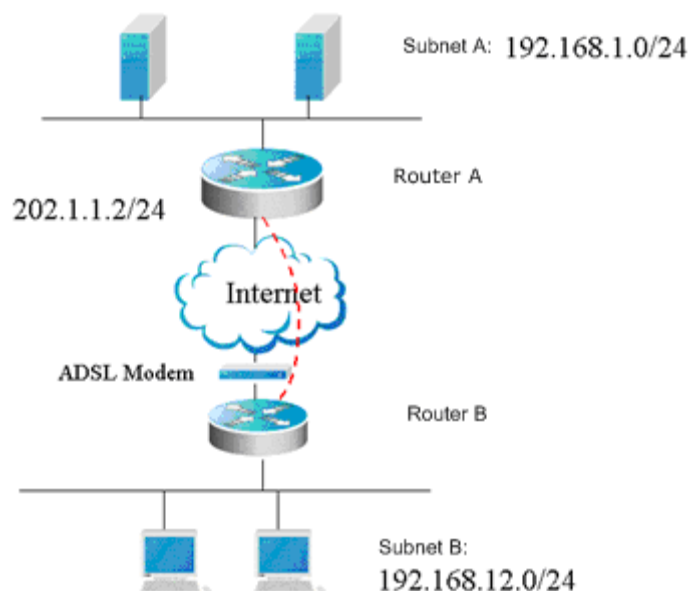
### 3.3.4.3 Initiating Negotiation with the Domain Name

#### Case analysis

In this case, the IP traffic between two subnets is protected by using Qtech Router A connected to Subnet A as the gateway at one side, and using Qtech Router B connected to Subnet B as the branch gateway at the other side. The following requirements should be met:

- The tunnel mode is used.
- The protection method is ESP-DES-MD5 (the encryption and authentication services are available).
- The IP address of the WAN interface of Router A is always 202.1.1.2/24. The router is connected to the Internet through a dedicated line.
- Router B is connected to the Internet through ADSL using the PPPOE protocol. Its IP address is allocated by ISP dynamically.
- Use the pre-shared key, and specify the pre-shared key for the central router using the host name.
- Use IKE to establish the SA.

Figure 11



#### Router configuration

This section describes how to establish a SA between Qtech routers, namely Router B and Router A.

Configuration of Router B:

```
!
hostname "RouterB"

# Enable IKE
crypto isakmp enable

# Configure the local identity
self-identity fqdn www.google.com

# Configure a pre-shared key and a transform set
crypto isakmp key 0 preword address 202.1.1.2
crypto ipsec transform-set myset esp-des esp-md5-hmac
```

## # Define a crypto map set

```
crypto map mymap 5 ipsec-isakmp
  set peer 202.1.1.2
  set exchange-mode aggressive
  set transform-set myset
  match address 101
!
interface FastEthernet0
  ip address 192.168.12.1 255.255.255.0
interface FastEthernet1
  no ip address
  pppoe enable
  pppoe-client 1 dial-pool-number 1 dial-on-demand
```

## # Apply the crypto map to the interface

```
interface Dialer0
  mtu 1488
ip address negotiate
  encapsulation ppp
  ppp pap sent-username xxx password xxx
  crypto map mymap
dialer idle-timeout 2400
  dialer pool 1
  dialer-group 1
!
dialer-list protocol ip permit
ip route 0.0.0.0 0.0.0.0 Dialer0 permanent
```

## # Define an encryption access list to protect the IP traffic between the subnet 192.168.12.0/24 and the subnet 192.168.1.0/24

```
access-list 101 permit ip 192.168.12.0 0.0.0.255 192.168.1.0 0.0.0.255
!
end
```

## Configuration of Router A:

```
!
hostname "RouterA"
```

## # Define an IKE policy, using the pre-shared key for authentication, and using the default values for other parameters

```
crypto isakmp policy 1
  authentication pre-share
```

## # Configure a default pre-shared key. Because the IP address of the remote end is dynamic, the pre-shared key is found by specifying the hostname

```
crypto isakmp key 0 preword hostname www.google.com
```

## # Configure automatic recognition for the center

```
crypto isakmp mode-detect
```

## # Define a transform set

```
crypto ipsec transform-set myset esp-des esp-md5-hmac
```

## # Define a dynamic crypto map

```
crypto dynamic-map dymymap 5
  set transform-set myset
  match address 101
!
```

## # Add a dynamic crypto map set to a static crypto map set

```
crypto map mymap 10 ipsec-isakmp dynamic dymymap
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
```

# Apply the crypto map to the interface

```
interface Serial0
 ip address 202.1.1.2 255.255.255.0
 encapsulation ppp
 crypto map mymap
!
ip route 0.0.0.0 0.0.0.0 Serial0
```

# Define an encryption access list to protect the IP traffic between the subnet 192.168.1.0/24 and the subnet 192.168.12.0/24

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.12.0 0.0.0.255
!
End
```

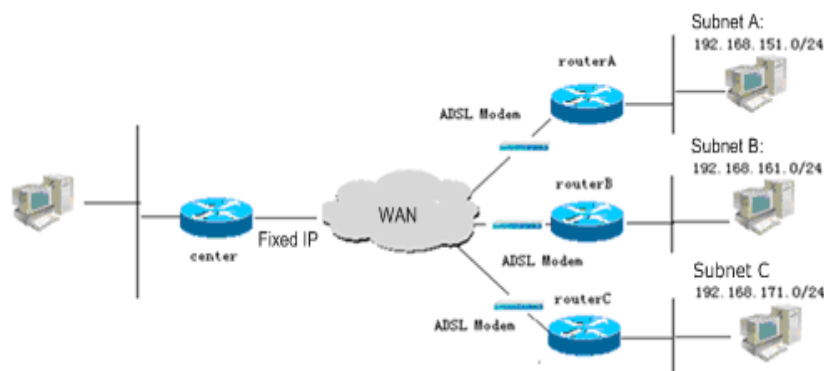
### 3.3.4.4 Dynamically Configuring to Use Certificate Negotiation

#### Case analysis

Configure a dynamic crypto map set for the center. The IKE negotiation policy uses the digital signature for authentication. The branch is connected to the center through L2TP. L2TP will trigger IKE negotiation. The IPSec tunnel must be established successfully before the L2TP tunnel can be established. L2TP is used to run OSPF, so that both the center and the branch can learn their own subnet routes. The following requirements should be met:

- The tunnel mode is used.
- The protection method is ESP-DES (the encryption service is available).
- The IP address of the WAN interface of the center is always 63.23.12.212/29. The center is connected to the Internet through a dedicated line.
- The branch router is connected to the Internet through ADSL using the PPPOE protocol. Its IP address is allocated by the ISP dynamically.
- The central router is configured with IKE negotiation policies and uses the certificate for authentication.

Figure 12



Configuration of Center:

```
hostname center
!
!
route-map static-ospf permit 10
 match ip address 1
!
access-list 1 permit 0.0.0.0 255.255.255.0
!
vpdn enable
!
vpdn-group 1
```



```
! Default L2TP VPDN group
accept-dialin
protocol l2tp
virtual-template 1
l2tp tunnel force_ipsec
source-ip 63.23.12.212
!
username RGOS password 0 RGOS
!
```

#### # Configure the certificate and root certificate for the local router

```
crypto pki certificate chain
certificate ca 56AE073C10A17E8C45AE8D3F15523357
3082032E 308202D8 A0030201 02021056 AE073C10 A17E8C45 AE8D3F15 52335730
0D06092A 864886F7 0D010105 05003081 AC312130 1F06092A 864886F7 0D010901
16126469 6E676A73 40737461 722D6E65 742E636E 310B3009 06035504 06130243
4E310F30 0D060355 04081306 46754A69 616E310F 300D0603 55040713 0646755A
686F7531 20301E06 0355040A 13175265 6769616E 74204E65 74776F72 6B20436F
2E204C74 64311D30 1B060355 040B1314 52657365 61726368 20417061 72746D65
6E742035 31173015 06035504 03130E43 41207465 73742073 65727665 72301E17
0D303530 32323530 38343630 325A170D 30373033 30313032 33363233 5A3081AC
3121301F 06092A86 4886F70D 01090116 1264696E 676A7340 73746172 2D6E6574
2E636E31 0B300906 03550406 1302434E 310F300D 06035504 08130646 754A6961
6E310F30 0D060355 04071306 46755A68 6F753120 301E0603 55040A13 17526567
69616E74 204E6574 776F726B 20436F2E 204C7464 311D301B 06035504 0B131452
65736561 72636820 41706172 746D656E 74203531 17301506 03550403 130E4341
20746573 74207365 72766572 305C300D 06092A86 4886F70D 01010105 00034B00
30480241 00D91F1A C60EF951 924CDC96 4D4443FA DABE53F2 DDF513B6 34B5A6A1
9FFD57A1 6C6F7AF4 A113C159 3D0C4C3E 8E62DE76 D8A24CF2 2CF8DA82 AA17D3E8
CC80C295 8F020301 0001A381 D33081D0 300B0603 551D0F04 04030201 C6300F06
03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 14724384 1C2B0345
2D8258F5 844377F5 21AA4B2C 21307F06 03551D1F 04783076 3038A036 A0348632
68747470 3A2F2F7A 6A2D726F 75746572 2F436572 74456E72 6F6C6C2F 43412532
30746573 74253230 73657276 65722E63 726C303A A038A036 86346669 6C653A2F
2F5C5C7A 6A2D726F 75746572 5C436572 74456E72 6F6C6C5C 43412532 30746573
74253230 73657276 65722E63 726C3010 06092B06 01040182 37150104 03020101
300D0609 2A864886 F70D0101 05050003 41007F2E 7D1676B5 560EDD1E D80B4205
3B39A742 B8E06813 786E9992 2E4C5860 AB4AF193 63A34170 50BD756A AEA7086A
7A9FC2AC D1D8A3A0 CC6779D0 76CE7D1A 7F4C
quit
!
certificate 1FFC97F0000100000029
308204B3 3082045D A0030201 02020A1F FC97F000 01000000 29300D06 092A8648
86F70D01 01050500 3081AC31 21301F06 092A8648 86F70D01 09011612 64696E67
6A734073 7461722D 6E65742E 636E310B 30090603 55040613 02434E31 0F300D06
03550408 13064675 4A69616E 310F300D 06035504 07130646 755A686F 75312030
1E060355 040A1317 52656769 616E7420 4E657477 6F726B20 436F2E20 4C746431
1D301B06 0355040B 13145265 73656172 63682041 70617274 6D656E74 20353117
30150603 55040313 0E434120 74657374 20736572 76657230 1E170D30 35303332
31303632 3335395A 170D3036 30333231 30363333 35395A30 81A63122 30200609
2A864886 F70D0109 0116137A 68616F6A 756E4073 7461722D 6E65742E 636E310B
30090603 55040613 02434E31 0F300D06 03550408 13064675 4A69616E 310F300D
06035504 07130646 755A686F 75312030 1E060355 040A1317 52656769 616E7420
4E657477 6F726B20 436F2E20 4C746431 1D301B06 0355040B 13145265 73656172
63682041 70617274 6D656E74 20353110 300E0603 55040313 077A6861 6F6A756E
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00BB70FF 351D18F5
7735FE4F C890AF42 8E8744BA D946C4B8 61F046DF 614E4A37 D8A3BA80 7003D7E1
BC5394F3 58DDE033 4ABA82D1 AEAAD4C10 3135C2AE BB58FA2F 75020301 0001A382
02633082 025F300E 0603551D 0F0101FF 04040302 06C03013 0603551D 25040C30
0A06082B 06010505 08020230 1D060355 1D0E0416 0414420E 87E0F7C1 B744AFE3
2C1EFD64 E03E2144 844C3081 E8060355 1D230481 E03081DD 80147243 841C2B03
452D8258 F5844377 F521AA4B 2C21A181 B2A481AF 3081AC31 21301F06 092A8648
86F70D01 09011612 64696E67 6A734073 7461722D 6E65742E 636E310B 30090603
```

```

55040613 02434E31 0F300D06 03550408 13064675 4A69616E 310F300D 06035504
07130646 755A686F 75312030 1E060355 040A1317 52656769 616E7420 4E657477
6F726B20 436F2E20 4C746431 1D301B06 0355040B 13145265 73656172 63682041
70617274 6D656E74 20353117 30150603 55040313 0E434120 74657374 20736572
76657282 1056AE07 3C10A17E 8C45AE8D 3F155233 57307F06 03551D1F 04783076
3038A036 A0348632 68747470 3A2F2F7A 6A2D726F 75746572 2F436572 74456E72
6F6C6C2F 43412532 30746573 74253230 73657276 65722E63 726C303A A038A036
86346669 6C653A2F 2F5C5C7A 6A2D726F 75746572 5C436572 74456E72 6F6C6C5C
43412532 30746573 74253230 73657276 65722E63 726C3081 AC06082B 06010505
07010104 819F3081 9C304B06 082B0601 05050730 02863F68 7474703A 2F2F7A6A
2D726F75 7465722F 43657274 456E726F 6C6C2F7A 6A2D726F 75746572 5F434125
32307465 73742532 30736572 76657228 31292E63 7274304D 06082B06 01050507
30028641 66696C65 3A2F2F5C 5C7A6A2D 726F7574 65725C43 65727445 6E726F6C
6C5C7A6A 2D726F75 7465725F 43412532 30746573 74253230 73657276 65722831
292E6372 74300D06 092A8648 86F70D01 01050500 034100AF 173B4A23 E95C8042
ED4F2F97 0D869C1E 715800E6 F64F505F 1A6F291C 4B8C95C8 2FE04F9C CA81778F
07A2DE20 C9640A8B DD36BCC0 359C26BB D5A5E434 B5F46B
quit
!
!

```

# The IKE negotiation uses a certificate for authentication by default

```
!
```

# Configure a transform set

```
crypto ipsec transform-set myset esp-des
```

# Configure a dynamic crypto map set

```

crypto dynamic-map dy 1
  set transform-set myset
!
!
crypto map mymap 1 ipsec-isakmp dynamic dy
!
interface FastEthernet 0/0
  ip address 63.23.12.212 255.255.255.248
  crypto map mymap
  duplex auto
  speed auto
!
interface FastEthernet 0/1
  ip address 192.168.216.1 255.255.255.0
  ip address 192.168.217.1 255.255.255.0 secondary
  ip address 192.168.218.1 255.255.255.0 secondary
  ip address 192.168.219.1 255.255.255.0 secondary
  duplex auto
  speed auto
!
interface Null 0
!
interface Virtual-Template 1
  mtu 1400
  ip ospf mtu-ignore
  ip unnumbered FastEthernet 0/1
  ip mtu 1360
!
!
router ospf
  redistribute static subnets route-map static-ospf
  network 192.168.216.0 0.0.0.255 area 0.0.0.0
  network 192.168.217.0 0.0.0.255 area 0.0.0.0
  network 192.168.218.0 0.0.0.255 area 0.0.0.0
  network 192.168.219.0 0.0.0.255 area 0.0.0.0

```

```

!
line con 0
  exec-timeout 0 0
line aux 0
  disconnect-character 240
line vty 0 4
  exec-timeout 0 0
  privilege level 15
  no login
!
!
end

```

#### Configuration of router A:

```

hostname routerA
!
# Configure an access list
access-list 101 permit ip interface dialer 0 host 63.23.12.212
access-list 177 deny icmp any any unreachable
access-list 177 permit ip any any
dialer-list 1 protocol ip permit
!
l2tp-class l2x
  hostname rg36_1
!
pseudowire-class pw
  encapsulation l2tpv2
  protocol l2tpv2 l2x
  ip local interface dialer 0
!
!

```

#### # Configure the certificate and root certificate for the local router

```

crypto pki certificate chain
certificate ca 56AE073C10A17E8C45AE8D3F15523357
3082032E 308202D8 A0030201 02021056 AE073C10 A17E8C45 AE8D3F15 52335730
0D06092A 864886F7 0D010105 05003081 AC312130 1F06092A 864886F7 0D010901
16126469 6E676A73 40737461 722D6E65 742E636E 310B3009 06035504 06130243
4E310F30 0D060355 04081306 46754A69 616E310F 300D0603 55040713 0646755A
686F7531 20301E06 0355040A 13175265 6769616E 74204E65 74776F72 6B20436F
2E204C74 64311D30 1B060355 040B1314 52657365 61726368 20417061 72746D65
6E742035 31173015 06035504 03130E43 41207465 73742073 65727665 72301E17
0D303530 32323530 38343630 325A170D 30373033 30313032 33363233 5A3081AC
3121301F 06092A86 4886F70D 01090116 1264696E 676A7340 73746172 2D6E6574
2E636E31 0B300906 03550406 1302434E 310F300D 06035504 08130646 754A6961
6E310F30 0D060355 04071306 46755A68 6F753120 301E0603 55040A13 17526567
69616E74 204E6574 776F726B 20436F2E 204C7464 311D301B 06035504 0B131452
65736561 72636820 41706172 746D656E 74203531 17301506 03550403 130E4341
20746573 74207365 72766572 305C300D 06092A86 4886F70D 01010105 00034B00
30480241 00D91F1A C60EF951 924CDC96 4D4443FA DABE53F2 DDF513B6 34B5A6A1
9FFD57A1 6C6F7AF4 A113C159 3D0C4C3E 8E62DE76 D8A24CF2 2CF8DA82 AA17D3E8
CC80C295 8F020301 0001A381 D33081D0 300B0603 551D0F04 04030201 C6300F06
03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 14724384 1C2B0345
2D8258F5 844377F5 21AA4B2C 21307F06 03551D1F 04783076 3038A036 A0348632
68747470 3A2F2F7A 6A2D726F 75746572 2F436572 74456E72 6F6C6C2F 43412532
30746573 74253230 73657276 65722E63 726C303A A038A036 86346669 6C653A2F
2F5C5C7A 6A2D726F 75746572 5C436572 74456E72 6F6C6C5C 43412532 30746573
74253230 73657276 65722E63 726C3010 06092B06 01040182 37150104 03020101
300D0609 2A864886 F70D0101 05050003 41007F2E 7D1676B5 560EDD1E D80B4205
3B39A742 B8E06813 786E9992 2E4C5860 AB4AF193 63A34170 50BD756A AEA7086A
7A9FC2AC D1D8A3A0 CC6779D0 76CE7D1A 7F4C
quit

```

```

!
certificate 11F7C51700010000003E
308204B1 3082045B A0030201 02020A11 F7C51700 01000000 3E300D06 092A8648
86F70D01 01050500 3081AC31 21301F06 092A8648 86F70D01 09011612 64696E67
6A734073 7461722D 6E65742E 636E310B 30090603 55040613 02434E31 0F300D06
03550408 13064675 4A69616E 310F300D 06035504 07130646 755A686F 75312030
1E060355 040A1317 52656769 616E7420 4E657477 6F726B20 436F2E20 4C746431
1D301B06 0355040B 13145265 73656172 63682041 70617274 6D656E74 20353117
30150603 55040313 0E434120 74657374 20736572 76657230 1E170D30 35303431
32303932 3935335A 170D3036 30343132 30393339 35335A30 81A43121 301F0609
2A864886 F70D0109 01161264 696E676A 73407374 61722D6E 65742E63 6E310B30
09060355 04061302 434E310F 300D0603 55040813 0646754A 69616E31 0F300D06
03550407 13064675 5A686F75 3120301E 06035504 0A131752 65676961 6E74204E
6574776F 726B2043 6F2E204C 7464311D 301B0603 55040B13 14526573 65617263
68204170 6172746D 656E7420 35310F30 0D060355 04031306 64696E67 6A73305C
300D0609 2A864886 F70D0101 01050003 4B003048 024100CD 2C3B2981 FF9BF7E6
F9DFFCF9 495FE6AA 6691FD76 BB5EBEC3 5A1E48F8 8B75DD68 9E79AC5A 36C0B4F4
AA959323 49EEEE7F 24B546B8 74421F17 401033AE EC3F4102 03010001 A3820263
3082025F 300E0603 551D0F01 01FF0404 030204F0 30130603 551D2504 0C300A06
082B0601 05050802 02301D06 03551D0E 04160414 216567F3 E72263B2 4990E14D
ECC22471 1596A71F 3081E806 03551D23 0481E030 81DD8014 7243841C 2B03452D
8258F584 4377F521 AA4B2C21 A181B2A4 81AF3081 AC312130 1F06092A 864886F7
0D010901 16126469 6E676A73 40737461 722D6E65 742E636E 310B3009 06035504
06130243 4E310F30 0D060355 04081306 46754A69 616E310F 300D0603 55040713
0646755A 686F7531 20301E06 0355040A 13175265 6769616E 74204E65 74776F72
6B20436F 2E204C74 64311D30 1B060355 040B1314 52657365 61726368 20417061
72746D65 6E742035 31173015 06035504 03130E43 41207465 73742073 65727665
72821056 AE073C10 A17E8C45 AE8D3F15 52335730 7F060355 1D1F0478 30763038
A036A034 86326874 74703A2F 2F7A6A2D 726F7574 65722F43 65727445 6E726F6C
6C2F4341 25323074 65737425 32307365 72766572 2E63726C 303AA038 A0368634
66696C65 3A2F2F5C 5C7A6A2D 726F7574 65725C43 65727445 6E726F6C 6C5C4341
25323074 65737425 32307365 72766572 2E63726C 3081AC06 082B0601 05050701
0104819F 30819C30 4B06082B 06010505 07300286 3F687474 703A2F2F 7A6A2D72
6F757465 722F4365 7274456E 726F6C6C 2F7A6A2D 726F7574 65725F43 41253230
74657374 25323073 65727665 72283129 2E637274 304D0608 2B060105 05073002
86416669 6C653A2F 2F5C5C7A 6A2D726F 75746572 5C436572 74456E72 6F6C6C5C
7A6A2D72 6F757465 725F4341 25323074 65737425 32307365 72766572 2831292E
63727430 0D06092A 864886F7 0D010105 05000341 00148479 89448BB7 E6D3A7A7
34376464 C8D857C2 D9075263 9E278FC3 2D6C5041 036B66C7 F59ADCA5 39C9F824
A40A4C57 05373965 66671538 921FF39C B95C90F4 3F
quit
!
crypto pki revocation-check none
!

```

```
# Configure that DPD is triggered periodically
```

```
crypto isakmp keepalive 20 periodic
```

```
# Configure a transform set
```

```
crypto ipsec transform-set myset esp-des
```

```
# Configure a crypto map set
```

```
crypto map mymap 1 ipsec-isakmp
 set peer 63.23.12.212
 set transform-set myset
 match address 101
!
!
!
interface FastEthernet 0/0
 pppoe enable
 pppoe-client dial-pool-number 1 no-ddr
 duplex auto
```

```
speed auto
!
interface FastEthernet 0/1
 ip address 192.168.161.1 255.255.255.0
 duplex auto
 speed auto
!
interface dialer 0
 mtu 1488
 encapsulation PPP
 ppp chap hostname abcd@163.com
 ppp chap password 0 123456
 ppp pap sent-username abcd@163.com password 0 123456
 ip access-group 177 in
 ip address negotiate
 crypto map mymap
 dialer pool 1
 dialer idle-timeout 1200
 dialer-group 1
 bandwidth 2048
!
interface Null 0
!
interface Virtual-ppp 1
 pseudowire 63.23.12.212 20 encapsulation l2tpv2 pw-class pw
 mtu 1400
 ppp pap sent-username RGOS password 0 RGOS
 ip ospf mtu-ignore
 no ip route-cache policy
 ip unnumbered FastEthernet 0/1
 ip mtu 1360
!
!
router ospf
 network 192.168.161.0 0.0.0.255 area 0.0.0.0
!
ip route 0.0.0.0 0.0.0.0 dialer 0
!
!
line con 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 no login
!
!
end
```

For configurations of Router B and Router C, refer to the configuration of Router A.



#### Caution

Because the private key of a device is confidential information that does not exist in the system configuration file, when you copy and paste the preceding configuration information to the device console or use the **copy tft flash** command to copy this configuration file to the device configuration file **config.txt**, the preceding certificate-related configurations cannot be performed. To configure a certificate, you must run the **crypto pki import pem terminal** command to import a certificate. This example only shows the configurations that are visible to you.

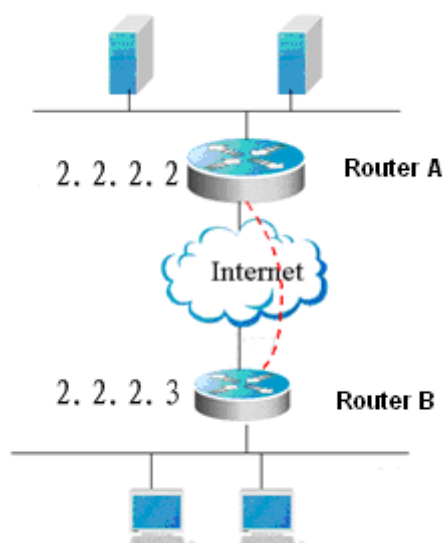
### 3.3.4.5 Reverse Route Injection

#### Analysis

In this case, the IP traffic between two subnets is protected by using the Router A as the central gateway at one side, and using Router B as the branch gateway at the other side, as shown in Figure 5. The following requirements should be met:

- The 3DES algorithm is used in phase 1.
- The tunnel mode is used.
- The protection method is ESP-3des (the encryption and authentication services are available).

Figure 13



#### Router configuration

##### 10) Router A

```
ip host peerhost 2.2.2.2
ip access-list extended 110
10 permit ip host 2.2.2.3 host 2.2.2.2
crypto isakmp policy 1
authentication pre-share
!
!
crypto isakmp key 7 01334b46391e033004 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set myset esp-3des
crypto dynamic-map dymap 100
set transform-set myset
reverse-route
match address 111
!
!
crypto map mymap 7 ipsec-isakmp dynamic dymap
interface GigabitEthernet 1/0/0
 ip ref
ip address 2.2.2.3 255.255.255.0
crypto map mymap
duplex auto
speed auto
end
```

##### 11) Router B

```
ip access-list extended 110
10 permit ip host 2.2.2.2 host 2.2.2.3
```



```
crypto isakmp policy 1
authentication pre-share
crypto isakmp key 7 0424100330052a1b15 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set myset esp-3des
crypto map mymap 10 ipsec-isakmp
set peer 2.2.2.3
set transform-set myset
match address 110
interface FastEthernet 0/0
ip address 2.2.2.2 255.255.255.0
crypto map mymap
duplex auto
speed auto
!
interface FastEthernet 0/1
ip address 200.1.1.10 255.255.255.0
duplex auto
speed auto
end
```

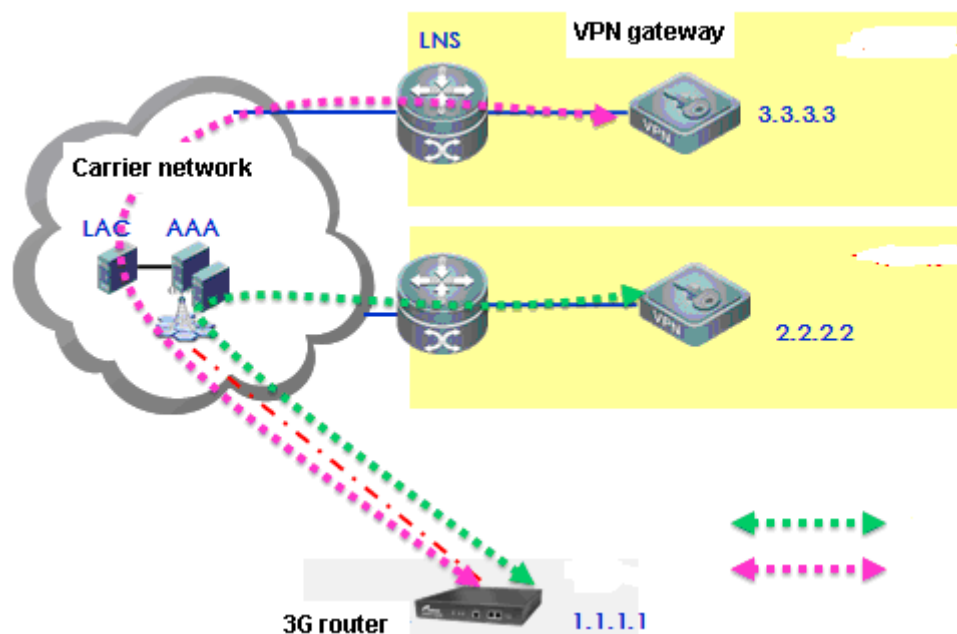
### 3.3.4.6 Mutual Backup of Multiple Peers

#### Analysis

In this case, there are multiple servers and each server uses a different certificate chain. The access device is configured with multiple peers and certificate chains. While the convergence device has the same configuration as that in the other case. As shown in the figure below, the following requirements should be met:

- Multiple VPN gateways are located in different places to provide access services.
- Every convergence router uses a different certificate chain.
- The access router changes according to the peer configuration.

Figure 14



#### Router configuration

- 12) Convergence router A
- //Use the default policy.

```
!  
crypto ipsec transform-set myset esp-3des  
crypto dynamic-map dymap 100  
  set transform-set myset  
  reverse-route  
!  
!  
crypto map mymap 7 ipsec-isakmp dynamic dymap  
interface GigabitEthernet 1/0/0  
  ip ref  
  ip address 2.2.2.3 255.255.255.0  
  crypto map mymap  
  duplex auto  
  speed auto  
end
```

13) Convergence router B whose configuration is the same as router A except the local address and certificate

//Use the default policy.

```
!  
crypto ipsec transform-set myset esp-3des  
crypto dynamic-map dymap 100  
  set transform-set myset  
  reverse-route  
!  
!  
crypto map mymap 7 ipsec-isakmp dynamic dymap  
interface GigabitEthernet 1/0/0  
  ip ref  
  ip address 2.2.2.2 255.255.255.0  
  crypto map mymap  
  duplex auto  
  speed auto  
end
```

14) Access router A

```
ip access-list extended 110  
  10 permit ip host 2.2.2.1 any  
!  
//Use the default policy: certificate-based authentication  
crypto isakmp keepalive 10 2 periodic  
//Use 3DES for encryption  
crypto ipsec transform-set myset esp-3des  
!  
crypto map mymap 7 ipsec-isakmp  
set peer 2.2.2.2 //The default certificate chain is used if this parameter is not  
specified.  
set peer 2.2.2.3 trustpoint backup  
set transform-set myset  
match address 100  
  
interface GigabitEthernet 1/0/0  
  ip ref  
  ip address 2.2.2.1 255.255.255.0  
  crypto map mymap  
  duplex auto  
  speed auto  
end
```

## Applying Profile crypto map entries in different tunnels

- Analysis

In this case, the IP traffic between two subnets is protected by using a Cisco device connected to Subnet A as the gateway at one side, and using a Qtech device connected to Subnet B as the gateway at the other side. The following requirements should be met:

- The 3DES algorithm is used in phase 1
- The transmission mode is used.
- The protection method is ESP-DES-MD5 (the encryption and authentication services are available).

In the following application, a Cisco device is used as the center, and Qtech devices are used as remote branches. See Figure 15.

Figure 15

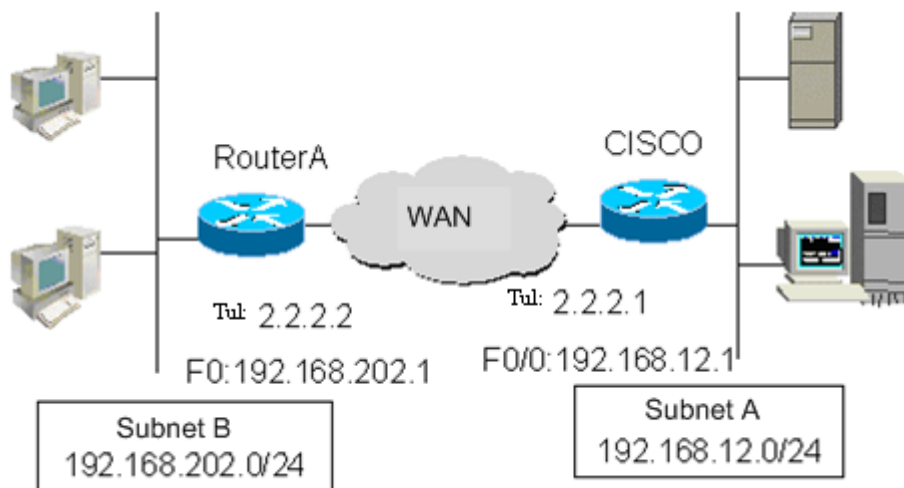
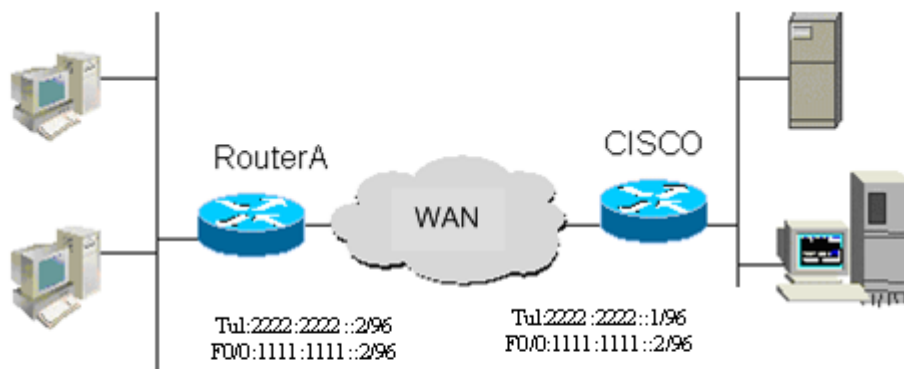


Figure 16



### Applying the Profile map to a GRE tunnel

Configuration of Router A:

```
!
hostname "RouterA"

# Enable IKE

crypto isakmp enable
crypto isakmp policy 1
authentication pre-share
```

```
encryption 3des
```

#### # Configure a pre-shared key and a transform set

```
crypto isakmp key 0 123 address 192.168.12.1
crypto ipsec transform-set t1 esp-des esp-md5-hmac
mode transport
```

#### # Define a crypto map set

```
crypto ipsec profile profi-map
set transform-set t1
!
interface FastEthernet0
ip address 192.168.202.1 255.255.255.0
# Apply the crypto map to a GRE tunnel interface
interface tunnel 1
tunnel source 192.168.202.1
tunnel destination 192.168.12.1
tunnel protection ipsec profile profile-map
ip address 2.2.2.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 tunnel 1
```

#### Configuration of Cisco device:

```
!
hostname Cisco
```

#### # Define an IKE policy, using the pre-shared key for authentication, and using the default values for other parameters

```
crypto isakmp policy 1
authentication pre-share
encryption 3des
```

#### # Configure the pre-shared key

```
crypto isakmp key 0 123 address 192.168.202.1
```

#### # Define a transform set

```
crypto ipsec transform-set t1 esp-des esp-md5-hmac
mode transport
```

#### # Define a crypto map

```
crypto ipsec profile profile-name
set transform-set t1
!
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

#### # Apply the crypto map to the tunnel interface

```
interface tunnel 1
tunnel source 192.168.12.1
tunnel destination 192.168.202.1
tunnel protection ipsec profile profile-map
ip address 2.2.2.1 255.255.255.0
!
```

### Applying the Profile map to an IPSEC-IPV4 tunnel

#### Configuration of Router A:

```
!
hostname "RouterA"
```

#### # Enable IKE

```
crypto isakmp enable
crypto isakmp policy 1
authentication pre-share
encryption 3des
```

#### # Configure a pre-shared key and a transform set

```
crypto isakmp key 0 123 address 192.168.12.1
crypto ipsec transform-set t1 esp-des esp-md5-hmac
mode transport
```

#### # Define a crypto map set

```
crypto ipsec profile profi-map
set transform-set t1
match any
!
interface FastEthernet0
ip address 192.168.202.1 255.255.255.0
# Apply the crypto map to the tunnel interface
interface tunnel 1
    tunnel mode ipip
    tunnel source 192.168.202.1
    tunnel destination 192.168.12.1
    tunnel protection ipsec profile profile-map
ip address 2.2.2.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 tunnel 1
```

Configuration of Cisco device:

```
!
hostname Cisco
```

#### # Define an IKE policy, using the pre-shared key for authentication, and using the default values for other parameters

```
crypto isakmp policy 1
authentication pre-share
encryption 3des
```

#### # Configure a pre-shared key

```
crypto isakmp key 0 123 address 192.168.202.1
```

#### # Define a transform set

```
crypto ipsec transform-set t1 esp-des esp-md5-hmac
mode transport
```

#### # Define a crypto map

```
crypto ipsec profile profile-name
set transform-set t1
!
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

#### # Apply the crypto map to the tunnel interface

```
interface tunnel 1
tunnel mode ipsec ipv4
tunnel source 192.168.12.1
tunnel destination 192.168.202.1
tunnel protection ipsec profile profile-map
ip address 2.2.2.1 255.255.255.0
```

### Applying the Profile map to an IPV6 tunnel

Configuration of Router A:

```
!  
hostname "RouterA"  
  
# Enable IKE  
  
crypto isakmp enable  
crypto isakmp policy 1  
authentication pre-share  
encryption 3des  
  
# Configure a pre-shared key and a transform set  
  
crypto isakmp key 0 123 ipv6  ::/0  
crypto ipsec transform-set t1  esp-des esp-md5-hmac  
mode transport  
  
# Define a crypto map set  
  
crypto ipsec profile profi-map  
set transform-set t1  
match any  
!  
interface FastEthernet0  
ipv6 address 1111:1111::2/96  
# Apply the crypto map to the tunnel interface  
interface tunnel 1  
    tunnel mode ipv6  
tunnel source 1111:1111::2  
tunnel destination 1111:1111::1  
tunnel protection ipsec profile profile-map  
ipv6 address 2222:2222::2/96  
!  
ipv6 route ::/0 tunnel 1
```

**Configuration of Cisco device:**

```
!  
hostname Cisco  
  
# Define an IKE policy, using the pre-shared key for authentication, and using the default values for other  
parameters  
  
crypto isakmp policy 1  
authentication pre-share  
encryption 3des  
# Configure a pre-shared key  
crypto isakmp key 0 123 ipv6  ::/0  
crypto ipsec transform-set t1  esp-des esp-md5-hmac  
mode transport  
  
# Define a crypto map set  
  
crypto ipsec profile profi-map  
set transform-set t1  
!  
interface FastEthernet0  
ipv6 address 1111:1111::1/96  
# Apply the crypto map to the tunnel interface  
interface tunnel 1  
    tunnel mode ipv6  
tunnel source 1111:1111::1  
tunnel destination 1111:1111::2  
tunnel protection ipsec profile profile-map  
ipv6 address 2222:2222::1/96
```



## Applying the Profile map to an IPIP tunnel when NAT is available

Configuration of Router A:

```
!  
hostname "RouterA"  
  
# Enable IKE  
crypto isakmp enable  
crypto isakmp policy 1  
authentication pre-share  
encryption 3des  
  
# Configure a pre-shared key and a transform set  
crypto isakmp key 0 123 address 192.168.12.1  
crypto ipsec transform-set t1 esp-des esp-md5-hmac  
mode transport  
  
# Define a crypto map set  
crypto ipsec profile profi-map  
set transform-set t1  
!  
interface FastEthernet0  
ip address 192.168.202.1 255.255.255.0  
  
# Apply the crypto map to the GRE tunnel interface  
interface tunnel 1  
    tunnel mode ipip  
tunnel source 192.168.202.1  
tunnel destination 192.168.12.1  
tunnel protection ipsec profile profi-map  
ip address 2.2.2.2 255.255.255.0  
!  
ip route 0.0.0.0 0.0.0.0 tunnel 1
```

Configuration of the NAT device:

```
hostname "NAT"  
  
#An ACL for NAT translation  
ip access standard 1  
10 permit any  
!  
  
#Connected to Router A  
interface FastEthernet 0/0  
ip address 192.168.202.2 255.255.255.0  
ip nat inside  
!  
  
#Connected to Router B  
interface FastEthernet0/1  
ip add 192.168.12.2 255.255.255.0  
ip nat outside  
!  
  
#NAT translation rule, translating the source IP address of packets through F0/0 into the IP address of F0/1  
ip nat inside source list 1 interface fastEthernet 0/1  
!
```

Configuration of Cisco device:

```
!
```

```
hostname Cisco
```

# Define an IKE policy, using the pre-shared key for authentication, and using the default values for other parameters

```
crypto isakmp policy 1
authentication pre-share
encryption 3des
```

# Configure a pre-shared key

```
crypto isakmp key 0 123 address 192.168.202.1
```

# Define a transform set

```
crypto ipsec transform-set t1 esp-des esp-md5-hmac
mode transport
```

# Define a crypto map

```
crypto ipsec profile profile-name
set transform-set t1
!
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

# Apply the crypto map to the tunnel interface

```
interface tunnel 1
 tunnel mode ipip
 tunnel source 192.168.12.1
 tunnel destination 192.168.12.2
 tunnel protection ipsec profile profile-map
 ip address 2.2.2.1 255.255.255.0
!
```

### Applying the Profile map to an IPSEC-Ipv4 tunnel when NAT is available

Configuration of Router A:

```
!
hostname "RouterA"
```

# Enable IKE

```
crypto isakmp enable
crypto isakmp policy 1
authentication pre-share
encryption 3des
```

# Configure a pre-shared key and a transform set

```
crypto isakmp key 0 123 address 192.168.12.1
crypto ipsec transform-set t1 esp-des esp-md5-hmac
mode transport
```

# Define a crypto map set

```
crypto ipsec profile profi-map
set transform-set t1
match any
!
interface FastEthernet0
ip address 192.168.202.1 255.255.255.0
```

# Apply the crypto map to the GRE tunnel interface

```
interface tunnel 1
 tunnel mode ipip
 tunnel source 192.168.202.1
 tunnel destination 192.168.12.1
```

```
tunnel protection ipsec profile profile-map
ip address 2.2.2.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 tunnel 1
```

Configuration of the NAT device:

```
hostname "NAT"
```

#An ACL for NAT translation

```
ip access standard 1
10 permit any
!
```

#Connected to Router A

```
interface FastEthernet 0/0
ip address 192.168.202.2 255.255.255.0
ip nat inside
!
```

#Connected to Router B

```
interface FastEthernet0/1
ip add 192.168.12.2 255.255.255.0
ip nat outside
!
```

#NAT translation rule, translating the source IP address of packets through F0/0 into the IP address of F0/1

```
ip nat inside source list 1 interface fastEthernet 0/1
!
```

Configuration of Cisco device:

```
!
hostname Cisco
```

# Define an IKE policy, using the pre-shared key as the authentication method, and using the default values for other parameters

```
crypto isakmp policy 1
authentication pre-share
encryption 3des
```

# Configure a pre-shared key

```
crypto isakmp key 0 123 address 192.168.202.1
```

# Define a transform set

```
crypto ipsec transform-set t1 esp-des esp-md5-hmac
mode transport
```

# Define a crypto map

```
crypto ipsec profile profile-name
set transform-set t1
!
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

# Apply the crypto map to the tunnel interface

```
interface tunnel 1
tunnel mode ipsec ipv4
tunnel source 192.168.12.1
tunnel destination 192.168.12.2
tunnel protection ipsec profile profile-map
```

```
ip address 2.2.2.1 255.255.255.0
!
```

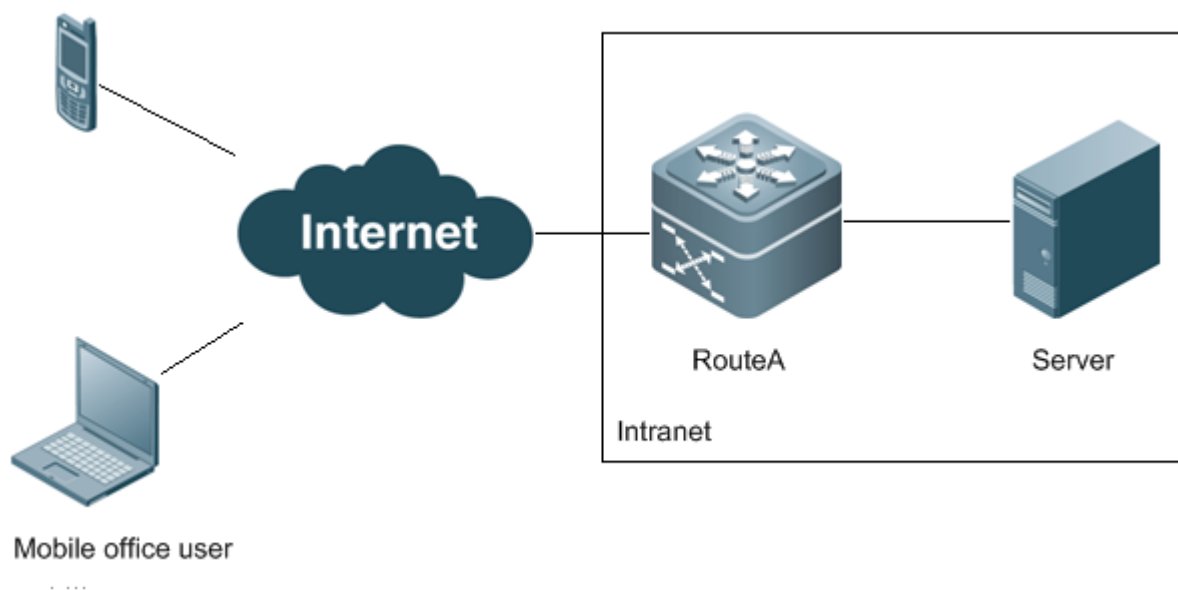
### Extended authentication

#### ■ Analysis

In this case, a mobile office user wants to establish an IPSec connection with Route A through Internet for access to intranet resources, as shown in Figure 9. The following requirements should be met:

- Authentication is required.
- IPSec policies are dynamically downloaded to clients.

Figure 17



Configuration of Route A:

#### # Configure AAA authentication

```
aaa new-model
```

#### # Configure local authentication

```
aaa authentication login lab-remote-access local
```

#### # Configure the username and password for authentication

```
username Qtech password 0 Qtech
```

#### # Configure an IKE policy

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
```

#### # Configure an IKE address pool

```
crypto isakmp ippool Remote-Pool
 address 172.16.1.200 172.16.1.250
```

#### # Configure a policy to be delivered to clients

```
crypto isakmp client configuration group test
 key VPNKEY
 dns 220.170.0.18
 pool Remote-Pool
 network center 192.168.52.0/24
```

## # Configure a transform set

```
crypto ipsec transform-set VPNTRANSFORM esp-3des esp-sha-hmac
```

## # Define a dynamic crypto map set

```
crypto dynamic-map Dynamic-Map 10
set transform-set VPNTRANSFORM
reverse-route
```

## # Use AAA authentication

```
crypto map ClientMap client authentication list lab-remote-access
```

## # Add a dynamic crypto map set to the static crypto map set

```
crypto map ClientMap 65535 ipsec-isakmp dynamic Dynamic-Map
```

## # Apply the crypto map to the interface

```
interface FastEthernet0/0
ip address 61.168.202.1 255.255.255.0
crypto map ClientMap
!
interface FastEthernet0/1
ip address 192.168.202.1 255.255.255.0
```

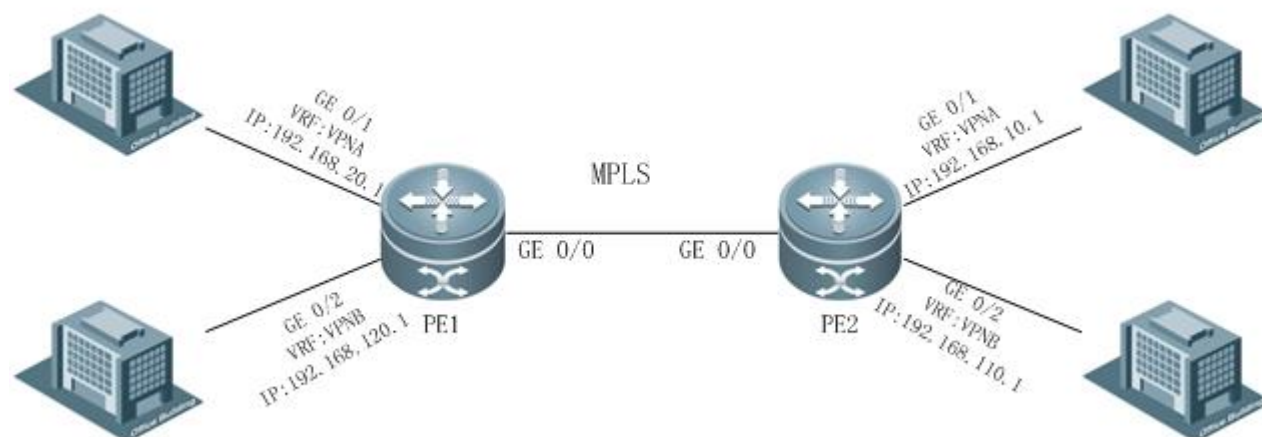
**3.3.4.7 IPSEC OVER MPLS****Analysis**

MPLS on E-government extranet connects networks of official organs. To enhance MPLS networking security, encryption protection is adopted for network communication data. The following requirements should be met:

The data transferring on MPLS networks must be encrypted by IPSec.

To make sure the IPSEC encryption do not interfere with data transferring on MPLS networks, adopt IPSEC OVER MPLS.

Figure 18



PE1:

## # configure VRF

```
ip vrf VPNA
rd 1:100
route-target both 1:100
!
```

```
ip vrf VPNB
rd 1:200
route-target both 1:200
```

#### # configure MPLS network

```
mpls ip
interface Loopback 0
 ip address 172.168.0.1 255.255.255.255
router bgp 1
 bgp log-neighbor-changes
 neighbor 172.168.0.2 remote-as 1
 neighbor 172.168.0.2 update-source Loopback 0
 !
 address-family ipv4
  neighbor 172.168.0.2 activate
 exit-address-family
 !
 address-family vpnv4 unicast
  neighbor 172.168.0.2 activate
  neighbor 172.168.0.2 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf VPNA
  maximum-prefix 10000
  redistribute connected
  neighbor 172.168.10.2 remote-as 65002
  neighbor 172.168.10.2 activate
 exit-address-family
 !
 address-family ipv4 vrf VPNB
  maximum-prefix 10000
  redistribute connected
  neighbor 172.168.10.2 remote-as 65002
  neighbor 172.168.10.2 activate
 exit-address-family
 !
 !
router ospf 10
 network 172.168.0.1 0.0.0.0 area 0
 network 172.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.120.0 0.0.0.255 area 0!
 !
mpls router ldp
 ldp router-id interface Loopback 0 force
```

#### # configure IPSEC

```
ip access-list extended 110
 10 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
 !
 !
ip access-list extended 111
 10 permit ip 192.168.120.0 0.0.0.255 192.168.110.0 0.0.0.255
 !
crypto isakmp policy 1
 encryption 3des
 authentication pre-share
 !
crypto ipsec transform-set myset esp-3des esp-sha-hmac
 !
crypto map mymap1 1 ipsec-isakmp
 set local 192.168.20.2
 set peer 192.168.10.2
```



```
set transform-set myset
match vrf VPNA
match address 110
!
crypto map mymap1 2 ipsec-isakmp
set local 192.168.120.2
set peer 192.168.110.2
set transform-set myset
match vrf VPNB
match address 111
!
interface GigabitEthernet 0/0
ip address 172.168.10.1 255.255.255.0
label-switching
mpls ip
crypto map mymap
duplex auto
speed auto
!
interface GigabitEthernet 0/1
ip vrf forwarding VPNA
ip address 192.168.20.2 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet 0/1
ip vrf forwarding VPNB
ip address 192.168.120.2 255.255.255.0
duplex auto
speed auto
```

PE2:

#### # configure VRF

```
ip vrf VPNA
rd 1:100
route-target both 1:100
!
ip vrf VPNB
rd 1:200
route-target both 1:200
```

#### # configure MPLS network

```
mpls ip
!
router bgp 1
bgp log-neighbor-changes
neighbor 172.168.0.1 remote-as 1
neighbor 172.168.0.1 update-source Loopback 0
!
address-family ipv4
neighbor 172.168.0.1 activate
exit-address-family
!
address-family vpnv4 unicast
neighbor 172.168.0.1 activate
neighbor 172.168.0.1 send-community extended
exit-address-family
!
address-family ipv4 vrf VPNA
maximum-prefix 10000
redistribute connected
neighbor 172.168.10.1 remote-as 65002
```

```
neighbor 172.168.10.1 activate
exit-address-family
!
address-family ipv4 vrf VPNB
maximum-prefix 10000
redistribute connected
neighbor 172.168.10.1 remote-as 65002
neighbor 172.168.10.1 activate
exit-address-family
!
!
!
!
router ospf 10
network 172.168.0.2 0.0.0.0 area 0
network 172.168.10.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.255 area 0
network 192.168.110.0 0.0.0.255 area 0
!
!
!
!
mpls router ldp
ldp router-id interface Loopback 0 force
```

#### # configure IPSEC

```
crypto isakmp policy 1
encryption 3des
authentication pre-share
!
!
crypto isakmp key 7 021211644c536854774c address 0.0.0.0 0.0.0.0
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto dynamic-map dy 1
set transform-set myset
reverse-route
!
crypto map mymap 1 ipsec-isakmp dynamic dy
!
interface GigabitEthernet 0/0
ip address 172.168.10.1 255.255.255.0
label-switching
mpls ip
crypto map mymap
duplex auto
speed auto
!
interface GigabitEthernet 0/1
ip vrf forwarding VPNA
ip address 192.168.10.2 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet 0/1
ip vrf forwarding VPNB
ip address 192.168.110.2 255.255.255.0
duplex auto
speed auto
```

## 4 CONFIGURING THE DIGITAL CERTIFICATE

### 4.1 Overview

To ensure the security, authenticity, reliability, integrity and non-repudiation of the information transmitted between clients over network, the identity of clients must be verified, while the digital certificate is one of the methods to realize this function. PKI digital certificate technology associates the identity of individual or entity with a public key, and centrally issues the certificate through Certificate Authority (CA) to guarantee the validity and security of certificates. The digital certificates are electronic files issued by CA and binding the identity, public key and CA signature of the entity, with public key and private key forming a key pair in the public key cryptography system. Both sides of communication verify the validity of the certificate through CA signature in digital certificate, and use the public key contained in the certificate to verify the digital signature created by the peer device using the private key, thus completing authentication. There are two types of digital certificates: X.509 certificates and PGP certificates. X.509 certificates are supported by Qtech products.

Digital certificates can be used in the IKE negotiation and SSL of IPSec. Certificate authentication can be used in the IKE configuration of IPSec and boasts the following merits:

- Higher security than PSK
- No need to separately configure PSK between every two peers of communication (easy to use)
- Security problems caused by key compromise can be addressed through certificate revocation.
- Use of overdue keys can be avoided by controlling the duration of key pairs through certificate validity

The X.509 certificate on the router can be acquired manually and through SCEP protocol. The merits of using the SCEP protocol to acquire the digital certificate of the router are shown below:

- The private key remains in the cryptographic equipment, ensuring higher security.
- The SCEP protocol adopts PKCS7 digital envelop during communication, ensuring the security of communication process.
- Supported by CA, SCEP is capable of updating digital certificates automatically.

#### 4.1.1 Terminology

**Public-Key Infrastructure (PKI)** is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

**X.509:** X.509 is an international standard recommended by ITU-T, and defines a widely accepted PKI, including data format and the process of public key distribution through the digital certificate issued by CA.

**CA:** As an authoritative, trustworthy and impartial third-party organization, CA is responsible for issuing and managing the digital certificates of all entities participating in online transaction. It effectively manages the key and issues digital certificates to prove the validity of such key, and associates the public key with one entity.

**Root CA: CA at the top of the hierarchy.**

**Certificate or digital certificate:** In this chapter, it refers to X.509 certificate (data structure defined by X.509), and is used to associate an entity with a public key to indicate the identity of the entity. A certificate contains a public key, name and digital signature of CA. Generally, the certificate also contains the validity period of the key, name of CA, serial number and etc, with format complying with ITUT X.509 standard.

**CA root certificate:** the self-signed certificate issued by root CA for itself; it is used to sign the other certificates issued by root CA.

**Privacy-enhanced Mail (PEM):** base64 encoded text format defined in RFC 1421-RFC 1424; generally used for e-mail and certificate import/export.

**PKCS:** A group of public-key cryptography standards devised and published by RSA Security, and is a widely-applied industry standard in information transfer. PKCS#1 defines a RSA encryption and signature algorithm; PKCS#7 defines a syntactic representation of enciphered message; PKCS#12 defines a method to create the security archive (PKCS12 can contain certificate, private key and other security achieves, and is a commonly used format for issuing certificates). The files exported in PKCS format are DER encoded binary files, and sometimes need to be converted into PEM encoded text files.

**Certificate Revocation List (CRL):** a list with time stamp to specify the certificates revoked by a CA. It can be freely obtained from the public directory, and is one of the two methods specified by Internet Public-Key Infrastructure

(X.509) working group (PKIX) to check certificate state. Each certificate in the CRL is identified using its serial number. Therefore, by querying the serial number of certificate in the recently released CRL, the user's certificate system can check whether a certificate has been revoked; if the certificate is contained in CRL, then the certificate should be rejected. X.509 version 2 CRL contains version number, issuer DN (globally unique), validity period, serial number of the revoked certificate, time of revocation, reason of revocation, the algorithm for CA to issue this CRL and the signature thereof.

**Simple Certificate Enrollment Protocol (SCEP):** A draft protocol defined by Cisco to securely apply for a certificate for the router from CA. It is currently deployed on various network devices.

## 4.2 Configuring CA Server and Applying for & Exporting a Certificate

### 4.2.1 Installing the Certificate Services on a Windows 2003 Server

Step 1: Select Add/Remove Programs in Control Panel and click Add/Remove Windows Components.

Step 2: Select **Certificate Services** in the pop-up window.

Step 3: Click **Next** and select **Stand-alone root CA** in the pop-up window.

Step 4: Click **Next** and fill in CA related information.

Step 5: Click **Next** and set a database directory (or use the default path).

Step 6: Click **Next** to install the certificate services.

### 4.2.2 Setting Up CA Server on IIS

Step 1: Select Add/Remove Programs and click Add/Remove Windows Components.

Step 2: Select **Application Server** and then click **Details**.

Step 3: Select **Internet information services (IIS)** and then click **Details**.

Step 4: Select **World Wide Web Service** and then click **Details**.

Step 5: In the following dialog box, select **Active Server Pages** and **World Wide Web Service** and click **OK** for three times. If **World Wide Web Publishing Service** is selected, **Common Files** and **Internet Service Manager** will be selected as well by default.

Step 6: Return to the main window and click **Next** to proceed with installation.

Step 7: Enter Control Panel and select Administrative Tools; select Internet Services Manager.

Step 8: Right-click the default website.

Step 9: Select **Virtual Directory**, as shown below.

Step 10: Click **Next** and enter the alias of the virtual directory.

Step 11: Click **Next** and configure a content directory.

Step 12: Click the **Browse** button and select the directory for installing certificate services.

**Note**

On a Windows 2003 server, the installation directory of certificate services is shown below:

---

Step 13: Click **Next** and complete virtual directory configuration using default settings.

Step 14: Start the Internet explorer on the CA server and type in "127.0.0.1/Cert\_Server".

### 4.2.3 Applying for and Exporting a Certificate

Currently, certificates to be installed on Qtech routers are acquired on the PC. Suppose the IP address of a CA server is 192.168.64.130. Perform the following steps to apply for a certificate.

Step 1: Start the Internet explorer on a client (usually a PC) and type in "192.168.64.130/Cert\_Server".

Step 2: Click **Next** and select **Advanced Application** as the application type.

Step 3: Click **Next** and select a method of submitting an application (using a form).

Step 4: Click **Next** and fill in detailed information.



#### Note

**Mark keys as exportable** must be checked, as RSA key pairs applicable to Qtech routers are generated by a CA server, and certificates and key pairs must be exported eventually.

---

Step 5: Click **Submit** to complete certificate application.

Step 6: Return to homepage and select **Check on a pending certificate**.

Step 7: Click **Next**. If the CA center has issued a certificate, the certificate is displayed.

Step 8: Click **Next** and prepare to install this certificate, as shown below:

Step 9: Click **Install this certificate**. The system will prompt that this certificate is successfully installed.

Step 10: After installation of a certificate, the certificate needs to be exported.

Step 11: Select **Internet Options** and click the **Content** tab.

Step 12: Click the **Certificate** button.

Step 13: Select the certificate to be exported and click **Export**:

Step 14: Click **Next**.

Step 15: Click **Next**.



#### Note

**Include all certificates in the certification path if possible** must be checked. This export certificate file contains the issued certificate, private key and CA root certificate.

---

Step 16: Click **Next** and enter a file protection password.

Step 17: Click **Next** and enter the name of the file saving this certificate.

Step 18: Click **Next** and confirm the information, and then Click **Finish** to export the certificate.

Step 19: The certificate is exported as a pfx file. Then you need to convert the pfx file into a pem file by using "pfx2pem" tool available in the CD-ROM.

Step 20: Click **Convert**,

By this time, you will find the converted pem file in the corresponding directory. Use the Wordpad program to open this pem file; you will find the private key, certificate and the corresponding root certificate.



#### Caution

The password of source file is the password entered while exporting the certificate on IE; the password of the target file is the password you need to set currently. This password must be entered when you import the certificate to a device. See the "Exporting a certificate" section.

---

#### 4.2.4 Configuring the URL of CRL

After the certificate services are installed, the default URLs of CRL are:

http://%SERVER\_DNS\_NAME%/CertEnroll/%CA\_NAME%%CRL\_SUFFIX%.cr

file://\%SERVER\_DNS\_NAME%\CertEnroll\%CA\_NAME%%CRL\_SUFFIX%.cr

Where, the default value of %SERVER\_DNS\_NAME% is the hostname of this system rather than the domain name or IP address; if the domain name or stationary IP address must be used, CA server configurations must be changed. To change CA server configurations, perform the following steps:

Step 1: Select **Control Panel** and double-click **Administrative Tools**, and select **Certification Authority**.

Step 2: Right-click **CA Server**.

Step 3: Select **Properties** and click the **Policy Module** tab in the pop-up window.

Step 4: Click **Configure** and click the **X.509 Extensions** tab in the **Properties** window.

Step 5: Click **Add CDP**.

Step 6: Click **OK** to add a new CRL address

Example:

To specify an IP address:

Type in: http://192.168.64.130/CertEnroll/%CA\_NAME%%CRL\_SUFFIX%.cr

Type in: file://192.168.64.130\CertEnroll\%CA\_NAME%%CRL\_SUFFIX%.cr

To specify a domain name:

Type in: http://www.qtech.ru/CertEnroll/%CA\_NAME%%CRL\_SUFFIX%.cr

Type in: file://\www.qtech.ru\CertEnroll\%CA\_NAME%%CRL\_SUFFIX%.cr

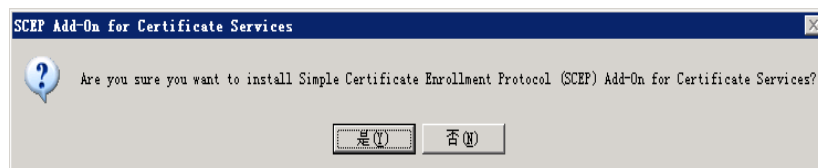


#### Note

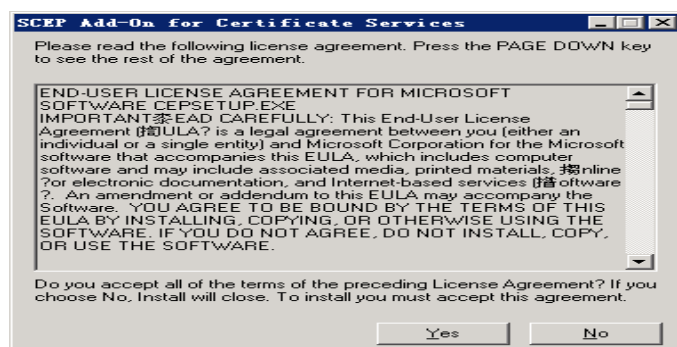
Currently, only the first CRL address is considered valid on Qtech routers. Therefore, the desired CRL address should be placed on the top.

#### 4.2.5 Installing SCEP Add-on

Step 1: Download the SCEP add-on for Windows Server 2003 from the following website: <http://go.microsoft.com/fwlink/?LinkId=32060>, and then double-click it to install.



Step 2: Click **Yes** to accept the license agreement.

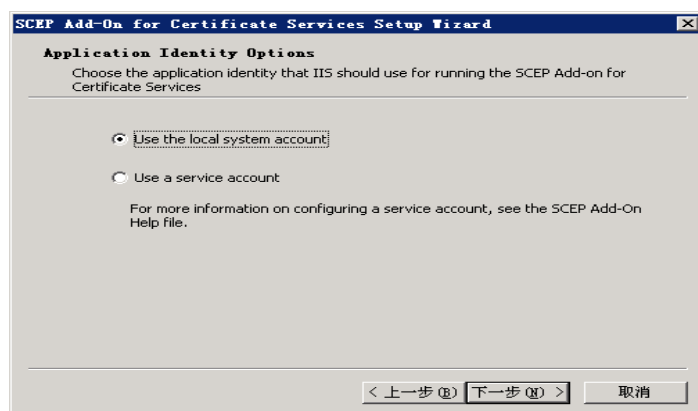




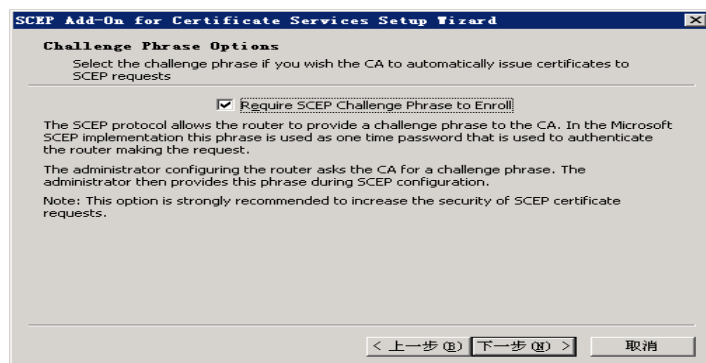
Step 3: Click **Next** to proceed with installation.



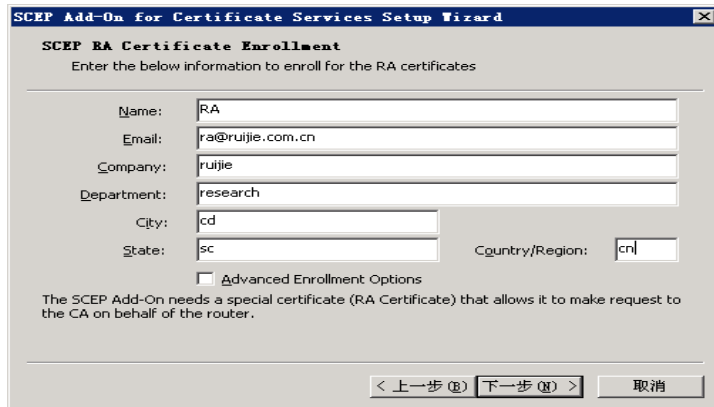
Step 4: Select **Use the local system account** and then click **Next**.



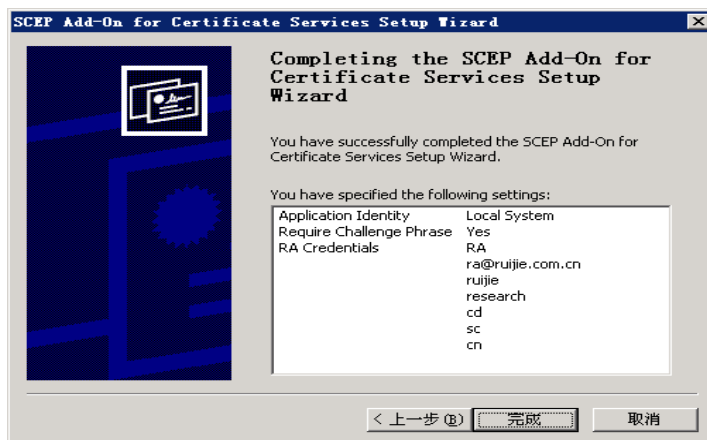
Step 5: It is suggested that you check **Require SCEP Challenge Phrase to Enroll**. After the device is ready to use CA to enroll, visit <http://ca/certsrv/mscep/msdep.dll> (from any client). The user will be required to provide the "passphrase" needed for enrollment. The "passphrase" is effective within 60 minutes. Click **Next**.



Step 6: Click **Next**.



Step 7: Check the settings and click **Finish**.



Step 8: The URL used for SCEP enrollment is shown below:



### 4.3 Digital Certificate Configuration

#### 4.3.1 Digital Certificate Configuration Tasks

The purpose of digital certificate configuration is to enable the device to have its own certificate and verify the certificate of the communication peer.

Digital certificate configuration involves the following tasks:

- **Acquire certificate:** Acquire CA root certificate and the router certificate and private key issued directly by this CA. RGOS currently supports offline certificate application. The detailed steps are shown in the "Applying for and Exporting a Certificate" section. It also supports online SCEP certificate application and application for a certificate application file.
- **Import certificate:** Import the CA root certificate and router certificate and private key issued directly by this CA into the device.
- **Acquire router certificate through SCEP:** Acquire router certificate from the specified CA through SCEP.
- **Certificate configuration command (optional):** Configure a certificate chain and configure a certificate by importing binary certificate file (DER formatted file) in hexadecimal format.
- **Configure certificate revocation checking policy (optional):** Configure whether to check CRL during certificate check in order to verify whether the certificate has been revoked.

- Download CRL (optional):** Configure the URL for downloading a CRL and start CRL download immediately through the command.

### 4.3.2 Importing a Certificate

Through the aforementioned steps, you may have acquired PEM-formatted CA root certificate, router certificate and private key. Run the following commands in global configuration mode to import these contents into the device:

Command	Function
Qtech(config)# <b>crypto pki import pem terminal password [id string]</b>	Starts the interactive process to import CA root certificate, router certificate and private key. Password refers to the protective password of PEM-formatted private key. For details, see the "Applying for and Exporting a Certificate" section.



**Caution**

**Caution** The system will check certificate validity during the import process, and expired or inactive certificates will not be imported. Therefore, before importing a certificate, you must check whether the system time is the current Beijing time. To change system time, you can use the **clock** or **calendar** command. Refer to the "Basic System Management" chapter of *Basic Configuration Guide* for details. If the certificate is sm2, you need to set the ID. You can use the **crypto pki sm2-identity** command in global configuration mode to configure the ID.

Certificate import interface and process are shown below:

Assuming that PEM-formatted certificate data you acquired have been archived in one file, use a text editor (Windows Wordpad is recommended) to open the file and you will see the following contents:

```

Bag Attributes
localKeyID: 01 00 00 00
1.3.6.1.4.1.311.17.1: Microsoft Base Cryptographic Provider v1.0
friendlyName: 0929c7381e7517bdc65cdc7cc2ea0374_60e7aaa8-2e04-4953-9ba8-96bcaf0bdfd7
Key Attributes
X509v3 Key Usage: 10
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, 251F9D955610C376
GDG2slmbs/MJCpo5w2bu972jKlOZYtv3RQunH4I29c9H5uq3LtyvNA9RwrlpRQ3t
iUmkvQrU3/6SBp4Rqx1EU2UWgv1KRqqYwRVbdPdBZYVJLrso3Ov/9eaS4TiD+4Dl
NfJlsAA4OONdVKDCLcGZIB43Wq5rAlqzsyjcf6tx3fWssankVjQfroTv7UvP+ijj
uGndmJwbXEiATxlt+Smvt2/CGjr8nIC55T1W+tW0itkBdZhnvBJekOFM4BdgoLZc
3vueTIHmTurHvvdLYtYjQHsxVsf3vRGMcQhohM98nAYsIDBil40Ih1hc+ZnhGsn
TFLPMmMuJnBWMYopfaMPNrcdbpu+n4Qj2QiRoVTEoI7P1IAY/Oa2uc+kDuUX3KlW
sQQPnFNiU0Q/T9BrsolxI2Wkak7cvaNxbmhuU+5wNUGybQfcfP3CWg==
-----END RSA PRIVATE KEY-----
Bag Attributes
localKeyID: 01 00 00 00
subject=/Email=dingjs@star-net.cn/C=CN/ST=FuJian/L=FuZhou/O=Regiant Network Co.
Ltd/OU=Research Apartment 5/CN=dingjs
issuer=/Email=dingjs@star-net.cn/C=CN/ST=FuJian/L=FuZhou/O=Regiant Network Co.
Ltd/OU=Research Apartment 5/CN=CA test server
-----BEGIN CERTIFICATE-----
MIIEsTCBfugAwIBAgIkeffFwABAAAAPjANBgkqhkiG9w0BAQUFADCBrdEhMB8G
CSqGSIb3DQEJARYSZGluZ2pzQHN0YXItbmV0LmNumQswCQYDVQQGEwJDTjEPMA0G
A1UECBMGRnVKaWFuMQ8wDQYDVQQHEwZGdVpob3UxIDAeBgNVBAoTF1JlZ2lhbncQ
TmV0d29yayBDby4gTHRkMR0wGwYDVQQLEwRSZXNlYXJjaCBBCGFydG11bnQgNTEEX
MBUGA1UEAxMOQ00EgdGVzdCBzZXJ2ZXIwHhcNMDUwNDEyMDkyOTUzWhcNMDYwNDEy
MDkzOTUzWjCBPDEhMB8GCsqGSIb3DQEJARYSZGluZ2pzQHN0YXItbmV0LmNumQsw
CQYDVQQGEwJDTjEPMA0GA1UECBMGRnVKaWFuMQ8wDQYDVQQHEwZGdVpob3UxIDAe
BgNVBAoTF1JlZ2lhbncQTMV0d29yayBDby4gTHRkMR0wGwYDVQQLEwRSZXNlYXJja
aCBBCGFydG11bnQgNTEEXMBUGA1UEAxMGZGluZ2pzZmFwdDQYJKoZIhvcNAQEBBQAD
SwAwSAJBAM0sOymB/5v35vnf/P1JX+aqZpH9drtevsNaHkj4i3XdaJ55rFo2wLT0
    
```

```

qpWTI0nu638ktUa4dEIff0AQM67sP0ECAwEAAaOCAMwggJfMA4GA1UdDwEB/wQE
AwIE8DATBgNVHSUEDDAKBggrBgEFBQgCAjAdBgNVHQ4EFgQUiWVn8+ciY7JjkOFN
7MIkcRWWpx8wgawgITAFBgqhkiG9w0BCQEQEWEmRpbmdqc0BzdGFyLW5ldC5jbjELMAkGA1UE
BhMCQ04xDzANBgNVBAGTBkZ1Sm1hbJEPMA0GA1UEBxMGRnVaaG91MSAwHgYDVQK
ExdSZWdpYW50IE5ldHdvcmsgQ28uIEEx0ZDEdMBSGA1UECXMUUmVzZWZyY2ggQXBh
cnRtZW50IDUxXzFzAVBgNVBAMTDkNBTHRlc3Qgc2VydMvYghBWRgc8EKF+jEWUjT8V
UjNXMH8GA1UdHwR4MHYwOKA2oDSGMmh0dHA6Ly96aileyb3V0ZXIvQ2VydEVucm9s
bc9DQSUyMHRlc3Q1MjBzZXJ2ZXIuY3JsMDqgOKA2hjRmaWxlOi8vXFx6aileyb3V0
ZXJcQ2VydEVucm9sbFxDQSUyMHRlc3Q1MjBzZXJ2ZXIuY3JsMIGsBggrBgEFBQcB
AQSBNzCBnDBLBggrBgEFBQcwoY/aHR0cDovL3pqLXJvdXRlcj9DZXJ0RW5yb2xs
L3pqLXJvdXRlcj9DQSUyMHRlc3Q1MjBzZXJ2ZXIOMSkuy3J0ME0GCCSGAQUFBzAC
hkFmaWxlOi8vXFx6aileyb3V0ZXJcQ2VydEVucm9sbFxDQSUyMHRlc3V0ZXJfQ0ElMjB0
ZXN0JTlwc2VydMvYkDEpLmNydDANBgkqhkiG9w0BAQUFAANBABSSEeYlEi7fm06en
NDdkZmJyYV8LZlB1JjniePwylsUEEDA2bH9ZrcpTnJ+CskCkxXBtC5ZWZnFTiSH/Oc
uVyQ9D8=
-----END CERTIFICATE-----
Bag Attributes: <Empty Attributes>
subject=/Email=dingjs@star-net.cn/C=CN/ST=FuJian/L=FuZhou/O=Regiant Network Co.
Ltd/OU=Research Apartment 5/CN=CA test server
issuer=/Email=dingjs@star-net.cn/C=CN/ST=FuJian/L=FuZhou/O=Regiant Network Co.
Ltd/OU=Research Apartment 5/CN=CA test server
-----BEGIN CERTIFICATE-----
MIIDLjCCAtigAwIBAgIQVq4HPBChfoxFro0/FVIzVzANBgkqhkiG9w0BAQUFADCB
rDEhMB8GCSqGSIb3DQEJARYSZGluZ2pzQHN0YXItbmV0LmNlMjBzZXJ2ZXIuY3JsMDqg
TjEPMAG0GA1UECBMGRnVkaWwzQ2VydVQHEwZGdVpob3UxIDAeBgNVBAoTF1Jl
Z21hbnQgTmV0d29yayBDbj4gTHRkMR0wGwYDVQQLZXN1YXJjaCBBCGFydG1l
bnQgNTEYMBUGA1UEAxMQ0EgdGVzdCBzZXJ2ZXIwHhcNMDUwMjI1MDg0NjA5WWhc
MDcwMzAxMDIzNjIzWjBjCBrDEhMB8GCSqGSIb3DQEJARYSZGluZ2pzQHN0YXItbmV0
LmNlMjBzZXJ2ZXIuY3JsMDqgTjEPMAG0GA1UECBMGRnVkaWwzQ2VydVQHEwZGdVp
ob3UxIDAeBgNVBAoTF1JlZ21hbnQgTmV0d29yayBDbj4gTHRkMR0wGwYDVQQLZXN1
YXJjaCBBCGFydG1lbnQgNTEYMBUGA1UEAxMQ0EgdGVzdCBzZXJ2ZXIwXDAN
BgkqhkiG9w0BAQEFAANLADBIAkEA2R8axg75UZJM3JZNREP62r5T8t31E7Y0taah
n/1XoWxvevShE8FZPQxMPO5i3nbYokzyLPjagqoX0+jMgMKVjwIDAQABO4HTMIHQ
MASGA1UdDwQEAwIBxjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBRRyQ4QcKwNF
LYJY9YRdd/UhqkssITB/BgNVHR8EeDB2MDigNqA0hjJodHRwOi8vemotcm91dGvy
L0N1cnRFbnJvbGwvQ0ElMjB0ZXN0JTlwc2VydMvYkDEpLmNybDA6oDigNoY0ZmlsZTov
L1xcemotcm91dGvyXEN1cnRFbnJvbGwvQ0ElMjB0ZXN0JTlwc2VydMvYkDEpLmNybDAQ
BgkrBgEEAYI3FQEEAwIBATANBgkqhkiG9w0BAQUFAANBAH8ufRZ2tVYO3R7YC0IF
OzmnQrjgaBN4bpmSLkxYYKtK8Znj0FwUL1laq6nCGp6n8Ks0dijomXnedB2zn0a
f0w=
-----END CERTIFICATE-----

```



**Caution**

**Caution** Where, contents between “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----” are certificate texts; contents between “-----BEGIN RSA PRIVATE KEY-----” and “-----END RSA PRIVATE KEY-----” are private key texts; other contents are descriptions about the PKCS12#format.



**Note**

the difference between CA root certificate and router certificate: The subject and issuer of CA root certificate are the same, while those of router certificate are different. Taking the above-given process as the example, the relevant information about CA root certificate is shown below:

```

subject=/Email=dingjs@star-net.cn/C=CN/ST=FuJian/L=FuZhou/O=Regiant Network Co.
Ltd/OU=Research Apartment 5/CN=CA test server
issuer=/Email=dingjs@star-net.cn/C=CN/ST=FuJian/L=FuZhou/O=Regiant Network Co.
Ltd/OU=Research Apartment 5/CN=CA test server
The subject and issuer of router certificate are shown below:

```





```

-----BEGIN CERTIFICATE-----
MIIEStCCBFugAwIBAgIKEffFFwABAAAAPjANBgkqhkiG9w0BAQUFADCBrDEhMB8G
CSqGSIb3DQEJARYSZGluZ2pzQHNOYXItbmV0LmNumQswCQYDVQGEwJDTjEPMA0G
A1UECBMRnVKAwFuMQ8wDQYDVQQHEwZGdVpob3UxIDAeBgNVBAoTF1JlZ21hbnQg
TmV0d29yayBDby4gTHRkMR0wGwYDVQQLEwRSZXNlYXJjaCBBCGFydG11bnQgNTE
XMBUGA1UEAxMOQ0EgdGVzdCBzZXJ2ZXIwHhcNMDUwNDEyMDkyOTUzWhcNMDYwNDE
yMDkzOTUzWjCBpDEhMB8GCSqGSIb3DQEJARYSZGluZ2pzQHNOYXItbmV0LmNumQsw
CQYDVQGEwJDTjEPMA0G1UECBMRnVKAwFuMQ8wDQYDVQQHEwZGdVpob3UxIDAe
BgNVBAoTF1JlZ21hbnQgTmV0d29yayBDby4gTHRkMR0wGwYDVQQLEwRSZXNlYXJja
aCBBCGFydG11bnQgNTEPMA0G1UEAxMGZGluZ2pzMFwwDQYJKoZIhvcNAQEBBQAD
SwAwSAJBAM0sOymB/5v35vnf/P1JX+aqZpH9drtevsNaHkj4i3XdaJ55rFo2wLT0
qpWTI0nu638ktUa4dEiff0AQM67sP0ECAwEAAaOCAMwggJfMA4GA1UdDwEB/wQE
AwIE8DATBgNVHSUEDDAKBggrBgEFBQgCAjAdBgNVHQ4EFgQUiWVn8+ciY7JkOFN
7MIkcRWWpx8wgegGA1UdIwSB4DCB3YAUckOEHCsDRS2CWPWEQ3f1IapLLCGhgBkK
ga8wgawxITAFBgkqhkiG9w0BCQFEWEmRpbmdqc0BzdGFyLW5ldC5jbjELMAKGA1UE
BhMCQ04xDzANBgNVBAGTBkZ1Sm1hbGJEPMA0G1UEBxMGRnVaaG91MSAwHgYDVQQK
ExdSZWdpYW50IE5ldHdvcmsgQ28uIEEx0ZDEdMBsGA1UECXMUUmVzZWZyY2ggQXBh
cnRtZW50IDUxZmVzAVBgNVBAMTDkNBIEHRlc3Qgc2VydMvYghBWrgc8EKF+jEWujT8V
UjNXMH8GA1UdHwR4MHYwOKA2oDSGMmh0dHA6Ly96a1lyb3V0ZXIvQ2VydEVucm9s
bc9DQSUyMHRlc3Q1MjBzZXJ2ZXIuY3JsMDqgOKA2hjRmaWx1Oi8vXFx6a1lyb3V0
ZXJcQ2VydEVucm9sbFxDQSUyMHRlc3Q1MjBzZXJ2ZXIuY3JsMIGsBggrBgEFBQcB
AQSBNzCBnDBLBggrBgEFBQcwoY/aHR0cDovL3pqLXJvdXRlc3Q1MjBzZXJ2ZXI0MSkuY3J0ME0GCCsGAQUFBzAC
hkFmaWx1Oi8vXFx6a1lyb3V0ZXJcQ2VydEVucm9sbFxDQSUyMHRlc3Q1MjBzZXJ2ZXIvQ2VydEVucm9sbFxDQSUyMHRlc3Q1MjBz
ZXN0JTIwY2VydMvYghBkDEpLmNydDANBgkqhkiG9w0BAQUFAANBABSSEeY1Ei7fm06en
NDdkZmJyV8LZBlJjniePwylsUEEDa2bH9ZrcpTnJ+CSkCkxXBtc5ZWZnFTiSH/Oc
uVyQ9D8=
-----END CERTIFICATE-----
quit
% Certificate successfully imported
Qtech (config)#

```



### Caution

**Caution** Currently, Qtech products can only support one CA root certificate and one router certificate. If another certificate is imported, the previous one is overwritten.

The import is only considered successful when CA root certificate, private key and router certificate are all successfully imported, and device configurations will be updated then, or else all import operations will be cancelled without causing any impact on the configurations. For example, when the import of router certificate fails, the import of CA root certificate and private key will all be cancelled.

While copying and pasting certificate texts, do not omit any character, especially the "begin" and "end" lines.

After successful import, execute the "write" operation to store the certificate and private key into FLASH, or else the import contents will be lost after shutdown.

The fingerprint of CA root certificate is used to avoid the artificial falsification of CA root certificate during the process of transmission. The CA will issue fingerprint information (including fingerprint and the hmac algorithm for fingerprint calculation) together with the CA root certificate. The user of CA root certificate must use the same fingerprint algorithm used by CA to calculate fingerprint, and check with the fingerprint issued by the CA. RGOS supports the fingerprint algorithm of SHA-1.

Verify the result of certificate import. After a successful import, the certificate will be stored in DER-encoded hexadecimal format in the system configuration file. Run the **show running** command to query the serial number and DER encoded contents of the certificate (refer to the "Configuration Example" section), or you can also run the **show crypto pki cert** command (see the "Monitoring and Maintenance" section). Note that the private key will not be displayed.

### 4.3.3 Acquiring Router Certificate Through SCEP

To configure a trustpoint, run the following commands:



Command	Function
Qtech (config)# <b>crypto pki trustpoint</b> <i>CA_name</i>	Enters trustpoint configuration mode. <i>CA_name</i> is the common name of the CA corresponding to this trustpoint, namely the character string entered in the <b>Common name for this CA</b> field in Step 9 of the "Installing the Certificate Services on a Windows 2003 Server" section.
Qtech (ca-trustpoint)# <b>asymmetric</b> sm2	Specifies a certificate algorithm and uses RSA (optional) in a default condition.
Qtech (ca-trustpoint)# <b>enrollment url</b> <i>http://192.168.50.203/certsrv/mscep/mscep.dll</i>	Configures the certificate enrollment URL of this trustpoint, namely the URL shown in step 8 of the "Installing SCEP add-on" section (domain name); if there is no DNS server, an IP address can also be used; manually replace the domain name with the corresponding IP address.
Qtech (ca-trustpoint)# <b>enrollment retry period</b> <i>number</i>	Configures the polling period when this trustpoint enters the polling state during certificate enrollment. Number is a numeric value (unit: minute); the default value is one minute.
Qtech (ca-trustpoint)# <b>enrollment retry count</b> <i>number</i>	Configures the polling count when this trustpoint enters the polling state during certificate enrollment. Number is a numeric value (unit: time); the default value is 60 times.
Qtech (ca-trustpoint)# <b>enrollment auto-enroll</b> <i>percentage</i>	Specifies the update period of the certificate corresponding to the trustpoint; percentage ranges from 1 through 100 to specify when the certificate will be updated.
Qtech (ca-trustpoint)# <b>enrollment renewable</b>	Enables the CA server corresponding to the trustpoint to support certificate update
Qtech (ca-trustpoint)# <b>exit</b>	Exits trustpoint configuration mode.

To acquire a CA root certificate, run the following command:

Command	Function
Qtech (config)# <b>crypto pki authenticate</b> <i>CA_name</i>	Acquires the CA root certificate.

To register a certificate, run the following command:

Command	Function
Qtech (config)# <b>crypto pki enroll</b> <i>CA_name</i>	Enrolls trustpoint and acquires the router certificate corresponding to this trustpoint.

The process of acquiring a router certificate through SCEP is as follows:

Ensure the time matches with standard time on each device. Use the **show clock** command on the router to ensure that the time is correct.

Configure an IP address to ensure that the router can access the CA server.

Configure the hostname of the router

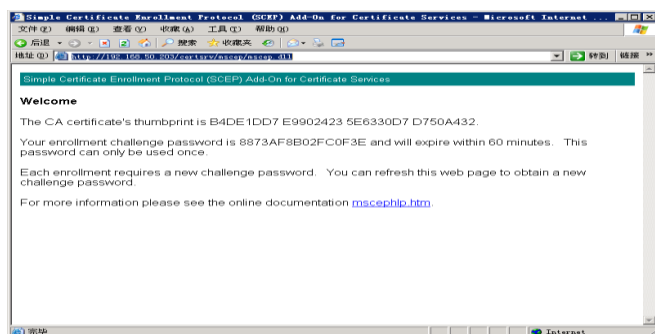
```
Qtech(config)#hostname router
router(config)#
Generate a key
router(config)#crypto pki key generate rsa
generate-key
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus:1024 //Modulus size of the key
Configure the trustpoint corresponding to the CA
router(config)#crypto pki trustpoint CA
router(ca-trustpoint)#enrollment url http://192.168.50.203/certsrv/mscep/mscep.dll
//URL for enrollment
router(ca-trustpoint)#exit
```

Acquire and verify the CA root certificate.

```
router(config)#crypto pki authenticate CA
Certificate has the following attributes:
MD5 fingerprint: B4DE1DD7 E9902423 5E6330D7 D750A432
SHA1 fingerprint: AD070162 672A7C57 BD5EE522 A95AAFA1 351524D0
% Do you accept this certificate?[yes/no]:yes //Enter yes to accept the CA
certificate
Trustpoint CA certificate accepted.
```

To acquire the fingerprint and passphrase of the certificate, visit: <http://ca-ip-address/certsrv/mscep/mscep.dll>.

The following webpage will be displayed, prompting you to proceed with authentication. Make sure that the administrator can visit this website using the fingerprint and passphrase.



Now the fingerprint and passphrase are acquired. You need to enter the following contents on the router (replies from CA are also provided for your reference)

```
router(config)#crypto pki enroll CA
```

```
%
%Start certificate enrollment ..
%Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:F4EEE4FEB3766007 //Enter the password acquired from CA
Re-enter password:F4EEE4FEB3766007
%The subject name in the certificate will include: router
```

Display the state of the trustpoint

```
router(config)#show crypto pki trustpoints CA status
```

```
Trustpoint CA Status:
Issuing CA certificate configured:
Subject Name:
/CN=CA
Fingerprint MD5: B4DE1DD7 E9902423 5E6330D7 D750A432
Fingerprint SHA1: AD070162 672A7C57 BD5EE522 A95AAFA1 351524D0
Router General Purpose certificate pending: Requested Subject Name:
/unstructuredName=router
Request Fingerprint MD5: E8F50E2A 1FB46B00 52C6A9DB CC20AA42
Request Fingerprint SHA1: B1031204 E7A2D547 CC48F0A6 2BAE8420 829637D8
Enrollment polling: 2 times (58 left)
Last enrollment status: Pending //In pending state
State:
Keys generated ..... Generated
Issuing CA authenticated ..... Yes
Certificate request(s) ..... Pending
```

When "Certificate requests pending" shows up (as shown above), check "Pending Requests" on the CA server and issue this certificate. Generally, the request will take 10 to 15 seconds.

Right-click the certificate and choose **All Tasks > Issue**.

The certificate will then be moved to the "Issued Certificate" node. Return to the router console and query trustpoint status.

```
router(config)#show crypto pki trustpoints CA status
```

```
Trustpoint CA Status:
  Issuing CA certificate configured:
    Subject Name:
      /CN=CA
    Fingerprint MD5: B4DE1DD7E 99024235 E6330D7D 750A432
    Fingerprint SHA1: AD070162 672A7C57 BD5EE522 A95AAFA1 351524D0
  Router General Purpose certificate configured:
    Subject Name:
      /unstructuredName=router
    Fingerprint MD5: 7FFF7F4C 225850A3 D0D39EA3 EFAD8D5A
    Fingerprint SHA1: 84E3678C F2DE94DD 63397145 87CDC9C6 1010A82F
  Last enrollment status: Granted //Certificate application is successful
  State:
    Keys generated ..... Generated
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Yes
```

### 4.3.4 Configuring SNC certificate

Configure trustpoint:

Command	Function
Qtech (config)# <b>crypto pki trustpoint</b> <i>CA_name</i>	Enters trustpoint configuration mode. <i>CA-name</i> is the common name of the corresponding CA, namely, the string entered in the <b>CA common name (C)</b> field in step 9 in the "Installing Certificate Services on a Windows 2003 Server" section.
Qtech (ca-trustpoint)# <b>enrollment url</b> <i>http://192.168.50.203/certsrv/mscep/mscep.dll auto-up</i>	Configures the certificate enrollment URL of this trustpoint, namely the URL shown in step 8 of the "Installing SCEP add-on" section; if there is no DNS server, an IP address can also be used; manually replace the domain name with the corresponding IP address. adds <b>auto-up</b> in this command to get automatically generated certificate.
Qtech (ca-trustpoint)# <b>exit</b>	Exits trustpoint configuration mode.

The configuration of getting SNC certificate and SECP certificate are similar. The only difference lies in **auto-up** at the end of SNC certificate enrollment URL configuration., as shown below:

```
router(config)#crypto pki trustpoint CA
router(ca-trustpoint)#enrollment url http://192.168.50.203/certsrv/mscep/mscep.dll
auto-up //enrollment url
router(ca-trustpoint)#exit
```

### 4.3.5 Configuring an Offline Certificate

Configure trustpoint:

Command	Function
Qtech (config)# <b>crypto pki trustpoint</b> <i>CA_name</i>	Enters trustpoint configuration mode. <i>CA-name</i> is the common name of the corresponding CA, namely, the string entered in the <b>CA common name (C)</b> field in step 9 in the "Installing Certificate Services on a Windows 2003 Server" section.
Qtech (ca-trustpoint)# <b>asymmetric</b> sm2	Specifies a certificate algorithm and uses RSA (optional) in a default condition.
Qtech (ca-trustpoint)# <b>enrollment offline subject</b>	Configures the unique name of the router.

Qtech (ca-trustpoint)#exit	Exits trustpoint configuration mode.
----------------------------	--------------------------------------

To register a certificate, run the following command:

Command	Function
Qtech (config)# <b>crypto pki enroll</b> CA_name	Registers trustpoint and obtains the router certificate corresponding to the trustpoint.

The process for configuring an offline certificate is as follows:

- Step 1 Generate an RSA public/private key pair (mandatory).
- Step 2 Define a CA (mandatory).
- Step 3 Register an offline certificate (mandatory).
- Step 4 The CA issues a certificate (mandatory).
- Step 5 Import the certificate (mandatory).

Generate an RSA key pair:

```
Qtech (config)#crypto pki key generate rsa //Generate a key.
Qtech (config)#crypto pki trustpoint CA_name //Define a CA. CA-name: FQDN of the
CA, which will be provided by the CA administrator
Qtech(ca-trustpoint)#enrollment offline subject //Set DN information of the
offline certificate
```

You are about to be asked to enter your Distinguished Name(DN) information that will be incorporated into your certificate request. There are quite a few fields but you can leave some blank.

```
Common Name (eg, YOUR name) []: //Your first name and last name
Organizational Unit Name (eg, section) []: //Your organizational unit name
Organization Name (eg, company) []: //Your organization name
Locality Name (eg, city) []: //Your city or region
State or Province Name (full name) []: //Your state or province
Country Name (2 letter code) [CN]: //2-letter country code of your organization
```

```
The subject name is: cn=fhsjflsdgingsd,ou=research,o=Qtech,l=CD,st=SC,c=CN
Is it correct[yes/no]:yes
Qtech(config)#crypto pki enroll CA_name //Register an offline certificate
%The subject name in the certificate will include:
cn=fhsjflsdgingsd,ou=research,o=Qtech,l=CD,st=SC,c=CN
-----BEGIN CERTIFICATE REQUEST-----
MIIBpDCCAQ0CAQAwZDEXMBUGAlUEAxMOZmhzamZsc2RnaW5nc2QxETAPBgNVBAsT
CHJlc2VhcmNoMQ8wDQYDVQQKEWZydWlqaWUxZzA5BjBgNVBACTAkNEMQswCQYDVQQLI
EwJTRzELMAkGALUEBhMCQ04wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANep
/WFr0uBBp7ZIPMC7Dq22mUtzc3xWrT3V5sk/P98+KTX1KYy7aYCKZqhgCw/5XHP
6fAV9d7kKcs9ynptjbagjdfpewSRpRzJ0U+fYglmuJf7U3ZuyFMBOQgwOvoFwcOa
sJ53RhmazqdAHZpDtQT9XVb14tSNYckGiOm3My3AgMBAAGgADANBgkqhkiG9w0B
AQQFAA0BgQBFAc/oAVXrKpVvks0Mvk+84bKIR0tY2opqyRo9Ax26rZM8hK4oULQS
n3Ar7O3pBoWt1YbX0ZpUpEgulIRCm0PwIeQ6uN6KwnO3a6A3AMLgWrwQ29rn7kQG
JbsHZ+Okk80CzZu6s80BtasB6VU4LFCGwBAtbL83Syp973c8cYGPWg==
-----END CERTIFICATE REQUEST-----
Copy the contents (PKCS10 format) between "-----BEGIN CERTIFICATE REQUEST-----" and "
-----END CERTIFICATE REQUEST-----" to the CA to issue a certificate.
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.
```

//Paste the CA root certificate in PEM format.

Certificate has the following attributes:

```
MD5 fingerprint: D869FAEE D797E625 B248217D 2050BF48
SHA1 fingerprint: D0B10C45 751402F0 646B4DBF E5B26AE2 74207498
%% Do you accept this certificate?[yes/no]:yes
```

```
% CA Certificate successfully imported
% Enter PEM-formatted certificate.
% End with a blank line or "quit" on a line by itself.
```

//Paste the router certificate in PEM format issued by the CA.

```
% Router Certificate successfully imported
```

### 4.3.6 Certificate Configuration Commands (Optional)

Certificate configuration commands include certificate chain configuration commands and certificate configuration commands.

To create a certificate chain, run the following command in global configuration mode. Use the **no** form of this command to delete a certificate chain:

Command	Function
Qtech(config)# <b>crypto pki certificate chain</b>	Creates a router certificate chain and enters certificate chain configuration mode (config_cert_chain).

To add a certificate to the certificate chain, run the following command in certificate chain configuration mode. Use the **no** form of this command to delete the certificate:

Command	Function
Qtech(config_cert_chain)# <b>certificate [CA] serial_num</b>	Enters certificate configuration mode (config-pubkey) in order to enter certificate data with the specified serial number; <i>serial_num</i> is the serial number of the certificate; The <i>CA</i> parameter indicates the CA root certificate.

To enter certificate data, run the following command line by line in certificate configuration mode (config-pubkey).

Command	Function
Qtech(config-pubkey)# <b>308202E6 30820290 A0030201 0202107F FFBB3997 39B4814B E16B4FF9 067A4B30</b>	Enters certificate data.

To exit certificate configuration mode, type in "quit" and the system will immediately analyze and verify the certificate data. If the certificate data is illegal, the contents entered will be cancelled. Note that "exit" and "Ctrl+Z" do not take effect in certificate configuration mode.

Command	Function
Qtech(config-pubkey)# <b>quit</b>	Ends certificate data input and exits certificate configuration mode.



#### Caution

The commands configured in this section are only used to store, display and delete certificates. It is not recommended that you configure the certificate by entering certificate data line by line manually, as it is quite troublesome. Refer to relevant instructions for certificate import. After a successful import, run the **show running** command and you will see that the system has automatically created the certificate chain and converted CA certificate and router certificate into the format shown herein as system configurations. Actually, as Qtech products do not provide the command for separately configuring private keys, you can only import the certificate as per relevant instructions.

If you want to manually configure the certificate by using the **certificate** command, configure the CA root certificate first and then configure the router certificate, as the former one will be needed for verification while configuring the later one.

When using the **no** form of the command to delete a CA root certificate or certificate chain, the CA root certificate, router certificate and private key in system configuration all will be deleted.



To check certificate configurations, run the **show running** command or the **show crypto pki cert** command. For details, refer to the "Monitoring and Maintenance" section.

Example of manually configuring a CA root certificate:

```
Qtech(config)# crypto pki certificate chain
Qtech(config-cert-chain)# certificate ca
7FFFBB399739B4814BE16B4FF9067A4B
Qtech(config-pubkey)# 308202E6 30820290 A0030201 0202107F FFBB3997 39B4814B E16B4FF9
067A4B30
Qtech(config-pubkey)# 0D06092A 864886F7 0D010105 05003081 8F312330 2106092A 864886F7
0D010901
Qtech(config-pubkey)# 1614776C 6370796A 77624073 7461722D 6E65742E 636E310B 30090603
55040613
Qtech(config-pubkey)# 02434E31 0B300906 03550408 1302666A 310F300D 06035504 07130666
757A686F
Qtech(config-pubkey)# 75311230 10060355 040A1309 52656420 4769616E 74311530 13060355
040B130C
Qtech(config-pubkey)# 44657061 72746D65 6E742035 31123010 06035504 03130943 41205365
72766572
Qtech(config-pubkey)# 301E170D 30353036 32323035 34363332 5A170D30 37303632 32303535
3434355A
Qtech(config-pubkey)# 30818F31 23302106 092A8648 86F70D01 09011614 776C6370 796A7762
40737461
Qtech(config-pubkey)# 722D6E65 742E636E 310B3009 06035504 06130243 4E310B30 09060355
04081302
Qtech(config-pubkey)# 666A310F 300D0603 55040713 0666757A 686F7531 12301006 0355040A
13095265
Qtech(config-pubkey)# 64204769 616E7431 15301306 0355040B 130C4465 70617274 6D656E74
20353112
Qtech(config-pubkey)# 30100603 55040313 09434120 53657276 6572305C 300D0609 2A864886
F70D0101
Qtech(config-pubkey)# 01050003 4B003048 024100BE D1E81427 7A302B5E 11CA43FD 2F2B7EA9
8A0796A2
Qtech(config-pubkey)# CFFE9DB7 D3DA54C3 034AA844 B3F011DC 8ABB7253 9758B13F DF6B8A9E
5F46D300
Qtech(config-pubkey)# 402E24D3 85A74142 55F77502 03010001 A381C530 81C2300B 0603551D
0F040403
Qtech(config-pubkey)# 0201C630 0F060355 1D130101 FF040530 030101FF 301D0603 551D0E04
16041464
Qtech(config-pubkey)# 4612C027 A49E010C 65DAF86E E7FEC656 ECADD430 71060355 1D1F046A
30683031
Qtech(config-pubkey)# A02FA02D 862B6874 74703A2F 2F7A6A2D 726F7574 65722F43 65727445
6E726F6C
Qtech(config-pubkey)# 6C2F4341 25323053 65727665 722E6372 6C3033A0 31A02F86 2D66696C
653A2F2F
Qtech(config-pubkey)# 5C5C7A6A 2D726F75 7465725C 43657274 456E726F 66C65C43 41253230
53657276
Qtech(config-pubkey)# 65722E63 726C3010 06092B06 01040182 37150104 03020100 300D0609
2A864886
Qtech(config-pubkey)# F70D0101 05050003 4100342F 8D936843 607B685F F07E910C 5CE35898
7C5395AE
Qtech(config-pubkey)# C2B81CFF 82A4AE95 A881A88A FFF96F92 723EFA6F 847D8347 930F8576
48AE68B9
Qtech(config-pubkey)# 5A72CF09 50BE1BA7 E187
Qtech(config-pubkey)# quit
```

### 4.3.7 Configuring Certificate Revocation Check Policy (Optional)

When checking whether the certificate of the communication peer is valid, Qtech products provide strict and loose verification. In strict verification mode, the certificate must be verified for revocation. If the correct CRL is not found, the peer certificate will not be accepted; in loose verification mode, the certificate will not be verified for revocation. By default, the strict mode will be used. Run the following command in global configuration mode, you can change the check policy to loose mode, and use the **no** form of this command to restore to strict mode.



Command	Function
Qtech(config)# <b>crypto pki revocation-check none</b>	When this command is used, there is no need to check whether the certificate has been revoked according to CRL while checking the certificate of communication peer.



#### Note

The check policy shall be determined according to the fact that whether the device may receive the revoked peer certificate. For example, when the certificate is used in IKE center-branch network model, as the central device needs to accept the negotiation requests initiated by many dialers, and some certificates may have been revoked, the strict mode must be configured then to avoid unauthorized access. The branch devices only initiate the negotiation attempt with the central device, and are not possible to receive a revoked certificate. Therefore, the loose mode will be sufficient and network resources needed for CRL update can also be saved.

### 4.3.8 Downloading a CRL (Optional)

By default, strict certificate revocation is used. At this time, you must download a CRL. The maximum size of a CRL file allowed by the RGOS is 1 MB; otherwise, CRL download will be rejected. On Qtech products, a CRL file can be downloaded through HTTP from a URL obtained in the following methods (priority arranged in descending order):

15) Specified by using the **crypto pki crl url** <http://www.myca.cn/certsrv/certcrl.crl> command

16) Extension of CRL distribution point of CA root certificate configured on the device;

17) Extension of CRL distribution point of router certificate configured on the device;

CRL can be downloaded by the following means:

- Manually download CRL by using the **crypto pki crl request** command;
- When CA root certificate and router certificate are configured and strict mode is adopted for certificate check, the CRL will be detected every one minute for presence and expiration, and will be downloaded automatically;
- When strict mode is adopted for certificate check, the system will verify whether the local CRL has expired or not and download immediately during certificate check if the local CRL has expired.



#### Note

**Note** When a digital certificate is no longer needed by the device, delete relevant configurations or configure a loose certificate revocation check policy for the following considerations:

1. CRL expiration check executed once every minute can be saved;
2. If the CRL file is large, automatic update will consume certain network resources and occupy FLASH space and memory space.

To manually specify the URL for downloading CRL, run the following command in global configuration mode; use the **no** form of this command to delete this configuration:

Command	Function
Qtech(config)# <b>crypto pki crl url</b> <i>url_string</i>	Manually specifies the URL for downloading a CRL file.



#### Caution

*url\_string* must begin with <http://>; port 80 is used as the downloading port by default, or else you must specify a port after the domain name, for example, <http://www.myca.cn:1020/>; the directory name is **certsrv** by default, or you can specify a directory by running the <http://www.myca.cn/CertDir/> command; the CRL file is **certcrl.crl** by default, or you can specify it by running the <http://www.myca.cn/certsrv/mycertcrl.crl>; the value of *url\_string* must contain no space; if your URL must contain spaces, you can type in "%20" instead, for example, <http://www.myca.cn/certsrv/CA%20Server%20Crl.crl>.

The domain of `url_string` can use an IP address directly, such as `http://202.101.211.123`, or an internal host name, such as `http://myserver`. No matter the URL is obtained through manual configuration or certificate, the device will automatically proceed with domain name resolution or host name resolution while starting to download CRL file. Make sure the relevant configurations are correct. If domain name resolution is needed, the correct DNS server address must be configured; if internal host name resolution is needed, use the **ip host** command to configure the IP address of the host. The extension of CRL distribution point may contain multiple URLs. RGOS can only use one URL. Pay attention to this issue during CA server configuration.

To manually download a CRL, run the following command in global configuration mode:

Command	Function
Qtech(config)# <b>crypto pki crl request</b>	Manually starts CRL download; start CRL download according to the currently configured certificate and URL (this command cannot be stored).

During CRL download, run the **crypto pki crl request** command and the system will prompt that the download process has started. Upon successful download, the message “%Crl download and decode successfully!” will be displayed on the console; use the **dir** command to check the file in FLASH and its creation time, or you can check the result of CRL download, as shown below:

```
Qtech# dir
Directory of flash:/
5   an      68 0xdc28957 Jan  1 2005 00:00:00 tftp_config.bin
8   an 4301816 0x3e415b47 Jun 28 2005 15:03:46 rgos.bin
20  an      5311 0xeaa56cb0 Jul  4 2005 10:04:37 config.text
26  an      427 0x5bd43f32 Jun 29 2005 10:00:07 certcrl.crl
Qtech# show clock
clock: 2005-6-29 10:0:19
```

The name of the CRL file is **certcrl.crl**; the download time is 2005-6-29 10:00:07; the current time is 10:00:19. We can see that this CRL was downloaded just now.

In addition, Qtech products also allow you to use the **show crypto pki crl** command to query information about the present CRL file (see the "Monitoring and Maintenance" section).

### 4.3.9 Configuration Example

This section shows the outputs of the **show running** command after completing certificate configuration. It shall be noted that the private key will not be displayed in the system configuration file as it is considered private information. Therefore, certificate configuration cannot be completed by copying and pasting the following configurations to the console or running the **copy tft flash** command to copy the configuration file to **config.txt**. To configure a certificate, you must run the **crypto pki import pem terminal** Command to import the certificate. This example only shows the visible configuration results.



**Caution** For how the certificate application module uses the digital certificate, refer to instructions on relevant application modules.

Configuration example is shown below:

```
Qtech# sh run
Building configuration...
Current configuration : 5331 bytes
!
version 8.31(building 1)
hostname Qtech
!
crypto pki certificate chain
certificate ca 7FFFBB399739B4814BE16B4FF9067A4B
308202E6 30820290 A0030201 0202107F FFBB3997 39B4814B E16B4FF9 067A4B30
0D06092A 864886F7 0D010105 05003081 8F312330 2106092A 864886F7 0D010901
1614776C 6370796A 77624073 7461722D 6E65742E 636E310B 30090603 55040613
```

```

02434E31 0B300906 03550408 1302666A 310F300D 06035504 07130666 757A686F
75311230 10060355 040A1309 52656420 4769616E 74311530 13060355 040B130C
44657061 72746D65 6E742035 31123010 06035504 03130943 41205365 72766572
301E170D 30353036 32323035 34363332 5A170D30 37303632 32303535 3434355A
30818F31 23302106 092A8648 86F70D01 09011614 776C6370 796A7762 40737461
722D6E65 742E636E 310B3009 06035504 06130243 4E310B30 09060355 04081302
666A310F 300D0603 55040713 0666757A 686F7531 12301006 0355040A 13095265
64204769 616E7431 15301306 0355040B 130C4465 70617274 6D656E74 20353112
30100603 55040313 09434120 53657276 6572305C 300D0609 2A864886 F70D0101
01050003 4B003048 024100BE D1E81427 7A302B5E 11CA43FD 2F2B7EA9 8A0796A2
CFFE9DB7 D3DA54C3 034AA844 B3F011DC 8ABB7253 9758B13F DF6B8A9E 5F46D300
402E24D3 85A74142 55F77502 03010001 A381C530 81C2300B 0603551D 0F040403
0201C630 0F060355 1D130101 FF040530 030101FF 301D0603 551D0E04 16041464
4612C027 A49E010C 65DAF86E E7FEC656 ECADD430 71060355 1D1F046A 30683031
A02FA02D 862B6874 74703A2F 2F7A6A2D 726F7574 65722F43 65727445 6E726F6C
6C2F4341 25323053 65727665 722E6372 6C3033A0 31A02F86 2D66696C 653A2F2F
5C5C7A6A 2D726F75 7465725C 43657274 456E726F 6C6C5C43 41253230 53657276
65722E63 726C3010 06092B06 01040182 37150104 03020100 300D0609 2A864886
F70D0101 05050003 4100342F 8D936843 607B685F F07E910C 5CE35898 7C5395AE
C2B81CFF 82A4AE95 A881A88A FFF96F92 723EFA6F 847D8347 930F8576 48AE68B9
5A72CF09 50BE1BA7 E187
quit
!

```

```
certificate 162A7A1D0000000000002
```

```

308204F9 308204A3 A0030201 02020A16 2A7A1D00 00000000 02300D06 092A8648
86F70D01 01050500 30818F31 23302106 092A8648 86F70D01 09011614 776C6370
796A7762 40737461 722D6E65 742E636E 310B3009 06035504 06130243 4E310B30
09060355 04081302 666A310F 300D0603 55040713 0666757A 686F7531 12301006
0355040A 13095265 64204769 616E7431 15301306 0355040B 130C4465 70617274
6D656E74 20353112 30100603 55040313 09434120 53657276 6572301E 170D3035
30363232 30353530 34385A17 0D303630 36323230 36303034 385A3081 80311630
1406092A 864886F7 0D010901 16077A68 616F6A75 6E310B30 09060355 04061302
434E310B 30090603 55040813 02666A31 0F300D06 03550407 13066675 7A686F75
31123010 06035504 0A130952 65642047 69616E74 31153013 06035504 0B130C44
65706172 746D656E 74203531 10300E06 03550403 13077A68 616F6A75 6E308201
22300D06 092A8648 86F70D01 01010500 0382010F 00308201 0A028201 0100C6E2
7AE88D6D D8BB56A8 9C036214 E52E23E5 A526313D B22465B1 F2CC07E3 EFCC023C
D06E008D FCCE3AB6 457ACBA0 87941FC3 9243366A B27C9CD5 CA7E83BA 76497FBE
F41F4AA1 0B982296 E27954A0 ED1C6230 B7EE6A6E CB72E99C D9E8B0DC F5C6198F
2B2A85FA BFFF0840 7EF2A1DF D18BEF68 321E1A45 FA16DE33 B06290BD 9C8EEC7C
6E494875 E65CCEB1 8E1C80F3 5B796CA1 31B2A948 379FED45 9585BA98 0F42C578
4C3DA245 73903D0B 1A7C53B5 971AA643 2F44540F A1513A0E 9F8B2ED1 70CB3699
9157D2B7 9D7CCEE07 CF4AC7CD 71DCCE72 DC75A003 B236BE8E AFCA9946 038327D3
FF241E4C 0C2199B4 FE5A4D61 B5E9B438 DC592C37 F39302FC 0988021B D0450203
010001A3 82022430 82022030 0E060355 1D0F0101 FF040403 0206C030 13060355
1D25040C 300A0608 2B060105 05080202 301D0603 551D0E04 16041484 7E33A391
A5261D2D BB5465BF C72A2A2E 87D5A930 81CB0603 551D2304 81C33081 C0801464
4612C027 A49E010C 65DAF86E E7FEC656 ECADD4A1 8195A481 9230818F 31233021
06092A86 4886F70D 01090116 14776C63 70796A77 62407374 61722D6E 65742E63
6E310B30 09060355 04061302 434E310B 30090603 55040813 02666A31 0F300D06
03550407 13066675 7A686F75 31123010 06035504 0A130952 65642047 69616E74
31153013 06035504 0B130C44 65706172 746D656E 74203531 12301006 03550403
13094341 20536572 76657282 107FFFBB 399739B4 814BE16B 4FF9067A 4B307106
03551D1F 046A3068 3031A02F A02D862B 68747470 3A2F2F7A 6A2D726F 75746572
2F436572 74456E72 6F6C6C2F 43412532 30536572 7665722E 63726C30 33A031A0
2F862D66 696C653A 2F2F5C5C 7A6A2D72 6F757465 725C4365 7274456E 726F6C6C
5C434125 32305365 72766572 2E63726C 30819806 082B0601 05050701 0104818B
30818830 4106082B 06010505 07300286 35687474 703A2F2F 7A6A2D72 6F757465
722F4365 7274456E 726F6C6C 2F7A6A2D 726F7574 65725F43 41253230 53657276
65722E63 72743043 06082B06 01050507 30028637 66696C65 3A2F2F5C 5C7A6A2D
726F7574 65725C43 65727445 6E726F6C 6C5C7A6A 2D726F75 7465725F 43412532
30536572 7665722E 63727430 0D06092A 864886F7 0D010105 05000341 0037500C
D66C236D 2D813702 6C22EFE2 9598DC91 25FE0A3B B0F24869 2C6B9866 BE6B09EF

```

```

DE2FDBED 710E04A5 12388B30 2BEB9D9 881EA210 2C86D23D 25FD9CDF B4
quit
!
!
crypto pki crl url http://zj-router/certsrv/certcrl.crl
!
ip host zj-router 192.168.64.145
!
interface FastEthernet 0/0
ip address 202.101.100.1 255.255.255.0
ip address 192.168.64.199 255.255.255.0 secondary
!
interface FastEthernet 1/0
duplex auto
speed auto
!
interface Null 0
!
!
!
line con 0
line vty 0 4
exec-timeout 0 0
privilege level 15
no login
!
!
end
Qtech#

```

## 4.4 Monitoring and Maintenance

Qtech products allow you to query certificate information by using the following command in privileged user mode:

Command	Function
Qtech# <b>show crypto pki certificate</b>	Displays CA root certificate and router certificate configured in the system. When no certificate is configured, there will be no output.

The following shows an example of the **show crypto pki certificate** command output:

```

Qtech# show crypto pki certificate
%CA certificate info: //CA certificate information
Certificate:
Data:
Version: 3 (0x2) //X.509v3
Serial Number: //Certificate serial number
7f:ff:bb:39:97:39:b4:81:4b:e1:6b:4f:f9:06:7a:4b
Signature Algorithm: sha1WithRSAEncryption //Signature algorithm
Issuer: emailAddress=wlcpyjwb@star-net.cn, C=CN, ST=fj, L=fuzhou, O=Red Giant,
OU=Department 5, CN=CA Server //DN name of the issuer
Validity //Certificate validity
information
Not Before: Jun 22 05:46:32 2005 GMT //Effective time in UTC
Not After : Jun 22 05:54:45 2007 GMT //Time of expiration in UTC
Subject: emailAddress=wlcpyjwb@star-net.cn, C=CN, ST=fj, L=fuzhou, O=Red Giant,
OU=Department 5, CN=CA Server
//DN name of certificate subject
Subject Public Key Info: //Information about the subject
public key
Public Key Algorithm: rsaEncryption //Public key algorithm: RSA encryption
RSA Public Key: (512 bit) //512-bit RSA public key
Modulus (512 bit):
00:be:d1:e8:14:27:7a:30:2b:5e:11:ca:43:fd:2f:

```

```
2b:7e:a9:8a:07:96:a2:cf:fe:9d:b7:d3:da:54:c3:
03:4a:a8:44:b3:f0:11:dc:8a:bb:72:53:97:58:b1:
3f:df:6b:8a:9e:5f:46:d3:00:40:2e:24:d3:85:a7:
41:42:55:f7:75
Exponent: 65537 (0x10001)
X509v3 extensions: //Certificate extensions
X509v3 Key Usage: //Key usage flag
Digital Signature, Non Repudiation, Certificate Sign, CRL Sign //Including
digital signature, anti-replay, certificate signature, and CRL signature
X509v3 Basic Constraints: critical
CA:TRUE
X509v3 Subject Key Identifier: //Subject key identifier
64:46:12:C0:27:A4:9E:01:0C:65:DA:F8:6E:E7:FE:C6:56:EC:AD:D4
X509v3 CRL Distribution Points: //Information about CRL distribution
point
URI:http://zj-router/CertEnroll/CA%20Server.crl
URI:file://\\zj-router\CertEnroll\CA%20Server.crl
1.3.6.1.4.1.311.21.1:
...
Signature Algorithm: sha1WithRSAEncryption //Signature algorithm
34:2f:8d:93:68:43:60:7b:68:5f:f0:7e:91:0c:5c:e3:58:98:
7c:53:95:ae:c2:b8:1c:ff:82:a4:ae:95:a8:81:a8:8a:ff:f9:
6f:92:72:3e:fa:6f:84:7d:83:47:93:0f:85:76:48:ae:68:b9:
5a:72:cf:09:50:be:1b:a7:e1:87 //Certificate signature
%Router certificate info: //Information about the router
certificate
Certificate:
Data:
Version: 3 (0x2) //X.509v3
Serial Number: //Certificate serial number
16:2a:7a:1d:00:00:00:00:00:02
Signature Algorithm: sha1WithRSAEncryption //Signature algorithm
Issuer: emailAddress=wlcpyjwb@star-net.cn, C=CN, ST=fj, L=fuzhou, O=Red Giant,
OU=Department 5, CN=CA Server //DN name of the issuer
Validity //Certificate validity
information
Not Before: Jun 22 05:50:48 2005 GMT //Effective time in UTC
Not After : Jun 22 06:00:48 2006 GMT //Time of expiration in UTC
Subject: emailAddress=zhaojun, C=CN, ST=fj, L=fuzhou, O=Red Giant, OU=De partment 5,
CN=zhaojun //DN name of certificate subject
Subject Public Key Info: //Information about the subject
public key
Public Key Algorithm: rsaEncryption //Public key algorithm: RSA encryption
RSA Public Key: (2048 bit) //2048-bit RSA public key
Modulus (2048 bit):
00:c6:e2:7a:e8:8d:6d:d8:bb:56:a8:9c:03:62:14:
e5:2e:23:e5:a5:26:31:3d:b2:24:65:b1:f2:cc:07:
e3:ef:cc:02:3c:d0:6e:00:8d:fc:ce:3a:b6:45:7a:
cb:a0:87:94:1f:c3:92:43:36:6a:b2:7c:9c:d5:ca:
7e:83:ba:76:49:7f:be:f4:1f:4a:a1:0b:98:22:96:
e2:79:54:a0:ed:1c:62:30:b7:ee:6a:6e:cb:72:e9:
9c:d9:e8:b0:dc:f5:c6:19:8f:2b:2a:85:fa:bf:ff:
08:40:7e:f2:a1:df:d1:8b:ef:68:32:1e:1a:45:fa:
16:de:33:b0:62:90:bd:9c:8e:ec:7c:6e:49:48:75:
e6:5c:ce:b1:8e:1c:80:f3:5b:79:6c:a1:31:b2:a9:
48:37:9f:ed:45:95:85:ba:98:0f:42:c5:78:4c:3d:
a2:45:73:90:3d:0b:1a:7c:53:b5:97:1a:a6:43:2f:
44:54:0f:a1:51:3a:0e:9f:8b:2e:d1:70:cb:36:99:
91:57:d2:b7:9d:7c:ee:07:cf:4a:c7:cd:71:dc:ce:
72:dc:75:a0:03:b2:36:be:8e:af:ca:99:46:03:83:
27:d3:ff:24:1e:4c:0c:21:99:b4:fe:5a:4d:61:b5:
e9:b4:38:dc:59:2c:37:f3:93:02:fc:09:88:02:1b:
d0:45
```



```

Exponent: 65537 (0x10001)
X509v3 extensions: //Certificate extensions
X509v3 Key Usage: critical //Key usage flag, which is a key extension
Digital Signature, Non Repudiation //Including digital signature and anti-
replay
X509v3 Extended Key Usage: //Extended key usage
1.3.6.1.5.5.8.2.2
X509v3 Subject Key Identifier: //Subject key identifier
84:7E:33:A3:91:A5:26:1D:2D:BB:54:65:BF:C7:2A:2A:2E:87:D5:A9
X509v3 Authority Key Identifier: //Authority key identifier
keyid:64:46:12:C0:27:A4:9E:01:0C:65:DA:F8:6E:E7:FE:C6:56:EC:AD:D4
DirName:/emailAddress=wlcpyjwb@star-net.cn/C=CN/ST=fj/L=fuzhou/O
=Red Giant/OU=Department 5/CN=CA Server
serial:7F:FF:BB:39:97:39:B4:81:4B:E1:6B:4F:F9:06:7A:4B
X509v3 CRL Distribution Points: //Information about CRL distribution
point
URI:http://zj-router/CertEnroll/CA%20Server.crl
URI:file://\\zj-router\CertEnroll\CA%20Server.crl
Authority Information Access: //Authority information access point
CA Issuers - URI:http://zj-router/CertEnroll/zj-router_CA%20Serv
er.crt
CA Issuers - URI:file://\\zj-router\CertEnroll\zj-router_CA%20Se
rver.crt
Signature Algorithm: sha1WithRSAEncryption //Signature algorithm
37:50:0c:d6:6c:23:6d:2d:81:37:02:6c:22:ef:e2:95:98:dc:
91:25:fe:0a:3b:b0:f2:48:69:2c:6b:98:66:be:6b:09:ef:de:
2f:db:ed:71:0e:04:a5:12:38:8b:30:2b:eb:c9:d9:88:1e:a2:
10:2c:86:d2:3d:25:fd:9c:df:b4/ //Certificate signature
Qtech#

```

Qtech products allow you to query the CRL information by using the following command in privileged user mode:

Command	Function
<b>Qtech# show crypto pki crls</b>	Displays CRL information downloaded by the system.

The following shows an example of the **show crypto pki crl** command output:

```

Qtech# sh crypto pki crls
Certificate Revocation List (CRL):
Version 2 (0x1) //CRL version of X.509v2
Signature Algorithm: sha1WithRSAEncryption //Signature algorithm
Issuer: /emailAddress=wlcpyjwb@star-net.cn/C=CN/ST=fj/L=fuzhou/O=Red
Giant/OU=Department 5/CN=CA Server //DN of the issuer
Last Update: Jun 22 06:10:27 2005 GMT //Time of last update in UTC
Next Update: Jun 29 18:30:27 2005 GMT //Time of next update in UTC, namely the
expiration time of CRL
CRL extensions: //CRL extensions are shown below
X509v3 Authority Key Identifier: //Authority key identifier
keyid:64:46:12:C0:27:A4:9E:01:0C:65:DA:F8:6E:E7:FE:C6:56:EC:AD:D4
1.3.6.1.4.1.311.21.1:
...
Revoked Certificates: //List of revoked certificates are
shown below
Serial Number: 162A7A1D000000000002 //Serial number of the revoked
certificate
Revocation Date: Jun 22 06:19:53 2005 GMT //Revocation date
CRL entry extensions: //CRL entry extensions
X509v3 CRL Reason Code: //CRL revocation reason code
Key Compromise //Key compromise
Serial Number: 1635E5E3000000000003
Revocation Date: Jun 22 06:19:53 2005 GMT
CRL entry extensions:
X509v3 CRL Reason Code:

```



```
Key Compromise //Key compromise
Signature Algorithm: sha1WithRSAEncryption //Signature algorithm
5d:a2:ab:07:ff:7e:0e:9a:af:b2:25:11:7f:31:86:aa:21:48:
37:e7:22:99:e3:b2:15:e0:f9:80:63:66:5e:2f:f2:d6:c0:ea:
ef:46:7e:d1:c1:b2:66:0e:0b:d3:74:d1:55:bc:5c:13:46:e8:
56:ec:40:83:7b:1b:75:f2:68:87 //Signature value
Qtech#
```



**Caution**

**Caution** When the **crypto pki revocation-check none** command is used during startup, the existing URL file will not be resolved automatically after startup, and the **show crypto pki crl** command has no output.

Qtech products allow you to query system debugging information displayed in certificate operations by using the following commands in privileged user mode:

Command	Function
Qtech# <b>debug crypto pki event</b>	Displays event tracking information about relevant certificate operations
Qtech# <b>debug crypto pki error</b>	Displays error tracking information about relevant certificate operations

The preceding debugging information will help you diagnose the problems arising during digital certificate configuration and application.

## 5 CONFIGURING VPDN

### 5.1 Overview of VPDN

RGOS supports two types of VPDN tunnels: L2TP and PPTP.

Layer Two Tunneling Protocol (L2TP);

Point-to-Point Tunneling Protocol (PPTP).

These two types of VPDN tunneling protocols have their own history. For their configuration and usage, see the following sections. PPTP is commonly used in the Microsoft Windows series products, while L2TP is commonly used in the network devices from such vendors as Cisco. As an industry standard, L2TP is supported by Windows 2000/XP.



**Caution** In this chapter, a router refers to the generic route and security gateway unless specially specified.

---

## 6 CONFIGURING PPTP

### 6.1 Overview of PPTP

Point-to-Point-Tunneling Protocol (PPTP) is a network technology that supports multi-protocol VPN. With the PPTP protocol, remote users can dial in the local ISP through Microsoft Windows NT® Workstation, Windows® 95, Windows® 98, Windows® 2000 and other systems with the PPP function enabled, so as to connect and access the corporate network over the Internet securely. Its standard description document is RFC 2637, which is proposed jointly by Microsoft and several industry leading communication device developers. Now it has been recommended to Internet Engineering Task Force(IETF).

The PPTP protocol transmits PPP packets through the tunnel in the IP network. Although it does not modify the PPP protocol in any way, it defines a new PPP packet carrier. By defining the client-server architecture, PPTP divides the functions of the network access server (NAS) and has them implemented by PPTP network server (PNS) and PPTP access concentrator (PAC). The PNS is designed to run on general operating systems. Based on the TCP/IP network, it only requires IP interfaces. The PAC typically has one or more PSTNs, ISDNs or other PPP-enabled physical interfaces.

RGOS now can be used as the PNS, that is, it accepts the PPTP tunnel initiated by the remote client. In this case, the router accepts connection requests from the remote PPTP client and negotiates with the client to establish tunnels.



#### Note

Now the PNS is only supported on the R26, R36, SecVPN, and RSR series routers but not on the NBR1000.

### 6.2 Configuring the PPTP Server

#### 6.2.1 Configuration Tasks

#### 6.2.2 Configuring a Local Address Pool (Optional)

In order to accept the PPTP connection initiated by the remote client, the PNS must allocate an IP address to the remote client if no IP address is set for it to use internal VPN. Generally, an idle IP address in a specified address pool is allocated to the client. RGOS provides the following commands to configure the local address pool.

Command	Function
Qtech(config)# <b>ip local pool</b> <i>poolname first-ip [last-ip]</i>	Creates a local address pool.
Qtech(config)# <b>no ip local pool</b> <i>poolname</i>	Deletes a specified address pool.

*poolname* is the name of the local address pool to be created, *first-ip* and *last-ip* are the first and last address in the address range set for the local address pool, respectively.

#### 6.2.3 Configuring User Information (Optional)

To authenticate the remote client that tries to access the local PNS, run the following command.

Command	Function
Qtech(config)# <b>username</b> <i>user-name password password</i>	Configures the user information.
Qtech(config)# <b>no username</b> <i>user-name</i>	Deletes the specified user.

*user-name* is the name of the user who is allowed to dial in, and *password* is the password of the user. The router maintains a local database that contains the user names and passwords.

## 6.2.4 Configuring VPDN Globally

### 6.2.5 Enabling/Disabling the VPDN Function

If the user requires the router to accept the PPTP access by the remote client and establish a PPTP tunnel, the VPDN function must be enabled on the router. To enable or disable the VPDN function, run the following command:

Command	Function
Qtech(config)# <b>vpdn enable</b>	Enables the VPDN function.
Qtech(config)# <b>no vpdn enable</b>	Disables the VPDN function.



**Note** that if the VPDN function is disabled, all the existing PPTP tunnels and sessions are retained, but new PPTP tunnels and sessions cannot be created.

#### 6.2.5.1 Setting Source Address of VPDN

RGOS offers the following commands for users to set the (local) source address of the VPDN function. After the source address of VPDN is set, the destination address of the tunnel set for the remote client must match it before a PPTP tunnel can be established properly.

Command	Function
Qtech(config)# <b>vpdn source-ip</b> <i>ip-address</i>	Sets the source address of VPDN.
Qtech(config)# <b>no vpdn source-ip</b> <i>ip-address</i>	Cancels the set source address of VPDN.

By default, the system does not check whether the destination address in the received tunnel establishment request is a specific value.

#### 6.2.5.2 Setting Maximum Number of VPDN Sessions

To set the maximum number of sessions allowed by the VPDN server, run the following command. Once specified, the access requests that exceed the maximum value will be denied.

Command	Function
Qtech(config)# <b>vpdn session-limit sessions</b>	Sets the maximum number of VPDN sessions.
Qtech(config)# <b>no vpdn session-limit</b>	Restores the maximum number of VPDN sessions to the default value.

By default, the maximum number of sessions is one configured with this command.

#### 6.2.5.3 Setting Domain Resolution

RGOS offers the following commands for users to set the domain resolution in VPDN domain authentication. With this command configured, the domain type can be identified.

Command	Function
Qtech(config)# <b>vpdn domain-delimiter</b> <i>@/%#-\</i>	Sets the domain delimiter: prefix and suffix.
Qtech(config)# <b>no vpdn domain-delimiter</b>	Cancels the VPDN domain authentication option.

By default, the system does not resolve the domain field.

#### 6.2.5.4 Enabling Domain Authentication

RGOS offers the following commands for users to set the VPDN domain authentication function.

Command	Function
Qtech(config)# <b>vpdn authorize domain split</b>	Enables the domain authentication, and enables the domain split.
Qtech(config)# <b>no vpdn authorize domain</b>	Disables the domain authentication.

By default, the system does not enable the domain authentication.

#### 6.2.5.5 Setting VPDN Rate Limiting

RGOS offers the following commands for users to limit the rate of creating VPDN sessions, namely, to limit the number of VPDN tunnels allowed to be created at one time.

Command	Function
Qtech(config)# <b>vpdn limit_rate</b> <i>rate_num</i>	Enables rate limiting. The <i>rate_num</i> parameter indicates the number of tunnels allowed to be created, ranging from 5 to 100.
Qtech(config)# <b>no vpdn limit_rate</b>	Disables rate limiting.

By default, the system does not enable rate limiting.

### 6.2.6 Configuring a Virtual-Template Interface

#### 6.2.6.1 Setting a Virtual-Template Interface

To set the virtual-template interface, run the following commands.

Command	Function
Qtech(config)# <b>interface virtual-template</b> <i>number</i>	Creates a specified virtual -template interface.
Qtech(config)# <b>no interface virtual-template</b> <i>number</i>	Deletes the specified virtual- template interface.

*number* is the sequence number of the specified virtual-template interface. The created virtual-template will act as the configuration profile of the virtual-access interface that binds and carries PPTP sessions.

### 6.2.7 Configuring VPDN Group

#### 6.2.7.1 Setting VPDN Group

To set a VPDN group, run the following commands:

Command	Function
Qtech(config)# <b>vpdn-group</b> <i>name</i>	Configures a VPDN group.
Qtech(config)# <b>no vpdn-group</b> <i>name</i>	Deletes a VPDN group.

*name* is the name of the VPDN group. Users can access the VPDN group to establish a tunnel.

#### 6.2.7.2 Setting Tunneling Mode

To set the tunneling mode, run the following commands:

Command	Function
---------	----------

Qtech (config-vpdn)# <b>accept-dialin</b>	Permits the remote client's access.
Qtech (config-vpdn)# <b>no accept-dialin</b>	Denies the remote client's access.

If a user wants the local router to perform the PNS function, the user must allow the remote client to dial in.

### 6.2.7.3 Setting Tunneling Protocol

To set the tunneling protocol, run the following commands.

Command	Function
Qtech(config-vpdn-acc-in)# <b>protocol</b> {any   l2tp   pptp}	Sets the tunneling protocol.
Qtech(config-vpdn-acc-in)# <b>no protocol</b>	Cancels the set tunneling protocol.

The tunneling mode must be set before the tunneling protocol is set. To make the local router perform the PNS function, the user must run the **protocol pptp** or **protocol any** command.

### 6.2.7.4 Setting Virtual Template to Be Used

To set a virtual template used by a VPDN group, run the following commands.

Command	Function
Qtech(config-vpdn-acc-in)# <b>virtual-template</b> <i>number</i>	Sets a virtual template to be used.
Qtech(config-vpdn-acc-in)# <b>no virtual-template</b>	Cancels the virtual template in use.

The tunneling mode must be set first before a virtual template used by a VPDN group is set.

### 6.2.7.5 Setting the Name of the Remote Peer

If the name of the remote client has been set, this VPDN group is effective only for the remote client that matches the host name. If not, this VPDN group will become the default VPDN group of the system, and can provide the VPDN service for any remote client. If the name of remote client is not configured for any VPDN group, the system will use the first found VPDN group that matches conditions to accept access from a remote dial-in user.

Command	Function
Qtech(config-vpdn)# <b>terminate-from hostname</b> <i>name</i>	Sets the name of the remote host.
Qtech(config-vpdn)# <b>no terminate-from</b>	Cancels the set name of the remote host.

*name* indicates the name of the remote host.

### 6.2.7.6 Setting Local Name

To set the local name, run the following commands. This name will be sent to the remote peer as a record property.

Command	Function
Qtech(config-vpdn)# <b>local name</b> <i>name</i>	Sets the local name.
Qtech(config-vpdn)# <b>no local</b> <i>name</i>	Cancels the set local name.

*name* indicates the local name. By default, RGOS uses the name of the router as the local name and sends it to the remote host of the tunnel.



### 6.2.7.7 Setting Source Address of VPDN group

To set the source address of a VPDN group, run the following commands. Only when the destination address in the tunnel establishment request sent by the remote client matches it, will the corresponding VPDN group apply.

Command	Function
Qtech(config-vpdn)# <b>source-ip</b> <i>src-ip</i>	Sets the source address of a VPDN group.
Qtech(config-vpdn)# <b>no source-ip</b>	Cancels the set source address of a VPDN group.

### 6.2.7.8 Setting PPTP Flow Control Parameters

To set the PPTP flow control parameters, run the following commands. In general application, the default value of this parameter can be used.

Command	Function
Qtech(config-vpdn)# <b>pptp flow-control receive-window</b> <i>winsize</i>	Sets the size of the receive window of the PPTP session. The value range is 1 to 64
Qtech(config-vpdn)# <b>no pptp flow-control receive-window</b>	Cancels the set size of the receive window of the PPTP session and restores to the default value. PAC is 16, and PNS is 64
Qtech(config-vpdn)# <b>pptp flow-control</b> <i>static-rtt interval</i>	Sets the static reference time of waiting for ACK on receiving/sending PPTP session packets. The value range is 100 to 5000 (in milliseconds).
Qtech(config-vpdn)# <b>no pptp flow-control</b>	Cancels the set static reference time of waiting for ACK on receiving/sending PPTP session packets, and restore to the default value 1500 milliseconds.

*winsize* is the size of the receive window of the PPTP session, and *interval* is the static reference time of waiting for an ACK message.

### 6.2.7.9 Setting PPTP Tunnel Parameters

To set the PPTP tunnel parameters, run the following commands. In general application, the default value of this parameter can be used.

Command	Function
Qtech(config-vpdn)# <b>pptp tunnel echo</b> <i>interval</i>	Sets the time interval at which the PPTP tunnel actively sends echo messages. The value range is 0 to 1000 (in seconds).
Qtech(config-vpdn)# <b>no pptp tunnel echo</b>	Cancels the set interval of sending PPTP echo messages, and restore to the default value 60 seconds.

*interval* is the time interval at which the PPTP tunnel actively sends ECHO messages. Value **0** indicates that the tunnel does not actively send ECHO messages. The values other than **0** indicates that the tunnel actively sends ECHO messages to detect the tunnel status after it does not receive any valid packet from the remote end of the tunnel within this time interval.

### 6.2.7.10 Setting the Supported Domain Name

To set the domain name, run the following commands. After the domain authentication is enabled, this command will take effect. Only the domain matching the content of this command can be identified. If the domain does not match the content of this command, another VPDN group will be used for matching. If no matched group is found, the authentication will fail.

Command	Function
Qtech(config-vpdn)# <b>domain</b> <i>domain-name vrf vrf-name</i>	Sets the authentication domain name and the corresponding VRF instance.
Qtech(config-vpdn)# <b>no pool</b>	Removes the domain setting.

*domain-name* is the name of a domain, and *vrf-name* is the name of a VRF instance.

### 6.2.7.11 Binding a Domain Name to an Address Pool

To bind a domain name to an address pool, run the following command in vpdn-domain configuration mode. The domain name is verified during the process of VPDN tunnel negotiation to obtain the address pool binding information configured with this command. After the PPP negotiation is successful, the specified address pool will be used to assign an address to the peer end of the tunnel. By default, the address is assigned by the address pool configured in the virtual-template interface.

Command	Function
Qtech(config-vpdn)# <b>domain</b> <i>domain-name</i> <b>vrf</b> <i>vrf-name</i> Qtech(config-vpdn-domain)# <b>pool</b> <i>pool-name</i>	Sets the address pool bound to the authentication domain name.
Qtech(config-vpdn)# <b>no domain</b> <i>domain-name</i>	Removes address pool binding.

*domain-name* is the name of a domain, *vrf-name* is the name of a VRF instance and *pool-name* is the name of an address pool.

### 6.2.7.12 Setting the DNS Negotiation Address for Binding PPP to the Domain Name

To set the DNS negotiation address of PPP through domain name matching, run the following command in vpdn-domain configuration mode. By default, the DNS address of PPP configured in the virtual-template interface is used for negotiation.

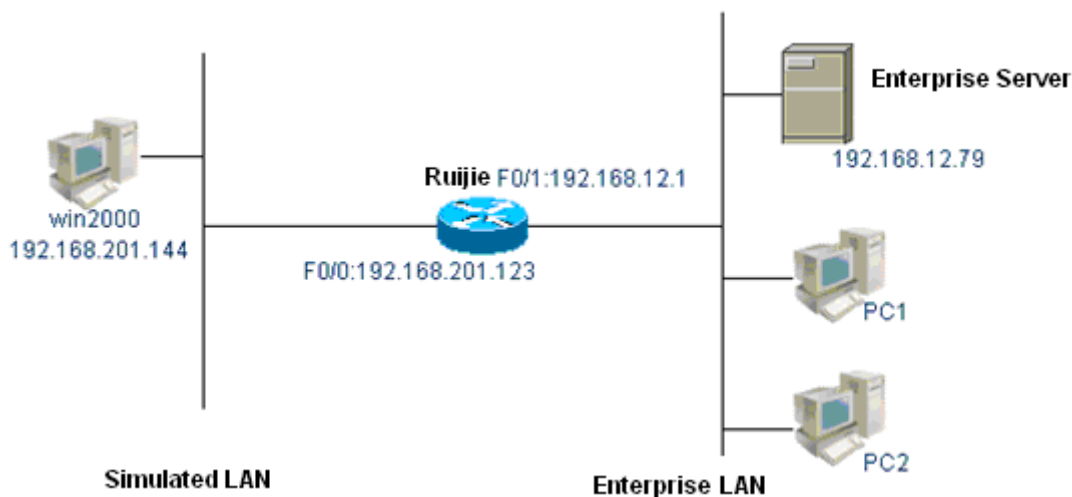
Command	Function
Qtech(config-vpdn)# <b>domain</b> <i>domain-name</i> <b>vrf</b> <i>vrf-name</i> Qtech(config-vpdn-domain)# <b>dns</b> <i>A.B.C.D</i> <i>A.B.C.D</i>	Sets the DNS negotiation address of PPP bound to the authentication domain name.
Qtech(config-vpdn)# <b>no dns</b>	Removes DNS binding.

*domain-name* is the name of a domain, *vrf-name* is the name of a VRF instance and *A.B.C.D* is the address of the DNS.

## 6.2.8 Configuration Examples

The network topology in this example is shown in the following figure. The Qtech router is used as the gateway of the corporate LAN, and the PPTP protocol is used to provide the VPDN dial-in service. Use a Windows 2000 PC as the VPDN remote client to create a PPTP tunnel to the router and access the server in the corporate LAN. To reduce testing complexity, use Ethernet to simulate the IP WAN between the remote client and R3660. The IP addresses are configured as shown in the following diagram.

Figure 19 Using a router as the PNS



The configurations of R3660 and Windows 2000 PC are respectively described as follows:

#### 18) Configuration of R3660:

```
Qtech# show running-config
Building configuration...
Current configuration : 1053 bytes
!
enable password 1
!
vpdn enable
!
vpdn-group pptp
! Default PPTP VPDN group
accept-dialin
protocol pptp
virtual-template 1
!
username pc password 0 1111
!
ip local pool pptp 1.1.1.2 1.1.1.254
interface FastEthernet 0/0
ip address 192.168.201.123 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet 0/1
ip address 192.168.12.1 255.255.255.0
duplex auto
speed auto
!
interface Virtual-Template 1
ppp authentication pap
ip unnumbered FastEthernet 0/1
peer default ip address pool pptp
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
line con 0
session-timeout 0
escape-character 29
line aux 0
session-timeout 0
escape-character 29
password 1
line vty 0
login
terminal-type ANSI
escape-character 29
line vty 1 4
login
escape-character 29
!
!
end
Qtech#
```

#### 19) Configuration of the Windows 2000 PC:

```
F:\>ver
Microsoft Windows 2000 [Version 5.00.2195]
F:\>ipconfig /all
Windows 2000 IP Configuration
   Host Name . . . . . : topding
   Primary DNS Suffix . . . . . :
   Node Type . . . . . : Hybrid
   IP Routing Enabled. . . . . : Yes
```

```

WINS Proxy Enabled. . . . . : No
Ethernet adapter local connection:
  Connection-specific DNS Suffix . :
  Description . . . . . : STAR 901 Family Fast Ethernet
r (ACPI)
  Physical Address. . . . . : 00-D0-F8-00-68-E5
  DHCP Enabled. . . . . : No
  IP Address. . . . . : 192.168.201.144
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.201.123
  DNS Servers . . . . . : 202.101.143.141
  Primary WINS Server . . . . . : 192.168.9.7
F:\>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 d0 f8 00 68 e5 ..... PCI Bus Master Adapter
=====Active Routes:
Network Destination Netmask Gateway Interface Metric
  0.0.0.0 0.0.0.0 192.168.201.123 192.168.201.144 1
  127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1
192.168.201.0 255.255.255.0 192.168.201.144 192.168.201.144 1
192.168.201.144 255.255.255.255 127.0.0.1 127.0.0.1 1
192.168.201.255 255.255.255.255 192.168.201.144 192.168.201.144 1
224.0.0.0 224.0.0.0 192.168.201.144 192.168.201.144 1
255.255.255.255 255.255.255.255 192.168.201.144 192.168.201.144 1
Default Gateway: 192.168.201.123
=====
Persistent Routes:
None

```

Double-click **Network and Dial-up Connections** on the Windows 2000 PC to create a network connection. Select **Connect to a private network through the Internet for Network connection type**, select **Do not dial initial connection for Public network**, and fill in the destination address 192.168.201.123. Name this connection as Vpdnconnect. On the page for setting the properties of Vpdnconnect, use PPTP as the VPDN server type, and define the PAP authentication and optional encryption in the security settings. After you click **Dial**, enter the user name **PC** and password **1111** configured in the router.

Upon completion of configuration, the Windows 2000 PC can access the server, for example, the server with the IP address as 192.168.12.79, in the corporate intranet after dialing in the router, as shown below:

```

F:\>ipconfig /all
Windows 2000 IP Configuration
  Host Name . . . . . : testpc
  Primary DNS Suffix . . . . . :
  Node Type . . . . . : Hybrid
  IP Routing Enabled. . . . . : Yes
  WINS Proxy Enabled. . . . . : No
Ethernet adapter local connection:
  Connection-specific DNS Suffix . :
  Description . . . . . : STAR 901 Family Fast Ethernet Adapte
r (ACPI)
  Physical Address. . . . . : 00-D0-F8-00-68-E5
  DHCP Enabled. . . . . : No
  IP Address. . . . . : 192.168.201.144
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :
  DNS Servers . . . . . : 202.101.143.141
  Primary WINS Server . . . . . : 192.168.9.7
PPP adapter vpn_RGOS:
  Connection-specific DNS Suffix . :
  Description . . . . . : WAN (PPP/SLIP) Interface
  Physical Address. . . . . : 00-53-45-00-00-00
  DHCP Enabled. . . . . : No
  IP Address. . . . . : 1.1.1.4

```

```

Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 192.168.12.1
DNS Servers . . . . . :
F:\>
F:\>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 d0 f8 00 68 e5 ..... PCI Bus Master Adapter
0x30000004 ...00 53 45 00 00 00 ..... WAN (PPP/SLIP) Interface
=====
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 192.168.12.1 1.1.1.4 1
1.1.1.4 255.255.255.255 127.0.0.1 127.0.0.1 1
1.255.255.255 255.255.255.255 1.1.1.4 1.1.1.4 1
127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1
192.168.201.0 255.255.255.0 192.168.201.144 192.168.201.144 1
192.168.201.123 255.255.255.255 192.168.201.144 192.168.201.144 1
192.168.201.144 255.255.255.255 127.0.0.1 127.0.0.1 1
192.168.201.200 255.255.255.255 192.168.201.100 192.168.201.144 1
192.168.201.255 255.255.255.255 192.168.201.144 192.168.201.144 1
224.0.0.0 224.0.0.0 1.1.1.4 1.1.1.4 1
224.0.0.0 224.0.0.0 192.168.201.144 192.168.201.144 1
255.255.255.255 255.255.255.255 192.168.201.144 192.168.201.144 1
Default Gateway: 192.168.12.1
=====
Persistent Routes:
None
F:\>
F:\>ping 192.168.12.1
Pinging 192.168.12.1 with 32 bytes of data:
Reply from 192.168.12.1: bytes=32 time<10ms TTL=255
Reply from 192.168.12.1: bytes=32 time<10ms TTL=255
Reply from 192.168.12.1: bytes=32 time<10ms TTL=255
Reply from 192.168.12.1: bytes=32 time<10ms TTL=255
Ping statistics for 192.168.12.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
F:\>ping 192.168.12.79
Pinging 192.168.12.79 with 32 bytes of data:
Reply from 192.168.12.79: bytes=32 time=10ms TTL=127
Reply from 192.168.12.79: bytes=32 time<10ms TTL=127
Reply from 192.168.12.79: bytes=32 time<10ms TTL=127
Reply from 192.168.12.79: bytes=32 time<10ms TTL=127
Ping statistics for 192.168.12.79:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 2ms

```

The routing information on the router is shown below:

```

Qtech#sh ip route
Codes: C - connected, S - static, R - RIP
O - OSPF, IA - OSPF inter area
E1 - OSPF external type 1, E2 - OSPF external type 2
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 1.1.1.0/24 is directly connected, Virtual-Access1
C 1.1.1.4/32 is directly connected, Virtual-Access1
C 192.168.12.0/24 is directly connected, FastEthernet0/1
C 192.168.201.0/24 is directly connected, FastEthernet0/0
S* 0.0.0.0/0 is directly connected, FastEthernet0/0

```

Qtech#

**Note**

that in order to enable remote VPDN users to access the intranet servers, routes to these users must be configured on the servers. Generally, you can simply set the default gateway of these servers to the internal gateway address of the router, which is 192.168.12.1 in this example.

## 6.3 Monitoring and Maintaining PPTP

### 6.3.1 Monitoring PPTP

To query the information about currently created tunnels and remote dial-in users, run the **show vpdn** command.

Command	Function
Qtech# <b>show vpdn tunnel</b>	Displays information about all the existing VPDN tunnels.
Qtech# <b>show vpdn session</b>	Displays information about all the existing VPDN sessions.
Qtech# <b>show vpdn</b>	Displays information about all the existing VPDN tunnels and sessions.

In the configuration example, the following information can be viewed:

```
Qtech# sh vpdn
%No active L2TP tunnels
PPTP Tunnel and Session Information Total tunnels 1 sessions 1
LocID Remote Name State Remote Address Port Sessions
1 estbed 192.168.201.144 1436 1
LocID RemID TunID Intf Username State Last Chg
1 49152 1 Vi1 pc connected 00:31:33
Qtech#
```

Information about the L2TP and PPTP tunnels and sessions are displayed by category. The tunnel type and statistical values are displayed first, and all the tunnel and session information is displayed later. Statistical values of the tunnels and sessions: Total tunnels 1 sessions 1. The tunnel information includes tunnel ID (LocID), remote host name (Remote Name), tunnel state (State), IP address of the remote host (Remote Address), TCP port number of the PPTP tunnel (Port), number of sessions in this tunnel (Sessions). The session information about the local call ID (LocID), remote call ID (RemID), the ID of the tunnel to which this session belongs (TunID), name of the Virtual-Access interface used by this session (Intf), user name (Username), session state (State), and the time of last state change (Last Chg).

To view detailed tunnel information, run the **show vpdn tunnel pptp locid** command. In this example, the following information can be viewed:

```
R3660# show vpdn tunnel pptp 1
PPTP tunnel id 1 is up, remote id is 0, 1 active session
Tunnel state is estbed
Remote tunnel name is
Internet Address 192.168.201.144, port 1436
Local tunnel name is
Internet Address 192.168.201.123
```

The command output contains the tunnel status, name of the peer user, peer IP address, local host name, and local IP address.

### 6.3.2 Maintaining PPTP

RGOS provides the **clear vpdn** command to clear the specified tunnel and all its sessions.

Command	Function
---------	----------



Qtech# <b>clear vpdn tunnel</b> [ [l2tp   pptp] [remote name] ]	Clears all the tunnels or the tunnel of the specified type and with the specified remote host name, and all their or its sessions.
---	--

*remote name* is the remote host name for which the tunnel should be cleared. In the configuration example, if **clear vpdn tunnel pptp** or **clear vpdn tunnel** is used after a tunnel is created, the session and the tunnel will be cleared. The command output is as follows:

```
Qtech# show vpdn
%No active L2TP tunnels
%No active PPTP tunnels
```

During network debugging, you can run the **debug vpdn** command to track the establishment process of PPTP tunnels and sessions. In addition, the debugging information obtained by using the **debug pptp** command is extremely important for tracking call failures. For details, refer to description of the PPP protocol.

Command	Function
Qtech# <b>debug vpdn</b> { error   event   packet }	Displays the debugging information during creation and use of the VPDN tunnel and session on the configuration terminal. <b>Error</b> indicates error information, <b>Event</b> indicates a general event, and <b>Packet</b> indicates the content in the control packet.



**Note** The debugging information may vary slightly with the RGOS software version.

During creation of PPTP tunnels and sessions, the **debug vpdn event** command outputs the following information:

```
VPDN: Pptp rcv start-control-connection-request from host 192.168.200.114
PPTP: New tunnel socket id =9
VPDN: Pptp get tunnel info for 192.168.200.114 ok!
VPDN: Pptp send start-control-connection-reply, ok
VPDN: Pptp tunnel id 0 state change: idle --> estbed
PPTP: Add send-echo-request timer, interval = 60
VPDN: Pptp tunnel id 0 rcv outgoing-call-request!
Pptp: Tunnel to 192.168.200.114 get config para. from vpdn-group pptp!
VPDN: Must process using ACCEPT_DIALIN parameters
Pptp: Session va0 get config para. from vpdn-group pptp!
VPDN: Pptp session va0 state change: idle --> connected
PPTP: Receive outcall request,process ok!assign local call id = 1
VPDN: Pptp tunnel id 0 send out-call reply
%LINK CHANGED: Interface virtual-access 0, changed state to up
VPDN: Pptp tunnel to 192.168.200.114 peer callid 1 rcv set-linkinfo
VPDN: Pptp tunnel to 192.168.200.114 peer callid 1 rcv set-linkinfo
%LINE PROTOCOL CHANGE: Interface virtual-access 0, changed state to UP
```

During creation of PPTP tunnels and tunnels, the **debug vpdn packet** command outputs the following information:

```
PPTP: I Start-Control-Connection-Request len 156 Magic Cookie 0x1A2B3C4D
  Protocol Version 0x100
  Framing Type 0x1
  Bearer Type 0x1
  Maximum Channels 0x0
  Firmware Revision 0x893
  Host Name:
  Vendor String: Microsoft Windows NT
PPTP: O Start-Control-Connection-Reply len 156 Magic Cookie 0x1A2B3C4D
  Protocol Version 0x100
  Framing Type 0x2
  Bearer Type 0x3
  Maximum Channels 0x0
  Firmware Revision 0x100
  Host Name: Dingjs
  Vendor String: Ret-Giant Network Operating System
```

```

PPTP: I Outgoing-Call-Request len 168 Magic Cookie 0x1A2B3C4D
  Call Id 0x4000
  Call Serial Number 0x96A5
  Min BPS 0x12C
  Max BPS 0x5F5E100
  Bearer Type 0x3
  Framing Type 0x3
  Rec Window Size 0x40
  Proc Delay 0x0
  Phone Number Length 0x0
  Phone Number:
  Subaddress:
PPTP: O Outgoing-Call-Reply len 32 Magic Cookie 0x1A2B3C4D
  Call Id 0x1
  Peer Call Id 0x4000
  Result Code 0x1
  Error Code 0x0
  Cause Code 0x0
  Connect Speed 0xFA00
  Rec Window Size 0x10
  Physical Channel Id 0x0
PPTP: I Set-Link-Info len 24 Magic Cookie 0x1A2B3C4D
  Peer Call Id 0x1
  Send ACCM 0xFFFFFFFF
  Recv ACCM 0xFFFFFFFF
%UPDOWN: Interface Virtual-Access1, changed state to up
Vi1 VPDN PROCESS Into tunnel: Sending 54 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 64 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
PPTP: I Set-Link-Info len 24 Magic Cookie 0x1A2B3C4D
  Peer Call Id 0x1
  Send ACCM 0xFFFFFFFF
  Recv ACCM 0xFFFFFFFF
Vi1 VPDN PROCESS Into tunnel: Sending 45 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 46 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 187 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 56 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 64 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 52 byte pak

```

If the physical connection with the client is interrupted, output of the **debug vpdn error** command is as follows:

```

VPDN: PPTP session Virtual-Access1 wait pak ack timeout(wait seq=37, ack=36), de
crease send window to half of current = 33!
VPDN: PPTP session Virtual-Access1 adjust ATO to 220 ms!
VPDN: PPTP session Virtual-Access1 wait pak ack timeout(wait seq=38, ack=36), de
crease send window to half of current = 16!
VPDN: PPTP session Virtual-Access1 adjust ATO to 280 ms!
VPDN: PPTP session Virtual-Access1 wait pak ack timeout(wait seq=39, ack=36), de
crease send window to half of current = 8!
VPDN: PPTP session Virtual-Access1 adjust ATO to 400 ms!
VPDN: Pptp EGRE encap fail, err=-4!
VPDN: PPTP session Virtual-Access1 wait pak ack timeout(wait seq=40, ack=36), de
crease send window to half of current = 4!
VPDN: PPTP session Virtual-Access1 adjust ATO to 640 ms!

```

### 6.3.3 FAQs

The following gives an FAQ about VPDN access over PPTP.

Suppose a PPTP dial-up connection is created on a Windows 2000 PC.

When setting the properties of the new dial-up connection, set **Security measure options** to **Advanced (user-defined setting) (D)**, set **Data encryption** to **Optional encryption (connect even if no encryption available)** on the **Setting** tab page, and allow PAP, CHAP and MS-CHAP authentication according to the authentication type configured in virtual-template that RGOS uses for PPTP dial-in. Additionally, **VPN server type** on the **Network** tab page is set to **Automatic**. After this setting, the Windows 2000 PC will try to create an L2TP tunnel before it creates a PPTP tunnel. This takes a long time. Therefore, you can set **VPN server type** to **Point-to-Point Tunneling Protocol (PPTP)**. As a result, a PPTP tunnel is directly created without an attempt to creating an L2TP tunnel.

When the RGOS router is located behind other firewalls, the TCP port 1723 of the firewall must be enabled.

## 7 CONFIGURING L2TP

### 7.1 Overview

The Layer 2 Tunnel Protocol (L2TP), as specified in RFC 2661, is a standard tunneling protocol that Internet Engineering Task Force (IETF) proposes by combining two existing tunneling protocols, namely, Cisco Layer 2 Forwarding (L2F) protocol and Microsoft Point-to-Point Tunneling Protocol (PPTP).

L2TP, an extension of the Point-to-Point Protocol (PPP), implements user authentication and data transmission using PPP. Different from PPTP, L2TP uses UDP as the transmission protocol for control and data messages.

L2TP is also an important and effective way to implement VPN. VPN allows network users to access the enterprise intranet more conveniently and securely, no matter whether the users access the network in dial-up mode or in other modes.

RGOS supports L2TP tunnels in two modes.

- L2TP tunnel initiated by the local client: In this mode, the router acts as the L2TP client and actively initiates negotiation with the L2TP server to establish a tunnel.
- L2TP tunnel initiated by the remote client: In this mode, the router accepts a connection request from the remote L2TP client and negotiates with it to establish a tunnel.



#### Note

Both modes are supported on the R26, R36, and SecVPN platforms, but the NBR platform supports only L2TP tunnel initiated by the local client.

### 7.2 Initiation by the Local Client

#### 7.2.1 Configuration Task List

- Creating and configuring an L2TP-class interface (optional)
- Creating and configuring a pseudowire-class interface (optional)
- Creating and configuring a virtual-ppp interface (mandatory)

#### 7.2.2 Creating and Configuring an L2TP-class Interface

This is an optional step for establishing an L2TP tunnel initiated by the local client. In this step, you can set the parameters for the L2TP control connection. The operations of configuring an L2TP-class interface include:

- Setting an L2TP-class unit
- Setting time for the L2TP control connection
- Setting authentication for the L2TP control connection
- Setting maintenance and update for the L2TP control connection

##### 7.2.2.1 Setting an L2TP-class Unit

Use the following commands to set an L2TP-class unit for setting parameters for the L2TP control connection.

Command	Function
Qtech(config)# <b>l2tp-class</b> <i>l2tp-class-name</i>	Configures or creates an L2TP-class interface of the specified name.
Qtech(config)# <b>no l2tp-class</b> <i>l2tp-class-name</i>	Deletes an L2TP-class interface of the specified name.

*l2tp-class-name* is the name of the created or set L2TP-class unit. The L2TP-class interface created here can be referenced by the pseudowire-class interface by name.

### 7.2.2.2 Setting Time for the L2TP Control Connection

Use the following commands to set time for the L2TP control connection.

Command	Function
Qtech(config-l2tp-class)# <b>receive-window</b> <i>size</i>	Sets the size of the receiving window of the control connection.
Qtech(config-l2tp-class)# <b>no receive-window</b>	Restores the default size of the receiving window of the control connection.
Qtech(config-l2tp-class)# <b>retransmit</b> { <b>initial</b> { <b>retries</b> <i>initial-retries</i>   <b>timeout</b> { <b>max</b>   <b>min</b> } <i>initial-timeout</i> }   <b>retries</b> <i>retries</i>   <b>timeout</b> { <b>max</b>   <b>min</b> } <i>timeout</i> }	Sets retransmission of the control connection.
Qtech(config-l2tp-class)# <b>no retransmit</b> { <b>initial</b> { <b>retries</b>   <b>timeout</b> { <b>max</b>   <b>min</b> } }   <b>retries</b>   <b>timeout</b> { <b>max</b>   <b>min</b> } }	Restores default retransmission setting of the control connection.
Qtech(config-l2tp-class)# <b>timeout setup</b> <i>seconds</i>	Sets the timeout period for establishing a control connection.
Qtech(config-l2tp-class)# <b>no timeout setup</b>	Restores the default timeout period for establishing a control connection.

*size* is the size of the receiving window, and the default value is 8.

*initial-retries* is the number of SCCRQ retransmission times, and the default value is 2.

*initial-timeout* is the interval of SCCRQ retransmission. The default minimum interval is 1 second, and the default maximum interval is 8 seconds.

*retries* is the number of retransmission times of control messages, and the default value is 5.

*timeout* is the interval of control message retransmission. The default minimum interval is 1 second, and the default maximum interval is 8 seconds.

*seconds* is the upper limit of time for establishing a control connection (tunnel), and the default value is 120 seconds.

### 7.2.2.3 Setting Authentication for the L2TP Control Connection

Use the following commands to set authentication for the L2TP control connection (tunnel).

Command	Function
Qtech(config-l2tp-class)# <b>authentication</b>	Enables authentication.
Qtech(config-l2tp-class)# <b>no authentication</b>	Disables authentication.
Qtech(config-l2tp-class)# <b>no hostname</b>	Uses the default local host name.
Qtech(config-l2tp-class)# <b>hostname</b> <i>host-name</i>	Sets the local host name corresponding to this control connection.
Qtech(config-l2tp-class)# <b>password</b> <i>pass-words</i>	Sets the tunnel password.
Qtech(config-l2tp-class)# <b>no password</b>	Cancels the tunnel password.

RGOS does not require tunnel authentication by default, but uses the name of the router as the local host name. If tunnel authentication is required, both ends must use the same tunnel password. *host-name* is the local host name set by users, and *pass-words* is the password used for tunnel authentication.

### 7.2.2.4 Setting Maintenance and Update for the L2TP Control Connection

Use the following commands to set maintenance and update for the control connection (tunnel).

Command	Function
Qtech(config-l2tp-class)# <b>hello</b> <i>interval</i>	Sets the interval of sending Hello messages.

Qtech(config-l2tp-class)# <b>no hello</b>	Restores the default interval of sending Hello messages.
---	--

Here, *interval* is the interval of sending Hello messages. Its default value is 60 seconds.

### 7.2.3 Creating and Configuring a Pseudowire-class Interface

This is an optional step for establishing an L2TP tunnel initiated by the local client. In this step, you can set L2TP data transmission parameters. The operations of setting a pseudowire-class interface include:

- Setting a pseudowire-class unit
- Setting the encapsulation mode for L2TP data transmission
- Setting IP parameters for L2TP data transmission
- Setting the L2TP control connection

#### 7.2.3.1 Setting a Pseudowire-class Unit

Use the following commands to set a pseudowire-class unit for setting L2TP data transmission parameters.

Command	Function
Qtech(config)# <b>pseudowire-class</b> <i>pseudowire-class-name</i>	Creates or configures a pseudowire-class interface of the specified name.
Qtech(config)# <b>no pseudowire-class</b> <i>pseudowire-class-name</i>	Deletes the pseudowire-class interface of the specified name.

*pseudowire-class-name* is the name of the created or set pseudowire-class unit. Here, the created pseudowire-class interface can be referenced by the pseudowire rule of the virtual-ppp interface by name.

#### 7.2.3.2 Setting the Encapsulation Mode for L2TP Data Transmission

Use the following command to set the encapsulation mode for L2TP data transmission.

Command	Function
Qtech (config-pw-class)# <b>encapsulation l2tpv2</b>	Sets the encapsulation mode for L2TP data transmission.

Note that once the encapsulation mode is set for data transmission in L2TP channels, it cannot be changed. If a user needs to set L2TP data transmission parameters on the pseudowire-class interface, the user must first set the encapsulation mode for L2TP data transmission.

#### 7.2.3.3 Setting IP Parameters for L2TP Data Transmission

Use the following commands to set IP parameters for L2TP data transmission.

Command	Function
Qtech (config-pw-class)# <b>ip dfbit set</b>	Disables channel data fragmentation.
Qtech (config-pw-class)# <b>no ip dfbit set</b>	Enables channel data fragmentation.
Qtech (config-pw-class)# <b>ip ttl</b> <i>ttl-value</i>	Sets TTL for the IP header of the channel.
Qtech (config-pw-class)# <b>no ip ttl</b>	Restores the default TTL.
Qtech (config-pw-class)# <b>ip local interface</b> <i>interface-name</i>	Specifies the local interface (address) of the channel.
Qtech(config-pw-class)# <b>no ip local interface</b> <i>interface-name</i>	Cancels the specified local interface (address) of the channel.

Setting IP parameters for L2TP data transmission actually means setting the IP header of the UDP data that carries L2TP. The system allows channel data fragmentation by default. The default TTL is 255, and the system will set the nearest local address (interface) in the route for it based on the specified peer address.



### 7.2.3.4 Setting the L2TP Control Connection

Use the following commands to set the L2TP control connection.

Command	Function
Qtech(config-pw-class)# <b>protocol l2tpv2</b> [ <i>l2tp-class-name</i> ]	Sets the L2TP control connection parameter.
Qtech(config-pw-class)# <b>no protocol</b>	Use the default control connection parameter.

Here, **l2tpv2** creates a control connection in compliance with the L2TP protocol specified in the RFC 2661. *l2tp-class-name* is set to an existing L2TP-class interface to limit the control connection parameter. If no L2TP-class interface is available, the default L2TP control connection parameter is used.

### 7.2.4 Creating and Configuring a Virtual-ppp Interface

This is a mandatory step for establishing an L2TP tunnel initiated by the local client. A specified L2TP session will be created in this step. The operations of setting a virtual-ppp interface include:

- Setting a virtual-ppp interface
- Setting the IP address
- Setting authentication
- Setting the pseudowire rule

For information about setting the IP address and authentication parameter, see related sections in the interface configuration guide.

#### 7.2.4.1 Setting a Virtual-ppp Interface

Use the following commands to set a virtual-ppp interface for establishing an L2TP session.

Command	Function
Qtech(config)# <b>interface virtual-ppp</b> <i>number</i>	Creates or configures a specified virtual-ppp interface.
Qtech(config)# <b>no interface virtual-ppp</b> <i>number</i>	Deletes the specified virtual-ppp interface.

*number* is the name of the specified virtual-ppp interface. The created virtual-ppp interface will be used to create and bind an L2TP session.

#### 7.2.4.2 Setting the Pseudowire Rule

Use the following commands to set the pseudowire rule on the virtual-ppp interface for establishing an L2TP session.

Command	Function
Qtech (config-if)# <b>pseudowire</b> <i>peer-ip-address vcid</i> { <b>encapsulation l2tpv2</b> [ <b>pw-class</b> <i>pw-class-name</i> ]   <b>pw-class</b> <i>pw-class-name</i> }	Sets the pseudowire rule.
Qtech (config-if)# <b>no pseudowire</b>	Deletes the pseudowire rule.

Once the pseudowire rule is set on a virtual-ppp interface, the virtual-ppp interface will automatically attempt to establish an L2TP session with the specified LNS. If a failure occurs, the virtual-ppp interface will attempt to establish an L2TP session 10 seconds later again. Here, *peer-ip-address* is the address of the remote LNS, *vcid* is the global ID, and *pw-class-name* is the name of the referenced pseudowire-class interface.

You can set an L2TP session with the specified LNS name when the DNS service is enabled. Our products support only the DNS client service, and the name of specified LNS must be registered on the DNS server.

Command	Function
---------	----------

Qtech (config-if)# <b>pseudowire</b> peer-ip-address vcid {encapsulation l2tpv2 [pw-class pw-class-name]   pw-class pw-class-name }	Sets the pseudowire rule.
Qtech (config-if)# <b>no pseudowire</b>	Deletes the pseudowire rule.

Once the pseudowire rule is set on a virtual-ppp interface, the virtual-ppp interface will automatically attempt to establish an L2TP session with the specified LNS. If a failure occurs, the virtual-ppp interface will attempt to establish an L2TP session 10 seconds later again. Here, *peer-hostname* is the hostname of the remote LNS. Qtech DNS will convert this hostname to a specific IP address (note that the hostname must be registered on the DNS server). *vcid* is the global ID, and *pw-class-name* is the name of the referenced pseudowire-class interface.

### 7.2.4.3 Setting the VRF Attribute

Use the following commands to set the VRF attribute on the virtual-ppp interface for establishing an L2TP session.

Command	Function
Qtech(config-Virtual-ppp 1)# <b>vpdn vrf</b> vrf-name	Sets the name of the VRF to which L2TP tunnel packets belong.
Qtech(config-Virtual-ppp 1)# <b>no vpdn vrf</b>	Deletes the VRF attribute configuration.

The command for setting the VRF attribute is generally used together with the **ip vrf forward** command of an interface. Once the VRF attribute is configured on the virtual-ppp interface, the encapsulated packets will be sent to the specified VRF. If the VRF of the interface is different from that of the tunnel, the VRF attribute of packets changes before and after encapsulation, implementing VRF spanning.

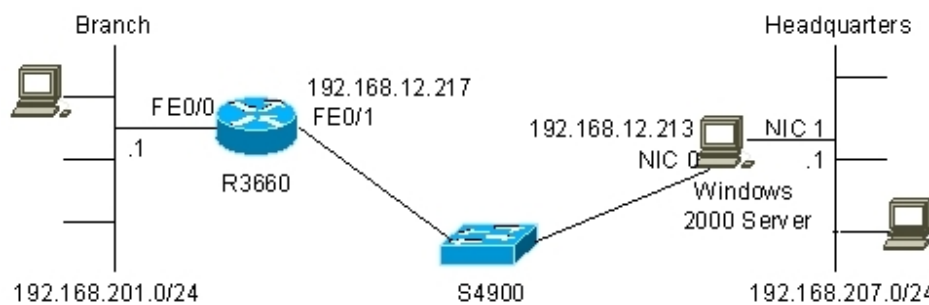
### 7.2.5 Configuration Examples

Two configuration examples are given below. In one configuration example, The Windows 2000 server is used as the remote L2TP server, and the tunnel authentication is not performed due to limitations of the Windows 2000 server. In the other configuration example, Cisco 2620 is used as the L2TP server, and tunnel authentication is performed.

#### 7.2.5.1 Establishing a Tunnel with the Windows 2000 Server

Figure shows the networking topology of the L2TP tunnel established by using Qtech router and the Windows 2000 server.

Figure 20 Networking topology of the L2TP tunnel established by using the Windows 2000 server (LNS)



The configurations of the R3660 and Windows 2000 server are respectively described as follows:

#### 20) R3660 configuration:

```
R3660# show running-config
Building configuration...
Current configuration : 868 bytes
!
hostname R3660
access-list 101 permit ip any 192.168.207.0 0.0.0.255
access-list 102 deny ip any 192.168.207.0 0.0.0.255
access-list 102 permit ip any any
```

```

!
l2tp-class l2x
hostname branch
!
pseudowire-class pw
encapsulation l2tpv2
protocol l2tpv2 l2x
ip local interface FastEthernet 0/1
!
!
!
!
!
!
interface FastEthernet 0/0
ip address 192.168.201.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface FastEthernet 0/1
ip address 192.168.12.217 255.255.255.0
ip nat outside
duplex auto
speed auto
!
interface Null 0
!
interface Virtual-ppp 1
pseudowire 192.168.12.213 12 pw-class pw
ppp pap sent-username rgnos password 7 072C04211A01
ip mtu 1460
ip address negotiate
ip nat outside
!
ip nat inside source list 102 interface FastEthernet0/1 overload
ip nat inside source list 101 interface Virtual-PPP1 overload
ip route 0.0.0.0 0.0.0.0 FastEthernet 0/1 192.168.12.1
ip route 192.168.207.0 255.255.255.0 Virtual-ppp 1
!
line con 0
line aux 0
line vty 0 4
!
!
end

```

In this configuration, the intranet of the branch shares (using the NAT function) the L2TP tunnel that the interface virtual-ppp 1 establishes with the headquarters, to access the intranet of the headquarters. The intranet of the branch shares (using the NAT function) the WAN interface FastEthernet 0/1 to access the Internet. Distribution of such data streams is controlled by using the access control list (ACL).

#### 21) Configuration of the Windows 2000 server:

```

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\>ipconfig /all
Windows 2000 IP Configuration
    Host Name . . . . . : BLIZZARD
    Primary DNS Suffix . . . . . :
    Node Type . . . . . : Broadcast
    IP Routing Enabled. . . . . : Yes
    WINS Proxy Enabled. . . . . : No
Ethernet adapter local connection 2:
    Connection-specific DNS Suffix . :

```

```

Description . . . . . : NE2000 Compatible
Physical Address. . . . . : 00-10-88-01-A5-C3
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.12.213
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.12.1
DNS Servers . . . . . : 202.101.143.141
PPP adapter RAS Server (Dial In) Interface:
Connection-specific DNS Suffix . . . . . :
Description . . . . . : WAN (PPP/SLIP) Interface
Physical Address. . . . . : 00-53-45-00-00-00
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.103.2
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . :
DNS Servers . . . . . :

C:\>route print

=====
Interface List
0x1 . . . . . MS TCP Loopback interface
0x1000002 ...00 53 45 00 00 00 . . . . . WAN (PPP/SLIP) Interface
0x1000003 ...00 10 88 01 a5 c3 . . . . . Novell 2000 Adapter.
=====
Active Routes:
Network Destination          Netmask          Gateway          Interface        Metric
0.0.0.0                      0.0.0.0          192.168.12.1    192.168.12.213   1
127.0.0.0                    255.0.0.0        127.0.0.1       127.0.0.1        1
192.168.12.0                 255.255.255.0    192.168.12.213  192.168.12.213   1
192.168.12.213              255.255.255.255  127.0.0.1       127.0.0.1        1
192.168.12.217              255.255.255.255  192.168.12.213  192.168.12.213   1
192.168.12.255              255.255.255.255  192.168.12.213  192.168.12.213   1
192.168.103.2               255.255.255.255  127.0.0.1       127.0.0.1        1
192.168.103.6               255.255.255.255  192.168.103.2   192.168.103.2    1
224.0.0.0                   224.0.0.0        192.168.12.213  192.168.12.213   1
255.255.255.255             255.255.255.255  192.168.12.213  192.168.12.213   1
Default Gateway:            192.168.12.1

=====
Persistent Routes:
None
C:\>
    
```

Note that the routing and remote access function must be enabled on the Windows 2000 server to accept the remote VPDN access. Set the access control policies (including the ACL, authentication type, IP address allocation policies, and encryption method). Default values are used here. Then, in **Network and Dial-up Connections**, click **New connection** and **Accept incoming connections** to accept the access from the remote L2TP, and set which users' L2TP access requests are accepted.



**Note**

On Windows 2000/XP, L2TP is bound with IPSec/IKE, which undoubtedly increases the workload of network administrators, because most L2TP clients (such as network devices from Cisco and Quidway) do not bind L2TP to IPSec/IKE. Establishing an L2TP tunnel by using a Windows 2000/XP PC is also difficult due to such binding. Fortunately, network administrators can cancel the binding by modifying the registry on Windows 2000/XP. To do so, choose **Start > Run**, and then enter **regedit** to open the registry editor. Find the directory **HKEY\_LOCAL\_MACHINE/ SYSTEM / CurrentControlSet / Services / RasMan /Parameters**. Create a double-byte value named **ProhibitIpSec** and set it to **1**. Press **F5** to refresh the registry, and finally, restart the Windows 2000. Then, network administrators do not need to consider the complicated IPSec/IKE setting when using L2TP. L2TP tunnels of Windows 2000/XP mentioned in this document are not bound with IPSec/IKE unless otherwise specified.

The following shows how the host "DENGL-NECBOOK" of the branch accesses the Internet and the intranet of the headquarters.

```

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\WINNT\system32>ipconfig /all
Windows 2000 IP Configuration
    Host Name . . . . . : DENGL-NECBOOK
    Primary DNS Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
Ethernet adapter local connection:
    Connection-specific DNS Suffix . :
    Description . . . . . : Realtek RTL8139(A)-based PCI Fast Ethernet Adapter
    Physical Address. . . . . : 00-10-60-75-BD-7A
    DHCP Enabled. . . . . : No
    IP Address. . . . . : 192.168.201.78
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.201.1
    DNS Servers . . . . . : 202.101.143.141
                          202.101.98.55

C:\WINNT\system32>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x1000003...00 10 60 75 bd 7a ..... NDIS 5.0 driver
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.201.1   192.168.201.78   1
127.0.0.0                  255.0.0.0        127.0.0.1       127.0.0.1        1
192.168.201.64             255.255.255.192  192.168.201.78  192.168.201.78   1
192.168.201.78             255.255.255.255  127.0.0.1       127.0.0.1        1
192.168.201.255           255.255.255.255  192.168.201.78  192.168.201.78   1
224.0.0.0                  224.0.0.0        192.168.201.78  192.168.201.78   1
255.255.255.255           255.255.255.255  192.168.201.78  192.168.201.78   1
Default Gateway:          192.168.201.1
=====
Persistent Routes:
    Network Address        Netmask          Gateway Address  Metric
    192.168.2.0            255.255.255.0   192.168.1.1      1
    192.168.9.0            255.255.255.0   192.168.12.1     1
    61.154.22.0            255.255.255.0   192.168.12.1     1
C:\WINNT\system32>ping 192.168.12.1
Pinging 192.168.12.1 with 32 bytes of data:
Reply from 192.168.12.1: bytes=32 time=50ms TTL=254
Reply from 192.168.12.1: bytes=32 time=20ms TTL=254
Reply from 192.168.12.1: bytes=32 time<10ms TTL=254
Reply from 192.168.12.1: bytes=32 time=60ms TTL=254
Ping statistics for 192.168.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 60ms, Average = 32ms
C:\WINNT\system32>ping 192.168.103.2
Pinging 192.168.103.2 with 32 bytes of data:
Reply from 192.168.103.2: bytes=32 time<10ms TTL=128
Reply from 192.168.103.2: bytes=32 time<10ms TTL=128
Reply from 192.168.103.2: bytes=32 time<10ms TTL=128
Reply from 192.168.103.2: bytes=32 time<10ms TTL=128
Ping statistics for 192.168.103.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\WINNT\system32>

```

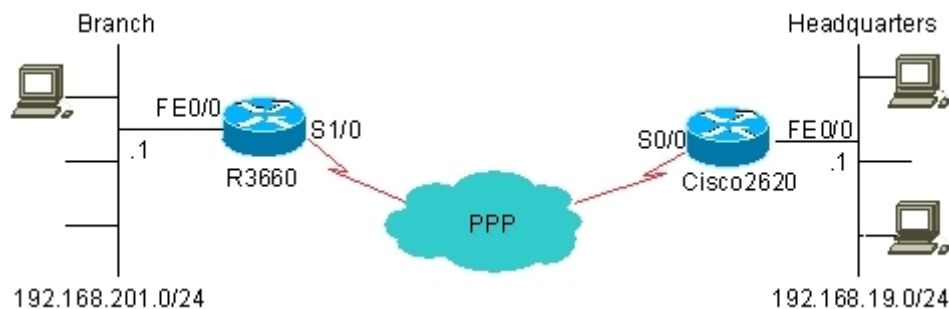
The preceding shows that the host "DENGL-NECBOOK" of the branch successfully accesses the Internet and the intranet of the headquarters. This host does not need VPDN configuration. Network administrators need to only allocate an intranet address (192.168.201.78 here) to it and set its gateway address to 192.168.201.1, which can be seen in the following information in the NAT recording node of the R3660.

```
Qtech# show ip nat translations
Pro Inside global      Inside local          Outside local         Outside global
icmp 192.168.103.6:512  192.168.201.78:512  192.168.207.2:512   192.168.207.2:512
icmp 192.168.12.217:512 192.168.201.78:512  192.168.12.1:512    192.168.12.1:512
Qtech# show ip route
Codes: C - connected, S - static, R - RIP
       O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
Gateway of last resort is 192.168.12.1 to network 0.0.0.0
 192.168.103.0/32 is subnetted, 2 subnets
C      192.168.103.6 is directly connected, Virtual-PPP1
C      192.168.103.2 is directly connected, Virtual-PPP1
C      192.168.12.0/24 is directly connected, FastEthernet0/1
C      192.168.201.0/24 is directly connected, FastEthernet0/0
S*    0.0.0.0/0 [1/0] via 192.168.12.1, FastEthernet0/1
Qtech#
```

### 7.2.5.2 Establishing a Tunnel with Cisco 2620

Figure 21 shows the networking topology of the L2TP tunnel established by using Qtech router and Cisco 2620. Cisco 2620 acts as the L2TP network server (LNS).

Figure 21 Networking topology of the L2TP tunnel established by using Cisco 2620 (LNS)



The configurations of R3660 and Cisco 2620 are respectively described as follows:

#### 22) R3660 configuration

```
R3660# show running-config
Building configuration...
Current configuration : 1136 bytes
!
hostname R3660
access-list 1 permit any
!
l2tp-class l2x
authentication
hostname branch
password share
!
pseudowire-class pw
encapsulation l2tpv2
protocol l2tpv2 l2x
ip local interface serial1/0
!
!
!
!
```



```
!  
!  
interface serial 1/0  
encapsulation PPP  
ip address 202.101.93.21 255.255.255.192  
ip nat outside  
!  
interface serial 1/1  
clock rate 64000  
!  
interface serial 1/2  
clock rate 64000  
!  
interface serial 1/3  
clock rate 64000  
!  
interface FastEthernet 0/0  
ip address 192.168.201.1 255.255.255.0  
ip nat inside  
duplex auto  
speed auto  
!  
interface FastEthernet 0/1  
duplex auto  
speed auto  
!  
interface Null 0  
!  
interface Virtual-ppp 1  
pseudowire 202.101.93.23 7 pw-class pw  
ppp pap sent-username rgnos password 7 072C04211A01  
ip mtu 1460  
ip address 192.168.103.3 255.255.255.0  
!  
router ospf  
network 192.168.103.0 0.0.0.255 area 0.0.0.1  
network 192.168.201.0 0.0.0.255 area 0.0.0.1  
!  
ip nat inside source list 1 interface Serial1/0 overload  
ip route 0.0.0.0 0.0.0.0 serial 1/0  
ip route 192.168.19.0 255.255.255.0 Virtual-ppp 1  
!  
line con 0  
line aux 0  
line vty 0 4  
!  
!  
end  
R3660#
```

In this configuration, the intranet of the branch shares (through route setting) the L2TP tunnel that the interface virtual-ppp 1 establishes with the headquarters, to access the intranet of the headquarters. The intranet of the branch shares (using the NAT function) the WAN interface Serial 0 to access the Internet. Distribution of such data streams is controlled by means of route setting. Users can also use the interface FastEthernet 0 as the WAN interface as required (for example, using the ADSL line as the WAN line), share this interface through NAT, and use the line connected to the interface Serial 0 for connecting to the headquarters. This configuration can be seen in the routing table and the ARP table.

```
R3660# show ip route  
Codes: C - connected, S - static, R - RIP  
O - OSPF, IA - OSPF inter area  
E1 - OSPF external type 1, E2 - OSPF external type 2  
Gateway of last resort is 0.0.0.0 to network 0.0.0.0  
192.168.103.0/32 is subnetted, 2 subnets
```

```
C 192.168.103.3 is directly connected, Virtual-PPP1
C 192.168.103.2 is directly connected, Virtual-PPP1
S 192.168.19.0/24 is directly connected, Virtual-PPP1
C 192.168.201.0/24 is directly connected, FastEthernet0/0
  202.101.93.0/24 is variably subnetted, 2 subnets, 2 masks
C 202.101.93.23/32 is directly connected, Serial1/0
C 202.101.93.0/26 is directly connected, Serial1/0
S* 0.0.0.0/0 is directly connected, Serial1/0
R3660#show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.201.213 3 0010.8801.a5c3 ARPA FastEthernet0/0
Internet 192.168.201.1 - 00d0.f8fb.126e ARPA FastEthernet0/0
R3660#
```

### 23) Cisco 2620 configuration

```
Cisco2620# show running-config
Building configuration...
Current configuration : 1212 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Cisco2620
!
!
username 163 password 0 163
username rgnos password 0 rgnos
username 263 password 0 263
ip subnet-zero
!
!
no ip domain-lookup
!
vpdn enable
!
vpdn-group 1
! Default L2TP VPDN group
accept-dialin
protocol l2tp
virtual-template 1
l2tp tunnel password 7 0832444F1B1C
!
call rsvp-sync
!
interface FastEthernet0/0
ip address 192.168.19.1 255.255.255.0
duplex auto
speed 10
!
interface Serial0/0
ip address 202.101.93.23 255.255.255.192
encapsulation ppp
fair-queue
clockrate 2000000
!
interface Serial0/1
no ip address
shutdown
!
interface Virtual-Template1
ip address 192.168.103.2 255.255.255.0
ppp authentication pap
```

```

!
router ospf 100
log-adjacency-changes
network 192.168.103.0 0.0.0.255 area 1
!
ip classless
ip http server
!
!
voice-port 1/0/0
!
voice-port 1/0/1
!
dial-peer cor custom
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
line aux 0
privilege level 15
line vty 0 4
privilege level 15
no login
line vty 5 15
login
!
end

```

Different from the Windows 2000 server, L2TP on Cisco 2620 is not bound with IPSec/IKE. Nevertheless, Cisco L2TP requires tunnel authentication by default, while L2TP on the Windows 2000 server does not support tunnel authentication. Cisco 2620 learns routes reachable to the network 192.168.201.0/24 over OSPF, a dynamic routing protocol, which can be seen in the routing table.

```

Cisco2620# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
O    192.168.201.0/24 [110/20] via 192.168.103.3, 00:06:26, Virtual-Access1
192.168.103.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.103.3/32 is directly connected, Virtual-Access1
C    192.168.103.0/24 is directly connected, Virtual-Access1
202.101.93.0/24 is variably subnetted, 2 subnets, 2 masks
C    202.101.93.21/32 is directly connected, Serial0/0
C    202.101.93.0/26 is directly connected, Serial0/0
C    192.168.19.0/24 is directly connected, FastEthernet0/0
Cisco2620#

```

The following shows how the host "BLIZZARD" of the branch accesses the Internet and the intranet of the headquarters.

```

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\>ipconfig /all
Windows 2000 IP Configuration
    Host Name . . . . . : BLIZZARD
    Primary DNS Suffix . . . . . :

```

```

Node Type . . . . . : Broadcast
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter local connection 2:
Connection-specific DNS Suffix . :
Description . . . . . : NE2000 Compatible
Physical Address. . . . . : 00-10-88-01-A5-C3
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.201.213
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.201.1
DNS Servers . . . . . : 202.101.143.141
C:\>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x3000003 ...00 10 88 01 a5 c3 ..... Novell 2000 Adapter.
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.201.1   192.168.201.213  1
127.0.0.0                  255.0.0.0        127.0.0.1       127.0.0.1        1
192.168.201.0              255.255.255.0   192.168.201.213 192.168.201.213  1
192.168.201.213           255.255.255.255 127.0.0.1       127.0.0.1        1
192.168.201.255           255.255.255.255 192.168.201.213 192.168.201.213  1
224.0.0.0                  224.0.0.0        192.168.201.213 192.168.201.213  1
255.255.255.255           255.255.255.255 192.168.201.213 192.168.201.213  1
Default Gateway:          192.168.201.1
=====
Persistent Routes:
None
C:\>ping 192.168.103.2
Pinging 192.168.103.2 with 32 bytes of data:
Reply from 192.168.103.2: bytes=32 time=10ms TTL=0
Reply from 192.168.103.2: bytes=32 time<10ms TTL=0
Reply from 192.168.103.2: bytes=32 time<10ms TTL=0
Reply from 192.168.103.2: bytes=32 time<10ms TTL=0
Ping statistics for 192.168.103.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
C:\>ping 192.168.19.1
Pinging 192.168.19.1 with 32 bytes of data:
Reply from 192.168.19.1: bytes=32 time<10ms TTL=254
Reply from 192.168.19.1: bytes=32 time<10ms TTL=254
Reply from 192.168.19.1: bytes=32 time<10ms TTL=254
Reply from 192.168.19.1: bytes=32 time<10ms TTL=254
Ping statistics for 192.168.19.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 202.101.93.23
Pinging 202.101.93.23 with 32 bytes of data:
Reply from 202.101.93.23: bytes=32 time<10ms TTL=254
Reply from 202.101.93.23: bytes=32 time<10ms TTL=254
Reply from 202.101.93.23: bytes=32 time<10ms TTL=254
Reply from 202.101.93.23: bytes=32 time<10ms TTL=254
Ping statistics for 202.101.93.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>

```

The preceding shows that the host "BLIZZARD" of the branch successfully accesses the Internet and the intranet of the headquarters. This host does not need VPDN configuration. Network administrators need to only allocate an intranet address (192.168.201.213 here) to it and set its gateway address to 192.168.201.1, which can be seen in the following information in the NAT recording node of the R3660.

```
R3660# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 202.101.93.21:1024 192.168.201.213:1024 202.101.93.23:1024 202.101.93.23:1024
R3660#
```

### 7.2.5.3 Establishing a Tunnel with the Windows 2000 PC by Using hostname

Connect Qtech router to a Windows 2000 PC. For information about the networking topology and PC configuration, see "Establishing a Tunnel with the Windows 2000 Server."

The hostname of the Windows 2000 PC must have been registered on the DNS server. The DNS client function must be enabled on Qtech router and route configuration must be correct so that Qtech router can ping the DNS server successfully.

Qtech LAC router configuration:

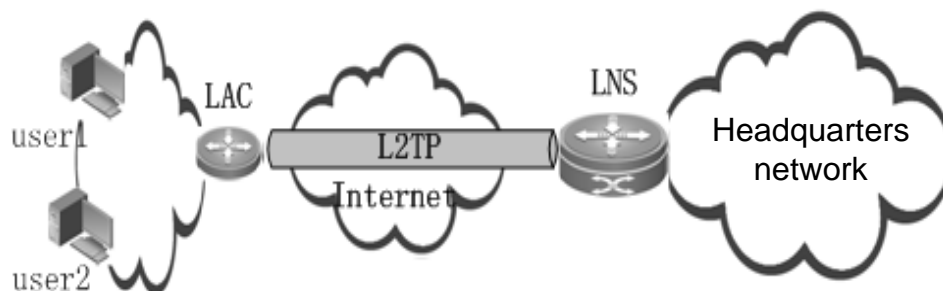
```
l2tp-class 1
!
pseudowire-class 1
 encapsulation l2tpv2
!
no service password-encryption
!
ip name-server 192.168.5.119
ip name-server 61.154.22.41
!
no ip ref load-sharing original
!
interface FastEthernet 0/0
 ip ref
 ip address 192.168.52.90 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet 0/1
 duplex auto
 speed auto
!
interface Virtual-ppp 1
 pseudowire hostname mm.hxs.meibu.com 1 encapsulation l2tpv2
 ppp pap sent-username user1 password 11
 ip address negotiate
!
ip route 0.0.0.0 0.0.0.0 192.168.52.1
!
ref parameter 75 400
line con 0
line aux 0
line vty 0 4
 login
```

The tunnel is automatically triggered for connection.

### 7.2.5.4 IPv6 over L2TP Configuration Example

In the following figure, Qtech RG-RSR20 (LAC) and RG-RSR30 (LNS) are used to establish a network connection of the L2TP tunnel. To establish an IPv6 over L2TP tunnel, the LNS assigns an IPv6 prefix to the client connected to the virtual PPP interface of the LAC over Dynamic Host Configuration Protocol version 6 Prefix Delegation (DHCPv6-PD), and delivers the domain name and DNS address over DHCPv6.

Figure 22 Establishing the IPv6 over L2TP Tunnel by RG-RSR20 (LAC) and RG-RSR30 (LNS)



The configuration of RG-RSR20 is as follows:

```
RSR20# show running-config
Building configuration...
Current configuration : 1136 bytes
!
hostname RSR20
access-list 1 permit any
!
!
l2tp-class l2x
authentication
hostname branch
password share
!
pseudowire-class pw
encapsulation l2tpv2
protocol l2tpv2 l2x
ip local interface FastEthernet 0/0
!
!
interface FastEthernet 0/0
ip address 192.168.201.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet 0/1
duplex auto
speed auto
!
interface Null 0
!
interface Virtual-ppp 1
pseudowire 192.168.202.1 7 pw-class pw
ppp pap sent-username rgnos password 7 123
ip mtu 1460
ipv6 address prefix-from-provider ::1111/64
ipv6 enable
ipv6 dhcp client pd prefix-from-provider
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
RSR20#
```

The configuration of RG-RSR30 is as follows:



```
RSR30# show running-config
Building configuration...
Current configuration : 766 bytes
!
hostname RSR30
!
ipv6 dhcp pool ipv6_dhcp_pool1
prefix-delegation pool client-prefix-pool lifetime 2000 1000
  dns-server 2001:DB8:3000:3000::42
  domain-name example.com
!
ipv6 local pool client-prefix-pool1 2001:DB8:1200::/40 48
!
vpdn enable
!
vpdn-group 1
! Default L2TP VPDN group
accept-dialin
protocol l2tp
virtual-template 1
l2tp tunnel authentication
l2tp tunnel password share
!
!
!
username rgnos password 7 123
!
interface FastEthernet 0/0
ip address 192.168.202.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet 0/1
ip address 192.168.12.217 255.255.255.0
duplex auto
speed auto
!
interface Loopback 1
ipv6 address 2001:1200::2/64
!
interface Null 0
!
interface Virtual-Template 1
ppp authentication pap
ipv6 enable
no ipv6 nd suppress-ra
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp server ipv6_dhcp_pool1
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
RSR30#
```

## 7.3 Initiation by the Remote Client

### 7.3.1 Configuration Task List

- Configuring a local address pool (optional)
- Configuring user information (optional)
- Setting VPDN global parameters (mandatory)
- Configuring a virtual-template interface (mandatory)
- Configuring VPDN-group (mandatory)

### 7.3.2 Configuring a Local Address Pool

This is an optional step for establishing an L2TP tunnel initiated by the remote client. In order to accept the L2TP connection initiated by the remote client, the LNS must allocate an IP address to the remote client if an IP address used inside the VPN is not set for the remote client. Generally, an idle IP address in a specified address pool is allocated to the client.

Use the following commands to configure a local address pool.

Command	Function
Qtech(config)# <b>ip local pool</b> <i>poolname</i> <i>first-ip</i> [ <i>last-ip</i> ]	Creates or sets a local address pool.
Qtech(config)# <b>no ip local pool</b> <i>poolname</i>	Deletes an address pool of the specified name.

*poolname* is the name of the local address pool to be created or set, *first-ip* is the first address in the address range set for the local address pool, and *last-ip* is the last address in the address range set for the local address pool.

### 7.3.3 Configuring User Information

This is an optional step for establishing an L2TP tunnel initiated by the remote client. The purpose of configuring user information is to authenticate remote L2TP clients that attempt to access the local client.

Use the following commands to configure user information.

Command	Function
Qtech(config)# <b>username</b> <i>user-name</i> <b>password</b> {0 7} <i>password</i>	Configures user information.
Qtech(config)# <b>no username</b> <i>user-name</i>	Deletes the specified user.

*user-name* is the name of the dial-in user who is allowed to access, and *password* is the password of the user. The router locally maintains a database that records names of dial-in users permitted to access and their passwords.

### 7.3.4 Setting VPDN Global Parameters

This is a mandatory step for establishing an L2TP tunnel initiated by the remote client. VPDN global parameters are set in this step. The operations of setting VPDN global parameters include:

- Enabling or disabling the VPDN function
- Setting the VPDN source address
- Setting the maximum number of VPDN sessions
- Setting the domain resolution option
- Enabling or disabling domain authentication
- Ignoring the source-address check of VPDN
- Setting VPDN rate limit
- Enabling or disabling the VPDN function is mandatory and setting the VPDN source address is optional.

#### 7.3.4.1 Enabling or Disabling the VPDN Function

If a user requires the router to accept the L2TP access from the remote client and establish an L2TP tunnel and session, the VPDN function must be enabled on the router.

Use the following commands to enable or disable the VPDN function.

Command	Function
Qtech(config)# <b>vpdn enable</b>	Enables the VPDN function.
Qtech(config)# <b>no vpdn enable</b>	Disables the VPDN function.

The VPDN enabling and disabling support instant configuration and use (that is, they are available immediately when they are configured). If the VPDN function is disabled, all the existing L2TP tunnels and sessions will be disconnected.

#### 7.3.4.2 Setting the VPDN Source Address

After the VPDN source address is set, the destination address of the tunnel set for the remote client must be consistent with the VPDN source address before an L2TP tunnel is established successfully.

Use the following commands to set the VPDN (local) source address.

Command	Function
Qtech(config)# <b>vpdn source-ip</b> <i>ip-address</i>	Sets the VPDN source address.
Qtech(config)# <b>no vpdn source-ip</b> <i>ip-address</i>	Cancels the set VPDN source address.

The system does not check whether the destination address in the received tunnel establishment request is a specific value by default.

#### 7.3.4.3 Setting the Maximum Number of VPDN Sessions

After the maximum number of VPDN sessions is set, access requests beyond the maximum value will be denied.

Use the following commands to set the maximum number of sessions supported by the VPDN server.

Command	Function
Qtech(config)# <b>vpdn session-limit</b> <i>sessions</i>	Sets the maximum number of VPDN sessions.
Qtech(config)# <b>no vpdn session-limit</b>	Restores the default maximum number of VPDN sessions.

The maximum number of sessions is the one configured by using this command by default.

#### 7.3.4.4 Setting the Domain Resolution Option

Use the following commands to set the domain resolution option in VPDN domain authentication. Domains of different types can be identified based on configuration.

Command	Function
Qtech(config)# <b>vpdn domain-delimiter</b> <i>@!%#\</i>	Sets the domain delimiter, prefix or suffix.
Qtech(config)# <b>no vpdn domain-delimiter</b>	Cancels the VPDN domain authentication option.

The system does not resolve the domain field by default.

#### 7.3.4.5 Enabling or Disabling Domain Authentication

Use the following commands to enable or disable the VPDN domain authentication, that is, determine whether to strip the domain field.

Command	Function
---------	----------

Qtech(config)# <b>vpdn authorize domain split</b>	Enables domain authentication, that is, enables domain splitting.
Qtech(config)# <b>no vpdn authorize domain</b>	Disables domain authentication.

Domain authentication is disabled by default.

#### 7.3.4.6 Ignoring the Source Address Check of VPDN

Use the following commands to ignore errors on received L2TP control packets that do not comply with the RFC specifications so as to ensure the normal negotiation.

Command	Function
Qtech(config-vpdn)# <b>vpdn ignore_source</b>	Ignores the source address check of packets sent from the peer end.
Qtech(config-vpdn)# <b>no vpdn ignore_source</b>	Strictly checks the source address of packets sent from the peer end.

The system strictly checks the source address by default.

#### 7.3.4.7 Setting VPDN Rate Limit

Use the following commands to limit the rate of establishing VPDN tunnels, namely, to limit the number of VPDN tunnels that can be established at one time.

Command	Function
Qtech(config)# <b>vpdn limit_rate rate_num</b>	Enables rate limit. <i>rate_num</i> is the number of tunnels that can be established at a time. The value range is 5 to 100.
Qtech(config)# <b>no vpdn limit_rate</b>	Disables rate limit.

Rate limit is disabled by default.

#### 7.3.4.8 Configuring Rate Limit Function for VPDN Transmission

Qtech products enable users to limit the L2TP session creation rate on the LAC, so as to limit the number of ICQ packets that can be sent at a time. To configure the rate limit function, run the following commands:

Command	Function
Qtech(config)# <b>vpdn send limit_rate rate_num</b>	Enables the rate limit function.  <i>rate_num</i> : Indicates the number of ICRQ packets that can be sent at a time. The value range is from <b>4</b> to <b>100</b> .
Qtech(config)# <b>no send vpdn limit_rate</b>	Disables the rate limit function.

The rate limit function is disabled by default.

### 7.3.5 Configuring a Virtual-Template Interface

This is a mandatory step for establishing an L2TP tunnel initiated by the remote client. This interface will become the template of the virtual-access interface that binds and carries L2TP sessions. The operations of configuring a virtual-template interface include:

For information about setting the local IP address, setting the authentication mode, and setting the peer IP address, see sections regarding the interface configuration guide.

### 7.3.5.1 Setting a Virtual-Template Interface

Use the following commands to set a virtual-template interface.

Command	Function
Qtech(config)# <b>interface virtual-template</b> <i>number</i>	Creates or configures a specified virtual-template interface.
Qtech(config)# <b>no interface virtual-template</b> <i>number</i>	Deletes the specified virtual-template interface.

*number* is the sequence number of the specified virtual-template interface. The created virtual-template interface will be used as the configuration template of the virtual-access interface that binds and carries L2TP sessions.

### 7.3.6 Configuring VPDN-group

This is a mandatory step for establishing an L2TP tunnel initiated by the remote client. VPDN-group parameters are set in this step. The operations of configuring VPDN-group include:

- Setting a VPDN-group interface (mandatory)
- Setting the tunneling mode (mandatory)
- Setting the tunneling protocol (mandatory)
- Setting a virtual template to be used (mandatory)
- Setting the peer name (optional)
- Setting the local name (optional)
- Setting the VPDN-group source address (optional)
- Setting the L2TP control connection parameters (optional)
- Setting L2TP data transmission parameters (optional)
- Setting the vrf option (optional)
- Setting the supported domain name (optional)
- Re-performing PPP negotiation (optional)
- Ignoring errors on control packets (optional)

#### 7.3.6.1 Setting a VPDN-group Interface

Use the following commands to set a VPDN-group interface.

Command	Function
Qtech(config)# <b>vpdn-group</b> <i>name</i>	Creates or configures the specified VPDN-group interface.
Qtech(config)# <b>no vpdn-group</b> <i>name</i>	Deletes the specified VPDN-group interface.

*name* is the name of the specified VPDN-group interface. The created VPDN-group interface allows related clients to access and establish tunnels.

#### 7.3.6.2 Setting the Tunneling Mode

Use the following commands to set the tunneling mode.

Command	Function
Qtech (config-vpdn)# <b>accept-dialin</b>	Allows access from the dial-in remote client.
Qtech (config-vpdn)# <b>no accept-dialin</b>	Denies the access from the dial-in remote client.

If a user needs the local router to provide the LNS function, access from the dial-in remote client must be allowed.

#### 7.3.6.3 Setting the Tunneling Protocol

Use the following commands to set the tunneling protocol.

Command	Function
Qtech(config-vpdn-acc-in)# <b>protocol</b> {any   l2tp   pptp}	Sets the tunneling protocol.
Qtech(config-vpdn-acc-in)# <b>no protocol</b>	Cancels the set tunneling protocol.

The tunneling mode must be set before a tunneling protocol is set.

#### 7.3.6.4 Setting a Virtual Template to Be Used

Use the following commands to set a virtual template used by the VPDN-group.

Command	Function
Qtech(config-vpdn-acc-in)# <b>virtual-template</b> <i>number</i>	Sets a virtual template to be used.
Qtech(config-vpdn-acc-in)# <b>no virtual-template</b>	Cancels the virtual template.

The tunneling mode must be set before a virtual template is set for the VPDN-group.

#### 7.3.6.5 Setting the Peer Name

If the peer name is set, this VPDN-group is effective only to the remote client that matches the host name. If no peer name is set, this VPDN-group is the default VPDN-group and can provide the VPDN service for any remote client.

Use the following commands to set the peer name.

Command	Function
Qtech(config-vpdn)# <b>terminate-from hostname</b> <i>name</i>	Sets the name of the peer host.
Qtech(config-vpdn)# <b>no terminate-from</b>	Cancels the set peer name.

*name* is the name of the peer host.

#### 7.3.6.6 Setting the Local Name

The local name is sent to the peer end as a record property.

Use the following commands to set the local name.

Command	Function
Qtech(config-vpdn)# <b>local name</b> <i>name</i>	Sets the local name.
Qtech(config-vpdn)# <b>no local name</b>	Cancels the set local name.

*name* is the local name. The router name is used as the local name and sent to the peer host of the tunnel by default.

#### 7.3.6.7 Setting the VPDN-group Source Address

The destination address in the tunnel establishment request sent from the remote client must match the VPDN-group source address. In this way, the VPDN-group can be applied.

Use the following commands to set the VPDN-group source address.

Command	Function
Qtech(config-vpdn)# <b>source-ip</b> <i>src-ip</i>	Sets the VPDN-group source address.



Qtech(config-vpdn)# <b>no source-ip</b>	Cancels the set VPDN-group source address.
---	--

*src-ip* is the VPDN-group source address.

### 7.3.6.8 Setting the L2TP Control Connection

Use the following commands to set the L2TP control connection.

Command	Function
Qtech(config-vpdn)# <b>l2tp tunnel authentication</b>	Enables tunnel authentication.
Qtech(config-vpdn)# <b>no l2tp tunnel authentication</b>	Disables tunnel authentication.
Qtech(config-vpdn)# <b>l2tp tunnel hello</b> <i>interval</i>	Sets the interval of sending Hello messages.
Qtech(config-vpdn)# <b>no l2tp tunnel hello</b>	Deletes the set interval of sending Hello messages.
Qtech(config-vpdn)# <b>l2tp tunnel password</b> <i>pass-word</i>	Sets the tunnel password.
Qtech(config-vpdn)# <b>no l2tp tunnel password</b>	Deletes the set tunnel password.
Qtech(config-vpdn)# <b>l2tp tunnel receive-window</b> <i>size</i>	Sets the size of the receiving window of the tunnel control connection.
Qtech(config-vpdn)# <b>no l2tp tunnel receive-window</b>	Restores the default size of the receiving window of the tunnel control connection.
Qtech(config-vpdn)# <b>l2tp tunnel retransmit</b> { <i>retries number</i>   <i>timeout {min   max} seconds</i> }	Sets retransmission of tunnel control messages.
Qtech(config-vpdn)# <b>no l2tp tunnel retransmit</b> { <i>retries</i>   <i>timeout {min max}</i> }	Restores the default retransmission setting of tunnel control messages.
Qtech(config-vpdn)# <b>l2tp tunnel timeout</b> { <i>no-session</i>   <i>setup</i> } <i>seconds</i>	Sets the maximum interval of establishing a no-session/control connection of the tunnel.
Qtech(config-vpdn)# <b>no l2tp tunnel timeout</b> { <i>no-session</i>   <i>setup</i> }	Restores the default maximum interval of establishing a no-session/control connection of the tunnel.
Qtech(config-vpdn)# <b>l2tp tunnel force_ipsec</b>	Enables forced encryption. It is used when external encryption is required. After this command is executed, packets can be sent to VPDN tunnels only after encryption.
Qtech(config-vpdn)# <b>no l2tp tunnel force_ipsec</b>	Disables forced encryption.
Qtech(config-vpdn)# <b>l2tp tunnel avp-hidden-compatible</b>	Supports the RFC2661 standard AVP Hidden parsing algorithm compatibly.
Qtech(config-vpdn)# <b>no l2tp tunnel avp-hidden-compatible</b>	Restores the default Cisco standard AVP Hidden parsing algorithm.

Tunnel authentication is not needed for establishing L2TP tunnels by default (but required on Cisco devices by default). The default interval of sending Hello control messages is 60 seconds. The default receiving window size of control messages is 4. The default number of retransmission times of control messages is 5. The default minimum and maximum intervals of retransmitting control messages are 1 second and 8 seconds respectively. The default maximum interval of no session in a tunnel is 600 seconds. The default maximum time supported by tunnels in establishing a control connection is 300 seconds. If L2TP tunnel authentication is required, the same tunnel password must be configured at both ends of the L2TP tunnel. Nevertheless, the system does not configure tunnel passwords for any L2TP tunnels by default and does not require tunnel authentication. The *interval* parameter is the interval of sending Hello messages, in seconds. The unit of the *seconds* parameter is also seconds. The forced IPsec encryption and authentication are disabled by default. The default AVP Hidden parsing algorithm uses the Cisco standard. After the RFC2661 standard AVP Hidden parsing algorithm is supported compatibly, the RFC2661 standard is used to parse and hide AVP.

### 7.3.6.9 Setting L2TP Data Transmission Parameters

Use the following commands to set IP/UDP parameters for transmitting L2TP messages.

Command	Function
Qtech(config-vpdn)# <b>l2tp ip udp checksum</b>	Sets the UDP checksum.
Qtech(config-vpdn)# <b>no l2tp ip udp Checksum</b>	Cancel the UDP checksum setting.
Qtech(config-vpdn)# <b>ip tos tos-value</b>	Sets the IP TOS field.
Qtech(config-vpdn)# <b>no ip tos</b>	Cancel the IP TOS setting.
Qtech(config-vpdn)# <b>ip precedence value</b>	Sets the IP Precedence field.
Qtech(config-vpdn)# <b>no ip precedence</b>	Cancel the IP Precedence setting.

*tos-value* is the value of the TOS field of the IP header that carries L2TP messages, and *value* is the value of the Precedence field of this IP header. For L2TP messages to be carried in L2TP tunnels of RGOS, the checksum field of UDP that carries L2TP messages must be blank, the TOS of the IP header that carries L2TP messages and the Precedence field of this IP header must be 0 by default.

Note that the TOS and Precedence fields are supported only in L2TP. Though they can be configured in PPTP, the configuration does not take effect.

### 7.3.6.10 Setting the VRF Option

Use the following commands to set the VRF to which specified L2TP tunnel packets belong. The configuration maps to the **ip vrf forward** command of the VT interface, implementing VRF spanning.

Command	Function
Qtech(config-vpdn)# <b>vpn vrf vrf-name</b>	Sets the VRF attribute for the tunnel.
Qtech(config-vpdn)# <b>no vpn vrf</b>	Deletes the VRF attribute setting of the tunnel.

*vrf-name* is the name of the VRF.

### 7.3.6.11 Setting the Supported Domain Name

The command for setting the supported domain name takes effect after the domain authentication is enabled. Only the domain matching the content of this command can be identified. If a domain does not match the content of this command, another VPDN group is used for matching. If no matched VPDN group is found, the authentication fails.

Use the following commands to set the domain name.

Command	Function
Qtech(config-vpdn)# <b>domain domain-name vrf vrf-name</b>	Sets the authentication domain name and the related VRF.
Qtech(config-vpdn)# <b>no domain domain-name</b>	Cancel the domain setting.

*domain-name* is the name of domain, and *vrf-name* is the name of the VRF.

### 7.3.6.12 Setting the Domain Name-Bound Address Pool

The command for setting the domain name-based address pool is configured in **vpdn-domain** command mode. Domain names are authenticated and information about the bound address pool configured using this command is obtained during VPDN tunnel negotiation. After the PPP negotiation is successful, the specified bound address pool is used to assign peer addresses of tunnels. The address pool configured in the virtual-template interface is used for address assignment by default.

Use the following commands to set the domain name-bound address pool.

Command	Function
---------	----------

Qtech(config-vpdn)# <b>domain</b> <i>domain-name</i> <b>vrf</b> <i>vrf-name</i> Qtech(config-vpdn-domain)# <b>pool</b> <i>pool-name</i>	Sets the address pool bound to the authentication domain name.
Qtech(config-vpdn)# <b>no domain</b> <i>domain-name</i>	Cancels the address pool binding.

*domain-name* is the name of the domain, *vrf-name* is the name of the VRF, and *pool-name* is the name of the address pool.

### 7.3.6.13 Setting the DNS Negotiation Address of PPP Bound to a Domain Name

The command for setting the DNS negotiation address of PPP bound to a domain name is configured in **vpdn-domain** command mode. The domain name is authenticated and information about the bound DNS negotiation address of PPP configured using this command is obtained during VPDN tunnel negotiation. This address is used for DNS negotiation during PPP negotiation. The DNS address of PPP configured in the virtual-template interface is used for negotiation by default.

Use the following commands to set addresses used by DNS during PPP negotiation by matching domain names.

Command	Function
Qtech(config-vpdn)# <b>domain</b> <i>domain-name</i> <b>vrf</b> <i>vrf-name</i> Qtech(config-vpdn-domain)# <b>dns</b> <i>A.B.C.D</i> <i>A.B.C.D</i>	Sets the DNS negotiation address of PPP bound to the authentication domain name.
Qtech(config-vpdn)# <b>no dns</b>	Cancels the DNS binding.

*domain-name* is the name of the domain, *vrf-name* is the name of VRF, and *A.B.C.D* is the DNS address.

### 7.3.6.14 Re-Performing PPP Authentication

When the client triggers the LAC to start dialing, the LAC acts as the LNS to authenticate the client. This command is used to perform CHAP authentication on the client again after an L2TP tunnel is established. This command is valid only on the LNS.

Use the following commands to forcibly perform complete PPP authentication again.

Command	Function
Qtech(config-vpdn)# <b>force-local-chap</b>	Forces the LNS to perform CHAP authentication on the client again.
Qtech(config-vpdn)# <b>no force-local-chap</b>	Cancels CHAP re-authentication.

### 7.3.6.15 Re-Performing PPP Negotiation

When the client triggers the LAC to start dialing, the LAC acts as the LNS to negotiate with the client. This command is used to perform LCP negotiation with the client again after an L2TP tunnel is established. This command is valid only on the LNS.

Use the following commands to forcibly perform PPP negotiation again.

Command	Function
Qtech(config-vpdn)# <b>force-local-lcp</b>	Forces the LNS to perform LCP negotiation with the client again.
Qtech(config-vpdn)# <b>no force-local-lcp</b>	Cancels LCP re-negotiation.

### 7.3.6.16 Ignoring Errors on Control Packets

Use the following commands to ignore errors on received L2TP control packets that do not comply with the RFC specifications to ensure normal negotiation.

Command	Function
---------	----------

Qtech(config-vpdn)# <b>lcp renegotiation always</b>	Ignores errors on packets from the peer end.
Qtech(config-vpdn)# <b>no lcp renegotiation always</b>	Checks whether control packets comply with RFC specifications.

### 7.3.6.17 Configuring the Function of Not Carrying Tunnel Authentication Response AVP in SCCRP Packets

This command enables the L2TP LNS to return SCCRP packets without Challenge Response AVP 13 when receiving SCCRQ packets without Challenge AVP 11 after tunnel authentication is configured. You can run the no form of this command to disable this function. This command is mainly used to ensure compatibility with the SCCRQ link detection function of devices provided by some manufacturer. It avoids returning SCCRP packets with all-zero authentication information when the other party sends SCCRQ packets without authentication information.

Command	Function
Qtech(config-vpdn)# <b>l2tp tunnel zxkeepalive-compatible</b>	Returns SCCRP packets without the challenge response AVP upon receiving SCCRQ packets without the challenge AVP.
Qtech(config-vpdn)# <b>no l2tp tunnel zxkeepalive-compatible</b>	Returns SCCRP packets with the all-zero challenge response AVP upon receiving SCCRQ packets without the challenge AVP.

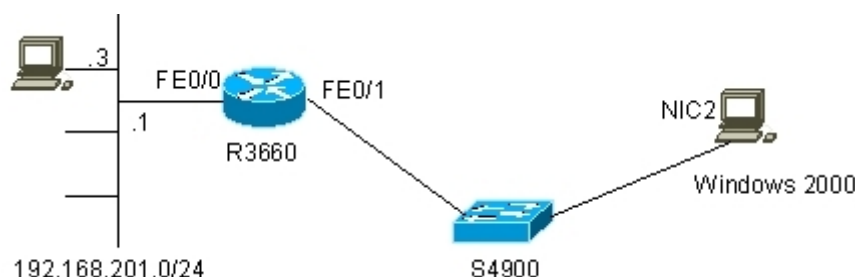
## 7.3.7 Configuration Examples

Three configuration examples are given below. In one configuration example, the Windows 2000 server is used as the remote L2TP client for access, and tunnel authentication is not performed due to limitations of the Windows 2000 server. In another example, Cisco 3640 is used as the remote L2TP client, and tunnel authentication is required. In the other example, Cisco 2620 is used as the L2TP client, and tunnel authentication is required.

### 7.3.7.1 Establishing a Tunnel with the Windows 2000 Server

Figure shows the networking topology of the L2TP tunnel established by using Qtech router R3660 and the Windows 2000 server.

Figure 23 Networking topology of the L2TP tunnel established by using the Windows 2000 server (LAC)



The configurations of the R3660 and Windows 2000 server are respectively described as follows:

24) R3660 configuration:

```
R3660# show running-config
Building configuration...
Current configuration : 708 bytes
!
hostname R3660
!
vpdn enable
!
vpdn-group 1
```

```
! Default L2TP VPDN group
accept-dialin
protocol l2tp
virtual-template 1
!
!
!
username rgnos password 7 04251F083110
!
ip local pool vpdnusers 192.168.101.3 192.168.101.253
!
interface FastEthernet 0/0
ip address 192.168.201.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet 0/1
ip address 192.168.12.217 255.255.255.0
duplex auto
speed auto
!
interface Loopback 1
ip address 192.168.101.2 255.255.255.0
!
interface Null 0
!
interface Virtual-Template 1
ppp authentication pap
ip unnumbered Loopback 1
peer default ip address pool vpdnusers
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
R3660#
```

#### 25) Configuration of the Windows 2000 server:

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\>ipconfig /all
Windows 2000 IP Configuration
    Host Name . . . . . : BLIZZARD
    Primary DNS Suffix . . . . . :
    Node Type . . . . . : Broadcast
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
Ethernet adapter local connection 2:
    Connection-specific DNS Suffix . :
    Description . . . . . : NE2000 Compatible
    Physical Address. . . . . : 00-10-88-01-A5-C3
    DHCP Enabled. . . . . : No
    IP Address. . . . . : 192.168.12.213
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.12.1
    DNS Servers . . . . . : 202.101.143.141
C:\>route print
=====
Interface List
0x1 . . . . . MS TCP Loopback interface
0x2000003 ...00 10 88 01 a5 c3 . . . . . Novell 2000 Adapter.
```

```

=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
          0.0.0.0            0.0.0.0         192.168.12.1    192.168.12.213    1
          127.0.0.0            255.0.0.0         127.0.0.1       127.0.0.1         1
          192.168.12.0        255.255.255.0    192.168.12.213  192.168.12.213    1
          192.168.12.213      255.255.255.255  127.0.0.1       127.0.0.1         1
          192.168.12.255      255.255.255.255  192.168.12.213  192.168.12.213    1
          224.0.0.0           224.0.0.0        192.168.12.213  192.168.12.213    1
          255.255.255.255     255.255.255.255  192.168.12.213  192.168.12.213    1
Default Gateway:          192.168.12.1
=====
Persistent Routes:
None
C:\>

```

In **Network and Dial-up Connections**, click **New connection** and select **Connect to a private network through the Internet** to establish a virtual private connection to the specified LNS, namely, R3660. Set the destination address to **192.168.12.217**. In the properties, set **Security measure to Advanced (user-defined setting)**. In **Advanced security settings**, set **Data encryption to Optional encryption (connect even if no encryption available)**, click **Password not encrypted (PAP)** to use PAP as the authentication protocol, and click **OK** to save these property settings. Then, you can use the user **RGNOS** set the R3660 and its password to establish a virtual connection.

The following shows the routing and communication information after a virtual connection is established successfully.

#### 26) R3660:

```

R3660# show ip route
Codes: C - connected, S - static, R - RIP
O - OSPF, IA - OSPF inter area
E1 - OSPF external type 1, E2 - OSPF external type 2
Gateway of last resort is not set
192.168.101.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.101.8/32 is directly connected, Virtual-Access1
C       192.168.101.0/24 is directly connected, Loopback1
C       192.168.12.0/24 is directly connected, FastEthernet0/1
C       192.168.201.0/24 is directly connected, FastEthernet0/0
R3660#ping 192.168.101.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.168.101.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R3660#show vpdn tunnel
L2TP Tunnel Information Total tunnels 1
LocID RemID Remote Name      State Remote Address  Port  Sessions L2TP Class/
                               VPDN Group
7      8      BLIZZARD      est   192.168.12.213  1701  1         1
%No active PPTP tunnels
R3660#
R3660# show vpdn session
L2TP Session Information Total sessions 1
LocID RemID TunID Username, Intf/ State
Last Chg
                               Vcid, Circuit
1      1      7      ,Vi1 est 00:02:08
%No active PPTP tunnels
R3660#

```

#### 27) Windows 2000 server:

```

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\>ipconfig /all
Windows 2000 IP Configuration
Host Name . . . . . : BLIZZARD

```



```

Primary DNS Suffix . . . . . :
Node Type . . . . . : Broadcast
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter local connection 2:
Connection-specific DNS Suffix . :
Description . . . . . : NE2000 Compatible
Physical Address. . . . . : 00-10-88-01-A5-C3
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.12.213
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.12.1
DNS Servers . . . . . : 202.101.143.141
PPP adapter L2TP:
Connection-specific DNS Suffix . :
Description . . . . . : WAN (PPP/SLIP) Interface
Physical Address. . . . . : 00-53-45-00-00-00
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.101.8
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 192.168.101.8
DNS Servers . . . . . :

C:\>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2000003 ...00 10 88 01 a5 c3 ..... Novell 2000 Adapter.
0xd000004 ...00 53 45 00 00 00 ..... WAN (PPP/SLIP) Interface
=====

Active Routes:
Network Destination          Netmask          Gateway          Interface        Metric
0.0.0.0                      0.0.0.0          192.168.12.1    192.168.12.213   2
0.0.0.0                      0.0.0.0          192.168.101.8   192.168.101.8    1
127.0.0.0                    255.0.0.0        127.0.0.1       127.0.0.1        1
192.168.12.0                 255.255.255.0    192.168.12.213  192.168.12.213   1
192.168.12.213               255.255.255.255  127.0.0.1       127.0.0.1        1
192.168.12.217               255.255.255.255  192.168.12.213  192.168.12.213   1
192.168.12.255               255.255.255.255  192.168.12.213  192.168.12.213   1
192.168.101.2                255.255.255.255  192.168.101.8   192.168.101.8    1
192.168.101.8                255.255.255.255  127.0.0.1       127.0.0.1        1
192.168.101.255              255.255.255.255  192.168.101.8   192.168.101.8    1
224.0.0.0                    224.0.0.0        192.168.12.213  192.168.12.213   1
224.0.0.0                    224.0.0.0        192.168.101.8   192.168.101.8    1
255.255.255.255              255.255.255.255  192.168.12.213  192.168.12.213   1
Default Gateway:            192.168.101.8

Persistent Routes:
None
C:\>ping 192.168.101.2
Pinging 192.168.101.2 with 32 bytes of data:
Reply from 192.168.101.2: bytes=32 time<10ms TTL=255
Reply from 192.168.101.2: bytes=32 time<10ms TTL=255
Reply from 192.168.101.2: bytes=32 time<10ms TTL=255
Reply from 192.168.101.2: bytes=32 time<10ms TTL=255
Ping statistics for 192.168.101.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.201.1
Pinging 192.168.201.1 with 32 bytes of data:
Reply from 192.168.201.1: bytes=32 time<10ms TTL=255
Reply from 192.168.201.1: bytes=32 time<10ms TTL=255

```

```

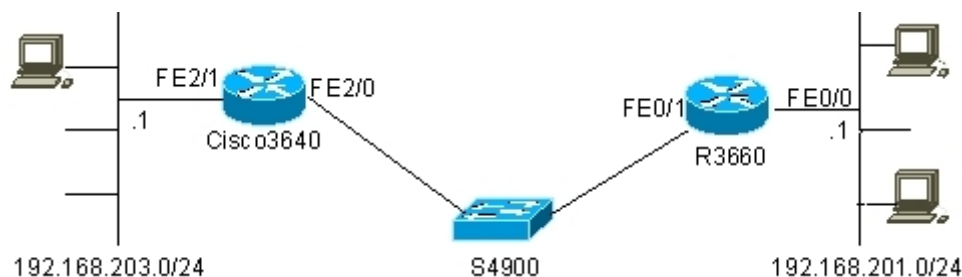
Reply from 192.168.201.1: bytes=32 time<10ms TTL=255
Reply from 192.168.201.1: bytes=32 time<10ms TTL=255
Ping statistics for 192.168.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.201.3
Pinging 192.168.201.3 with 32 bytes of data:
Reply from 192.168.201.3: bytes=32 time<10ms TTL=254
Reply from 192.168.201.3: bytes=32 time<10ms TTL=254
Reply from 192.168.201.3: bytes=32 time<10ms TTL=254
Reply from 192.168.201.3: bytes=32 time<10ms TTL=254
Ping statistics for 192.168.201.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.12.1
Pinging 192.168.12.1 with 32 bytes of data:
Reply from 192.168.12.1: bytes=32 time=10ms TTL=255
Reply from 192.168.12.1: bytes=32 time<10ms TTL=255
Reply from 192.168.12.1: bytes=32 time<10ms TTL=255
Reply from 192.168.12.1: bytes=32 time<10ms TTL=255
Ping statistics for 192.168.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
C:\>

```

### 7.3.7.2 Establishing a Tunnel with Cisco 3640

Figure shows the networking topology of the L2TP tunnel established by using Qtech router R3660 and Cisco 3640.

Figure 24 Networking topology of the L2TP tunnel established with Cisco 3640 (LAC)



The configurations of R3660 and Cisco 3640 are respectively described as follows:

#### 28) R3660 tconfiguration:

```

R3660# show running-config
Building configuration...
Current configuration : 766 bytes
!
hostname R3660
!
vpdn enable
!
vpdn-group 1
! Default L2TP VPDN group
accept-dialin
protocol l2tp
virtual-template 1
l2tp tunnel authentication
l2tp tunnel password share
!
!

```

```
!  
username rgnos password 7 025144391715  
!  
ip local pool vpdnusers 192.168.101.3 192.168.101.253  
!  
interface FastEthernet 0/0  
ip address 192.168.201.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface FastEthernet 0/1  
ip address 192.168.12.217 255.255.255.0  
duplex auto  
speed auto  
!  
interface Loopback 1  
ip address 192.168.101.2 255.255.255.0  
!  
interface Null 0  
!  
interface Virtual-Template 1  
ppp authentication pap  
ip unnumbered Loopback 1  
peer default ip address pool vpdnusers  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
!  
!  
end  
R3660#
```

#### 29) Cisco 3640 configuration:

```
C3640# show running-config  
Building configuration...  
Current configuration : 2096 bytes  
!  
version 12.3  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
no service dhcp  
!  
hostname C3640  
!  
!  
ip subnet-zero  
!  
l2tp-class l2x  
authentication  
password 0 share  
!  
pseudowire-class pw  
encapsulation l2tpv2  
protocol l2tpv2 l2x  
ip local interface FastEthernet2/0  
!  
no mpls ldp logging neighbor-changes  
no scripting tcl init  
no scripting tcl encdir  
!  
no voice hpi capture buffer
```

```
no voice hpi capture destination
!
controller E1 3/0
channel-group 1 timeslots 1-2
!
!
!
interface Loopback0
ip address 132.11.10.2 255.255.255.0
!
interface FastEthernet2/0
ip address 192.168.12.242 255.255.255.0
speed auto
duplex auto
!
interface FastEthernet2/1
ip address 192.168.203.1 255.255.255.0
duplex auto
speed auto
!
interface Serial3/0:1
ip address 192.168.1.2 255.255.255.0
!
interface Virtual-PPP1
ip address negotiated
no cdp enable
ppp pap sent-username rgos password 0 rgos
pseudowire 192.168.12.217 11 pw-class pw
!
no ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet2/0 192.168.12.1
!
!
dial-peer cor custom
!
dial-peer voice 111 voip
session protocol sipv2
codec g711alaw
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
privilege level 15
no login
line vty 5 871
login
!
!
end
```

The following shows the routing and communication information on the R3660 and Cisco 3640 after an L2TP tunnel is established.

### 30) R3660:

```
R3660# show ip route
Codes: C - connected, S - static, R - RIP
O - OSPF, IA - OSPF inter area
E1 - OSPF external type 1, E2 - OSPF external type 2
Gateway of last resort is not set
192.168.101.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.101.9/32 is directly connected, Virtual-Access1
```

```

C      192.168.101.0/24 is directly connected, Loopback1
C      192.168.12.0/24 is directly connected, FastEthernet0/1
C      192.168.201.0/24 is directly connected, FastEthernet0/0
R3660# show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name      State Remote Address  Port  Sessions L2TP Class/
                                         VPDN Group
9      21511 C3640          est   192.168.12.242  1701  1        1
LocID  RemID      TunID          Username, Intf/   State  Last Chg
                                         Vcid, Circuit
1      14        9              ,Vil             est    00:18:06
%No active PPTP tunnels
R3660#ping 192.168.101.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.168.101.9, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R3660#

```

The preceding information shows that an L2TP tunnel has been established successfully and communication can be made successfully.

### 31) Cisco 3640:

```

C3640# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 192.168.12.1 to network 0.0.0.0
C      192.168.12.0/24 is directly connected, FastEthernet2/0
C      132.11.0.0/24 is subnetted, 1 subnets
C      132.11.10.0 is directly connected, Loopback0
C      192.168.1.0/24 is directly connected, Serial3/0:1
C      192.168.101.0/32 is subnetted, 2 subnets
C      192.168.101.9 is directly connected, Virtual-PPP1
C      192.168.101.2 is directly connected, Virtual-PPP1
S*    0.0.0.0/0 [1/0] via 192.168.12.1, FastEthernet2/0
C3640# show vpdn
%No active L2F tunnels
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name      State Remote Address  Port  Sessions L2TP Class/
                                         VPDN Group
21511 9      Qtech          est   192.168.12.217  1701  1        1
LocID  RemID      TunID          Username, Intf/   State  Last Chg Uniq ID
                                         Vcid, Circuit
14     1         21511         11, Vp1          est    00:23:58 2
%No active PPTP tunnels
C3640# ping 192.168.101.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.168.101.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
C3640#

```

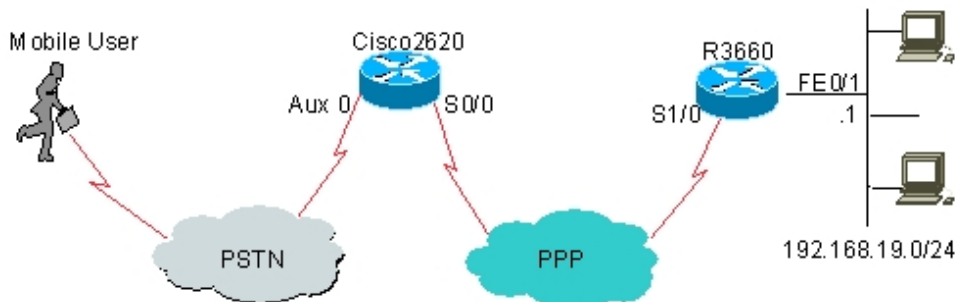
The preceding information shows that an L2TP tunnel has been established successfully on Cisco 3640 and communication can be made successfully.

### 7.3.7.3 Establishing a Tunnel with Cisco 2620

Figure shows the networking topology of the L2TP tunnel established by using the Qtech router R3660 and Cisco 2620. Here, Cisco 2620 actually works as both the access server (AS) and LAC. The AS and LAC functions are

generally provided by ISPs, and devices with the same functions but with more powerful performance, such as Cisco AS5300 or Cisco AS5800, are often used to provide the functions. Cisco 2620 is used to establish an L2TP tunnel here. The L2TP tunnel is established between Cisco 2620 and the R3660, but PPP negotiation is performed between mobile or dial-up users (mobile user in Figure ) and the R3660. The mobile user needs to only configure a dial-up connection and connect to the server in dial-up mode by using the allocated user name and password, which are not closely related to L2TP here. This is also an advantage of this tunneling mode. L2TP tunnel settings are transparent to users. The mobile user configuration and usage are not described here. For information about dial-up setting, see instructions of the related operating system.

Figure 25 Networking topology of the L2TP tunnel established with Cisco 2620 (LAC)



The configurations of R3660 and Cisco 2620 are respectively described as follows:

### 32) R3660 configuration:

```
R3660# show running-config
Building configuration...
Current configuration : 989 bytes
!
hostname R3660
!
vpdn enable
!
vpdn-group 1
! Default L2TP VPDN group
accept-dialin
protocol l2tp
virtual-template 1
l2tp tunnel authentication
l2tp tunnel password share
!
!
!
username rgnos password 7 025144391715
username pc@i-net.com.cn password 7 127654431B
!
ip local pool vpdnusers 192.168.101.3 192.168.101.253
!
interface serial 1/0
encapsulation PPP
ip address 202.101.93.21 255.255.255.0
!
interface serial 1/1
clock rate 64000
!
interface serial 1/2
clock rate 64000
!
interface serial 1/3
clock rate 64000
!
interface FastEthernet 0/0
duplex auto
```



```
speed auto
!
interface FastEthernet 0/1
ip address 192.168.19.1 255.255.255.0
duplex auto
speed auto
!
interface Loopback 1
ip address 192.168.101.2 255.255.255.0
!
interface Null 0
!
interface Virtual-Template 1
ppp authentication pap
ip unnumbered Loopback 1
peer default ip address pool vpdnusers
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
R3660#
```

### 33) Cisco 2620 configuration:

```
Cisco2620# show running-config
Building configuration...
Current configuration : 1677 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service dhcp
!
hostname Cisco2620
!
!
username pc password 0 1111
username 163 password 0 163
no aaa new-model
ip subnet-zero
!
!
!
vpdn enable
!
vpdn-group 1
request-dialin
protocol l2tp
domain i-net.com.cn
initiate-to ip 202.101.93.21
l2tp tunnel password 7 0832444F1B1C
!
interface FastEthernet0/0
ip address 192.168.7.1 255.255.255.0
duplex auto
speed 10
!
interface Serial0/0
ip address 202.101.93.23 255.255.255.0
encapsulation ppp
```

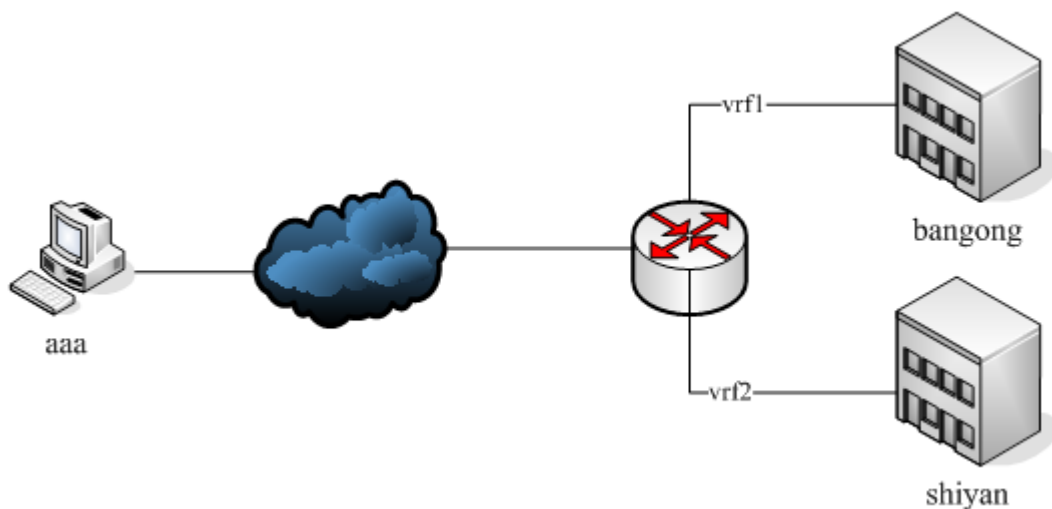
```
fair-queue
clockrate 2000000
!
interface Serial0/1
no ip address
shutdown
!
interface Async65
ip address 5.5.5.5 255.255.255.0
encapsulation ppp
dialer in-band
dialer idle-timeout 30000
dialer string 8435
dialer-group 1
async mode dedicated
peer default ip address 5.5.5.6
ppp authentication pap
!
no ip http server
ip classless
!
dialer-list 1 protocol ip permit
!
!
line con 0
exec-timeout 0 0
line aux 0
login local
modem InOut
transport input all
autoselect during-login
autoselect ppp
line vty 0 4
privilege level 15
no login
line vty 5 15
login
!
no scheduler allocate
end
Cisco2620#
```

The mobile user can access the intranet 192.168.19.0/24 connected to the R3660 through the L2TP tunnel simply by using the user name **pc@i-net.com.cn** and password **1111**.

#### 7.3.7.4 Configuration Example of Domain Authentication

The following figure shows the networking topology for one user to connect to two networks by using one public network address based on domain information.

Figure 26



```

ip vrf vrf1
ip vrf vrf2
!
vpdn enable
vpdn domain-delimiter @/%#-\ suffix
vpdn authorize domain split
!
vpdn-group 1
! Default L2TP VPDN group
accept-dialin
protocol l2tp
virtual-template 1
domain bangong vrf vrf1 /*Specify the domain name*/
domain shiyan vrf vrf2 /*Specify the domain name*/
!
!
username rgos password 7 025144391715
username pc@i-net.com.cn password 7 127654431B
!
ip local pool vpdnusers 192.168.101.3 192.168.101.253
!
interface FastEthernet 0/1
ip address 192.168.19.1 255.255.255.0
duplex auto
speed auto
!
interface Loopback 1
ip vrf forward vrf1
ip address 192.168.101.2 255.255.255.0
!
interface Loopback 2
ip vrf forward vrf2
ip address 192.168.101.2 255.255.255.0
!
interface Null 0
!
interface Virtual-Template 1
ppp authentication pap
ip unnumbered Loopback 1
peer default ip address pool vpdnusers
!
!
line con 0
line aux 0

```

```
line vty 0 4
!
!
End
```

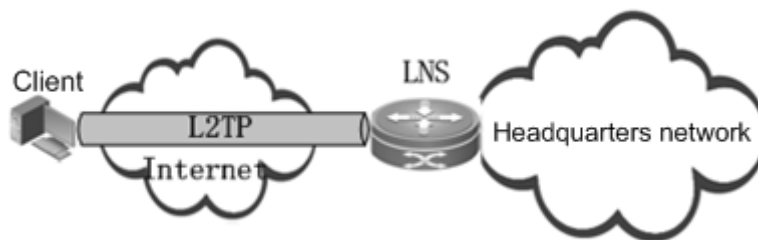
**Note**

When you need to connect to the same LNS in dial-up mode on the same device, VP ports must belong to different VRFs if different domains are used. Otherwise, the same destination address will be assigned to two VP ports, the routes of the two VP ports are duplicated, and only one route is available. On the LNS side, two VA ports belong to different VRFs, and packets forwarded by different tunnels will be sent to different VRFs. Packets sent from the LNS to one VP port may be returned by the other VP port, resulting in route dissymmetry. In this case, data forwarding is not affected, but pinging the peer address from the LNS may fail.

**7.3.7.5 IPv6 over L2TP**

In the following figure, Qtech RG-RSR30 (LNS) and a client establish the IPv6 over L2TP tunnel. The LNS assigns the IPv6 address to the client via ND, and delivers the domain name and DNS address over DHCPv6.

Figure 27 Establishing IPv6 over L2TP Tunnel by RG-RSR30 (LNS) and Client



The configuration of RG-RSR30 is as follows:

```
RSR30# show running-config
Building configuration...
Current configuration : 766 bytes
!
hostname RSR30
!
ipv6 dhcp pool ipv6_dhcp_pool1
  dns-server 2001:DB8:3000:3000::42
  domain-name example.com
  iana-address prefix 2001:1200::/64 lifetime 2000 1000
!
vpdn enable
!
vpdn-group 1
! Default L2TP VPDN group
accept-dialin
protocol l2tp
virtual-template 1
!
!
!
username rgnos password 7 025144391715
!
!
interface FastEthernet 0/0
ip address 192.168.201.1 255.255.255.0
duplex auto
speed auto
!
```

```

interface FastEthernet 0/1
ip address 192.168.12.217 255.255.255.0
duplex auto
speed auto
!
interface Loopback 1
ipv6 address 2001:1200::2/64
!
interface Null 0
!
interface Virtual-Template 1
ppp authentication pap
ipv6 enable
no ipv6 nd suppress-ra
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 unnumbered Loopback 1
ipv6 dhcp server ipv6_dhcp_pool1
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
RSR30#

```

## 7.4 Monitoring and Maintaining L2TP Tunnels

RGOS provides L2TP monitoring and maintenance functions.

### 7.4.1 Monitoring L2TP Tunnels

Use the following commands to monitor L2TP tunnels.

Command	Function
Qtech# <b>show vpdn</b> [session   tunnel [ I2tp locid ] ] Or Qtech> <b>show vpdn</b> [session   tunnel [ I2tp locid ] ]	Displays information about the current VPDN tunnel and session. Displays information about the tunnel of the specified ID.
Qtech# <b>debug vpdn error</b>	Enables the VPDN error debugging function.
Qtech# <b>no debug vpdn error</b>	Disables the VPDN error debugging function.
Qtech# <b>debug vpdn event</b>	Enables the VPDN event debugging function.
Qtech# <b>no debug vpdn event</b>	Disables the VPDN event debugging function.
Qtech# <b>debug vpdn packet</b>	Enables the VPDN packet debugging function.
Qtech# <b>no debug vpdn packet</b>	Disables the VPDN packet debugging function.
Qtech# <b>debug vpdn I2x-data</b>	Enables the VPDN I2x-data debugging function.
Qtech# <b>no debug vpdn I2x-data</b>	Disables the VPDN I2x-data debugging function.
Qtech# <b>debug vpdn I2x-errors</b>	Enables the VPDN I2x-errors debugging function.
Qtech# <b>no debug vpdn I2x-errors</b>	Disables the VPDN I2x-errors debugging function.
Qtech# <b>debug vpdn I2x-events</b>	Enables the VPDN I2x-events debugging function.

Command	Function
Qtech# <b>no debug vpdn l2x-events</b>	Disables the VPDNI2x-events debugging function.
Qtech# <b>debug vpdn l2x-packets</b>	Enables the VPDN l2x-packets debugging function.
Qtech# <b>no debug vpdn l2x-packets</b>	Disables the VPDN l2x-packets debugging function.

#### 7.4.1.1 Displaying Information About the Current L2TP Tunnel

You can use the **show vpdn** command in real time as required to view information about the current L2TP tunnel (including channel information and session information).



#### Note

The length of usernames is unlimited. The **show vpdn** command displays only the first 12 characters of a username for the sake of format alignment. You can use the **show vpdn tunnel l2tp locid** command to view the full username.

```
Qtech# show vpdn tunnel
L2TP Tunnel Information Total tunnels 1
LocID RemID Remote Name State Remote Address Port Sessions L2TP Class/
VPDN Group
1 35390 C3640 est 192.168.12.242 1701 1 1
%No active PPTP tunnels
Qtech# show vpdn session
L2TP Session Information Total sessions 1
LocID RemID TunID Username, Intf/ State
Last Chg
Vcid, Circuit
1 1261 1 rgnos,Vil1 est
01:04:42
%No active PPTP tunnels
Qtech# show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name State Remote Address Port Sessions L2TP Class/
VPDN Group
1 35390 C3640 est 192.168.12.242 1701 1 1
LocID RemID TunID Username, Intf/ State Last Chg
Vcid, Circuit
1 1261 1 rgnos,Vil1 est
01:04:45
%No active PPTP tunnels
Qtech#
Qtech# show vpdn tunnel l2tp 1
L2TP tunnel locid 1 is up, remote id is 35390, 1 active sessions
Tunnel state is est
Tunnel transport is UDP
Remote tunnel name is C3640
Internet Address 192.168.12.242, port 1701
Local tunnel name is Qtech
Internet Address 192.168.12. 217, port 1701
VPDN group for tunnel is 1
Tunnel domain unknown
ip mtu adjust disabled
Control Ns 2, Nr 4
```



### 7.4.1.2 Performing Overall VPDN Debugging

RGOS provides VPDN debugging functions, which are useful to both L2TP and PPTP. The following is an overall VPDN debugging example, in which the LNS accepts the dial-in request from the peer end and finally establishes a tunnel (including channels and sessions).

```
Qtech# debug vpdn error
vpdn protocol errors debugging is on
Qtech# debug vpdn event
vpdn events debugging is on
Qtech# debug vpdn packet
vpdn packet debugging is on
Qtech# show debug
VPDN:
vpdn events debugging is on
vpdn protocol errors debugging is on
vpdn packet debugging is on
Qtech#
VPDN PROCESS From tunnel: Received 158 byte pak
L2X: UDP socket write 168 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
L2X: UDP socket write 40 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
VPDN PROCESS From tunnel: Pak consumed
VPDN PROCESS From tunnel: Received 70 byte pak
L2X: UDP socket write 40 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
VPDN PROCESS From tunnel: Pak consumed
VPDN PROCESS From tunnel: Received 76 byte pak
Get virtual-access from free queue: Virtual-Access1
Clone virtual-access from interface Virtual-Template1
L2X: UDP socket write 56 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
L2X: UDP socket write 40 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
VPDN PROCESS From tunnel: Pak consumed
VPDN PROCESS From tunnel: Received 76 byte pak
L2X: UDP socket write 40 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
Vi1 Tn1/Sn 3/1 L2TP: Virtual interface created for unknown, bandwidth 1024 Kbps
Vi1 Tn1/Sn 3/1 L2TP: VPDN session up
VPDN PROCESS From tunnel: Pak consumed
VPDN PROCESS From tunnel: Received 50 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 14 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
%UPDOWN: Interface Virtual-Access1, changed state to up
Vi1 VPDN PROCESS Into tunnel: Sending 54 byte pak
L2X: UDP socket write 54 bytes, 255.255.255.255(1701) to 4.83.68.68(1701)
VPDN PROCESS From tunnel: Received 50 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 14 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
L2X: UDP socket write 50 bytes, 255.255.255.255(1701) to 4.83.68.68(1701)
Vi1 VPDN PROCESS Into tunnel: Sending 54 byte pak
L2X: UDP socket write 54 bytes, 255.255.255.255(1701) to 4.83.68.68(1701)
VPDN PROCESS From tunnel: Received 50 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 14 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
L2X: UDP socket write 50 bytes, 255.255.255.255(1701) to 4.83.68.68(1701)
Vi1 VPDN PROCESS Into tunnel: Sending 54 byte pak
L2X: UDP socket write 54 bytes, 255.255.255.255(1701) to 4.83.68.68(1701)
VPDN PROCESS From tunnel: Received 50 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 14 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
L2X: UDP socket write 50 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
Vi1 VPDN PROCESS Into tunnel: Sending 54 byte pak
L2X: UDP socket write 54 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
VPDN PROCESS From tunnel: Received 54 byte pak
```

```

Vi1 VPDN PROCESS From tunnel: Queue 18 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
VPDN PROCESS From tunnel: Received 56 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 20 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
Vi1 VPDN PROCESS Into tunnel: Sending 45 byte pak
L2X: UDP socket write 45 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
L2X: UDP socket write 50 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
VPDN PROCESS From tunnel: Received 50 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 14 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
L2X: UDP socket write 50 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
VPDN PROCESS From tunnel: Received 50 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 14 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
VPDN PROCESS From tunnel: Received 50 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 14 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
L2X: UDP socket write 50 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
%UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
Qtech# show ip route
Codes: C - connected, S - static, R - RIP
O - OSPF, IA - OSPF inter area
E1 - OSPF external type 1, E2 - OSPF external type 2
Gateway of last resort is not set
192.168.101.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.101.5/32 is directly connected, Virtual-Access1
C      192.168.101.0/24 is directly connected, Virtual-Access1
C      192.168.12.0/24 is directly connected, FastEthernet0
C      192.168.201.0/24 is directly connected, Ethernet0
Qtech#

```

### 7.4.1.3 Performing L2TP Data Debugging

If a user needs to check whether L2TP can send control messages successfully, enable the L2TP data debugging function. The following is an L2TP data debugging example, in which the LNS accepts the dial-in request from the peer end and finally establishes a tunnel (including channels and sessions) after the l2x-data debugging function is enabled.

```

Qtech# no debug all
All possible debugging has been turned off
Qtech# debug vpdn l2x-data
L2X data packets debugging is on
Qtech#
L2X: Punting to L2TP control message queue
L2X: Punting to L2TP control message queue
L2X: Punting to L2TP control message queue
L2X: Punting to L2TP control message queue
L2X: Punting to L2TP control message queue
L2X: Punting to L2TP control message queue
%UPDOWN: Interface Virtual-Access1, changed state to up
%UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
Qtech#

```

### 7.4.1.4 Performing L2TP Error Debugging

Users can enable the l2x-errors debugging function to check whether a tunnel establishment failure results from configuration inconsistency at both ends (for example, different tunnel authentication passwords at both ends). The following is an example of errors reported due to a tunnel authentication failure.

```

Qtech# no debug all

```

```
All possible debugging has been turned off
Qtech# debug vpdn l2x-errors
L2X protocol errors debugging is on
Qtech# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)# interface virtual-ppp 1
Qtech(config-if)# no shutdown
Qtech(config-if)# end
Qtech#
Tnl 14 L2TP: Tunnel auth failed for BLIZZARD
Tnl 14 L2TP: Expected
9E 8D 7A 8E 78 EA 41 9F A1 74 01 21 DE 4F F3 F0
Tnl 14 L2TP: Got
84 E5 62 69 AE 46 A5 98 4E FE E2 38 EE F2 B7 E2
Qtech# no debug all
All possible debugging has been turned off
Qtech#
```

#### 7.4.1.5 Performing L2TP Event Debugging

Users can enable the l2x-events debugging function to check the entire process of L2TP tunnel negotiation and establishment. The following is an L2TP event debugging example, in which the LNS accepts the dial-in request from the peer end and finally establishes a tunnel (including channels and sessions) after the l2x-events debugging function is enabled. The tunnel authentication function is enabled here.

```
Qtech# show vpdn tunnel
%No active L2TP tunnels
%No active PPTP tunnels
Qtech# no debug all
All possible debugging has been turned off
Qtech# debug vpdn l2x-events
L2X protocol events debugging is on
Qtech#
L2TP: I SCCRQ from C3640 tnl 26656
New tunnel created for remote C3640, address 192.168.12.242
Tnl 0 L2TP: Got a challenge in SCCRQ, C3640
Tnl 20 L2TP: O SCCRP to C3640 tnlid 26656
Tnl 20 L2TP: Control channel retransmit delay set to 1 seconds
Tnl 20 L2TP: Tunnel state change from idle to wait-ctl-conn
Tnl 20 L2TP: I SCCCN from C3640 tnl 26656
Tnl 20 L2TP: Got a Challenge Response in SCCCN, C3640
Tnl 20 L2TP: Tunnel Authentication success
Tnl 20 L2TP: Tunnel state change from wait-ctl-conn to established
Tnl 20 L2TP: SM State established
Tnl 20 L2TP: I ICRQ from C3640 tnl 26656
Tnl/Sn 20/1 L2TP: Accepted ICRQ, new session created
Tnl/Sn 20/1 L2TP: O ICRP to C3640 26656/1279
Tnl/Sn 20/1 L2TP: Session state change from idle to wait-connect
Tnl 20 L2TP: Control channel retransmit delay set to 1 seconds
Tnl/Sn 20/1 L2TP: I ICCN from C3640 tnl 26656, cl 1279
Tnl/Sn 20/1 L2TP: Session state change from wait-connect to wait-for-service-selection-iccn
Vil Tnl/Sn 20/1 L2TP: Session state change from wait-for-service-selection-iccn to established
%UPDOWN: Interface Virtual-Access1, changed state to up
%UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
Qtech# show ip route
Codes: C - connected, S - static, R - RIP
O - OSPF, IA - OSPF inter area
E1 - OSPF external type 1, E2 - OSPF external type 2
Gateway of last resort is not set
192.168.101.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.101.7/32 is directly connected, Virtual-Access1
C      192.168.101.0/24 is directly connected, Virtual-Access1
```

```

C 192.168.12.0/24 is directly connected, FastEthernet0
C 192.168.201.0/24 is directly connected, Ethernet0
Qtech# show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name State Remote Address Port Sessions L2TP Class/
VPDN Group
20 26656 C3640 est 192.168.12.242 1701 1 1
LocID RemID TunID Username, Intf/ State Last Chg
Vcid, Circuit
1 1279 20 rgnos,Vil est 00:00:38
%No active PPTP tunnels
Qtech#

```

The following is an L2TP event debugging example, in which the LNS accesses the remote L2TP server and finally establishes a tunnel (including channels and sessions) after the l2x-events debugging function is enabled. The tunnel authentication function is disabled here.

```

Qtech# no debug all
All possible debugging has been turned off
Qtech# debug vpdn l2x-events
L2X protocol events debugging is on
Qtech# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)# interface virtual-ppp 1
Qtech(config-if)# no shut
Qtech(config-if)# end
Qtech#
Tnl 21 L2TP: SM State idle
Tnl 21 L2TP: O SCCRQ
Tnl 21 L2TP: Control channel retransmit delay set to 1 seconds
Tnl 21 L2TP: Tunnel state change from idle to wait-ctl-reply
Tnl 21 L2TP: SM State wait-ctl-reply
Tnl 21 L2TP: O Resend SCCRQ, flg TLS, ver 2, len 96, tnl 0, ns 0, nr 0
Tnl 21 L2TP: Control channel retransmit delay set to 1 seconds
Tnl 21 L2TP: I SCCRP from
Tnl 21 L2TP: O SCCCN to BLIZZARD tnlid 40
Tnl 21 L2TP: Control channel retransmit delay set to 1 seconds
Tnl 21 L2TP: Tunnel state change from wait-ctl-reply to established
Tnl 21 L2TP: SM State established
Vil Tnl/Sn 21/1 L2TP: O ICRQ to BLIZZARD 40/0
Vil Tnl/Sn 21/1 L2TP: Control channel retransmit delay set to 1 seconds
Vil Tnl/Sn 21/1 L2TP: Session state change from wait-for-tunnel to wait-reply
Vil Tnl/Sn 21/1 L2TP: I ICRP from BLIZZARD
Vil Tnl/Sn 21/1 L2TP: O ICCN to BLIZZARD 40/1
Vil Tnl/Sn 21/1 L2TP: Control channel retransmit delay set to 1 seconds
Vil Tnl/Sn 21/1 L2TP: Session state change from wait-reply to established
%UPDOWN: Interface Virtual-PPP1, changed state to up
%UPDOWN: Line protocol on Interface Virtual-PPP1, changed state to up
Qtech# show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name State Remote Address Port Sessions L2TP Class/
VPDN Group
21 40 BLIZZARD est 192.168.12.213 1701 1
LocID RemID TunID Username, Intf/ State Last Chg
Vcid, Circuit
1 1 21 13,Vil est 00:00:27
%No active PPTP tunnels
Qtech#

```

#### 7.4.1.6 Performing L2TP Message Data Debugging

L2TP message data debugging refers to displaying the content of an L2TP control message after a user enables the l2x-packets debugging function. The following is an L2TP message data debugging example, in which the LNS

accepts the dial-in request from the peer end and finally establishes a tunnel (including channels and sessions) after the l2x-packets debugging function is enabled. The tunnel authentication function is enabled here.

```
Qtech# no debug all
All possible debugging has been turned off
Qtech# debug vpdn l2x-packets
L2X control packets debugging is on
Qtech# show vpdn
%No active L2TP tunnels
%No active PPTP tunnels
Qtech#
L2TP: I SCCRQ from C3640 tnl 18889
L2X: Parse AVP 0, len 8, flag 0x8000 (M)
L2X: Parse SCCRQ
L2X: Parse AVP 2, len 8, flag 0x8000 (M)
L2X: Protocol Ver 1
L2X: Parse AVP 6, len 8, flag 0x0
L2X: Firmware Ver 0x1130
L2X: Parse AVP 7, len 11, flag 0x8000 (M)
L2X: Hostname C3640
L2X: Parse AVP 8, len 25, flag 0x0
L2X: Vendor Name Cisco Systems, Inc.
L2X: Parse AVP 10, len 8, flag 0x8000 (M)
L2X: Rx Window Size 800
L2X: Parse AVP 11, len 22, flag 0x8000 (M)
L2X: Chlng
      98 20 4E 34 6A 4C E1 E7 FA CF 58 07 FF 4E 56 A3
L2X: Parse AVP 9, len 8, flag 0x8000 (M)
L2X: Assigned Tunnel ID 18889
L2X: Parse AVP 3, len 10, flag 0x8000 (M)
L2X: Framing Cap 0x3
L2X: Parse AVP 4, len 10, flag 0x8000 (M)
L2X: Bearer Cap 0x3
L2X: No missing AVPs in SCCRQ
L2X: I SCCRQ, flg TLS, ver 2, len 130, tnl 0, ns 0, nr 0 contiguous pak, size 130
C8 02 00 82 00 00 00 00 00 00 00 00 80 08 00 00
00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
00 06 11 30 80 0B 00 00 00 07 43 33 36 34 30 00
19 00 00 00 08 43 69 73 63 6F 20 53 79 73 74 65
6D 73 2C 20 49 6E 63 2E ...
Tnl 22 L2TP: O SCCRP to C3640 tnlid 18889
Tnl 22 L2TP: O SCCRP, flg TLS, ver 2, len 140, tnl 18889, ns 0, nr 1
C8 02 00 8C 49 C9 00 00 00 00 00 01 80 08 00 00
00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00
00 03 00 00 00 01 80 0A 00 00 00 04 00 00 00 00
00 08 00 00 00 06 11 30 80 0A 00 00 00 07 52 36
32 31 00 0E 00 00 00 08 ...
Tnl 22 L2TP: O ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 18889, ns 1, nr 1
C8 02 00 0C 49 C9 00 00 00 01 00 01
Tnl 22 L2TP: Parse AVP 0, len 8, flag 0x8000 (M)
Tnl 22 L2TP: Parse SCCCN
Tnl 22 L2TP: I SCCCN from C3640 tnl 18889
Tnl 22 L2TP: Parse AVP 13, len 22, flag 0x8000 (M)
Tnl 22 L2TP: Chlng Resp
5C D5 A4 37 36 A6 7D 0F FE EF 22 48 B8 DF F5 12
Tnl 22 L2TP: No missing AVPs in SCCCN
Tnl 22 L2TP: I SCCCN, flg TLS, ver 2, len 42, tnl 22, ns 1, nr 1 contiguous pak, size
42
C8 02 00 2A 00 16 00 00 00 01 00 01 80 08 00 00
00 00 00 03 80 16 00 00 00 0D 5C D5 A4 37 36 A6
7D 0F FE EF 22 48 B8 DF F5 12
Tnl 22 L2TP: O ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 18889, ns 1, nr 2
C8 02 00 0C 49 C9 00 00 00 01 00 02
Tnl 22 L2TP: Parse AVP 0, len 8, flag 0x8000 (M)
```



```

Tnl 22 L2TP: Parse ICRQ
Tnl 22 L2TP: I ICRQ from C3640 tnl 18889
Tnl 22 L2TP: Parse AVP 15, len 10, flag 0x8000 (M)
Tnl 22 L2TP: Serial Number -1714567290
Tnl 22 L2TP: Parse AVP 14, len 8, flag 0x8000 (M)
Tnl 22 L2TP: Assigned Call ID 1280
Tnl 22 L2TP: Parse AVP 18, len 10, flag 0x8000 (M)
Tnl 22 L2TP: Bearer Type 0
Tnl 22 L2TP: No missing AVPs in ICRQ
Tnl 22 L2TP: I ICRQ, flg TLS, ver 2, len 48, tnl 22, ns 2, nr 1 contiguous pak,size 48
C8 02 00 30 00 16 00 00 00 02 00 01 80 08 00 00
00 00 00 0A 80 0A 00 00 00 0F 99 CD C7 86 80 08
00 00 00 0E 05 00 80 0A 00 00 00 12 00 00 00 00
Tnl/Sn 22/1 L2TP: O ICRP to C3640 18889/1280
Tnl/Sn 22/1 L2TP: O ICRP, flg TLS, ver 2, len 28, tnl 18889, lsid 1, rsid 1280,ns 1,
nr 3
C8 02 00 1C 49 C9 05 00 00 01 00 03 80 08 00 00
00 00 00 0B 80 08 00 00 00 0E 00 01
Tnl 22 L2TP: O ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 18889, ns 2, nr 3
C8 02 00 0C 49 C9 00 00 00 02 00 03
Tnl/Sn 22/1 L2TP: I ICCN from C3640 tnl 18889, cl 1280
Tnl/Sn 22/1 L2TP: Parse AVP 0, len 8, flag 0x8000 (M)
Tnl/Sn 22/1 L2TP: Parse ICCN
Vil Tnl/Sn 22/1 L2TP: Parse AVP 24, len 10, flag 0x8000 (M)
Vil Tnl/Sn 22/1 L2TP: Connect Speed 0
Vil Tnl/Sn 22/1 L2TP: Parse AVP 19, len 10, flag 0x8000 (M)
Vil Tnl/Sn 22/1 L2TP: Framing Type 1
Tnl/Sn 22/1 L2TP: No missing AVPs in ICCN
Tnl/Sn 22/1 L2TP: I ICCN, flg TLS, ver 2, len 48, tnl 22, lsid 1, rsid 1280, ns 3, nr
2 contiguous pak, size 48
C8 02 00 30 00 16 00 01 00 03 00 02 80 08 00 00
00 00 00 0C 80 0A 00 00 00 18 00 00 00 00 80 0A
00 00 00 13 00 00 00 01 00 08 00 00 00 1D 00 04
Tnl 22 L2TP: O ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 18889, ns 2, nr 4
C8 02 00 0C 49 C9 00 00 00 02 00 04
%UPDOWN: Interface Virtual-Access1, changed state to up
%UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
Qtech# show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name State Remote Address Port Sessions L2TP Class/
VPDN Group
22 18889 C3640 est 192.168.12.242 1701 1 1
LocID RemID TunID Username, Intf/ State Last Chg
Vcid, Circuit
1 1280 22 ,Vil est 00:00:19
%No active PPTP tunnels
Qtech# show ip route
Codes: C - connected, S - static, R - RIP
O - OSPF, IA - OSPF inter area
E1 - OSPF external type 1, E2 - OSPF external type 2
Gateway of last resort is not set
192.168.101.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.101.8/32 is directly connected, Virtual-Access1
C 192.168.101.0/24 is directly connected, Virtual-Access1
C 192.168.12.0/24 is directly connected, FastEthernet0
C 192.168.201.0/24 is directly connected, Ethernet0
Qtech#

```

The following is an L2TP message data debugging example, in which the LAC accesses the remote L2TP server and finally establishes a tunnel (including channels and sessions), after the l2x-packets debugging function is enabled. The tunnel authentication function is disabled here.

```

Qtech# no debug all
All possible debugging has been turned off

```



```
Qtech# debug vpdn l2x-packets
L2X control packets debugging is on
Qtech# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)# interface virtual-ppp 1
Qtech(config-if)# no shutdown
Qtech(config-if)# end
Qtech#
Tnl 21 L2TP: O SCCRQ
Tnl 21 L2TP: O SCCRQ, flg TLS, ver 2, len 96, tnl 0, ns 0, nr 0
C8 02 00 60 00 00 00 00 00 00 00 80 08 00 00
00 00 00 01 80 08 00 00 00 02 01 00 80 0A 00 00
00 03 00 00 00 01 80 0A 00 00 00 04 00 00 00 00
00 08 00 00 00 06 11 30 80 0A 00 00 00 07 52 36
32 31 00 0E 00 00 00 08 ...
Tnl 21 L2TP: Parse AVP 0, len 8, flag 0x8000 (M)
Tnl 21 L2TP: Parse SCCRP
Tnl 21 L2TP: Parse AVP 2, len 8, flag 0x8000 (M)
Tnl 21 L2TP: Protocol Ver 1
Tnl 21 L2TP: Parse AVP 3, len 10, flag 0x8000 (M)
Tnl 21 L2TP: Framing Cap 0x1
Tnl 21 L2TP: Parse AVP 4, len 10, flag 0x8000 (M)
Tnl 21 L2TP: Bearer Cap 0x0
Tnl 21 L2TP: Parse AVP 6, len 8, flag 0x0
Tnl 21 L2TP: Firmware Ver 0x500
Tnl 21 L2TP: Parse AVP 7, len 14, flag 0x8000 (M)
Tnl 21 L2TP: Hostname BLIZZARD
Tnl 21 L2TP: Parse AVP 8, len 15, flag 0x0
Tnl 21 L2TP: Vendor Name Microsoft
Tnl 21 L2TP: Parse AVP 9, len 8, flag 0x8000 (M)
Tnl 21 L2TP: Assigned Tunnel ID 41
Tnl 21 L2TP: Parse AVP 10, len 8, flag 0x8000 (M)
Tnl 21 L2TP: Rx Window Size 8
Tnl 21 L2TP: No missing AVPs in SCCRP
Tnl 21 L2TP: I SCCRP, flg TLS, ver 2, len 101, tnl 21, ns 0, nr 1 contiguous pak, size
101
C8 02 00 65 00 15 00 00 00 00 01 80 08 00 00
00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00
00 03 00 00 00 01 80 0A 00 00 00 04 00 00 00 00
00 08 00 00 00 06 05 00 80 0E 00 00 00 07 42 4C
49 5A 5A 41 52 44 00 0F ...
Tnl 21 L2TP: O SCCCN to BLIZZARD tnlid 41
Tnl 21 L2TP: O SCCCN, flg TLS, ver 2, len 20, tnl 41, ns 1, nr 1
C8 02 00 14 00 29 00 00 00 01 00 01 80 08 00 00
00 00 00 03
Vi1 Tnl/Sn 21/1 L2TP: O ICRQ to BLIZZARD 41/1
Vi1 Tnl/Sn 21/1 L2TP: O ICRQ, flg TLS, ver 2, len 48, tnl 41, lsid 1, rsid 1, ns 2, nr
1
C8 02 00 30 00 29 00 00 00 02 00 01 80 08 00 00
00 00 00 0A 80 08 00 00 00 0E 00 01 80 0A 00 00
00 0F 00 00 00 00 80 0A 00 00 00 12 00 00 00 02
Tnl 21 L2TP: O ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 41, ns 3, nr 1
C8 02 00 0C 00 29 00 00 00 03 00 01
Tnl 21 L2TP: I ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 21, ns 1, nr 2
Tnl 21 L2TP: I ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 21, ns 1, nr 3
Vi1 Tnl/Sn 21/1 L2TP: Parse AVP 0, len 8, flag 0x8000 (M)
Vi1 Tnl/Sn 21/1 L2TP: Parse ICRP
Vi1 Tnl/Sn 21/1 L2TP: Parse AVP 14, len 8, flag 0x8000 (M)
Vi1 Tnl/Sn 21/1 L2TP: Assigned Call ID 1
Vi1 Tnl 21/1 L2TP: No missing AVPs in ICRP
Vi1 Tnl/Sn 21/1 L2TP: I ICRP, flg TLS, ver 2, len 28, tnl 21, lsid 1, rsid 1, ns 1, nr
3 contiguous pak, size 28
C8 02 00 1C 00 15 00 01 00 03 80 08 00 00
```

```

00 00 00 0B 80 08 00 00 00 0E 00 01
Vi1 Tnl/Sn 21/1 L2TP: O ICCN to BLIZZARD 41/1
Vi1 Tnl/Sn 21/1 L2TP: O ICCN, flg TLS, ver 2, len 40, tnl 41, lsid 1, rsid 1, ns 3, nr
2
C8 02 00 28 00 29 00 01 00 03 00 02 80 08 00 00
00 00 00 0C 80 0A 00 00 00 18 00 98 96 80 80 0A
00 00 00 13 00 00 00 01
Tnl 21 L2TP: O ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 41, ns 4, nr 2
C8 02 00 0C 00 29 00 00 00 04 00 02
Tnl 21 L2TP: I ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 21, ns 2, nr 4
%UPDOWN: Interface Virtual-PPp1, changed state to up
%UPDOWN: Line protocol on Interface Virtual-PPp1, changed state to up
Qtech# show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name      State Remote Address  Port  Sessions L2TP Class/
                                         VPDN Group
21      41      BLIZZARD              est   192.168.12.213  1701  1
LocID   RemID   TunID   Username, Intf/   State  Last Chg
        Vcid, Circuit
1       1       21      13,Vi1           est   00:00:13
%No active PPTP tunnels
Qtech#

```

### 7.4.2 Maintaining L2TP Tunnels

Use the following command to clear a specified L2TP tunnel.

Command	Function
Qtech# <b>clear vpdn tunnel</b> [{ <b>pptp</b>   <b>l2tp</b> } [ <i>remote-host-name</i> ]]	Clears a specified tunnel.

*remote-host-name* is the name of the peer host of a tunnel. In addition, all L2TP-related configuration commands in RGOS support instant configuration and use. Users can set or change L2TP parameters as required. The following is an example of clearing all tunnels.

```

Qtech# show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name      State Remote Address  Port  Sessions L2TP Class/
                                         VPDN Group
22      18889 C3640              est   192.168.12.242  1701  1
LocID   RemID   TunID   Username, Intf/   State  Last Chg
        Vcid, Circuit
1       1280   22      ,Vi1             est   00:14:52
%No active PPTP tunnels
Qtech# clear vpdn tunnel
Qtech#
%UPDOWN: Line protocol on Interface Virtual-Access1, changed state to down
%CHANGED: Interface Virtual-Access1, changed state to administratively down
Qtech# show vpdn
%No active L2TP tunnels
%No active PPTP tunnels
Qtech#

```

### 7.4.3 FAQs

Common questions about L2TP tunnel establishment on the RGOS and their answers are presented as follows:

- Establishing an L2TP tunnel by interconnecting with a Windows PC: Note that L2TP is supported only in Microsoft Windows 2000 and later versions. Only the PPTP tunneling protocol is supported in earlier versions. Windows 2000 and Windows XP support L2TP by binding L2TP to IPSec/IKE. If you need to use a Windows 2000/XP PC to establish L2TP tunnels with other non-Microsoft network products, you must modify its registry to cancel this binding.

- Establishing an L2TP tunnel by interconnecting with a Windows PC: When you click **New connection** in **Network and Dial-up Connections** to create a virtual private connection (namely, **Connect to a private network through the Internet (V)**), the **Require data encryption (disconnect if none)** checkbox is selected by default and **Password requiring security measure** instead of PAP is used for authentication. However, the commoner method is to use PAP or CHAP for authentication and not to encrypt data for transmission. Therefore, you need to modify the properties of this connection manually.
- Establishing an L2TP tunnel by interconnecting with a Windows PC: When you click **New connection** and **Accept incoming connections (A)** in **Network and Dial-up Connections** to create a connection, the MS-CHAPv2 method is used for user authentication by default and CHAP is forbidden for authentication. If you need to use CHAP for authentication, you must modify the configuration file of **Remote access policy** in the settings of the started **Routing and remote access** service, that is, add CHAP as an optional authentication method.
- Establishing an L2TP tunnel by interconnecting with a Windows PC: L2TP on Windows does not support the tunnel authentication function. The tunnel authentication function must be disabled in the L2TP settings of Qtech router connected to the Windows PC. Tunnel authentication is disabled on Qtech router by default.
- Establishing an L2TP tunnel by interconnecting with a Cisco device: Cisco IOS requires tunnel authentication by default, whereas tunnel authentication is disabled on Qtech router by default.
- Establishing an L2TP tunnel by interconnecting with a Cisco device: If Qtech router acts as the LNS and the Cisco device acts as the LAC to provide the L2TP tunnel service for remote dial-up users, **ip domain-lookup** instead of **ip cef** must be set on the Cisco device, just as on Cisco 2620 (LAC) in the preceding configuration example. Otherwise, the Cisco device will not forward PPP negotiation packets and other data to dial-up users.
- Establishing an L2TP tunnel by means of negotiation: The tunnel authentication settings at both ends of a tunnel must be consistent, that is, tunnel authentication is enabled or disabled at the same time at both ends. If it is enabled at both ends, the same tunnel authentication password must be set.
- Do not attempt to use Cisco routers (IOS versions 12.2 and 12.3) to establish an L2TP tunnel with a Windows 2000 PC, because it will be a waste of time.
- In consideration of being compatible with L2TP on different Windows versions and Cisco IOS of earlier versions, as well as the forwarding efficiency, RGOS does not support the AVP Hidden function and data message sequencing function. When an L2TP tunnel is established by interconnecting with Cisco IOS of later versions, ensure that the AVP Hidden function and data message sequencing function are disabled and default settings of the system are used.
- RGOS provides the LAC function, but does not support the LAC access server function.
- When RGOS is used to implement the LNS function, it is recommended that the address of the virtual-template interface be set in IP unnumbered mode, just as the settings on Cisco devices in consideration of fast route forwarding. Generally, IP unnumbered is bound to a loopback interface, as shown in the examples.
- In terms of instant configuration and use property of L2TP, effective changes (namely, non-repetitive operations) of control connection properties will cause the active disconnection of the related L2TP tunnel and all sessions on the tunnel. Effective changes of data transmission properties affects data transmission immediately.
- When the RGOS router is located behind a firewall, UDP port 1701 of the firewall must be enabled.
- When designing an L2TP tunnel, ensure that the route between the client and the server is available. When a router acts as the client, routes generated after an L2TP tunnel is established are different from those generated when a Windows PC acts as the client. If an L2TP tunnel is successfully established on a router (either a Cisco or a Qtech product), two routes are generated, just as routes generated after other PPP link interfaces become UP. One is reachable to the server network segment, and the other is a direct route. However, when a Windows PC is used as the client, after an L2TP tunnel is established, a new route that traverses the L2TP tunnel and is reachable to the network 0.0.0.0/0 is added, in addition to the original route and the preceding two new routes.

## 8 CONFIGURING VPDN 2.0

### 8.1 VPDN 2.0 Overview

VPDN 2.0, used to meet the need of VPDN with large capacity, has changed the configuration mode in VPDN server side.

The new virtual-vpdn interface configuration mode, which has replaced the original virtual-template one in VPDN server side, can meet the need of more tunnels' convergence.



#### Note

10.43b21 version support the function of VPDN 2.0, but only its L2TP tunnel mode. For the configuration in server side, only the configuration command related to interface has been changed. The original VPDN global parameter, and the configuration unrelated to interface have not. Users can continue to use them.

### 8.2 Configuring L2TP

#### 8.2.1 Configuring Large Capacity L2TP

##### 8.2.1.1 Configuration Task List

##### 8.2.1.2 Configuring VPDN Address Pool (Optional)

This is an optional step for establishing an L2TP tunnel initiated by the remote client. In order to accept the L2TP connection initiated by the remote client, the LNS must allocate an IP address to the remote client if an IP address used inside the VPN is not set for the remote client. Generally, an idle IP address in a specified address pool is allocated to the client. Use the following commands to configure a VPDN address pool. VPDN module will manage the allocation by itself.

Command	Function
Qtech(config)# <b>vpdn pool</b> <i>pool_name</i> <i>first-ip</i> <i>last-ip</i>	Creates or sets local address pool.
Qtech(config)# <b>no vpdn pool</b> <i>pool_name</i>	Deletes the specified address pool.

*poolname* is the name of the local address pool to be created or set, *first-ip* is the first address in the address range set for the local address pool, and *last-ip* is the last address. When allocating address by using AAA, user can choose not to configure it. When we delete the address pool with "no" command, the corresponding binding command `vpdn intf_pool` on interface will also be deleted.

#### 8.2.2 Configuring User Information

This is an optional step for establishing an L2TP tunnel initiated by the remote client. The purpose of configuring user information is to authenticate remote L2TP clients that attempt to access the local client.

Use the following commands to configure user information.

Command	Function
Qtech(config)# <b>username</b> <i>user-name</i> <b>password</b> {0 7} <i>password</i>	Configures user information.
Qtech(config)# <b>no username</b> <i>user-name</i>	Deletes the specified user.

*user-name* is the name of the dial-in user who is allowed to access, and *password* is the password of the user. The router locally maintains a database that records names of dial-in users permitted to access and their passwords.

### 8.2.3 Setting VPDN Global Parameters

This is a mandatory step for establishing an L2TP tunnel initiated by the remote client. VPDN global parameters are set in this step. The operations of setting VPDN global parameters include:

#### 8.2.3.1 Enabling or Disabling the VPDN Function

If a user requires the router to accept the L2TP access from the remote client and establish an L2TP tunnel and session, the VPDN function must be enabled on the router.

Use the following commands to enable or disable the VPDN function.

Command	Function
Qtech(config)# <b>vpdn enable</b>	Enables the VPDN function.
Qtech(config)# <b>no vpdn enable</b>	Disables the VPDN function.

The VPDN enabling and disabling support instant configuration and use (that is, they are available immediately when they are configured). If the VPDN function is disabled, all the existing L2TP tunnels and sessions will be disconnected.

#### 8.2.3.2 Setting the VPDN Source Address

After the VPDN source address is set, the destination address of the tunnel set for the remote client must be consistent with the VPDN source address before an L2TP tunnel is established successfully.

Use the following commands to set the VPDN (local) source address.

Command	Function
Qtech(config)# <b>vpdn source-ip</b> <i>ip-address</i>	Sets the VPDN source address.
Qtech(config)# <b>no vpdn source-ip</b> <i>ip-address</i>	Cancels the set VPDN source address.

The system does not check whether the destination address in the received tunnel establishment request is a specific value by default.

#### 8.2.3.3 Setting the Maximum Number of VPDN Sessions

After the maximum number of VPDN sessions is set, access requests beyond the maximum value will be denied.

Use the following commands to set the maximum number of sessions supported by the VPDN server.

Command	Function
Qtech(config)# <b>vpdn session-limit</b> <i>sessions</i>	Sets the maximum number of VPDN sessions.
Qtech(config)# <b>no vpdn session-limit</b>	Restores the default maximum number of VPDN sessions.

The maximum number of sessions is the one configured by using this command by default.

#### 8.2.3.4 Setting the Domain Resolution Option

Use the following commands to set the domain resolution option in VPDN domain authentication. Domains of different types can be identified based on configuration.

Command	Function
---------	----------

Qtech(config)# <b>vpdn domain-delimiter @/%%#\</b>	Sets the domain delimiter, prefix or suffix.
Qtech(config)# <b>no vpdn domain-delimiter</b>	Cancels the VPDN domain authentication option.

The system does not resolve the domain field by default.

### 8.2.3.5 Enabling or Disabling Domain Authentication

Use the following commands to enable or disable the VPDN domain authentication, that is, determine whether to strip the domain field.

Command	Function
Qtech(config)# <b>vpdn authorize domain split</b>	Enables domain authentication, that is, enables domain splitting.
Qtech(config)# <b>no vpdn authorize domain</b>	Disables domain authentication.

Domain authentication is disabled by default.

### 8.2.3.6 Ignoring the Source Address Check of VPDN

Use the following commands to ignore errors on received L2TP control packets that do not comply with the RFC specifications so as to ensure the normal negotiation.

Command	Function
Qtech(config-vpdn)# <b>vpdn ignore_source</b>	Ignores the source address check of packets sent from the peer end.
Qtech(config-vpdn)# <b>no vpdn ignore_source</b>	Strictly checks the source address of packets sent from the peer end.

The system strictly checks the source address by default.

### 8.2.3.7 Setting VPDN Rate Limit

Use the following commands to limit the rate of establishing VPDN tunnels, namely, to limit the number of VPDN tunnels that can be established at one time.

Command	Function
Qtech(config)# <b>vpdn limit_rate rate_num</b>	Enables rate limit. <i>rate_num</i> is the number of tunnels that can be established at a time. The value range is 5 to 100.
Qtech(config)# <b>no vpdn limit_rate</b>	Disables rate limit.

Rate limit is disabled by default. When negotiating tunnel with large capacity, please enable the function so that to reduce shaking. When using virtual-template interface, please configure the number as 40. When using virtual-vpdn interface, please configure the number as 100.

## 8.2.4 Resolving Device Serial Number of VPDN

Use the following commands to set VPDN to resolve device serial number. According to the options, users can choose the division method. If the system has enabled LNS( L2TP) function, VPDN will resolve the device serial number transmitted from the peer side.

Command	Function
Qtech(config)# <b>vpdn accept serial-number prefix</b>	Enables the function of resolving device serial number with prefix.
Qtech(config)# <b>vpdn accept serial-number suffix</b>	Enables the function of resolving device serial number with suffix.



Qtech(config)# <b>no vpdn accept serial-number</b>	Disables the function of resolving device serial number.
--	--

By default, the resolving device serial number function is disabled.

### 8.2.5 Transmitting Device Serial Number of VPDN

Use the following commands for to set VPDN to transmit device serial number. If the system has enabled LNS( L2TP) function, VPDN will transmit the device serial number to the peer side.

Command	Function
Qtech(config)# <b>vpdn lac-send-devid</b>	Enables the function of transmitting device serial number.
Qtech(config)# <b>no vpdn lac-send-devid</b>	Disables the function of transmitting device serial number.

By default, the transmitting device serial number function is disabled.

### Configuring a Virtual-Template Interface

This is a mandatory step for establishing an L2TP tunnel initiated by the remote client. This interface will become the logical interface that binds and carries L2TP sessions, and can only be used in LNS side. The operations of configuring a virtual-vpdn interface include:

For information about setting the local IP address and setting the authentication mode see sections regarding the interface configuration guide. The virtual-vpdn interface can not configure ip unnumbered command, but can configure IP address and Mask directly.

#### 8.2.5.1 Setting a Virtual-vpdn Interface

Use the following commands to set a virtual-vpdn interface. An interface can be binded with many sessions.

Command	Function
Qtech(config)# <b>interface virtual-vpdn</b> <i>number</i>	Creates or configures a specified virtual-vpdn interface.
Qtech(config)# <b>no interface virtual-vpdn</b> <i>number</i>	Deletes the specified virtual-vpdn interface.

*number* is the sequence number of the specified virtual-vpdn interface, and the range is <1-1024> . The created virtual-vpdn interface will be used as the logical interface that binds and carries L2TP sessions. When negotiating tunnels by using virtual-vpdn interface, the L2TP tunnel does not support IPV6 negotiation. All the PPP authentication of virtual-vpdn interface in vpdn-group's domain configuration need to be configured on the default virtual-vpdn interface of vpdn-group.

#### 8.2.5.2 Setting VPDN Address Pool

Use the following commands to set the binding address pool on virtual-vpdn interface.

Command	Function
Qtech(config)# <b>interface virtual-vpdn</b> <i>number</i>	Creates or configures a specified virtual-vpdn interface.
Qtech(config-Virtual-vpdn <i>number</i> )# <b>vpdn intf_pool</b> <i>pool_name</i>	Binds the address pool on the interface.
Qtech(config-Virtual-vpdn <i>number</i> )# <b>no vpdn intf_pool</b>	Deletes the binding address pool on the interface.

*number* is the sequence number of the specified virtual-vpdn interface, and the range is <1-1024>. *pool\_name* is the name of the binding address pool. The VPDN binding address pool can only be used on the virtual-vpdn interface of L2TP module.

## 8.2.6 Configuring VPDN-group

This is a mandatory step for establishing an L2TP tunnel initiated by the remote client. VPDN-group parameters are set in this step. The operations of configuring VPDN-group include:

### 8.2.6.1 Setting a VPDN-group Interface

Use the following commands to set a VPDN-group interface.

Command	Function
Qtech(config)# <b>vpdn-group</b> <i>name</i>	Creates or configures the specified VPDN-group interface.
Qtech(config)# <b>no vpdn-group</b> <i>name</i>	Deletes the specified VPDN-group interface.

*name* is the name of the specified VPDN-group interface. The created VPDN-group interface allows related clients to access and establish tunnels.

### 8.2.6.2 Setting the VPDN-group Source Address

The destination address in the tunnel establishment request sent from the remote client must match the VPDN-group source address. In this way, the VPDN-group can be applied.

Use the following commands to set the VPDN-group source address.

Command	Function
Qtech(config-vpdn)# <b>source-ip</b> <i>src-ip</i>	Sets the VPDN-group source address.
Qtech(config-vpdn)# <b>no source-ip</b>	Cancel the set VPDN-group source address.

*src-ip* is the VPDN-group source address. When configuring with VPDN 2.0, the command is mandatory.

### 8.2.6.3 Setting the Tunneling Mode

Use the following commands to set the tunneling mode.

Command	Function
Qtech (config-vpdn)# <b>accept-dialin</b>	Allows access from the dial-in remote client.
Qtech (config-vpdn)# <b>no accept-dialin</b>	Denies the access from the dial-in remote client.

If a user needs the local router to provide the LNS function, access from the dial-in remote client must be allowed.

### 8.2.6.4 Setting the Tunneling Protocol

Use the following commands to set the tunneling protocol.

Command	Function
Qtech(config-vpdn-acc-in)# <b>protocol</b> { <b>any</b>   <b>l2tp</b>   <b>pptp</b> }	Sets the tunneling protocol.
Qtech(config-vpdn-acc-in)# <b>no protocol</b>	Cancel the set tunneling protocol.

The tunneling mode must be set before a tunneling protocol is set.

### 8.2.6.5 Setting a Logical Interface to Be Used

Use the following commands to set a logical interface to be used by VPDN-group,.

Command	Function
Qtech(config-vpdn-acc-in)# <b>virtual-vpdn</b> <i>number</i>	Sets the using logical interface.
Qtech(config-vpdn-acc-in)# <b>no virtual-vpdn</b> <i>number</i>	Cancels the set logical interface.

Before setting a logical interface used by VPDN-group, users should set the tunnel mode as L2TP and configure source-ip command in distributed system first. The logical interface can only be used in L2TP mode, and can not be used together with virtual virtual-template interface. All the PPP authentication of virtual-vpdn interface in vpdn-group's domain configuration need to be configured on the default virtual-vpdn interface of vpdn-group.

### 8.2.6.6 Setting the Peer Name

If the peer name is set, this VPDN-group is effective only to the remote client that matches the host name. If no peer name is set, this VPDN-group is the default VPDN-group and can provide the VPDN service for any remote client.

Use the following commands to set the peer name.

Command	Function
Qtech(config-vpdn)# <b>terminate-from</b> <i>hostname name</i>	Sets the name of the peer host.
Qtech(config-vpdn)# <b>no terminate-from</b>	Cancels the set peer name.

*name* is the name of the peer host.

### 8.2.6.7 Setting the Local Name

The local name is sent to the peer end as a record property.

Use the following commands to set the local name.

Command	Function
Qtech(config-vpdn)# <b>local name</b> <i>name</i>	Sets the local name.
Qtech(config-vpdn)# <b>no local name</b>	Cancels the set local name.

*name* is the local name. The router name is used as the local name and sent to the peer host of the tunnel by default.

### 8.2.6.8 Setting the L2TP Control Connection

Use the following commands to set the L2TP control connection.

Command	Function
Qtech(config-vpdn)# <b>l2tp tunnel authentication</b>	Enables tunnel authentication.
Qtech(config-vpdn)# <b>no l2tp tunnel authentication</b>	Disables tunnel authentication.
Qtech(config-vpdn)# <b>l2tp tunnel hello</b> <i>interval</i>	Sets the interval of sending Hello messages.
Qtech(config-vpdn)# <b>no l2tp tunnel hello</b>	Deletes the set interval of sending Hello messages.
Qtech(config-vpdn)# <b>l2tp tunnel password</b> <i>pass-word</i>	Sets the tunnel password.

Command	Function
Qtech(config-vpdn)# <b>no l2tp tunnel password</b>	Deletes the set tunnel password.
Qtech(config-vpdn)# <b>l2tp tunnel receive-window size</b>	Sets the size of the receiving window of the tunnel control connection.
Qtech(config-vpdn)# <b>no l2tp tunnel receive-window</b>	Restores the default size of the receiving window of the tunnel control connection.
Qtech(config-vpdn)# <b>l2tp tunnel retransmit {retries number   timeout {min   max} seconds}</b>	Sets retransmission of tunnel control messages.
Qtech(config-vpdn)# <b>no l2tp tunnel retransmit {retries   timeout {min max}}</b>	Restores the default retransmission setting of tunnel control messages.
Qtech(config-vpdn)# <b>l2tp tunnel timeout {no-session  setup} seconds</b>	Sets the maximum interval of establishing a no-session/control connection of the tunnel.
Qtech(config-vpdn)# <b>no l2tp tunnel timeout {no-session   setup}</b>	Restores the default maximum interval of establishing a no-session/control connection of the tunnel.
Qtech(config-vpdn)# <b>l2tp tunnel force_ipsec</b>	Enables forced encryption. It is used when external encryption is required. After this command is executed, packets can be sent to VPDN tunnels only after encryption.
Qtech(config-vpdn)# <b>no l2tp tunnel force_ipsec</b>	Disables forced encryption.
Qtech(config-vpdn)# <b>l2tp tunnel avp-hidden-compatible</b>	Supports the RFC2661 standard AVP Hidden parsing algorithm compatibly.
Qtech(config-vpdn)# <b>no l2tp tunnel avp-hidden-compatible</b>	Restores the default Cisco standard AVP Hidden parsing algorithm.
Qtech(config-vpdn)# <b>l2tp tunnel clear timeout seconds</b>	Sets the unix of vpdn-group's delete on time of session.
Qtech(config-vpdn)# <b>no l2tp tunnel clear timeout</b>	Closes vpdn-group's delete on time function.

Tunnel authentication is not needed for establishing L2TP tunnels by default (but required on Cisco devices by default). The default interval of sending Hello control messages is 60 seconds. The default receiving window size of control messages is 4. The default number of retransmission times of control messages is 5. The default minimum and maximum intervals of retransmitting control messages are 1 second and 8 seconds respectively. The default maximum interval of no session in a tunnel is 600 seconds. The default maximum time supported by tunnels in establishing a control connection is 300 seconds. If L2TP tunnel authentication is required, the same tunnel password must be configured at both ends of the L2TP tunnel. Nevertheless, the system does not configure tunnel passwords for any L2TP tunnels by default and does not require tunnel authentication. The *interval* parameter is the interval of sending Hello messages, in seconds. The unit of the *seconds* parameter is also seconds. The forced IPsec encryption and authentication are disabled by default. The default AVP Hidden parsing algorithm uses the Cisco standard. After the RFC2661 standard AVP Hidden parsing algorithm is supported compatibly, the RFC2661 standard is used to parse and hide AVP. The interval of delete on time is 1 to 65535 minutes.

### 8.2.6.9 Setting L2TP Data Transmission Parameters

Use the following commands to set IP/UDP parameters for transmitting L2TP messages.

Command	Function
Qtech(config-vpdn)# <b>l2tp ip udp checksum</b>	Sets the UDP checksum.
Qtech(config-vpdn)# <b>no l2tp ip udp Checksum</b>	Cancels the UDP checksum setting.
Qtech(config-vpdn)# <b>ip tos tos-value</b>	Sets the IP TOS field.
Qtech(config-vpdn)# <b>no ip tos</b>	Cancels the IP TOS setting.
Qtech(config-vpdn)# <b>ip precedence value</b>	Sets the IP Precedence field.

Qtech(config-vpdn)# <b>no ip precedence</b>	Cancels the IP Precedence setting.
---	------------------------------------

*tos-value* is the value of the TOS field of the IP header that carries L2TP messages, and *value* is the value of the Precedence field of this IP header. For L2TP messages to be carried in L2TP tunnels of RGOS, the checksum field of UDP that carries L2TP messages must be blank, the TOS of the IP header that carries L2TP messages and the Precedence field of this IP header must be 0 by default.

Note that the TOS and Precedence fields are supported only in L2TP. Though they can be configured in PPTP, the configuration does not take effect.

#### 8.2.6.10 Setting the VRF Option

Use the following commands to set the VRF to which specified L2TP tunnel packets belong. The configuration maps to the **ip vrf forward** command of the VT interface, implementing VRF spanning.

Command	Function
Qtech(config-vpdn)# <b>vpn vrf</b> <i>vrf-name</i>	Sets the VRF attribute for the tunnel.
Qtech(config-vpdn)# <b>no vpn vrf</b>	Deletes the VRF attribute setting of the tunnel.

*vrf-name* is the name of the VRF.

#### 8.2.6.11 Setting the Supported Domain Name

Use the following commands to set the domain name. The command for setting the supported domain name takes effect after the domain authentication is enabled. When the domain matching the content of this command is identified, put the configuration info of the domain into the L2TP session. If no matched domain info is found, deal with it by default.

Command	Function
Qtech(config-vpdn)# <b>domain</b> <i>domain-name</i> <b>virtual-vpdn</b> <i>number</i>	Sets the authentication domain name and the related logical interface (when a virtual-vpdn logical interface is used).
Qtech(config-vpdn)# <b>no domain</b> <i>domain-name</i>	Cancels the domain setting.

*domain-name* is the name of domain. *number* is the number of the logical interface, and the range is <1-1024>.

#### 8.2.6.12 Re-Performing PPP Authentication

When the client triggers the LAC to start dialing, the LAC acts as the LNS to authenticate the client. This command is used to perform CHAP authentication on the client again after an L2TP tunnel is established. This command is valid only on the LNS.

Use the following commands to forcibly perform complete PPP authentication again.

Command	Function
Qtech(config-vpdn)# <b>force-local-chap</b>	Forces the LNS to perform CHAP authentication on the client again.
Qtech(config-vpdn)# <b>no force-local-chap</b>	Cancels CHAP re-authentication.

#### 8.2.6.13 Re-Performing PPP Negotiation

When the client triggers the LAC to start dialing, the LAC acts as the LNS to negotiate with the client. This command is used to perform LCP negotiation with the client again after an L2TP tunnel is established. This command is valid only on the LNS.

Use the following commands to forcibly perform PPP negotiation again.



Command	Function
Qtech(config-vpdn)# <b>force-local-lcp</b>	Forces the LNS to perform LCP negotiation with the client again.
Qtech(config-vpdn)# <b>no force-local-lcp</b>	Cancels LCP re-negotiation.

#### 8.2.6.14 Ignoring Errors on Control Packets

Use the following commands to ignore errors on received L2TP control packets that do not comply with the RFC specifications to ensure normal negotiation.

Command	Function
Qtech(config-vpdn)# <b>lcp renegotiation always</b>	Ignores errors on packets from the peer end.
Qtech(config-vpdn)# <b>no lcp renegotiation always</b>	Checks whether control packets comply with RFC specifications.

#### 8.2.6.15 Setting the Domain Name's Delete on Time of Session

Use the following commands to set the domain name's delete on time of session. The command will be configured in vpdn-domain's command mode.

Command	Function
Qtech(config-vpdn)# <b>domain domain-name vrf vrf-name</b>  Qtech(config-vpdn-domain)# <b>clear timeout seconds</b>	Sets the unix of domain name's delete on time of session.
Qtech(config-vpdn)# <b>no lcp renegotiation always</b>	Cancels the delete on time function.

*domain-name* is the name of domain, and *vrf-name* is the name of the VRF. Seconds is the interval of delete on time, and the range is 1 to 65535 minutes.

#### 8.2.6.16 Setting No Sending of STOP Packet

The command is used to configure the behavior unmatched the RFC standard. It can only support one behavior, that is, do not send stop packet, when receiving SCCRQ repeatedly.

Command	Function
Qtech(config-vpdn)# <b>l2tp tunnel none-rfc-compatible send-stop-pkt</b>	Does not send STOP packet, when receiving SCCRQ repeatedly
Qtech(config-vpdn)# <b>no l2tp tunnel none-rfc-compatible send-stop-pkt</b>	Does send STOP packet, when receiving SCCRQ repeatedly

#### 8.2.6.17 Setting SCCRQ Packet's No Carrying of Tunnel Authentication ResponseAVP

After configuring tunnel authentication of LNS side in L2TP, if the accepted SCCRQ packet does not carry challenge AVP 11, the replied SCCRQ packet will not carry challenge response AVP13. The no command will close the function. The command can be compatible with SCCRQ's link detection function developed by other vendor, so that to avoid that after the configuring of tunnel authentication, the accepted SCCRQ packet with no carrying of authentication information will get back with all the information being 0.

Command	Function
Qtech(config-vpdn)# <b>l2tp tunnel zxkeepalive-compatible</b>	If the accepted SCCRQ does not carry challenge AVP, the replied SCCRQ packet will not resend challenge resend AVP.



<p>Qtech(config-vpdn)#no l2tp tunnel zxkeepalive-compatible</p>	<p>If the accepted SCCRQ does not carry challenge AVP, the replied SCCRQ packet will resend challenge resend AVP with all the information being 0.</p>
---	--

### 8.2.6.18 Setting Supported Flow-limit QOS by VPDN

Use the following commands to set VPDN's supporting of flow-limit QOS rule. It can be configured in vpdn-group to show that all the sessions in the group will obey the rule. It can also be configured in domain to show that all the sessions in the domain will obey the rule. The function can only use together with virtual-vpdn interface.

Command	Function
Qtech(config-vpdn)# <b>flow-label</b> <i>flow-id</i>	Configures QOS rule in vpdn-group.
Qtech(config-vpdn)#no <b>flow-label</b>	Deletes QOS rule.
Qtech (config-vpdn-domain)# <b>flow-label</b> <i>flow-id</i>	Configures QOS rule in domain.
Qtech (config-vpdn-domain)# no <b>flow-label</b>	Deletes QOS rule.

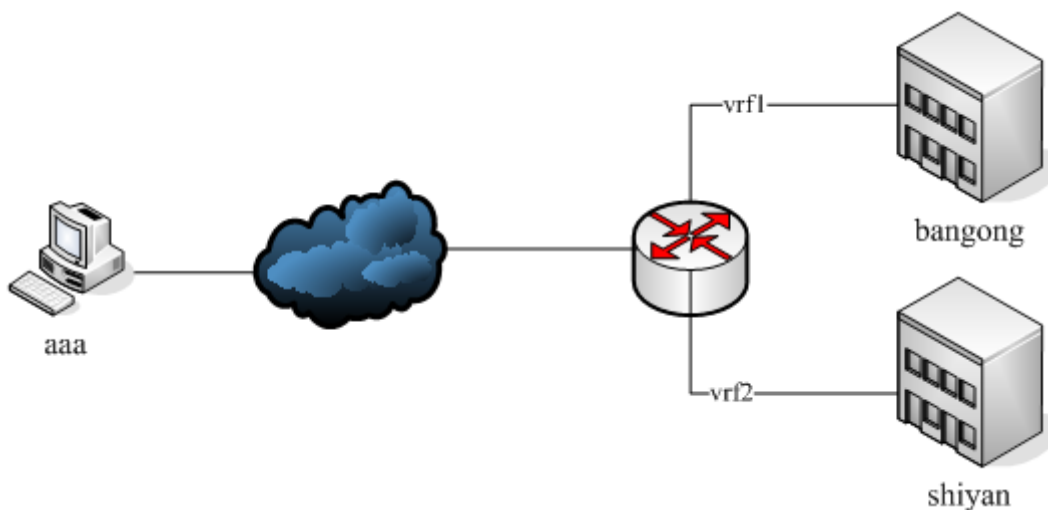
flow-id is the corresponding QOS rule's number, and its range is <1-1023>.

## 8.2.7 Configuration Examples

### 8.2.7.1 Configuration Example of L2TP Large Capacity and Domain Authentication

The following topology shows, according to domain information, a user dials in two networks by using one public network address.

Figure 28



```

ip vrf vrf1
ip vrf vrf2
!
vpdn enable
vpdn domain-delimiter @/%#-\ suffix
vpdn authorize domain split
vpdn pool vpdusers 192.168.101.3 192.168.101.50
vpdn pool bangong 192.168.101.51 192.168.101.150
vpdn pool shiyang 192.168.101.151 192.168.101.253
!
    
```

```
!  
username user@bangong password 7 025144391715  
username user@shiyang password 7 127654431B  
username user@Qtech password 7 164290823468  
!  
!  
interface GigabitEthernet 1/1/1  
ip address 192.168.19.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface Virtual-vpdn 1  
ppp authentication pap  
ip address 192.168.101.2 255.255.255.0  
vpdn intf_pool vpdnusers  
!  
interface Virtual-vpdn 2  
ip vrf forward vrf1  
ip address 192.168.101.2 255.255.255.0  
ppp authentication pap  
vpdn intf_pool bangong  
!  
interface Virtual-vpdn 3  
ip vrf forward vrf2  
ip address 192.168.101.2 255.255.255.0  
ppp authentication pap  
vpdn intf_pool shiyang  
!  
vpdn-group 1  
! Default L2TP VPDN group  
source-ip 192.168.19.1  
accept-dialin  
    protocol l2tp  
    virtual-vpdn 1          /* bind logical interface */  
domain bangong virtual-vpdn 2 /*specified domain*/  
domain shiyang virtual-vpdn 3 /* specified domain */  
!  
!  
line con 0  
line aux 0  
line vty 0 4
```

Sessions of dialing user who has no domain name will be binded with virtual-vpdn 1 interface. Sessions of dialing user whose domain name is bangong will be binded with virtual-vpdn 2 interface, and belongs to vrf1. Sessions of dialing user whose domain name is shiyang will be binded with virtual-vpdn 3 interface, and belongs to vrf2.

### 8.2.7.2 Configuration Example of Virtual-vpdn and OSPF

Different from virtual-access and virtual-ppp interface, virtual-vpdn interface can be binded with multichannel sessions. In this way, the configuration of its corresponding router protocol is also different.

LNS side:

```
username user1 password pass
```

```
!
```

```
vpdn enable
```

```
vpdn pool 10 76.1.11.1 76.1.11.100
vpdn pool 1 100.11.1.11 100.11.100.250
!
vpdn authorize domain split
vpdn domain-delimiter @ suffix
!
interface GigabitEthernet 2/1/5
ip address 200.11.1.10 255.255.255.0
duplex auto
speed auto
!
interface Loopback 99
ip address 99.9.9.9 255.255.255.0
!
interface Virtual-vpdn 1
ppp authentication pap
ip ospf network point-to-multipoint
ip ospf source-check-ignore
ip address 100.11.1.5 255.255.255.0
vpdn intf_pool 1
!
!
vpdn-group 1
! Default L2TP VPDN group
source-ip 200.11.1.10
accept-dialin
protocol l2tp
virtual-vpdn 1
domain a
!
!
router ospf 1
network 99.9.9.0 0.0.0.255 area 0
```

```
network 100.11.1.0 0.0.0.255 area 0
```

**LAC side:**

```
no service password-encryption
```

```
!
```

```
!
```

```
l2tp-class l2x1
```

```
!
```

```
pseudowire-class pw1
```

```
encapsulation l2tpv2
```

```
protocol l2tpv2 l2x1
```

```
!
```

```
interface GigabitEthernet 0/0
```

```
ip address 200.11.1.250 255.255.255.0
```

```
duplex auto
```

```
speed auto
```

```
!
```

```
!
```

```
interface Loopback 7777
```

```
ip address 77.7.7.7 255.255.255.0
```

```
!
```

```
interface Virtual-ppp 1
```

```
ppp pap sent-username user1 password pass
```

```
ip ospf source-check-ignore
```

```
ip ospf hello-interval 30
```

```
ip address negotiate
```

```
pseudowire 200.11.1.10 1 encapsulation l2tpv2 pw-class pw1
```

```
!
```

```
!
```

```
router ospf 1
```

```
network 77.7.7.0 0.0.0.255 area 0
```

```
network 100.11.1.0 0.0.0.255 area 0
```

### 8.2.7.3 Configuration Example of Irtual-vpdn and RIP

**LNS side:**

```
username user1 password pass
!
vpdn enable
vpdn pool 10 76.1.11.1 76.1.11.100
vpdn pool 1 100.11.1.11 100.11.100.250
!
vpdn authorize domain split
vpdn domain-delimiter @ suffix
!
interface GigabitEthernet 2/1/5
 ip address 200.11.1.10 255.255.255.0
 duplex auto
 speed auto
!
interface Loopback 99
 ip address 99.9.9.9 255.255.255.0
!
interface Virtual-vpdn 1
 ppp authentication pap
 ip address 100.11.1.5 255.255.255.0
 vpdn intf_pool 1
!
vpdn-group 1
! Default L2TP VPDN group
 source-ip 200.11.1.10
 accept-dialin
 protocol l2tp
 virtual-vpdn 1
 domain a
!
router rip
```

```
network 99.0.0.0
network 100.0.0.0
no validate-update-source
```

**LAC side:**

```
!
l2tp-class l2x1
!
pseudowire-class pw1
  encapsulation l2tpv2
  protocol l2tpv2 l2x1
!
interface GigabitEthernet 0/0
  ip address 200.11.1.250 255.255.255.0
  duplex auto
  speed auto
!
interface Loopback 7777
  ip address 77.7.7.7 255.255.255.0
!
interface Virtual-ppp 1
  ppp pap sent-username user1 password pass
  ip address negotiate
  pseudowire 200.11.1.10 1 encapsulation l2tpv2 pw-class pw1
!
router rip
  network 77.0.0.0
  network 100.0.0.0
  no validate-update-source
```

### 8.3 Monitoring and Maintaining VPDN 2.0

The methods of monitoring and maintaining VPDN 2.0 is just the same as the old one. Refer to the chapter of monitoring and maintaining L2TP.



## 9 CONFIGURING THE TUNNEL INTERFACE

### 9.1 Understanding the Tunnel interface

#### 9.1.1 Overview

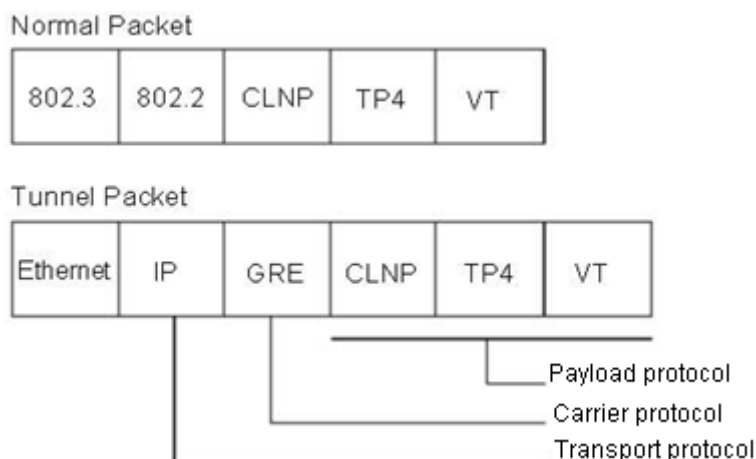
The tunnel interface is used to realize tunnel functions. Without specifically binding a certain transport protocol or payload protocol, the tunnel interface provides a standard point-to-point transmission link, and hence one tunnel interface must be configured for each separate link.

Tunnel function involves the following three key components:

- 34) Payload protocol: The protocol for encapsulating the payload (network data) transmitted through a tunnel. Currently, software of Qtech products only support the use of the IP protocol as the payload protocol on the tunnel interface;
- 35) Carrier protocol: The protocol for secondary encapsulation and identification of the payload to be transmitted. Qtech products support the following encapsulation modes on the tunnel interface: GRE and IP/IP;
- 36) Transport protocol: The network protocol for transmitting the payload packets further encapsulated by the carrier protocol. Qtech products use the most widely applied IP protocol as the transport protocol.

Figure shows the formation of a data packet encapsulated for transmission over an IP tunnel before and after the transmission.

Figure 29 The formation of data packet transmitted over the tunnel network before and after the transmission



IP tunnel transmission function is accomplished through GRE Ethernet encapsulation. In practice, if two private networks using the same protocol need to communicate with each other through the public network using a different protocol, they can use the tunnel function.

Tunnel transmission is applicable to the following circumstances:

- 37) Allowing the communication between non-IP local networks over a single-protocol network (IP network), as a tunnel supports different payload protocols; allowing the scope enlargement of a network running a hop-limited protocol;
- 38) Allowing the connection of discontinuous subnets over a single-protocol network (IP network);
- 39) Allowing the provision of VPN (virtual private network) over wide area network.

Since a tunnel will encapsulate the payload before transmission, such complexity in processing requires you to pay attention to the following issues under certain circumstances.

- 40) Since a tunnel is a point-to-point link which seems to have only one hop during routing, the actual routing overhead may involve multiple hops. Note that routing on a tunnel link may be different from the actual condition.
- 41) Since a tunnel will encapsulate the payload into a transport protocol, you need to give the corresponding consideration when configuring the firewall, especially the ACL. It shall also be noted that the transmission bandwidth (such as MTU) of a payload protocol is smaller than the theoretical value.

The followings will only introduce the attributes specific to the tunnel interface. The configuration of other attributes (including IP address and other relevant parameters, firewall and parameters of backup center) will be introduced in relevant sections.

## 9.1.2 Configuring the Tunnel Interface

### 9.1.2.1 Tunnel interface configuration tasks

#### Entering designated Tunnel interface configuration mode

To create a tunnel interface and enter interface configuration mode, run the following commands in global configuration mode:

Command	Function
Qtech(config)# <b>interface tunnel</b> <i>tunnel-number</i>	Enters designated tunnel interface configuration mode.
Qtech(config)# <b>no interface tunnel</b> <i>tunnel-number</i>	Deletes the existing tunnel interface.

Same as other logic interfaces, a tunnel interface is created once you enter the designated tunnel interface for the first time.

### 9.1.2.2 Configuring the source address of a Tunnel interface

A tunnel interface needs to identify the source address and destination address of the tunnel configured. In order to ensure the stability of a tunnel interface, the Loopback address is generally used as the source address and destination address of tunnel. Before normal operations of tunnel interface, check the connectivity between source address and destination address.

To configure the source address of a tunnel interface, run the following commands in tunnel interface configuration mode:

Command	Function
Qtech(config-if)# <b>tunnel source</b> { <i>ip-address</i>   <b>interface-name</b> <i>interface-number</i> }	Configures the source address of the tunnel interface.
Qtech(config-if)# <b>no tunnel source</b>	Removes the source address configuration of the tunnel interface.

The **tunnel source** command configures the actual source address for communication over a tunnel interface, namely the local endpoint of the tunnel.

### 9.1.2.3 Configuring the destination address of a Tunnel interface

To configure the destination address of a tunnel interface, run the following commands in tunnel interface configuration mode:

Command	Function
Qtech(config-if)# <b>tunnel destination</b> { <i>ip-address</i> }	Configures the destination address of the tunnel interface.
Qtech(config-if)# <b>no tunnel destination</b>	Removes destination address configuration of the tunnel interface.

The **tunnel destination** command configures the actual destination address for communication over a tunnel interface, namely the remote endpoint of the tunnel.



#### Caution

On the same router, tunnel interfaces that use the same encapsulation protocol cannot have the same source address or destination address.

### 9.1.2.4 Configuring Tunnel mode

The tunnel mode is referred to as the carrier protocol of a tunnel. The default tunnel mode is GRE. Of course, the user can also select a tunnel mode according to actual application.

Command	Function
Qtech(config-if)# <b>tunnel mode</b> { gre {ip   ipv6}  ipip   ipv6ip}	Configures tunnel mode.
Qtech(config-if)# <b>no tunnel mode</b>	Removes tunnel mode configuration and restores the default setting.



**Caution** The use of the **tunnel mode** command is related to device models.

### 9.1.2.5 Configuring Tunnel checksum

Under certain circumstances, tunnel checksum needs to be used to guarantee data integrity.

Command	Function
Qtech(config-if)# <b>tunnel checksum</b>	Configures tunnel checksum.
Qtech(config-if)# <b>no tunnel checksum</b>	Disables tunnel checksum.

By default, the checksum function of a tunnel interface is disabled.



**Caution** This command is only supported by the router.

### 9.1.2.6 Configuring the key of a tunnel interface

The key of a tunnel interface can ensure the security on both ends of a tunnel to a certain extent and prevent sniffing and attack from outside.

Command	Function
Qtech(config-if)# <b>tunnel key</b> <i>key-value</i>	Configures the key of the tunnel interface.
Qtech(config-if)# <b>no tunnel key</b>	Removes the key of the tunnel interface.

The key of a tunnel interface works only when the tunnel mode is GRE, as each GRE data packet will contain the tunnel key configured.



**Caution**

- (1) Both ends of a tunnel must use the same key configuration to allow normal communication;
- (2) Although each GRE data packet will contain the key configured when the encapsulation mode is GRE, it is still unwise to guarantee security by relying on this key.
- (3) This command is only supported by the router.

### 9.1.2.7 Configuring tunnel reception rules

If the payload protocol is inadequate to maintain the order of data packets, Qtech products allow the configuration of tunnel reception rules to drop the disordered data packets. If the payload protocol is inadequate to maintain the order of data packets, this function can help realize the sequential transmission of data packets.

Command	Function
Qtech(config-if)# <b>tunnel sequence-datagrams</b>	Configures sequential reception of packets on the tunnel.
Qtech(config-if)# <b>no tunnel sequence-datagrams</b>	Removes sequential reception configuration of the tunnel.

This configuration is effective only when the tunnel mode is GRE.



**Caution** This command is only supported by the router.

### 9.1.2.8 Configuring TTL of a tunnel

Since a tunnel is a point-to-point link which seems to have only one hop during routing, the actual routing overhead may involve multiple hops. Qtech products allow you to configure the TTL of a tunnel, namely to set the TTL in the transport protocol header of the packet transmitted over a tunnel. Being the intermediate node of tunnel, the router will reduce the TTL value in the transport protocol header and drop packets with TTL value being 0.

Command	Function
Qtech(config-if)# <b>tunnel ttl hop-count</b>	Configures the TTL of the tunnel.
Qtech(config-if)# <b>no tunnel ttl</b>	Removes TTL configuration of the tunnel and restores to the default value of 255.

By default, the TTL value of a tunnel transport protocol is 255.

### 9.1.2.9 Configuring TOS of a tunnel

In tunnel interface mode, configure the ToS byte of outer-layer transport protocol IPv4, or the 8 bits of traffic class of IPv6.

Command	Function
Qtech(config-if)# <b>tunnel tos num</b>	Configures the TOS of the tunnel.
Qtech(config-if)# <b>no tunnel tos</b>	Removes TOS configuration of the tunnel.

By default, if both the inner-layer carrier protocol and outer-layer encapsulation protocol of tunnel are IPv4, then the ToS byte of inner-layer IPv4 header will be copied to the outer-layer IPv4 header. If both the inner-layer carrier protocol and outer-layer encapsulation protocol of tunnel are IPv6, then the traffic class 8 bits of inner-layer IPv6 header will be copied to the outer-layer IPv6 header. In other cases, the outer-layer IPv4 ToS and IPv6 traffic class are 0.

### 9.1.2.10 Configuring PMTUD of a tunnel

Even if the payload IP message header is configured with DF (Don't Fragment) bit, the size of the payload protocol message may exceed the MTU of the destination outlet of tunnel after encapsulation, resulting in message fragmentation. On the way to the peer terminal of tunnel, the PMTU may become smaller and the intermediate forwarding device will fragment the encapsulated messages. Qtech products provide the **tunnel path-mtu-discovery** command in interface configuration mode, allowing automatic discovery of PMTU in order to adjust the MTU size of tunnel interface and avoid message fragmentation.

Command	Function
---------	----------

<pre>Qtech(config-if)# tunnel path-mtu-discovery [age-timer {aging-mins   infinite}   min-mtu mtu-bytes]</pre>	<p>Enables the PMTUD function of the tunnel interface;                  Age-timer (optional): configures the aging timer of MTU on the tunnel interface; upon expiration of this timer, the MTU on the tunnel interface will reset to the initial MTU less the header length of carrier protocol messages; aging-mins: aging time ranging from 10 to 30 minutes, with default value being 10 minutes; infinite: disable MTU age-timer.                  Min-mtu (optional): configures MTU lower limit that can be adjusted by PMTUD; mtu-bytes: lower limit of MTU, ranging from 92 to 65535 bytes, with default value being 95 bytes.</p>
<pre>Qtech(config-if)# no tunnel path-mtu-discovery [ age-timer   min-mtu ]</pre>	<p>Disables the PMTUD function of the tunnel interface</p>

PMTUD can work only in GRE or IPIP tunnel mode, and is not enabled by default.



**Caution**

The PMTUD function requires the tunnel interfaces on both ends of the tunnel to be able to receive and process ICMP messages, especially when there is a firewall. This command is only supported by RGOS 10.4(2) or later versions.

After you run the **show interface tunnel** command, states of PMTUD are as follows:

```
Path MTU Discovery state:init
Path MTU Discovery state:keep
Path MTU Discovery state:learning
PMTUD learning has three state machines:
Initially, PMTUD is in init state.
```

When the timer expires and probe packets are being sent, PMTUD changes to the learning state and then learning packets are sent.

If an MTU change is not detected after five consecutive probe packets are sent, PMTUD changes to the keep state and begins sending keep packets.

Command	Function
<pre>Qtech(config-if)# tunnel path-mtu-discovery aging-mins mtu-bytes</pre>	<p>Enables the PMTUD function of the tunnel interface.                  Age-timer: configures the aging timer of MTU on the tunnel interface; upon expiration of this timer, the tunnel will send probe messages to discover Path MTU; aging-mins: aging time ranging from 1 to 65535 seconds.                  Min-mtu: configures MTU lower limit that can be adjusted by PMTUD; mtu-bytes: lower limit of MTU, ranging from 92 to 1500 bytes.</p>
<pre>Qtech(config-if)# no tunnel path-mtu-discovery</pre>	<p>Disables the PMTUD function of the tunnel interface.</p>

PMTUD can work only in GRE or IPIP tunnel mode, and is not enabled by default.



**Caution**

The PMTUD function requires the tunnel interfaces on both ends of the tunnel to be able to receive and process ICMP messages, especially when there is a firewall. This command is only supported by RGOS 10.4(1) or later versions.

**9.1.2.11 Configuring the keepalive function of a tunnel**

When the physical interface sending tunnel messages is UP but the line failure prevents the tunnel messages from reaching the opposite terminal, the tunnel keepalive function can be used to detect the reachability of the tunnel interface.

Command	Function
---------	----------

Command	Function
Qtech(config-if)# <b>keepalive</b> [ <i>seconds</i> [ <i>retries</i> ]]	Configures the keepalive function of the tunnel.
Qtech(config-if)# <b>no keepalive</b>	Disables the keepalive function of the tunnel

**Caution**

This command is only supported by RGOS 10.4(2) or later versions.  
 This command cannot be used together with the **tunnel vrf** or **ip vrf forward** command.  
 This command applies only to GRE IP-capable 4 over 4 tunnels and IPIP tunnels.

Command	Function
Qtech(config-if)# <b>tunnel keepalive</b> <i>period retries</i>	Configures the keepalive function of the tunnel.
Qtech(config-if)# <b>no tunnel keepalive</b>	Disables the keepalive function of the tunnel

**Caution**

This command is only supported by RGOS 10.4(1).  
 This command cannot be used together with the **tunnel vrf** or **ip vrf forward** command.  
 This command applies only to GRE IP-capable 4 over 4 tunnels and IPIP tunnels.

### 9.1.2.12 Configuring Tunnel nested encapsulation limit

Tunnel nested encapsulation refers to the circumstance that messages have undergone multi-level nested tunnel encapsulation on the local device before being sent out. The route change on the local device may result in infinite nested encapsulation. Excessive nesting will result in the continual fragmentation and recombination operations of the router and severely compromise routing performance. In order to avoid the occurrence of aforementioned phenomena, RGOS software can automatically avoid infinite nested encapsulation. Only 4-level nesting is allowed by default. Use the **tunnel nested-limit** command to modify the default value. This command is used on the tunnel interface of the innermost layer.

Command	Function
Qtech(config-if)# <b>tunnel nested-limit</b> <i>num</i>	Configures the tunnel nested encapsulation limit. Default value: 4-level; value range: 0-10.
Qtech(config-if)# <b>no tunnel nested-limit</b>	Restores the nested encapsulation limit to the default value.

### 9.1.2.13 Configuring Tunnel VRF

Identify which VRF would be used by the outer-layer transport protocol IPv4 for route selection and forwarding. Run the following commands:

Command	Function
Qtech(config-if)# <b>tunnel vrf</b> <i>vrf-name</i>	Configures Tunnel VRF.
Qtech(config-if)# <b>no tunnel vrf</b>	Removes Tunnel VRF configuration.

By default, the outer-layer IPv4 uses a global VRF table for route selection and forwarding. The source IP address and destination IP address of outer-layer encapsulation must be in the same VRF table. If in the designated VRF, there is no available route to the destination IP address, then this tunnel interface will be in down state.



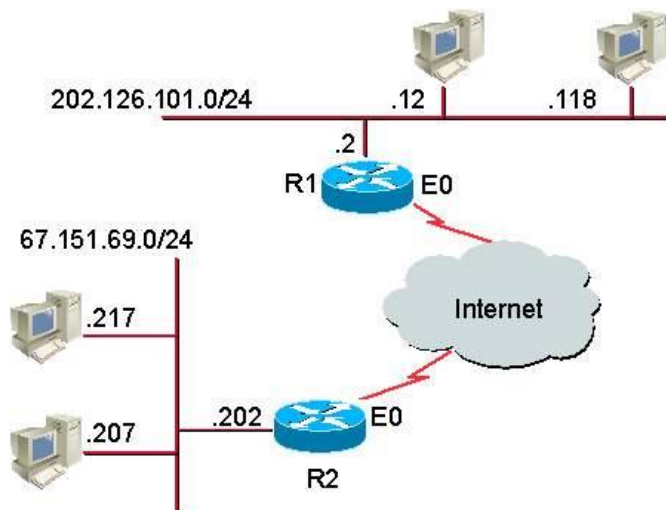
**Caution**

Currently, the tunnel VRF function can only support IPv4 over IPv4 GRE tunnel. This command is only supported by RGOS 10.4(2) or later versions.

### 9.1.3 Example of Tunnel Interface Configuration

The network connections of this configuration example are shown in Figure .

Figure 30 Network connections of Tunnel interface configuration example



In the configuration example, a tunnel is created between R1 and R2. The subnet 202.126.101.0/24 behind R1 communicates with the subnet 67.151.69.0/24 behind R2 via the tunnel between R1 and R2. Such communication is carried out through the tunnel. The external network between R1 and R2 is transparent and invisible: a virtual private network (VPN). Tunnel configurations of R1 and R2 are shown below.

#### Configuration of R1:

```
interface Tunnel0
ip address 21.21.21.3 255.255.255.0
tunnel source 179.208.12.221
tunnel destination 179.208.12.55
!
interface FastEthernet0/0
ip address 179.208.12.221 255.255.255.0
!
interface FastEthernet0/1
ip address 202.106.101.2 255.255.255.0
!
```

#### Configuration of R2:

```
interface Tunnel0
ip address 21.21.21.5 255.255.255.0
tunnel source 179.208.12.55
tunnel destination 179.208.12.221
!
interface FastEthernet0/0
ip address 179.208.12.55 255.255.255.0
!
interface FastEthernet0/1
ip address 67.151.69.202 255.255.255.0
!
```

From the preceding configuration, you can learn that both R1 and R2 use Ethernet interface f0/0 to create a tunnel and use Ethernet interface f0/1 to connect to Intranet and serve as the gateway of Intranet.

### 9.1.4 Monitoring and Maintaining Tunnel interfaces

Qtech products enable you to monitor and maintain tunnel interfaces by using the **show interfaces tunnel** and **debug [gre/ip | ipip]** commands.

Command	Function
Qtech# <b>show interfaces tunnel</b> <i>tunnel-number</i>	Queries the status of a tunnel interface
Qtech# <b>show tunnel gre</b>	Queries the general configurations of a GRE tunnel
Qtech# <b>debug [gre/ip   ipip]</b>	Turns on tunnel debug switch.
Qtech# <b>no debug [gre/ip   ipip]</b>	Turns off tunnel debug switch.

The examples show how to use **show interfaces tunnel** command and **debug** command.

#### 42) Usage of the show interfaces tunnel command

```
Qtech# show interfaces tunnel 1
Tunnel 1 is UP , line protocol is UP
Hardware is Tunnel
Interface address is: 1.1.1.1/24
MTU 1500 bytes, BW 9 Kbit
Encapsulation protocol is Tunnel, loopback not set
Keepalive interval is 0 sec , no set
Carrier delay is 0 sec
RXload is 1 ,Txload is 1
Tunnel source 192.168.200.200 (FastEthernet 0/0), destination 192.168.200.100
Tunnel protocol/transport GRE/IP, key 0xea
Order sequence numbers 0/0 (tx/rx)
Checksumming of packets enabled Queueing strategy: WFQ
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
```

You can learn about the parameter settings and working status of the tunnel interface from the above information, such as the status of interface and link, IP address configuration, MTU configuration, bandwidth configuration and etc.

#### 43) Usage of the debug command

```
Qtech# debug gre/ip
Qtech#
GRE: to decaps 192.168.200.100->192.168.200.200 (len=132
ttl=255) 112
```

The above information indicates that a GRE/IP data packet is received from destination terminal (192.168.200.100) and de-encapsulated to obtain the IP payload packet.

### 9.1.5 Troubleshooting Faults on the Tunnel Interface

If both ends of a tunnel cannot communicate normally, carry out troubleshooting from the following aspects:

- 44) Make sure there is a reachable physical path between two ends of the tunnel, that is, the two ends are reachable for each other even if this tunnel is unavailable. Normal communication can be carried out between the source address (local terminal) of the tunnel and the destination address (peer terminal) of the tunnel.
- 45) Make sure the source address corresponds with the destination address, i.e., the source address must be identical with the destination address.

- 46) Make sure the tunnel uses the correct encapsulation mode (GRE by default), and both ends of the tunnel must use the same encapsulation mode.
- 47) After using GRE as the tunnel encapsulation protocol, make sure the checksum, Key and reception rule configurations are identical on both ends.

## 10 CONFIGURING THE AAA FUNCTION

Access control specifies the users who are allowed to access a server and lists the services that are accessible on the network. Authentication, authorization and accounting (AAA) is a key security mechanism for access control.

### 10.1 Overview

AAA presents a unified framework for configuring the authentication, authorization and accounting functions, which is supported by Qtech products.

AAA provides the following services in a modular manner:

- **Authentication:** It verifies whether a user can get the right to access. User authentication is performed using RADIUS, TACACS+, or Local before a user accesses the network or a service on the network.
- **Authorization:** It determines the services which are accessible to a user by defining a series of attribute-value pairs (AVPs). These AVPs describe the operations the user is authorized to do. These AVPs can be stored on a network device or a remote RADIUS security server.
- **Accounting:** It records network resource usage of users. The network device starts sending resource usage of users to the Radius security server in the form of statistics when the accounting function is enabled. Every accounting record is stored in the security server as AVPs. These records can be read by special software to implement the accounting, statistics and tracing of network resource usage.



#### Note

Some products only provide the authentication function. For all problems with product specifications, contact the marketing or technical support personnel.

Although AAA is the primary access control method boasting superior security protection, Qtech products also provide simpler control access methods, such as the local username authentication and line password authentication.

AAA has the following advantages:

- Excellent flexibility and controllability
- Expandability
- Standardized authentication
- Multiple backup systems

#### 10.1.1 Basic AAA Principles

AAA types can be dynamically configured on a per-user (line) or per-server basis by creating method lists and applying them to specific services or interfaces.

#### 10.1.2 Method List

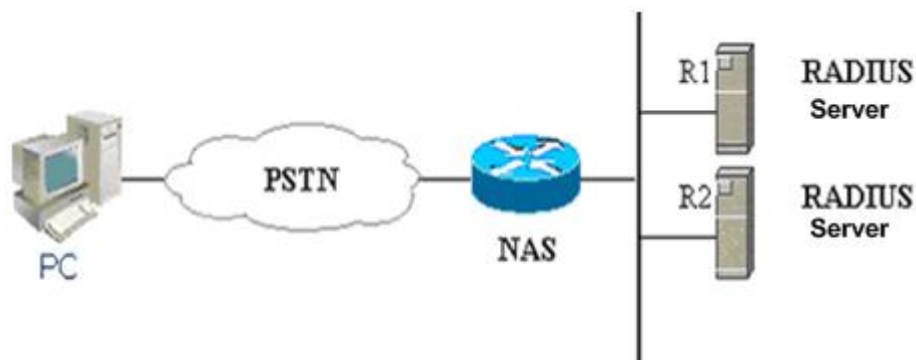
Since a variety of methods are available for user AAA, a method list should be used to define the sequence in which these methods are performed. The method list can define one or more security protocols for authentication, so that a backup system takes effect when the first method fails. In Qtech products, a next method is selected if no response is received from the previous method till there is successful communication with a method or all methods in the list are attempted. If all methods listed are attempted but communication is not set up, AAA fails.



#### Caution

Only when there is no response from a method, Qtech products will attempt the next method. During the authentication, if the user access is refused by a method, the authentication process ends and no other methods will be attempted.

Figure 31 Typical AAA network configuration



The preceding figure illustrates typical AAA network configuration, including two RADIUS security servers R1 and R2 and a network access server (NAS) that can function as a RADIUS server.

Supposed the system administrator has defined a method list, where user identity information is first obtained from R1, R2, and then the local username database on the NAS. If a remote PC user attempts to access the network via dialup, the NAS first queries the authentication information from R1. If the user is authenticated by R1, R1 sends a ACCEPT reply to the NAS, allowing the user to access the network. If R1 returns a REJECT reply, the user access is refused and connection from the user is rejected. If R1 does not reply, the NAS regards that timeout occurs and queries authentication information from R2. This process continues unless the user is authenticated, user access is rejected, or the session is terminated. If TIMEOUT is returned for all methods, the authentication fails and the user is disconnected.



#### Caution

The REJECT response is different from the TIMEOUT response. The server returns a REJECT message if a user fails to comply with the standard in the available authentication database. The server returns a TIMEOUT message if there is no response from the security server to the authentication. When an TIMEOUT message is detected, the next authentication method in the method list is selected to continue the authentication process.



#### Note

This document uses RADIUS for an example to describe the AAA function of security servers. For security access implementation based on TACACS+, see *Configuring TACACS+*.

## 10.2 AAA Configuration Steps

First you shall choose a security solution, evaluate the potential security risks in the specific network and select the proper measures to prevent unauthorized access. It is recommended that AAA be used to ensure network security.

### 10.2.1 AAA Configuration Description

AAA configuration may become simple when you understand the basic operation process of AAA. To configure AAA on network devices of Qtech, perform the following steps:

- 48) Enable AAA by using the **aaa new-model** command in global configuration mode.
- 49) Configure parameters of the security protocol, RADIUS for example if you decide to use the security server.
- 50) Define the authentication method list by using the **aaa authentication** command.
- 51) Apply the method list to specific interface or line, if necessary.

**Caution**

When the specific method list is used, if no named method list is specified, the default authentication method list will apply.  
As a result, if you do not want to use the default authentication method list, you shall define a specific method list.

For complete descriptions of the commands mentioned in this chapter, see related chapters in the *Security Configuration Command Reference*.

**10.2.2 Enabling AAA**

Before activating AAA security features, be sure to enable AAA.

To enable AAA, use the following command in global configuration mode:

Command	Function
Qtech(config)# <b>aaa new-model</b>	Enables AAA.

**10.2.3 Disabling AAA**

To disable AAA, use the following command in global configuration mode:

Command	Function
Qtech(config)# <b>no aaa new-model</b>	Disables AAA.

**10.2.4 Follow-up Configuration**

The following tables lists the possible configuration tasks that need to be completed after AAA enabling and chapters they are described in.

AAA access control security solution

Configuration task	Chapter
Configuring RADIUS Security Parameters	Configuring RADIUS
Configuring Local Login Authentication	Configuring Authentication
Defining AAA Authentication Method List	Configuring Authentication
Applying Method List to Specific Interface or Line	Configuring Authentication
Configuring RADIUS Authorization	Configuring Authorization
Enabling RADIUS Accounting	Configuring Accounting

If you are using AAA for authentication, see the "*Configuring Authentication*" section.

**10.3 Configuring Authentication**

Users need to be authenticated before they access network resources. In most cases, AAA is recommended for authentication.

**10.3.1 Defining AAA Authentication Method List**

To configure the AAA authentication, the first step is to define a named list of authentication methods, and then the applications use the defined method list for authentication. The method list defines the authentication types and sequence in which they are performed. The defined authentication methods, except the default method list, are specific to applications. Before a named method list is defined, all applications use the default method list.

A method list is simply a named list describing the authorization methods to be queried in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Qtech products use the first method listed to authorize users for specific network services; if that method fails to respond, Qtech products select the next method listed in the method list. This process continues till there is successful communication with a listed authorization method, or all methods defined are exhausted.



**Caution**

Only when there is no response from a method, Qtech products will attempt the next method. During the authentication, if the user access is refused by a method, the authentication process ends and no other methods will be attempted.

### 10.3.2 Configuration Examples

A typical AAA network has two RADIUS servers: R1 and R2. Suppose the network administrator has chosen a security solution, and the NAS authentication uses an authentication method to authenticate the Telnet connection. User authentication is initially attempted on R1, then on R2 if there is no response from R1, and finally in the local database of the NAS if there is no response from R2 either. To design such an authentication process, you must configure an authentication method list accordingly by using the following commands:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa authentication login default group radius local</b>	Configures a default authentication method list named <i>default</i> . The protocols included in this method list are arranged behind the name according to the order in which they will be queried. The default method list applies to all applications by default.

To apply a method list to a specific Login connection, the system administrator must create a named method list and then apply it to the specific connection. The following example shows how to apply the authentication method list to line 2 only.

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa authentication login test group radius local</b>	Defines a method list named <i>test</i> in global configuration mode.
<b>line vty 2</b>	Enters VTY line 2 configuration mode.
<b>login authentication test</b>	Applies the <i>test</i> method list to VTY line 2 in line configuration mode.

If a remote PC user attempts to Telnet the NAS, the NAS first queries the authentication information from R1. If the user is authenticated by R1, R1 sends a ACCEPT reply to the NAS, allowing the user to access the network. If R1 returns a REJECT reply, the user access is refused and connection from the user is rejected. If R1 does not reply, the NAS regards that timeout occurs and queries authentication information from R2. This process continues unless the user is authenticated, user access is rejected, or the session is terminated. If both servers (R1 and R2) return TIMEOUT, the authentication will be performed by the local database of the NAS.

**Caution**

The REJECT response is different from the TIMEOUT response. The server returns a REJECT message if a user fails to comply with the standard in the available authentication database. The server returns a TIMEOUT message if there is no response from the security server to the authentication. When an TIMEOUT message is detected, the next authentication method in the method list is selected to continue the authentication process.

### 10.3.3 Authentication Type

Qtech products support the following authentication types:

- Login authentication -- applies when a user tries to log in to the NAS through the command line interface (CLI).
- Enable authentication -- applies when an online user requests more rights on the CLI.
- PPP authentication -- applies to PPP dial-up users.
- DOT1X(IEEE802.1x) authentication -- applies to users who try to access through IEEE802.1x.

### 10.3.4 Configuring AAA Authentication

The following tasks are common for the configuration of AAA authentication.

- Enable AAA by using the **aaa new-model** command in global configuration mode.
- Configure the security protocol parameters if you decide to use the security server, such as RADIUS and TACACS+. See the "Configuring Radius" and "Configuring TACACS+" sections for details.
- Define the authentication method list by using the **aaa authentication** command.
- Applying the method list to a specific interface or line, if possible.



**Caution** TACACS+ is not supported by the DOT1X authentication on Qtech products.

### 10.3.5 Configuring the AAA Login Authentication

This section describes how to configure the AAA Login authentication methods supported by Qtech products:



**Caution** AAA security features can be made available only after AAA is enabled by using the **aaa new-model** command in global configuration mode. For the details, see the "AAA Overview" chapter.

In many cases, the user needs to Telnet the NAS for configuring the NAS remotely. To prevent unauthorized access to the NAS, user authentication is required.

The AAA security services make it easy for the network devices to perform line-based Login authentication. No matter which Login authentication method you use, you just need to use the **aaa authentication login** command to define one or more authentication method lists and apply them to the specific line that needs the Login authentication.

To configure the AAA Login authentication, run the following commands in global configuration mode:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa authentication login</b> {default   list-name} method1 [method2...]	Defines an accounting method list. To define multiple method lists, repeat this command.
<b>line vty</b> line-num	Enters the line to which the AAA authentication applies.
<b>login authentication</b> {default list-name}	Applies the method list to the line.

The keyword **list-name** is a character string used to name the created authentication method list, while **method** means the actual authentication algorithm. Only when the current method returns an ERROR message (no reply), the next authentication method will be attempted. If the current method returns a FAIL message, no authentication method will be used any more. To make sure that users can be authenticated even if no response is received from any method, use the **none** keyword.

In the following example, users can still be authenticated even if the RADIUS server returns TIMEOUT. Use the **aaa authentication login default group radius none** command.



**Caution** Since the keyword **none** enables every dial-up user to be authenticated even if the security server does not reply, it is used only as a backup authentication method. Normally, the **none** keyword is not recommended. You can use it as the last authentication method preceded by the local authentication method in the scenario where possible dial-up users are all trustful and their work are susceptible to any delay caused by system faults.

Keyword	Description
<b>local</b>	Uses the local username database for authentication.
<b>none</b>	User authentication is not performed.

Keyword	Description
<b>group radius</b>	Uses RADIUS to get authentication information.
<b>group tacacs+</b>	Uses TACACS+ to get authentication information.

The preceding table lists the AAA login authentication methods supported by Qtech products.

### 10.3.5.1 Using the Local Database for Login Authentication

To use the local database for Login authentication, configure the local database first. Qtech product supports authentication based on the local database. To enable the username authentication, run the following commands in global configuration mode:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>username name [password password]</b>	Creates a local user and sets a password.
<b>end</b>	Returns to privileged mode.
<b>show running-config</b>	Verifies the configuration.

To define and apply the local login authentication method list, use the following commands:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa authentication login {default   list-name} local</b>	Defines the local authentication method list.
<b>end</b>	Returns to privileged mode.
<b>show aaa method-list</b>	Verifies the configured method list.
<b>configure terminal</b>	Enters global configuration mode.
<b>line vty line-num</b>	Enters line configuration mode
<b>login authentication {default   list-name}</b>	Applies the method list.
<b>end</b>	Returns to privileged mode.
<b>show running-config</b>	Verifies the configuration.

### 10.3.5.2 Using Radius for Login Authentication

To use RADIUS for Login authentication, configure the RADIUS server. Qtech products support the authentication based on the RADIUS server. To configure the RADIUS server, use the following commands in global configuration mode:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>radius-server host ip-address [auth-port port] [acct-port port]</b>	Configures the RADIUS server
<b>end</b>	Returns to privileged mode.
<b>show radius server</b>	Shows the RADIUS server.

After the RADIUS server is configured, make sure there is successful communication with the RADIUS server before configuring RADIUS for authentication. For details about the RADIUS server configuration, see the "Configuring RADIUS" section.

Then you can configure the RADIUS server based method list. Use the following commands:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa authentication login {default   list-name} group radius</b>	Defines the local authentication method list.
<b>end</b>	Returns to privileged mode.
<b>show aaa method-list</b>	Verifies the configured method list.
<b>configure terminal</b>	Enters global configuration mode.
<b>line vty line-num</b>	Enters line configuration mode
<b>login authentication {default   list-name}</b>	Applies the method list.
<b>end</b>	Returns to privileged mode.

Command	Function
<code>show running-config</code>	Verifies the configuration.

### 10.3.6 Configuring the AAA Enable Authentication

This section describes how to configure the AAA Enable authentication methods supported by our product:

In many cases, the user needs to Telnet the NAS. After being authenticated, the user can access the CLI and is assigned 0–15 privilege levels initially, each having different commands. You can use the **show privilege** command to query the current level. For the details, see the "Using the CLI" section.

After logging in to the CLI, you can use the **enable** command to obtain higher privilege level if you fail to execute some commands. To prevent unauthorized access to the network, authentication needs to be performed when a user applies for a higher privilege level. This authentication type is called Enable authentication.

To configure the AAA Enable authentication, use the following commands in global configuration mode:

Command	Function
<code>configure terminal</code>	Enters global configuration mode.
<code>aaa new-model</code>	Enables AAA.
<code>aaa authentication enable default method1 [method2...]</code>	Defines an Enable authentication method list, for example RADIUS.

Only one Enable authentication method list can be defined globally, so there is no need to name the method list. The keyword **method** means the actual authentication algorithm. Only when the current method returns an ERROR message (no reply), the next authentication method will be attempted. If the current method returns a FAIL message, no authentication method will be used any more. To make sure that users can be authenticated even if no response is received from any method, use the **none** keyword.

Once configured, the Enable authentication method takes effect. When using **enable** command in privileged mode, the system prompts a message indicating authentication is required if you want to obtain a higher privilege level. There is no need to authenticate if the privilege level to be set is lower than or equal to the current one.



#### Caution

The current username will be recorded if the Login authentication (except for **none** method) is done when accessing the CLI. At this time, if the Enable authentication processes, a message indicating that the username must be entered will not be prompted and you can use the same username of Login authentication. Note that the password input must be consistent.

The username information will not be recorded if there is no Login authentication when you access the CLI, or the **none** method is used. At this time, if the Enable authentication is required, you shall enter the username again. This username will not be recorded, so you shall enter in each Enable authentication.

Some authentication methods can bind the security level. Then in the process of authentication, except for the returned response according to the security protocol, it is necessary to verify the bound security level. If the service protocol can bind the security level, the level shall be verified while authenticating. If the binded level is more than or equal to the level to be configured, the enable authentication and level switchover succeed. But if the bound level is less than the level to be configured, the Enable authentication fails, prompting an error message and keeping the current level. If the service protocol fails to be bound to the security level, you can configure the level without verification of the bound level. Now only RADIUS and Local authentication can be bound to security levels. To this end, security levels need to be checked only for these two methods.

#### 10.3.6.1 Using the Local Username Database for Enable Authentication

When configuring the local Enable authentication, you can configure the privilege level of local users. By default, the privilege level is 1. To configure the local Enable authentication, configure the local database and privilege levels. To enable the username authentication, use the following commands in global configuration mode:

Command	Function
<code>configure terminal</code>	Enters global configuration mode.
<code>username name [password password]</code>	Creates the local user and sets a password.
<code>username name [privilege level]</code>	Sets the user privilege level. (Optional)

Command	Function
<b>end</b>	Returns to privileged mode.
<b>show running-config</b>	Verifies the configuration.

To define the local Enable authentication method list, run the following commands:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa authentication enable default local</b>	Defines the local authentication method list.
<b>end</b>	Returns to privileged mode.
<b>show aaa method-list</b>	Verifies the configured method list.
<b>show running-config</b>	Verifies the configuration.

### 10.3.6.2 Using RADIUS for Enable Authentication

The standard RADIUS server can pass the privilege level bound to the Service-Type attribute (the standard attribute number is 6), can specify the privilege with 1 or 15 level. The extended RADIUS server (for example, SAM) can configure the privilege level of the administrator (the private attribute number is 42), can specify 0-15 privilege level. For the details of the RADIUS server, see the "Specifying the RADIUS Private Attribute Type" section in "Configuring RADIUS".

To configure the RADIUS Enable authentication, configure the RADIUS server and then the RADIUS Enable authentication method list. Use the following commands in global configuration mode:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa authentication enable default group radius</b>	Defines the RADIUS authentication method.
<b>end</b>	Returns to privileged mode.
<b>show aaa method-list</b>	Verifies the configured method list.
<b>show running-config</b>	Verifies the configuration.

### 10.3.7 Configuring the AAA Authentication for PPP Users

PPP is a link-layer protocol of carrying the network-layer datagram in the point-to-point link. In many circumstances, the user accesses the NAS by means of asynchronous or ISDN dial-up. Once the connection has been set up, the PPP negotiation will be enabled. To prevent the unauthorized access to the network, authentication is required for the dial-up user in the process of PPP negotiation.

This section describes how to configure the AAA Enable authentication methods supported by Qtech products. To configure the AAA Enable authentication, use the following command in global configuration mode:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa authentication ppp</b> {default   <i>list-name</i> } <i>method1</i> [ <i>method2...</i> ]	Defines a PPP authentication method list. RADIUS, TACACS+ remote authentication and using the local database are the supported authentication methods.
<b>interface</b> <i>interface-type interface-number</i>	Enters the asynchronous or ISDN interface to which AAA authentication applies.
<b>ppp authentication</b> {chap   pap} {default   <i>list-name</i> }	Applies the method list to the asynchronous or ISDN interface.

For details about PPP configuration, see the related chapter in *Configuring PPP and MP*.

### 10.3.8 Configuring the AAA Authentication for 802.1x Users

IEEE802.1x is a standard of Port-Based Network Access Control, providing the point-to-point secure access for the LAN, and a means of the authentication of the user connecting to the LAN device.

This section describes how to configure the 802.1x authentication methods supported by Qtech products. To configure the AAA Enable authentication, use the following command in global configuration mode:



Command	Function
<code>configure terminal</code>	Enters global configuration mode.
<code>aaa new-model</code>	Enables AAA.
<code>aaa authentication dot1x {default   list-name} method1 [method2...]</code>	Defines an IEEE802.1x authentication method list. RADIUS remote authentication and using the local database are the supported authentication methods.
<code>dot1x authentication list-name</code>	Applies the method list to 802.1x users.

For details about IEEE802.1x configuration, see the related chapter in *Configuring 802.1x*.

### 10.3.9 Example of Authentication Configuration

The following example illustrates how to apply both RADIUS authentication and local authentication to a network device.

```
Qtech(config)# aaa new-model
Qtech(config)# username Qtech password starnet
Qtech(config)# radius-server host 192.168.217.64
Qtech(config)# aaa authentication login test group radius local
Qtech(config)# line vty 0
Qtech(config-line)# login authentication test
Qtech(config-line)# end
Qtech# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius local
username Qtech password 0 starnet
!
radius-server host 192.168.217.64
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
!
```

In the preceding example, the access server uses the RADIUS server (IP address: 192.168.217.64) to perform Login authentication for users. If the RADIUS server does not reply, the local database will be used for authentication.

### 10.3.10 Example of Terminal Service Application Configuration

In the environment of the terminal service application, the terminal first connects to the asynchronous console, then offers the service accessing the network network server. However, if AAA is enabled, the Login authentication is necessary in all lines. To access the server, the terminal must pass the Login authentication and it influences the terminal service. You can separate two lines by configuration that makes the line using the terminal service directly connecting the server without the Login authentication, and ensures the device security by the Login authentication of the line connecting the device. That is to say, you can configure a login authentication list specific for the terminal service but the authentication method as **none**. Then apply the configured list to the line with terminal service enabled, while other lines connecting the local device is unchanged. In this way, the terminal can skip the local login authentication.

The following example illustrates the configuration steps:

```
Qtech(config)# aaa new-model
Qtech(config)# username Qtech password starnet
Qtech(config)# radius-server host 192.168.217.64
Qtech(config)# radius-server key test
Qtech(config)# aaa authentication login test group radius local
Qtech(config)# aaa authentication login terms none
Qtech(config)# line tty 1 4
Qtech(config-line)# login authentication terms
```



```
Qtech(config-line)# exit
Qtech(config)# line tty 5 16
Qtech(config-line)# login authentication test
Qtech(config-line)# exit
Qtech(config)# line vty 0 4
Qtech(config-line)# login authentication test
Qtech(config-line)# end
Qtech(config)# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius local
aaa authentication login terms none
username Qtech password 0 starnet
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line aux 0
line tty 1 4
login authentication terms
line tty 5 16
login authentication test
line vty 0 4
login authentication test
!
!
```

In the preceding example, the NAS uses the RADIUS server (IP address: 192.168.217.64) to perform login authentication for users. If the RADIUS server does not reply, the local database will be used for authentication. Login authentication is unnecessary for TTY 1-4 is the used line of the terminal service, while using other TTY and VTY lines needs the login authentication.

## 10.4 Configuring Authorization

The AAA authorization enables the administrator to control the use of services or rights. After the AAA authorization service is enabled, the network device configures the user sessions by using the user configuration file stored locally or in the server. After the authorization is completed, the user can only use the services allowed in the profile or has the assigned rights.

### 10.4.1 Authorization Types

Qtech products support the following AAA authorization methods:

- Exec authorization: The user terminal logs in to the CLI of the NAS and is granted the privilege level (0-15).
- Command authorization: After a user logs in to the CLI of the NAS, the user is specific commands are authorized.
- Network authorization: Grants the available service to the user session in the network.



#### Note

Only TACACS+ supports the command authorization method. For the detailed information, see the "Configuring TACACS+" section.

### 10.4.2 Preparations for Authorization

The following tasks must be completed before the AAA authorization is configured:

- Enable the AAA server. For details, see the AAA Overview chapter.

- (Optional) Configure the AAA authentication. The authorization is performed after the user is authenticated. But independent authorization can also be performed without authentication. For details of the AAA authentication, see the "Configuring Authentication section.
- (Optional) Configure security protocol parameters. If the security protocol is required for authorization, configure the security protocol parameters. The network authorization only supports RADIUS; the Exec authorization supports RADIUS and TACACS+. For details of the RADIUS, see the "Configuring RADIUS" section. For details of the TACACS+, see the "Configuring TACACS+ section.
- (Optional) If the local authorization is required, use the **username** command to define the user rights.

### 10.4.3 Configuring Authorization List

To enable AAA authorization, use the following commands in global configuration mode:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa authorization exec network</b> {default   <i>list-name</i> } <i>method1</i> [ <i>method2</i> ]...	Defines the AAA Exec authorization method.
<b>aaa authorization network network</b> {default   <i>list-name</i> } <i>method1</i> [ <i>method2</i> ]...	Defines the AAA Network authorization method.

### 10.4.4 Configuring AAA Exec Authorization

The Exec authorization grants the privilege level of command execution for the user terminal logging in to the NAS. You can use the **show privilege** command to display the specific level after the user logs in to the NAS CLI successfully (by telnet, for example).

No matter which Exec authorization method you use, you just need to use the **aaa authorization exec** command to define one or more authorization method lists and apply them to the line that needs the Exec authorization.

To configure the AAA Exec authorization, use the following commands in global configuration mode:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa authorization exec network</b> {default   <i>list-name</i> } <i>method1</i> [ <i>method2</i> ]...	Defines the AAA Exec authorization method. If you need to define multiple methods, execute this command repeatedly.
<b>line vty</b> <i>line-num</i>	Enters the line to which the AAA Exec authorization method is applied.
<b>authorization exec</b> {default   <i>list-name</i> }	Applies the method to the line.

The keyword **list-name** is a character string used to name the created authorization method list, while the keyword **method** means the actual authorization algorithm. Only when the current method returns an ERROR message (no reply), the next authorization method will be attempted. If the current method returns a FAIL message, no authorization method will be used any more. To make sure that users can be authorized successfully even if no response is received from any method, use the **none** keyword.

In the following example, the Exec authorization is still successful even if the RADIUS server returns TIMEOUT:

```
aaa authorization exec default group radius none
```

Keyword	Description
<b>local</b>	Uses the local username database for Exec authorization.
<b>none</b>	Exec authorization is not performed.
<b>group radius</b>	Uses RADIUS for Exec authorization.
<b>group tacacs+</b>	Uses TACACS+ for Exec authorization.

The preceding table lists the AAA Exec authorization methods supported by Qtech products.

**Caution**

The exec authorization is always used together with the login authentication, and they can be applied to the same line at the same time. But note that it is possible to have different results of the authentication and the authorization towards the same user because they can use different methods and servers. If the Exec authorization fails, a user cannot access the CLI even though the login authentication of the user is successful.

#### 10.4.4.1 Using the Local Username Database for Exec Authorization

To configure the local Exec authorization, configure the local database first. You can configure the privilege level of local users. By default, the privilege level is 1. Use the following commands in global configuration mode:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>username</b> <i>name</i> [ <b>password</b> <i>password</i> ]	Creates a local user and sets a password.
<b>username</b> <i>name</i> [ <b>privilege</b> <i>level</i> ]	Sets the user privilege level. (Optional)
<b>end</b>	Returns to privileged mode.
<b>show running-config</b>	Verifies the configuration.

To define the local Exec authorization method list, use the following commands:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa authorization exec</b> { <b>default</b>   <i>list-name</i> } <b>local</b>	Defines the local authorization method list.
<b>end</b>	Returns to privileged mode.
<b>show aaa method-list</b>	Verifies the configured method list.
<b>configure terminal</b>	Enters global configuration mode.
<b>line vty</b> <i>line-num</i>	Enters line configuration mode.
<b>authorization exec</b> { <b>default</b>   <i>list-name</i> }	Applies the method list.
<b>end</b>	Returns to privileged mode.
<b>show running-config</b>	Verifies the configuration.

#### 10.4.4.2 Using RADIUS for Exec Authorization

To configure the RADIUS Exec authorization, onfigure the RADIUS server. For details about the RADIUS server configuration, see the "Configuring RADIUS" section.

After configuring the RADIUS server, the RADIUS authorization method list can be configured. Use the following commands in global configuration mode:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa authentication enable</b> { <b>default</b>   <i>list-name</i> } <b>group radius</b>	Defines RADIUS authentication method.
<b>end</b>	Returns to privileged mode.
<b>show aaa method-list</b>	Verifies the configured method list.
<b>configure terminal</b>	Enters global configuration mode.
<b>line vty</b> <i>line-num</i>	Enters line configuration mode.
<b>authorization exec</b> { <b>default</b>   <i>list-name</i> }	Applies the method list.
<b>end</b>	Returns to privileged mode.
<b>show running-config</b>	Verifies the configuration.

#### 10.4.4.3 Example of Configuring Exec Authorization

The following example illustrates how to configure Exec authorization. The local login authentication and the "Radius+local" Exec authorization are used when the user logs in through VTY lines 0-4. The NAS uses the RADIUS

server with IP address set to 192.168.217.64 and shared keyword **test**. The local username and password are **Qtech**, and the privilege level is 6.

```
Qtech# configure terminal
Qtech(config)# aaa new-model
Qtech(config)# radius-server host 192.168.217.64
Qtech(config)# radius-server key test
Qtech(config)# username Qtech password Qtech
Qtech(config)# username Qtech privilege 6
Qtech(config)# aaa authentication login mlist1 local
Qtech(config)# aaa authentication exec mlist2 group radius local
Qtech(config)# line vty 0 4
Qtech(config-line)# login authentication mlist1
Qtech(config-line)# authorization exec mlist2
Qtech(config-line)# end
Qtech(config)# show running-config
!
aaa new-model
!
aaa authorization exec mlist2 group radius local
aaa authentication login mlist1 local
!
username Qtech password Qtech
username Qtech privilege 6
!
Radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line vty 0 4
authorization exec mlist2
login authentication mlist1
!
end
```

### 10.4.5 Configuring AAA Network Authorization

Qtech product support PPP and SLIP network authorization. The network authorization makes service configuration regarding traffic, bandwidth, and timeout available on the network connection. The network authorization only supports RADIUS and TACACS+. The authorization information assigned by the server are encapsulated in the RADIUS attribute or TACACS+ attribute. Authorization information may vary with network connections.



#### Caution

Now AAA network configuration does not support 802.1X. For details about the 802.1X authorization, see the "Configuring 802.1X" section.

To configure the AAA network authorization, use the following commands in global configuration mode:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa authorization network{default   list-name} method1 [method2]...</b>	Defines an AAA network authorization method. If you need to define multiple methods, use this command repeatedly.

The keyword **list-name** is a character string used to name the created authorization method list, while **method** means the actual authorization algorithm. Only when the current method returns an ERROR message (no reply), the next authorization method will be attempted. If the current method returns a FAIL message, no authorization method will be used any more. To make sure that users can be authenticated even if no response is received from any method, use the **none** keyword.

### 10.4.5.1 Using RADIUS for Network Authorization

To configure RADIUS Network authorization, configure the RADIUS server. For details about the RADIUS server configuration, see the "Configuring RADIUS" section.

After configuring the RADIUS server, the RADIUS Network authorization method list can be configured. Use the following commands in global configuration mode:

Command	Function
<code>configure terminal</code>	Enters global configuration mode.
<code>aaa new-model</code>	Enables AAA.
<code>aaa authentication network {default   list-name} group radius</code>	Defines a RADIUS Network authorization method.

### 10.4.5.2 Example of Configuring Network Authorization

The following example illustrates how to configure Network authorization.

```
Qtech# configure terminal
Qtech(config)# aaa new-model
Qtech(config)# radius-server host 192.168.217.64
Qtech(config)# radius-server key test
Qtech(config)# aaa authorization network test group radius local
Qtech(config-line)# end
Qtech(config)# show running-config
!
aaa new-model
!
aaa authorization network test group radius none
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
```

## 10.5 Configuring Accounting

The AAA accounting function enables you to trace the services and network resources used by the user. After the accounting function is enabled, the NAS or router sends network access records of users to the RADIUS security server by means of AVP. You may use some analysis software to analyze these data to implement the billing, audit and tracing function for the user's activities.

### 10.5.1 Accounting Types

Qtech products currently support the following accounting types:

- Exec accounting -- records the accounting information when users access or exit the CLI of the NAS.
- Command accounting – records the specific commands executed after the user logs in to the CLI of the NAS.
- Network accounting – records the related information on the user session in the network.



**Note** The command accounting function supports only TACACS+. For details, see the "Configuring TACACS+" section.

### 10.5.2 Preparations for Accounting

The following tasks must be completed before the AAA accounting is configured:

- Enable the AAA server. For details, see the "AAA Overview" chapter.
- Define the security protocol parameters. It is required to configure the security protocol parameters for accounting. The network accounting only supports RADIUS; the Exec accounting supports RADIUS and TACACS+; the Command accounting supports TACACS+ only. For details of RADIUS, see the "Configuring RADIUS" section. For details of TACACS+, see the "Configuring TACACS+" section.



- (Optional) Configure the AAA authentication. Certain types of accounting (for example, Exec accounting) are performed after the user is authenticated. In some circumstances, the accounting can also be performed without authentication. For details about AAA authentication, see the "Configuring Authentication" section.

### 10.5.3 Configuring AAA Exec Accounting

The Exec accounting records the information when users access or exit the CLI of the NAS. When a user logs in and accesses the NAS CLI, it sends the accounting start information to the security server. When the user exits the CLI, it sends the accounting stop information to the server.



#### Caution

Exec accounting starts only after login authentication of the user is successful. If no login authentication or **none** authentication method has been configured, Exec accounting is not performed. If a user does not send no accounting start information to the security server when logging in, no accounting stop information will be sent when the user logs out.

To configure the AAA Exec accounting, use the following commands in global configuration mode:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa accounting exec</b> {default   <i>list-name</i> } <b>start-stop</b> <i>method1</i> [ <i>method2</i> ]...	Defines the AAA Exec accounting method list. If you need to define multiple method lists, use this command repeatedly.
<b>line vty</b> <i>line-num</i>	Enters the line to which the AAA Exec accounting applies.
<b>accounting exec</b> {default   <i>list-name</i> }	Applies the method list to the line.

The keyword **list-name** is a character string used to name the created accounting method list, while the keyword **method** means the actual accounting algorithm. Only when the current method returns an ERROR message (no reply), the next accounting method will be attempted. If the current method returns a FAIL message, no accounting method will be used any more. To make sure that users can be authorized successfully even if no response is received from any method, use the **none** keyword.



#### Note

The keyword **start-stop** is used for the NAS to send the accounting information at the start and end of the network service to the security server.

#### 10.5.3.1 Using the RADIUS for Exec Accounting

To configure RADIUS Exec accounting, configure the RADIUS server. For details about the RADIUS server configuration, see the "Configuring RADIUS" section.

After configuring the RADIUS server, the RADIUS accounting method list can be configured. Use the following commands in global configuration mode:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa accounting exec</b> {default   <i>list-name</i> } <b>start-stop</b> <b>group radius</b>	Defines a RADIUS accounting method.
<b>end</b>	Returns to privileged mode.
<b>show aaa method-list</b>	Verifies the configured method list.
<b>configure terminal</b>	Enters global configuration mode.
<b>line vty</b> <i>line-num</i>	Enters the line configuration mode.
<b>accounting exec</b> {default   <i>list-name</i> }	Applies the method list.
<b>end</b>	Returns to privileged mode.
<b>show running-config</b>	Verifies the configuration.



### 10.5.3.2 Example of Configuring Exec Accounting

The following example illustrates how to configure Exec accounting. The local login authentication and the RADIUS Exec authorization are used when the user logs in through VTY lines 0-4. The IP address and shared key of the RADIUS server are 192.168.217.64 and *test* respectively. The local username and password both are *Qtech*

```
Qtech# configure terminal
Qtech(config)# aaa new-model
Qtech(config)# radius-server host 192.168.217.64
Qtech(config)# radius-server key test
Qtech(config)# username Qtech password Qtech
Qtech(config)# aaa authentication login auth local
Qtech(config)# aaa accounting exec acct start-stop group radius
Qtech(config)# line vty 0 4
Qtech(config-line)# login authentication auth
Qtech(config-line)# accounting exec acct
Qtech(config-line)# end
Qtech(config)# show running-config
!
aaa new-model
!
aaa accounting exec acct start-stop group radius
aaa authentication login auth local
!
username Qtech password Qtech
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line vty 0 4
accounting exec acct
login authentication auth
!
end
```

### 10.5.4 Configuring AAA Network Accounting

Network accounting records the accounting information about user sessions, including the numbers of packets and bytes, IP address and username. Now network accounting only supports RADIUS.



#### Note

The format of RADIUS accounting information varies with the RADIUS security server. The contents of the accounting records may also vary with Qtech product versions.

To configure the AAA network accounting, use the following commands in global configuration mode:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa accounting network</b> {default   <i>list-name</i> } start-stop <i>method1</i> [ <i>method2</i> ]...	Defines the AAA network accounting method list. If you need to define multiple method lists, use this command repeatedly.

The keyword **list-name** is a character string used to name the created accounting method list, while the keyword **method** means the actual accounting algorithm. Only when the current method returns an ERROR message (no reply), the next accounting method will be attempted. If the current method returns a FAIL message, no accounting method will be used any more. To make sure that users can be authorized successfully even if no response is received from any method, use the **none** keyword.

### 10.5.4.1 Using RADIUS for Network Accounting

To configure RADIUS network accounting, configure the RADIUS server. For details about the RADIUS server configuration, see the "Configuring RADIUS" section.

After configuring the RADIUS server, the RADIUS accounting method list can be configured. Use the following commands in global configuration mode:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa accounting network {default   list-name} start-stop group radius</b>	Defines a RADIUS accounting method.

### 10.5.4.2 Example of Configuring Network Accounting

The following example illustrates how to configure network authorization using RADIUS.

```
Qtech# configure terminal
Qtech(config)# aaa new-model
Qtech(config)# radius-server host 192.168.217.64
Qtech(config)# radius-server key test
Qtech(config)# aaa accounting network acct start-stop group radius
Qtech(config-line)# end
Qtech(config)# show running-config
!
aaa new-model
!
aaa accounting network acct start-stop group radius
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
```

## 10.6 Monitoring AAA users

To view the information of the current login users, use the following commands in privileged user mode:

Command	Function
<b>show aaa user { id   all }</b>	View the information of the current AAA user.

## 10.7 Configuring VRF-supported AAA Group

Virtual Private Networks (VPNs) provide a secure method for bandwidth share on the backbone networks of ISPs. One VPN is the collection of the shared routes. Users connect to the ISP network through one or multiple interfaces. The VPN routing table is also called VPN routing//forwarding(VRF) table. AAA can specify the VRF for each self-defined server group.

In global configuration mode, use the following commands to configure VRF for the AAA group:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa group server radius gs_name</b>	Configures the RADIUS server group and enters server group configuration mode.
<b>ip vrf forwarding vrf_name</b>	Specifies the VRF for the group.
<b>end</b>	Returns to privilege mode.



**Note** VRF must be supported by Qtech products.

## 10.8 Configuring Login Lockout for Failed Authentication

To prevent users from cracking passwords, use a command to specify the number of attempts. If the number of login attempts exceeds the limit, the user is locked and cannot log in again in a period.

In global configuration mode, use the following commands to configure login parameters:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa new-model</b>	Enables AAA.
<b>aaa local authentication attempts &lt;1-2147483647&gt;</b>	Configures the number of login attempt.
<b>aaa local authentication lockout-time&lt;1-2147483647&gt;</b>	Configures the time (in hours) in which a user is locked when the number of login attempts of the user exceeds the limit.
<b>show aaa user lockout {all   user-name &lt;word&gt;}</b>	Displays the list of locked users.
<b>clear aaa local user lockout {all   user-name &lt;word&gt;}</b>	Clears the lockout user list.
<b>End</b>	Returns to privilege mode.



### Note

By default, the number of login attempts is 3 and the lockout time is 15 hours.

## 10.9 Configuring Domain Name-based AAA Service

This section is organized as follows::

- Overview
- Domain name-based AAA service configuration tasks
- Domain name-based AAA service configuration notes



### Caution

The domain name-based AAA service is applied to the IEEE802.1x authentication service. For the detailed IEEE802.1x protocol configurations, see the "Configuring 802.1x" section.

### 10.9.1 Overview

In the multi-domain environment, one NAS can provide the AAA service for users in different domains. Due to the different user attributes (such as the username, password, service type, privilege, ect) in each domain, users need to be distinguished by setting domains and each domain is configured with a unique attribute set including the AAA service method list (RADIUS for example).



### Note

Qtech products support the following username formats:

1. userid@domain-name
2. domain-name\userid
3. userid.domain-name
4. userid

Users named in the format of "userid" belong to the default domain.

Basic principles for configuring the domain name-based AAA service are as follows:

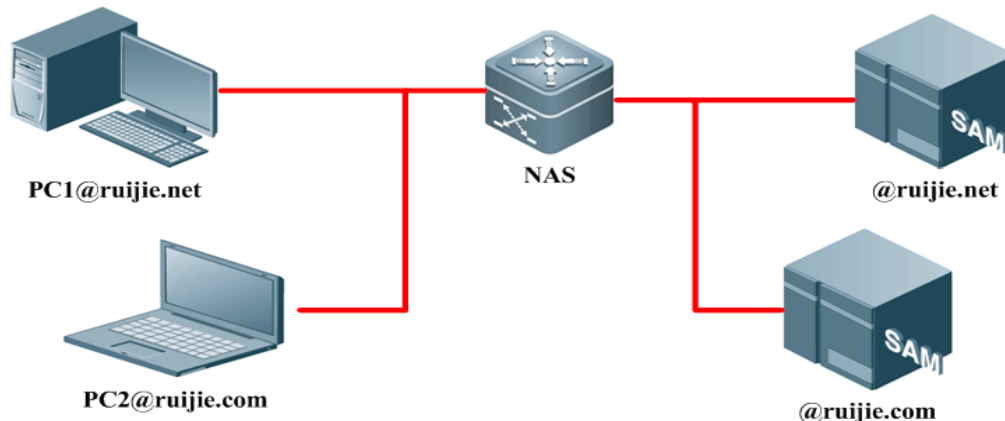
- Parsing the domain name of users
- Searching for the user domain according to the domain name
- Searching for the AAA service method list name according to the domain configurations
- Searching the corresponding method list according to the method list name in the system
- Providing the AAA service by using the method list



**Note** If one of the abovementioned steps fails, the AAA service cannot be used.

The following is the typical topology of a multi-domain environment:

Figure 32 Typical topology for a multi-domain network



### 10.9.2 Domain name-based AAA Service Configuration Tasks



**Note** The system supports up to 32 domains.

#### 10.9.2.1 Enabling AAA

Command	Function
<code>configure terminal</code>	Enters global configuration mode.
<code>aaa new-model</code>	Enables AAA.

For detailed command descriptions, see the "Enabling AAA" section.

#### 10.9.2.2 Defining the AAA Service Method List

Command	Function
<code>configure terminal</code>	Enters global configuration mode.
<code>aaa authentication dot1x {default   list-name} method1 [method2...]</code>	Defines the IEEE802.1x authentication method list.
<code>aaa accounting network {default   list-name} start-stop method1 [method2...]</code>	Defines the Network accounting method list.
<code>aaa authorization network {default   list-name} method1 [method2...]</code>	Defines the Network authorization method list.

For detailed command descriptions, see the "Configuring authentication", "Configuring Accounting" and "Configuring authorization" sections..

#### 10.9.2.3 Enabling the Domain Name-based AAA Service

Command	Function
<code>configure terminal</code>	Enters global configuration mode.
<code>aaa domain enable</code>	Enables the domain name-based AAA service.

### 10.9.2.4 Creating a Domain

You shall follow the following rules when searching for a domain by username:

- 52) A single character such as “.”, “\”, “@” can be used to distinguish between usernames and domain names.
- 53) The single “@” character is followed by the character string “domain-name”. With multiple “@” characters in the username, use the character string following the last “@” character as the domain-name. For example, if the username is a@b@c@d, use the a@b@c as the username and use the d as the domain-name.
- 54) The single “\” character follows the character string “domain-name”. With multiple “\” characters in the username, use the character string followed by the first “\” character as the domain-name. For example, if the username is a\b\c\d, use the b\c\d as the username and use the a as the domain-name.
- 55) The single “.” character is followed by the character string “domain-name”. With multiple “.” characters in the username, according to the pre-settings, use the character string following the last “.” character as the domain-name. For example, if the username is a.b.c.d, use the a.b.c as the username and use the d as the domain-name.
- 56) If all characters of “.”, “\” and “@” exist in the username, when matching the domain-name, use the rules in sequence of the “@”, “\” and “.” characters.

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>aaa domain domain-name</b>	Creates a domain and enters domain configuration mode.



#### Note

The AAA service supports domain names that have a maximum of 64 characters. Domain names are case insensitive.

### 10.9.2.5 Configuring the Domain Attribute Set

Use the following commands to select the AAA service method list in domain configuration mode:

Command	Function
<b>authentication dot1x {default   list-name}</b>	In domain configuration mode, select the authentication method list.
<b>accounting network {default   list-name}</b>	In domain configuration mode, select the accounting method list.
<b>authorization network {default   list-name}</b>	In domain configuration mode, select the authorization method list.

Use this command to configure the domain state:

Command	Function
<b>state {block   active}</b>	In domain configuration mode, set the domain state.

Use this command to check whether the username carries the domain name:

Command	Function
<b>username-format {without-domain   with-domain}</b>	In domain configuration mode, check whether the username carries the domain name information when the NAS is interacting with the server.

Use this command to set the maximum number of users supported in the domain:

Command	Function
<b>access-limit num</b>	In domain configuration mode, set the upper limit of users allowed in the domain. This function applies only to 802.1x users. By default, no upper limit is configured.

**Note**

1. Only AAA service method lists that have been configured can be selected in domain configuration mode. Otherwise, the system prompts that the AAA service method list you select does not exist.
2. With the domain name-based AAA service enabled, if there is no domain information carried by the username, use the default domain; if there is no configurations for the user domain in the system, the user is determined to be illegitimate and provides no AAA service.
3. In domain configuration mode, the default method list is selected if no other list is available.

### 10.9.2.6 Querying the Domain configuration

Use the following command to query the domain name-based AAA service information.

Command	Function
<b>show aaa domain</b> [domain-name]	Queries the current domain name-based AAA service information

### 10.9.3 Domain Name-based AAA Service Configuration Notes

When configuring the domain name-based AAA service, note the following points:

- 57) If the domain name-based AAA service is enabled, use the method list in the domain. If the service is not enabled, use the method list selected according to the access protocol (such as 802.1x, ect) for the AAA service. For example, if the service is not enabled, use the **dot1x authentication** *authen-list-name*, **dot1x accounting** *acct-list-name* *authen-list-name* and **dot1x accounting** *acct-list-name* *acct-list-name* command to provide the AAA service for the authentication and accounting method list name.
- 58) If the domain name-based AAA service is enabled, the default domain needs to be configured manually by default. The default domain is named "default" and is used to provide AAA services if the username does not contain domain name. Without the default domain configured, the user whose name does not carry the domain information fails to use the AAA services.
- 59) If the domain information is carried by the auth-user but the domain is not configured on the device, it fails to provide the AAA service for the user.
- 60) The AAA service method list selected by the domain must be consistent with the one defined by the AAA service. Or it fails to provide the AAA service for the users in the domain.
- 61) The domain name carried by the user shall accurately match the one configured on the device. For example, the domain.com and the domain.com.cn have been configured on the device, and the request message carried by the user is [aaa@domain.com](mailto:aaa@domain.com), the device determines that the user belongs to the domain.com but not the domain.com.cn.

### 10.9.4 Domain Name-based AAA Service Configuration Example

The following is an example of configuring the domain name-based AAA service:

```
Qtech(config)# aaa new-model
Qtech(config)# radius-server host 192.168.197.154
Qtech(config)# radius-server key test
Qtech(config)# aaa authentication dot1x default group radius
Qtech(config)# aaa domain domain.com
Qtech(config-aaa-domain)# authentication dot1x default
Qtech(config-aaa-domain)# username-format without-domain
```

After the configuration, with the user a1 in the radius server, use the 802.1x client to login the server for authentication by entering the username a1@domain.com and the correct password. The following shows the related domain name information:

```
Qtech#show aaa domain domain.com

=====Domain domain.com=====
State: Active
Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0
```



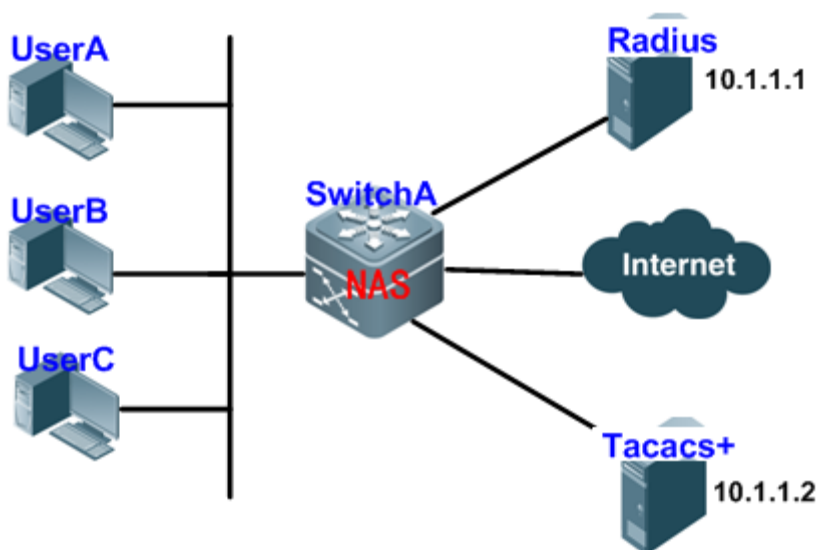
```
Selected method list:  
authentication dot1x default
```

## 10.10 Typical AAA Configuration Example

### 10.10.1 Typical AAA Application

#### 10.10.1.1 Network Topology

Figure 33 Typical AAA Application Topology



#### 10.10.1.2 Network Requirements

According to Figure 3, the following requirements must be met for better NAS security management:

- 62) The administrators shall have their own usernames and passwords, facilitating account management and preventing account leakage.
- 63) The user authentication methods are divided into local authentication and collection authentication. The method of combining the collection-authentication with the local-authentication shall be adopted, with the collection-authentication mainly-used and the local-authentication as backup. In the process of the collection-authentication, the Radius server authentication shall be passed first, if there is no reply, it will switch to the local authentication.
- 64) Different users can be configured to access the specified network device during the authentication.
- 65) Role-based management: Network management users are divided into the superusers and common users. Superusers have rights to query and configure the NAS, while common users only have limited query rights.
- 66) The user authentication information, the authorization information and the network information are recorded in the server for subsequent query and audit. (This example uses TACACS+ for accounting. )

#### 10.10.1.3 Configuration Key-points

From the analysis of the part of “*Network Requirements*”, deploying the AAA function can address the preceding requirements, which is to dynamically configure the ID authentication, authorization and accounting type for the user (line) or the server. Define the ID authentication, authorization and accounting type by creating the method list, and apply the method list to the specified service or interface. For details, see the “*Configuration Steps*” section.

#### 10.10.1.4 Configuration Steps

##### #Enable AAA:

! Enable the AAA function on the device

```
Qtech#configure terminal
Qtech(config)#aaa new-model
```

### # Configure the security server:

The security server provides the AAA services. Software of the server can record, calculate and analyze the various information in the form of logs.

! Configure the RADIUS server information (the shared key for the communication between the device and the RADIUS server is **Qtech**)

```
Qtech(config)#radius-server host 10.1.1.1
Qtech(config)#radius-server key Qtech
```

! Configure TACACS+ server information (the shared key for the communication between the device and the Tacacs+ server is **redgiant**)

```
Qtech(config)#tacacs-server host 10.1.1.2
Qtech(config)#tacacs-server key redgiant
```

### # Configure the local user:

! Configure password encryption (the key information for the local password and the security server are saved and displayed in the simply-encrypted format).

```
Qtech(config)#service password-encryption
```

! Configure the local user database (Configure the username and the password, and set the user privilege level).

```
Qtech(config)#username bank privilege 10 password yinhang
Qtech(config)#username super privilege 15 password star
Qtech(config)#username normal privilege 2 password normal
Qtech(config)#username test privilege 1 password test
```

! Configure the local enable password for the local Enable authentication.

```
Qtech(config)#enable secret w
```

! Configure the line login password (It does not work when the AAA function is enabled. So the line login password configuration is to prevent the login failure with the AAA function disabled).

```
Qtech(config)#line vty 0 15
Qtech(config-line)#password w
```

! Configure the line user privilege level (with the Exec authorization disabled, or no Exec authorization method list is applied in the line and no default Exec authorization method list, the configure line user privilege level should be used).

```
Qtech(config)#line vty 0 15
Qtech(config-line)#privilege level 10
```

### # Configure the authentication

#### 1. Login authentication

The Login authentication is used to control the user access. There are two methods to define the authentication method list: 1) Radius; 2) Local.

! Configure login authentication method list and apply it to the corresponding line

```
Qtech(config)# aaa authentication login hello group radius local
Qtech(config)# line vty 0 15
Qtech(config-line)# login authentication hello
```

To prevent the user from using the exhaust algorithm to crack the password during the Login authentication, AAA is used to limit the user Login attempts. When the the number of authentication attempts reaches the configured limit, the user is locked from login in a period (by default, three login authentication attempts are allowed and the lockout time is 15 hours.).

! Configure the number of allowed authentication attempts to 2 and the authentication lockout time to 10 hours

```
Qtech(config)#aaa local authentication attempts 2
Qtech(config)#aaa local authentication lockout-time 10
```

## 2. Enable authentication

The Enable authentication is used to switch the user privilege level. An authentication process is needed before the user switches the privilege level to the superuser using the **enable** command. There are two methods to define the authentication method list: 1) Radius; 2) Local. The Enable authentication can only set the default method list, which will be automatically applied after the configuration.

! Configure the enable authentication method list (RADIUS, TACACS+, and Local in descending order)

```
Qtech(config)#aaa authentication enable default group radius local
```

### # Configure the authorization

#### 1. Exec authorization

The Exec authorization is used to control the user command privilege level. For example, level 15 is assigned to the superuser, level 14 is assigned to the configuration user, level 2 is assigned to the common user. The remote Exec authorization takes precedence over the local one.

! Configure the Exec authorization method list (TACACS+ has higher priority over Local) and apply it to the line

```
Qtech(config)#aaa authorization exec shouquan group tacacs+ local
Qtech(config)#line vty 0 15
Qtech(config-line)#authorization exec shouquan
```

! Configure the exec authorization for the console (by default, the Exec authorization is not for the console)

```
Qtech(config)#aaa authorization console
```

#### 2. Command authorization

The Command authorization is used to offer the execution privilege of the key commands only to the administrators. The Command authorization authorizes the level of the command but not that of the current user. The RADIUS protocol is not supported.

! Configure the Command authorization method list (TACACS+ has higher priority over Local) and apply it to the line.

```
Qtech(config)#aaa authorization commands 2 abc group tacacs+ local
Qtech(config)#line vty 0 15
Qtech(config-line)#authorization commands 2 abc
```

### # Configure the accounting

#### 1. Exec accounting

The Exec accounting is used to send the information about a user when the user accesses and exits the server for subsequent query, statistics, and audit.

! Configure the Exec accounting method list (TACACS+ accounting) and apply it to the line.

```
Qtech(config)#aaa accounting exec default start-stop group tacacs+
```

#### 2. Command accounting

The Command accounting is used to send the commands of a specific level executed by the user to the server for subsequent query, statistics and the audit.

! Configure the command accounting method list (TACACS+ only) and apply it to all lines.

```
Qtech(config)#aaa accounting commands 2 default start-stop group tacacs+
```

### 10.10.1.5 Configuration verification

Step 1: Use the **show running-config** command to query the current configurations:

```
Qtech(config)#show run

Building configuration...
Current configuration : 2337 bytes

!
!
```

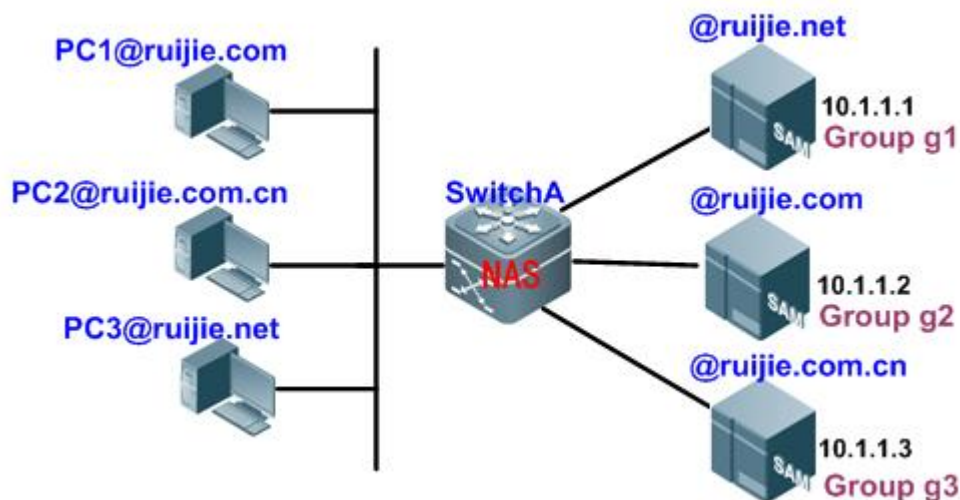
```
aaa new-model
aaa local authentication attempts 2
aaa local authentication lockout-time 10
!
!
!
aaa authorization exec shouquan group tacacs+ local
aaa authorization commands 2 abc group tacacs+
aaa accounting exec default start-stop group tacacs+
aaa authentication login hello group radius local
aaa authentication enable default group radius local
!
!
vlan 1
!
!
username bank password 7 09361c1c2f041c4d
username bank privilege 10
username super password 7 093c011335
username super privilege 15
username normal password 7 09211a002a041e
username normal privilege 2
username test password 7 093b100133
service password-encryption
!
!
!
!
tacacs-server key 7 072c062b121b260b06
tacacs-server host 10.1.1.2
radius-server host 10.1.1.1
radius-server key 7 072c16261f1b22
enable secret 5 $1$2MjW$xr1t0s1Euvt76xs2
!
!
!
!
line con 0
line vty 0 4
  authorization exec shouquan
  authorization commands 2 abc
  privilege level 10
  login authentication hello
  password 7 0938
line vty 5 15
  authorization exec shouquan
  authorization commands 2 abc
  privilege level 10
  login authentication hello
  password 7 005d
!
!
end
```

Step 2: In the actual application, use the **show aaa user { id | all }** command to query the current AAA user information.

## 10.10.2 AAA Multi-domain Authentication Application

### 10.10.2.1 Network Topology

Figure 34 AAA multi-domain authentication topology



### 10.10.2.2 Network Requirements

Configure the NAS device to enable the domain name-based AAA services:

- Use the 802.1x client for the login authentication with the username PC1@Qtech.com or PC2@Qtech.com.cn or PC3@Qtech,.net and the password.
- User network management: classify the users into superusers and common users, wherein the superusers are able to read and write while the common users are able to read only.
- The user authentication, authorization and network behavior are saved in the authentication server for subsequent query and audit.

### 10.10.2.3 Configuration Key Points

Configure the domain name-based AAA services to address the preceding network requirements.

The following example describes how to configure AAA multi-domain authentication on a 802.1x client.

### 10.10.2.4 Configuration Steps

#### #Enable AAA:

! Enable the AAA functions on the device

```
Qtech#configure terminal
Qtech(config)#aaa new-model
```

#### # Configure the security server:

The security server provides the AAA services. The user information is stored in the server and the software of the server can record, calculate and analyze the various information in the form of logs.

! Configure the RADIUS server information (the shared key for the communication between the device and the Radius server is **Qtech**)

```
Qtech(config)#aaa group server radius g1
Qtech(config-gs-radius)#server 10.1.1.1
Qtech(config-gs-radius)#exit
Qtech(config)#aaa group server radius g2
Qtech(config-gs-radius)#server 10.1.1.2
```

```
Qtech(config-gs-radius)#exit
Qtech(config)#aaa group server radius g3
Qtech(config-gs-radius)#server 10.1.1.3
Qtech(config-gs-radius)#exit
Qtech(config)#radius-server key Qtech
```

### # Configure the local user:

! Configure the password encryption (the key information for the local password and the security server is saved and displayed in the simply-encrypted format).

```
Qtech(config)#service password-encryption
```

! Configure the local user database (Configure the username and the password, and set the user privilege level).

```
Qtech(config)#username bank privilege 10 password yinhang
Qtech(config)#username super privilege 15 password star
Qtech(config)#username normal privilege 2 password normal
Qtech(config)#username test privilege 1 password test
```

! Configure the local Enable password for the local Enable authentication.

```
Qtech(config)#enable secret w
```

### # Define the AAA service method list

! Configure dot1x authentication.

```
Qtech(config)#aaa authentication dot1x renzheng group radius local
```

! Configure network authorization.

```
Qtech(config)#aaa authorization network shouquan group radius
```

! Configure network accounting.

```
Qtech(config)#aaa accounting network jizhang start-stop group radius
```

### # Enable the domain name-based AAA services

```
Qtech(config)#aaa domain enable
```

### # Create a domain and configure the domain attribute set

! Create a domain.

```
Qtech(config)#aaa domain Qtech.com
```

! Associate the AAA service method list

```
Qtech(config-aaa-domain)#authentication dot1x renzheng
Qtech(config-aaa-domain)#authorization network shouquan
Qtech(config-aaa-domain)#accounting network jizhang
```

! Configure the domain state.

```
Qtech(config-aaa-domain)#state active
```

! Exclude the domain name from the username.

```
Qtech(config-aaa-domain)#username-format without-domain
!
Qtech(config)#aaa authentication dot1x renzheng group g2
Qtech(config)#aaa authorization network shouquan group g2

Qtech(config)#aaa accounting network jizhang start-stop group g2
```

The configurations of the Qtech.com.cn and the Qtech.net are similar.



### 10.10.2.5 Configuration Verification

Step 1: Use the **show running-config** command to query the current configurations ( take the domain name **Qtech.com** for example):

```
Qtech#show run
Building configuration...
Current configuration : 2013 bytes

!
aaa new-model
aaa domain enable
!
aaa domain Qtech.com
 authentication dot1x renzheng
 accounting network jizhang
 authorization network shouquan
 username-format without-domain
!
!
aaa group server radius g1
 server 10.1.1.1
!
aaa group server radius g2
 server 10.1.1.2
!
aaa group server radius g3
 server 10.1.1.3
!
!
aaa accounting network jizhang start-stop group g2
aaa authorization network shouquan group g2
aaa authentication dot1x renzheng group g2
!
!vlan 1
!
!
no service password-encryption
!
!
radius-server key Qtech
!
!
!
```

Step 2: Query the domain name-based AAA service domain information:

```
Qtech#show aaa domain

=====Domain Qtech.com=====
State: Active
Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x renzheng
 authorization network shouquan

 accounting network jizhang
```

## 11 CONFIGURING RADIUS

### 11.1 Overview of RADIUS

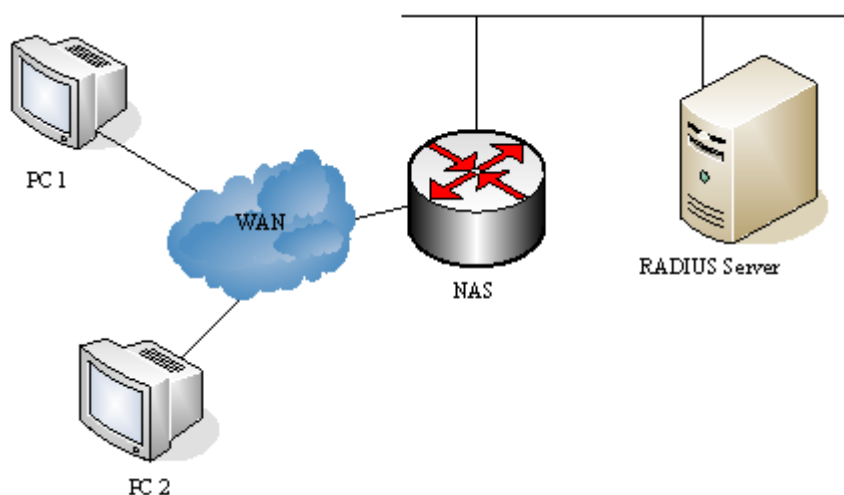
The Remote Authentication Dial-In User Service (Radius) is a distributed client/server system that works with the AAA to perform authentication for the users who are attempting to make connection and prevent unauthorized access. In the RGOS implementation, the RADIUS client runs on the router or the network access server (NAS) to send the authentication requests to the central RADIUS server. The central server stores all information of user authentication and network services.

Since RADIUS is a completely open protocol, it has become a component and been installed in such systems as Unix and Windows 2000, so it is the most popular security protocol for the time being.

The running process of RADIUS is as follows:

- Prompt the user to enter username and password.
- The username and the encrypted password are sent to the RADIUS server via the network.
- The RADIUS returns one of the following responses:
  - ACCEPT: indicating that the user is authenticated.
  - REJECT: indicating that the user authentication fails and the username and password must be entered again.
  - CHALLENGE: indicating that the RADIUS server requests more authentication information from the user.
- The user authorization information is included in the ACCEPT response.

Figure 35 Typical RADIUS network



In addition to the authentication service, the RADIUS server also provides authorization and accounting services.

The RADIUS security protocol, also called the RADIUS method, is configured in the unit of a RADIUS server group. Every RADIUS method corresponds to a RADIUS server group which may consist of one or more RADIUS servers. For details about the RADIUS method, refer to AAA-SCG. If a RADIUS server group has multiple RADIUS servers, these RADIUS servers are used in polling mode till there is successful communication or all servers become unreachable.

### 11.2 RADIUS Configuration Tasks

To configure RADIUS on the network device, perform the following tasks first:

- Enable AAA. For the details, see AAA-SCG.
- Define a RADIUS authentication method list by using the **aaa authentication** command. For details about usage of the **aaa authentication** command, see the “Configuring Authentication” section.
- Apply the defined authentication method list to the specific line; otherwise the default authentication method list will be used for authentication. For more details, see the “Configuring Authentication” section.

### 11.2.1 Configuring RADIUS Protocol Parameters

Before configuring RADIUS on the network device, ensure that the RADIUS server is reachable. To configure RADIUS protocol parameters, run the following commands:

Command	Function
Qtech# <b>configure terminal</b>	Enters global configuration mode.
Qtech(config)# <b>radius-server host</b> <i>ip-address [auth-port port] [acct-port port]</i>	Configures the IP address or hostname of the remote Radius security server and specifies the authentication port and accounting port.
Qtech(config)# <b>radius-server key</b> <i>string</i>	Configures the shared key used for the communication between the device and the Radius server.
Qtech(config)# <b>radius-server retransmit</b> <i>retries</i>	Specifies the times of sending a request before a RADIUS server is considered unreachable (3 by default).
Qtech(config)# <b>radius-server timeout</b> <i>seconds</i>	Specifies the waiting time before the network device resends a request (5 seconds by default).



#### Caution

When configuring RADIUS, you must configure a RADIUS Key. Ensure that the network device and the RADIUS server use the same shared key.

### 11.2.2 Specifying Radius Authentication

This means defining the authentication method list for the Radius after the After specifying a RADIUS server and a RADIUS shared key, you must define a RADIUS authentication method list. RADIUS authentication is performed via AAA, so you need to run the **aaa authentication** command to define an authentication method list and specify the RADIUS authentication method. For more details, see AAA-SCG.

### 11.2.3 Specifying the Standard Radius Attribute Type

This section describes how to configure types of standard attributes. Now the RADIUS Calling-Station-ID attribute (the attribute value is 31) is supported.

#### 11.2.3.1 Configuring Calling-Station-ID Format

The RADIUS Calling-Station-ID attribute is used to identify the NAS when the NAS is sending a request to the RADIUS server. The value of the RADIUS Calling-Station-ID is character strings, which can be in multiple formats. The MAC address for the NAS is usually used as the value of the Calling-Station-ID to solely identify the NAS. The table below describes the formats of the MAC address:

Format	Description
<b>ietf</b>	The standard format specified by IETF (in RFC3580). A hyphen (-) is used as the separator, for example: 00-D0-F8-33-22-AC.
<b>normal</b>	Normal format of the MAC address (dotted hexadecimal format). A dot (.) is used as the separator. For example: 00d0.f833.22ac.
<b>unformatted</b>	No format or separator. By default, unformatted is used. For example: 00d0f83322ac.

To configure the format of the RADIUS Calling-Station-ID MAC-based attribute, run the following commands:

Command	Function
<b>configure terminal</b>	Enters global configuration mode.
<b>radius-server attribute 31 mac format {ietf   normal   unformatted}</b>	Configures the format of the RADIUS Calling-Station-ID MAC-based attribute. The default format is <b>unformatted</b> .

### 11.2.4 Specifying Private Radius Attribute Type

This section describes how to configure private attributes of RADIUS. By default, private RADIUS attributes are classified into Qtech attributes and extended vendor types:

ID	Function	TYPE	Extended TYPE
----	----------	------	---------------

ID	Function	TYPE	Extended TYPE
1	max-down-rate	1	76
2	port-priority	2	77
3	user-ip	3	3
4	vlan-id	4	4
5	last-supPLICANT-version	5	5
6	net-ip	6	6
7	user-name	7	7
8	password	8	8
9	file-directory	9	9
10	file-count	10	10
11	file-name-0	11	11
12	file-name-1	12	12
13	file-name-2	13	13
14	file-name-3	14	14
15	file-name-4	15	15
16	max-up-rate	16	16
17	current-supPLICANT-version	17	17
18	flux-max-high32	18	18
19	flux-max-low32	19	19
20	proxy-avoid	20	20
21	dailup-avoid	21	21
22	ip-privilege	22	22
23	login-privilege	42	42
26	ipv6-multicast-address	79	79
27	ipv4-multicast-address	87	87
62	sdg-type	62	62
85	sdg-zone-name	85	85
103	sdg-group-name	103	103

**Note**

Some private attributes are supported only by specific products. You can run the **show radius vendor-specific** command to view private attribute lists supported by products.  
Two attributes cannot be configured with the same type number.

The following is an example about private attributes of network devices:

```
Qtech# show radius vendor-specific
id  vendor-specific  type-value
-----
1   max-down-rate    76
2   port-priority    77
3   user-ip          3
4   vlan-id         4
.....
Qtech# configure
Qtech(config)# radius attribute 4 vendor-type 67
Qtech(config)# show radius vendor-specific
id  vendor-specific  type-value
-----
1   max-down-rate    76
2   port-priority    77
3   user-ip          3
4   vlan-id         67
.....
Qtech(config)#
```

### 11.2.5 Configuring RADIUS Server Reachability Detection

The device maintains the reachability state of each RADIUS server configured: reachable or unreachable. The device does not send authentication, authorization and accounting requests of users to an unreachable RADIUS server, unless all RADIUS servers in the RADIUS server group are unreachable.

The device can carry out proactive detection of the specified RADIUS server, and this feature is disabled by default. If you enable proactive detection of the specified RADIUS server, the device will periodically send detection requests (authentication requests or accounting requests) to the RADIUS server at an interval of:

- 60 minutes (the default value) for reachable RADIUS servers
- 1 minute (a constant value) for unreachable RADIUS servers

**Note**

To enable proactive detection of the specified RADIUS server, the following conditions must be met:

1. The test user name for this RADIUS server has been configured on the device.
2. At least one tested port of this RADIUS server (authentication port or accounting port) has been configured on the device.

For a reachable RADIUS server, the device will consider this RADIUS server unreachable if the following two conditions are met:

1. The time configured by using the **radius-server dead-criteria time seconds** command has elapsed since the receipt of the last correct response from the RADIUS server.
2. After the receipt of the last correct response from the RADIUS server, the number of requests (including retransmitted requests) without a response reaches the value configured by using the **radius-server dead-criteria tries number** command.

For an unreachable RADIUS server, the device will consider this RADIUS server reachable if any of the following conditions is met:

- 67) A correct response is received from this RADIUS server.
- 68) The duration that this RADIUS server remains unreachable exceeds the time set by using the **radius-server deadtime** command, and proactive detection of this RADIUS server is not enabled.
- 69) The authentication port or accounting port of this RADIUS server is updated on the device.

RADIUS server reachability detection allows the user to judge whether a RADIUS server is unreachable and to configure proactive detection.

To configure RADIUS server reachability detection, run the following commands in global configuration mode:

Command	Function
Qtech# <b>configure terminal</b>	Enters global configuration mode.
Qtech(config)# <b>radius-server dead-criteria time seconds tries number</b>	Configures global criteria for judging whether a RADIUS server is reachable. The default value of <i>seconds</i> is <b>60</b> , and the default value of <i>number</i> is <b>10</b> .
Qtech(config)# <b>radius-server deadtime minutes</b>	Configures the duration for the device to stop sending request packets to the RADIUS server in unreachable state (default value: 0 minutes).
Qtech(config)# <b>radius-server host ip-address [auth-port port] [acct-port port] [test username name [idle-time time] [ignore-auth-port] [ignore-acct-port]]</b>	Configures the IP address of a remote RADIUS server, specifies the authentication port and accounting port, and specify relevant parameters of proactive detection (testing user name, interval for proactive detection of reachable RADIUS servers, and whether the authentication port or the accounting port shall be neglected).



#### Caution

In the configuration, a special testing user name shall be used. This user name cannot be used by other authorized users, avoiding adverse impact on authentication, authorization or accounting of these users.

### 11.3 Monitoring RADIUS

To monitor RADIUS, run the following command in privileged user mode:

Command	Function
<b>debug radius { event   detail }</b>	Turns on the Radius debug switch to view the Radius debug information.

### 11.4 Radius Configuration Example

In a typical Radius network configuration diagram, the RADIUS server performs authentication for the users who are attempting to access, enables the accounting function for these users and records the network service usage of them.



#### Note

The RADIUS server can be a component that comes with the Windows 2000/2003 server (IAS) or the Unix system, or special certified server software of some manufacturers.

The following example shows how to configure the Radius on the network device:

```
Qtech# configure terminal
Qtech(config)# aaa new-model
Qtech(config)# radius-server host 192.168.12.219 auth-port 1645 acct-port 1646
Qtech(config)# radius-server key aaa
Qtech(config)# aaa authentication login test group radius
Qtech(config)# end
Qtech# show radius server
Server IP:      192.168.12.219
Accounting Port: 1646
Authen Port:   1645
Test Username:  <Not Configured>
Test Idle Time: 60 Minutes
Test Ports:    Authen and Accounting
Server State:  Active
```



```
Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
  Authen: request 15, timeouts 1
  Author: request 0, timeouts 0
  Account: request 0, timeouts 0

Qtech# configure terminal
Qtech(config)# line vty 0
Qtech(config-line)# login authentication test
Qtech(config-line)# end
Qtech# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius
!
!
!
radius-server host 192.168.12.219 auth-port 1645 acct-port 1646
radius-server key aaa
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
```

## 11.5 RADIUS IPv6 Configuration Example

In the typical RADIUS network configuration diagram, the RADIUS server performs authentication and accounting of users, and records the network service usage of them.



**Note** The RADIUS server is deployed on a Windows 2008 Server or special IPv6 capable server software certified by manufacturers.

The following example shows how to configure RADIUS on the network device:

```
Qtech# configure terminal
Qtech(config)# aaa new-model
Qtech(config)# radius-server host 3000::100 auth-port 1645 acct-port 1646
Qtech(config)# radius-server key aaa
Qtech(config)# aaa authentication login test group radius
Qtech(config)# end
Qtech# show radius server
Server IP:      3000::100
Accounting Port: 1646
Authen Port:   1645
Test Username:  <Not Configured>
Test Idle Time: 60 Minutes
Test Ports:    Authen and Accounting
Server State:  Active
Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
  Authen: request 15, timeouts 1
  Author: request 0, timeouts 0
  Account: request 0, timeouts 0

Qtech# configure terminal
```

```
Qtech(config)# line vty 0
Qtech(config-line)# login authentication test
Qtech(config-line)# end
Qtech# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius
!
!
!
radius-server host 3000::100 auth-port 1645 acct-port 1646
radius-server key aaa
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
```

## 12 CONFIGURING TACACS+

### 12.1 Overview of TACACS+

TACACS+ is an enhancement of Terminal Access Controller Access Control System (TACACS) defined in RFC 1492. It implements authentication, authorization, and accounting (AAA) functions on multiple types of users by communicating with the TACACS server in client-server mode. Before using the TACACS+ server, you need to configure the related functions of the TACACS+ server.

TACACS+ supports user authentication, authorization and accounting. That is, one server is used for authentication, one for authorization, and another for accounting, which proceed concurrently. Each server has its own user data for authentication, authorization, and accounting.

The following table shows the format of a TACACS+ packet:

Figure 36

4	8	16	24	32 bit
Major	Minor	Packet type	Sequence no.	Flags
Session ID				
Length				

- Major Version —TACACS+ Version;
- Minor Version —TACACS+ release;
- Packet Type — Its values are as follows:  
TAC\_PLUS\_AUTHEN:= 0x01 (Authentication);  
TAC\_PLUS\_AUTHOR:= 0x02 (Authorization);  
TAC\_PLUS\_ACCT:= 0x03 (Accounting).
- Sequence Number — packet sequence number in the current session. The sequence number of the first TACACS+ packet in a session must be 1 and those of subsequent packet increment by one. Therefore, the client sends only the packet with an odd sequence number, while TACACS+ Daemon only sends only the packet with an even sequence number.
- Flags — This field includes flags with various bitmap formats. The Flag value indicates whether a packet is encrypted or not.
- Session ID — ID in a TACACS+ session.
- Length —body length of a TACACS+ packet (excluding the header). All the packets are transmitted in the network after being encrypted.

### 12.2 TACACS+ Application

Typically, TACACS+ is used to manage and control the login of terminal users. Network devices work as TACACS+ clients to send user names and passwords to the TACACS+ server for authentication. After authentication and authorization, you can log in to the switch for operation, as shown in Figure 2:

Figure 37

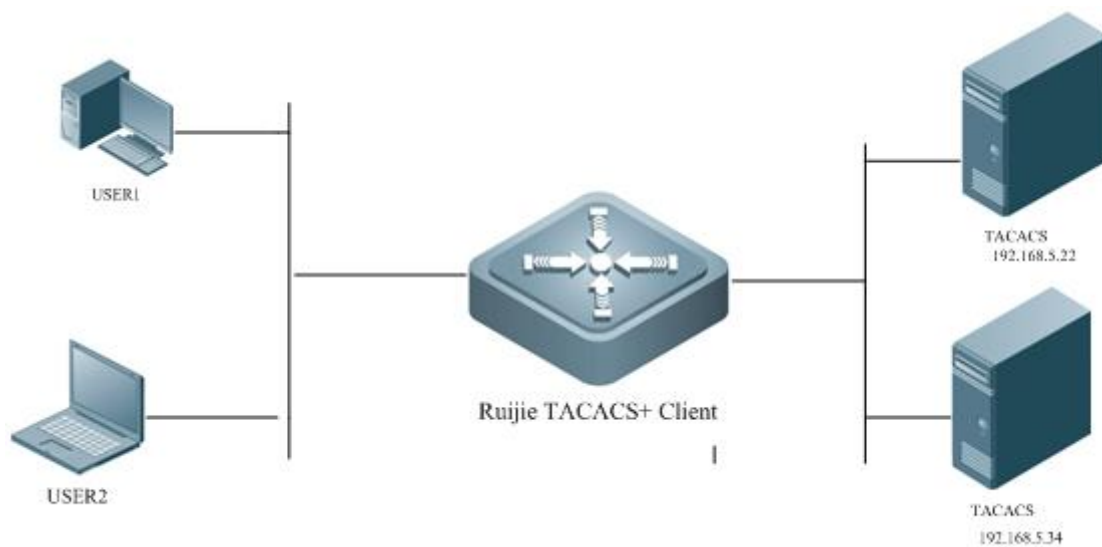
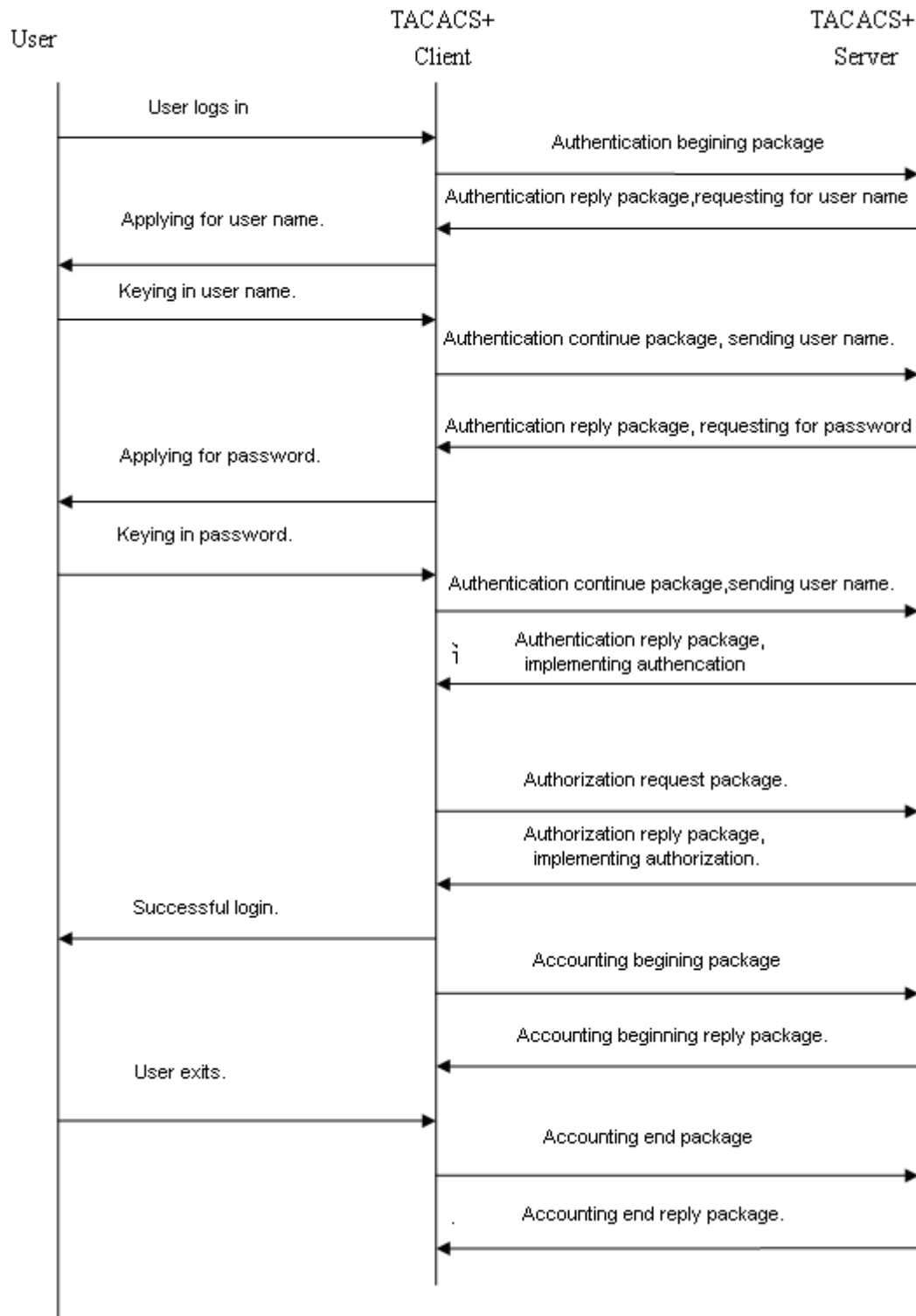


Figure describes the exchange of TACACS+ packets during AAA implementation in a login attempt.  
Figure 38



The whole process is divided into three parts:

**Authentication:**

- 70) A user sends a login request to the network device;
- 71) After receiving the request, the TACACS+ client sends an authentication start message to the TACACS+ server;
- 72) The TACACS+ server sends an authentication reply message, requesting the user name;
- 73) The TACACS+ client asks the user for the user name.
- 74) The user enters the login user name;
- 75) After receiving the user name, the TACACS+ client sends an authentication continue message containing the user name to the TACACS+ server;
- 76) The TACACS+ server sends an authentication reply message, requesting the login password;
- 77) The TACACS+ client receives the login password;
- 78) The user enters the login password;
- 79) After receiving the login password, the TACACS+ client sends an authentication continue message containing the login password to the TACACS+ server;
- 80) The TACACS+ server sends an authentication reply message, indicating that the user has been authenticated.

#### Authorization:

- 81) The TACACS+ client sends an authorization request message to the TACACS+ server.
- 82) The TACACS+ server sends an authorization reply message, indicating that the user has been authenticated;
- 83) The TACACS+ client receives a successful authorization reply message, displaying the interface for configuring the network device.

#### Accounting:

- 84) The TACACS+ client sends an accounting start message to the TACACS+ server;
- 85) The TACACS+ server sends an accounting reply message, indicating that it has received the accounting start message;
- 86) The user exits;
- 87) The TACACS+ Client sends an accounting end message to the TACACS+ server;
- 88) The TACACS+ server sends an accounting end reply message, indicating that it has received the accounting end message.

## 12.3 TACACS+ Configuration Task

The following tasks must be executed before you configure TACACS+ on the network device:

- Use the **aaa new-mode** command to enable AAA. Before using TACACS+, you must enable AAA. For usage of the **aaa new-mode** command, see the “AAA Overview” chapter in AAA-SCG.
- Use the **tacacs-server host** command to configure one or multiple TACACS+ servers.
- Use the **tacacs-server key** command to specify the key shared by the server and the network device.
- Use the **tacacs-server timeout** command to specify the timeout time for waiting a reply from the server;
- If authentication is required, use the **aaa authentication** command to define a TACACS+ authentication method list. For details, see the “Configuring Authentication” section in AAA-SCG.
- If authorization is required, use the **aaa authorization** command to define a TACACS+ authorization method list. For details, see the “Configuring Authorization” section in AAA-SCG.
- If accounting is required, use the **aaa accounting** command to define a TACACS+ accounting method list. For details, see the “Configuring Accounting” section in AAA-SCG.
- Apply a specific authentication method list to a specific line. Otherwise, a default method list is used.

### 12.3.1 Configuring TACACS+ Parameters

Before configuring TACACS+ on a network device, ensure that communication with the TACACS+ server is proper. To configure TACACS+ parameters, run the following commands:

Command	Function
Qtech# <b>configure terminal</b>	Enters global configuration mode.



Qtech(config)# <b>tacacs-server host</b> { <i>ip-address</i>   <i>ipv6-address</i> } [ <b>port</b> <i>integer</i> ] [ <b>timeout</b> <i>integer</i> ] [ <b>key</b> <i>string</i> ]	Configures the IP address of the remote TACACS+ security server. Different combinations of parameters are used to build parameters of the server. <i>ip-address</i> : IP address of the server; <i>ipv6-address</i> : IPv6 address of the server; <i>port integer</i> [optional]: port used by the server. By default, port 49 is used. The value ranges from 1 to 65535. <i>timeout integer</i> [optional]: response timeout time of the server. By default, the timeout time is 5s. The value ranges from 1 to 1000 (in seconds). <i>key string</i> [optional]: key shared with the server with the corresponding server.
Qtech(config)# <b>tacacs-server key</b> <i>string</i>	Configures the shared key used for communication between the network device and the TACACS+ server. When the corresponding server does not have an independent key, the global configuration is used.
Qtech(config)# <b>tacacs-server timeout</b> <i>seconds</i>	Configures the wait time before the network device retransmits a request. It is 5s by default. If no timeout time is specified for a host, the host uses the global configuration.
Qtech(config)# <b>ip tacacs source-interface</b> <i>interface</i>	Configures the source IP address used to send a TACACS+ request to the server. By default, the source IP address is not specified.
Qtech(config)# <b>aaa group server tacacs+</b> <i>group-name</i>	Configures TACACS+ server groups. Different TACACS+ servers are divided into different groups.
Qtech(config-gs-tacacs)# <b>server</b> { <i>ip-address</i>   <i>ipv6-address</i> }	Configures IP addresses of servers in a TACACS+ server group.
Qtech(config-gs-tacacs)# <b>ip vrf forwarding</b> <i>vrf-name</i>	Configures the VRF instance name used by a TACACS+ server group. This command is available on VRF-capable hosts.

**Caution**

When configuring TACACS+, you must configure the TACACS+ key. The network device and the TACACS+ server must use the same shared key.

The **tacacs-server timeout** is affected by **ip tcp syntime-out**, the real valid timeout value is that of the smaller one between the two.

## 12.4 Using TACACS+ for Implementing AAA Functions

In a typical TACACS+ network, the TACACS+ server implements AAA functions on users. The following example shows how AAA functions are implemented through TACACS+.

### 12.4.1 Using TACACS+ for Login Authentication

- Enables AAA:

```
Qtech# configure terminal
Qtech(config)# aaa new-model
```

- Configures TACACS+ server information:

```
Qtech(config)# tacacs-server host 192.168.12.219
Qtech(config)# tacacs-server key aaa
```

- Configures TACACS+ authentication methods:

```
Qtech(config)# aaa authentication login test group tacacs+
```

- Applies the authentication method to the interface:

```
Qtech(config)# line vty 0 4
Qtech (config-line)# login authentication test
```

Through the above configuration, TACACS+ login authentication is implemented. The configuration is as follows:

```
Qtech#show running-config
!
aaa new-model
!
aaa authentication login test group tacacs+
!
tacacs-server host 192.168.12.219
tacacs-server key aaa
!
line con 0
line vty 0 4
login authentication test
!
```

### 12.4.2 Using TACACS+ for Enable Authentication

89) Enables AAA:

```
Qtech# configure terminal
Qtech(config)# aaa new-model
```

90) Configures TACACS+ server information:

```
Qtech(config)# tacacs-server host 192.168.12.219
Qtech(config)# tacacs-server host 192.168.12.218
Qtech(config)# tacacs-server host 192.168.12.217
Qtech(config)# tacacs-server key aaa
```

Configures that some servers in a TACACS+ server group are used:

```
Qtech(config)# aaa group server tacacs+ tacgroup1
Qtech(config-gs-tacacs)# server 192.168.12.219
Qtech(config-gs-tacacs)# server 192.168.12.218
```

91) Configures to use authentication methods of TACACS+ server group 1:

```
Qtech(config)# aaa authentication enable default group tacgroup1
```

Through the above configuration, TACACS+ Enable authentication is implemented on some servers. The configuration is as follows:

```
Qtech#show running-config
!
aaa new-model
!
!
aaa group server tacacs+ tacgroup1
server 192.168.12.219
server 192.168.12.218
!
aaa authentication enable default group tacgroup1
!
!
tacacs-server host 192.168.12.219
tacacs-server host 192.168.12.218
tacacs-server host 192.168.12.217
tacacs-server key aaa
!
line con 0
line vty 0 4
!
```

### 12.4.3 Using TACACS+ for Login Authorization

92) Enables AAA:

```
Qtech# configure terminal
Qtech(config)# aaa new-model
```

93) Configures TACACS+ server information:

```
Qtech(config)# tacacs-server host 192.168.12.219
Qtech(config)# tacacs-server key aaa
```

94) Configures the authorization method of using tacacs+:

```
Qtech(config)# aaa authorization exec test group tacacs+
```

95) Applies the authorization method to the interface:

```
Qtech(config)# line vty 0 4
```

```
Qtech (config-line)# authorization exec test
```

Through the above configuration, TACACS+ Enable authorization is implemented. The configuration is as follows:

```
Qtech#show running-config
!
aaa new-model
!
!
aaa authorization exec test group tacacs+
!
tacacs-server host 192.168.12.219
tacacs-server key aaa
!
line con 0
line vty 0 4
authorization exec test
!
```

#### 12.4.4 Using TACACS+ for Level 15 Command Audit

■ Enables AAA:

```
Qtech# configure terminal
```

```
Qtech(config)# aaa new-model
```

■ Configures TACACS+ server information:

```
Qtech(config)# tacacs-server host 192.168.12.219
```

```
Qtech(config)# tacacs-server key aaa
```

■ Configures to use the accounting method of TACACS+:

```
Qtech(config)# aaa accounting commands 15 test start-stop group tacacs+
```

■ Applies the accounting method to the interface:

```
Qtech(config)# line vty 0 4
```

```
Qtech (config-line)# accounting commands 15 test
```

Through the above configuration, TACACS+ Enable accounting is implemented. The configuration is as follows:

```
Qtech# show running-config
!
aaa new-model
!
!
aaa accounting commands 15 default group tacacs+
!
!
tacacs-server host 192.168.12.219
tacacs-server key aaa
!
line con 0
line vty 0 4
accounting commands 15 test
!
```

## 13 CONFIGURING NAT

### 13.1 NAT Overview

Before Network Address Translation (NAT) configuration, it is necessary to understand the allocation of internal local addresses and internal global addresses. Perform the following configuration tasks according to different requirements.

#### 13.1.1 Configuring Static NAT for Internal Source Addresses

To enable an internal network to communicate with an external network, you need to configure NAT to translate internal private IP addresses into a globally unique IP address. In this case, you can choose to configure static NAT or dynamic NAT or even both of them.

Static NAT is to establish a one-to-one permanent mapping between internal local addresses and internal global addresses. It is necessary when an external network uses a fixed global address to access hosts on an internal network. To configure static NAT, run the following commands in global configuration mode:

Command	Function
Qtech(config)# <b>ip nat inside source static</b> <i>local-address global-address</i> [ <b>permit-inside</b> ] [ <b>vrf vrf_name</b> ]	Defines the static translation relationship of internal source addresses.
Qtech(config)# <b>interface</b> <i>interface-type interface-number</i>	Enters interface configuration mode.
Qtech(config-if)# <b>ip nat inside</b>	Defines the internal network the interface connects to.
Qtech(config)# <b>interface</b> <i>interface-type interface-number</i>	Enters interface configuration mode.
Qtech(config-if)# <b>ip nat outside</b>	Defines the external network the interface connects to.

The above configuration is the simplest one. You may configure several inside and outside interfaces.

Dynamic NAT is to establish a temporary mapping between internal local addresses and the internal global address pool, which will be deleted after a while. To configure dynamic NAT, run the following commands in global configuration mode:

Command	Function
Qtech(config)# <b>ip nat pool</b> <i>address-pool start-address end-address</i> { <b>netmask mask</b>   <b>prefix-length prefix-length</b> }	Defines a global IP address pool.
Qtech(config)# <b>access-list</b> <i>access-list-number permit ip-address wildcard</i>	Defines an ACL. Only the IP addresses that match the ACL are translated.
Qtech(config)# <b>ip nat inside source list</b> <i>access-list-number pool address-pool</i> [ <b>vrf vrf_name</b> ]	Defines the dynamic translation relationship of internal source addresses.
Qtech(config)# <b>interface</b> <i>interface-type interface-number</i>	Enters interface configuration mode.
Qtech(config-if)# <b>ip nat inside</b>	Defines the internal network the interface connects to.
Qtech(config)# <b>interface</b> <i>interface-type interface-number</i>	Enters interface configuration mode.
Qtech(config-if)# <b>ip nat outside</b>	Defines the external network the interface connects to.

**Note**

Only source addresses that match the ACL are translated. Note that the last rule of the ACL contains a deny any statement. The ACL should not permit a wide range of IP addresses to be translated; otherwise, unexpected results will be received.

### 13.1.2 Configuring NAT for Internal Source Addresses

Traditional NAT generally defines a one-to-one mapping and cannot enable all hosts on an internal network to communicate with an external network. NAT allows multiple internal local addresses to be mapped to an internal global address.

NAPT is classified into static NAPT and dynamic NAPT. Static NAPT maps the designated port of a designated internal host to a designated global port, whereas static NAT maps an internal address to a global address.

To configure static NAPT, run the following commands in global configuration mode:

Command	Function
Qtech(config)# <b>ip nat inside source static</b> {UDP   TCP} <i>local-address port global-address port</i> [permit-inside] [vrf vrf_name]	Defines the static translation relationship of internal source addresses.
Qtech(config)# <b>interface</b> <i>interface-type interface-number</i>	Enters interface configuration mode.
Qtech(config-if)# <b>ip nat inside</b>	Defines the internal network the interface connects to.
Qtech(config)# <b>interface</b> <i>interface-type interface-number</i>	Enters interface configuration mode.
Qtech(config-if)# <b>ip nat outside</b>	Defines the external network the interface connects to

Dynamic internal source address translation mentioned in previous section has automatically completed the internal source address dynamic NAPT and the configuration is to run the following command in global configuration mode.

Command	Function
Qtech(config)# <b>ip nat pool</b> <i>address-pool start-address end-address</i> {netmask mask   prefix-length prefix-length}	Defines a global IP address pool. For NAPT, only one IP address is defined.
Qtech(config)# <b>access-list</b> <i>ccess-list-number</i> <b>permit</b> <i>ip-address wildcard</i>	Defines an ACL. Only the IP addresses that match the ACL are translated.
Qtech(config)# <b>ip nat inside source list</b> <i>access-list-number</i> {[ pool address-pool]   [interface interface-type interface-number]} <b>overload</b> [vrf vrf_name]	Defines the dynamic translation relationship of source address. The translation effect is the same with or without overload, which is only for compatibility with mainstream manufacturers.
Qtech(config)# <b>interface</b> <i>interface-type interface-number</i>	Enters interface configuration mode.
Qtech(config-if)# <b>ip nat inside</b>	Defines the internal network the interface connects to.
Qtech(config)# <b>interface</b> <i>interface-type interface-number</i>	Enters interface configuration mode.
Qtech(config-if)# <b>ip nat outside</b>	Defines the external network the interface connects to.

NAPT may use the IP addresses in the address pool or directly uses the IP address of the interface. Generally, one address is enough to meet the address translation need of a network and can be translated into up to 64,512 addresses. In case of insufficient addresses, you can add IP addresses to the address pool.

### 13.1.3 Configuring NAT Overlap

Address Overlapping refers to the fact that two private networks in need of interconnection are allocated the same IP address or one private network and public network are allocated the same global IP address. Communication is

impossible between two network hosts with overlapping addresses since they deem their counterparts are in the local network. NAT overlap is configured to solve this problem by presenting the address of external network host as that of another network host and vice versa.

NAT Overlap configuration is actually divided into two parts: 1) Internal source address translation configuration; and 2) External source address translation configuration, which is only needed by an external network that has addresses overlapped with the inner network. Static NAT or dynamic NAT may be adopted for external source address translation.

To configure static NAT for external source addresses, run the following command in global configuration mode:

Command	Function
Qtech(config)# <b>ip nat outside source static</b> <i>global-address local-address [vrf vrf_name]</i>	Defines the static translation relationship of external source addresses.
Qtech(config)# <b>interface</b> <i>interface-type interface-number</i>	Enters interface configuration mode.
Qtech(config-if)# <b>ip nat inside</b>	Defines the internal network the interface connects to.
Qtech(config)# <b>interface</b> <i>interface-type interface-number</i>	Enters interface configuration mode.
Qtech(config-if)# <b>ip nat outside</b>	Defines the external network the interface connects to.

NPE80 does not support NAT overlap.

### 13.1.4 Configuring TCP Load Balancing

When TCP traffic overload is detected on an internal host, more hosts can be deployed to balance the TCP traffic. In this case, you may use NAT for TCP traffic load balancing. NAT creates a virtual host, which corresponds to several real hosts, to provide TCP services, so that destination addresses are polled for load balancing. To configure destination address polling, run the following commands in global configuration mode:

Command	Function
Qtech(config)# <b>ip nat pool</b> <i>address-pool start-address end-address {netmask mask   prefix-length prefix-length}</i>	Defines an IP address pool. The IP addresses of all real hosts are included in the pool.
Qtech(config)# <b>access-list</b> <i>access-list-number permit ip-address wildcard</i>	Defines an ACL to match the IP address of a virtual host. The ACL should be an extended ACL used to match destination IP addresses.
Qtech(config)# <b>ip nat inside destination list</b> <i>access-list-number pool address-pool [vrf vrf_name]</i>	Defines the dynamic translation relationship of internal destination addresses.
Qtech(config)# <b>interface</b> <i>interface-type interface-number</i>	Enters interface configuration mode.
Qtech(config-if)# <b>ip nat inside</b>	Defines the internal network the interface connects to.
Qtech(config)# <b>interface</b> <i>interface-type interface-number</i>	Enters interface configuration mode.
Qtech(config-if)# <b>ip nat outside</b>	Defines the external network the interface connects to.

NPE80 does not support TCP load balancing.



### 13.1.5 Configuring Special Protocol Gateway

The special protocol gateways are all enabled by default. You can disable a specific special protocol gateway by running a command. All of the special protocols are just switch commands except the File Transfer Protocol (FTP) and DNS protocol, which carry parameters. Run the following commands in global configuration mode:

Command	Function
Qtech(config)# <b>no ip nat translation ftp</b>	Disables the FTP gateway.
Qtech(config)# <b>ip nat translation ftp</b>	Enables the FTP gateway. The default port is Port 21.
Qtech(config)# <b>ip nat translation ftp 2121</b>	Enables the FTP gateway and designates Port 2121.

### 13.1.6 Configuring NAT Static Port Range Mapping

The network address translation (NAT) function can map a TCP/UDP port to an IP address one to one. However, if a continuous range of ports of the internal hosts need to be mapped to an external network, configure the NAT static port range mapping function to map the ports in the range. The port range is 1–65535.

Command	Function
Qtech(config)# <b>ip nat inside source static</b> <i>{UDP   TCP} local-address global-address port-range min-port max-port { [permit-inside]   [vrf vrf_name]   [match interface-type interface-number] }</i>	Defines the static translation relationship of the internal source addresses, for mapping the IP address of an external network.
Qtech(config)# <b>ip nat inside source static</b> <i>{UDP   TCP} local-address interface interface-type interface-number port-range min-port max-port [vrf vrf_name]</i>	Defines the static translation relationship of the internal source addresses, for mapping the interface address of an external network.
Qtech(config)# <b>interface interface-type</b> <i>interface-number</i>	Enters the interface configuration mode.
Qtech(config-if)# <b>ip nat inside</b>	Defines the interface for connecting to the internal network.
Qtech(config)# <b>interface interface-type</b> <i>interface-number</i>	Enters the interface configuration mode.
Qtech(config-if)# <b>ip nat outside</b>	Defines the interface for connecting to the external network.

### 13.1.7 Configuring ARP Response Function of NAT

In the VRRP dual-node hot backup scenario, if the same NAT function is configured on both the master and slave devices, when the router initiates an ARP request, both devices receive the ARP request and return an ARP response, causing an ARP conflict. Therefore, the slave device does not respond to the ARP request by default. If NAT configurations on the master and slave devices are different, sometimes the slave device needs to respond to

the ARP request. In this case, you can run the `ip nat arp reply` command, so that the slave device returns a response packet when receiving an ARP request. You can run the `no` form of this command so that the slave device does not return a response packet when receiving an ARP request. Run the following commands in global configuration mode:

Command	Function
Qtech(config)# <b>ip nat arp reply</b>	Enables the ARP response function of NAT on the slave device.
Qtech(config)# <b>no ip nat arp reply</b>	Disables the ARP response function of NAT on the slave device.

### 13.1.8 Configuring NAT Keepalive Function

The NAT keepalive function periodically sends ARP requests destined for the addresses in the NAT address pool to verify that the addresses exist. You can run the `ip nat keepalive` command to enable the keepalive function, or run the `no` form of this command to send no ARP request packets. The keepalive interval ranges from 1 to 86400 seconds. Run the following commands in global configuration mode:

Command	Function
Qtech(config)# <b>no ip nat keepalive</b>	Disables the NAT keepalive function.
Qtech(config)# <b>ip nat keepalive interval-num</b>	Enables the NAT keepalive function.

## 13.2 NAT Configuration Examples

### 13.2.1 Dynamic translation of internal source addresses

In the following configuration, local and global addresses are allocated from the NAT address pool of Net200, which defines the address range from 200.168.12.2 to 200.168.12.100. A NAT entry is created only when a packet whose internal source address matches ACL 1.

```
!
interface FastEthernet 0/0
ip address 192.168.12.1 255.255.255.0
ip nat inside
!
interface FastEthernet 1/0
ip address 200.168.12.1 255.255.255.0
ip nat outside
!
ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0
ip nat inside source list 1 pool net200
!
access-list 1 permit 192.168.12.0 0.0.0.255
```

### 13.2.2 Reuse of internal global addresses

Reuse of internal global address is equivalent to NAT actually. RGOS 8.1 and later versions automatically implement NAT for dynamic NAT. In the following configuration, local and global addresses are allocated from NAT address pool—Net200, which only defines one IP address 200.168.12.200 that can be reused. A NAT entry is created only when a packet whose internal source address matches ACL 1.

```
!  
interface FastEthernet 0/0  
ip address 192.168.12.1 255.255.255.0  
ip nat inside  
!  
interface FastEthernet 1/0  
ip address 200.168.12.200 255.255.255.0  
ip nat outside  
!  
ip nat pool net200 200.168.12.200 200.168.12.200 netmask 255.255.255.0  
ip nat inside source list 1 pool net200  
access-list 1 permit 192.168.12.0 0.0.0.255  
Whether correct NAT entries can be created can be checked by looking up the  
NAT mapping table.  
Qtech# show ip nat translations  
Pro Inside global   Inside local   Outside local   Outside global  
tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23
```

### 13.2.3 Static NAT for Internal Source Addresses

Static NAT may be used for creating a virtual server. Creating a virtual server here refers to setting up a server and mapping it to an external network through static NAT. Thus, access to the virtual server with a global address is diverted to an internal server.

The following example describes how to map IP address 192.168.12.3 of an internal web server to a global IP address 200.198.12.1 of port 80. The configuration script is as follows:

```
!  
interface FastEthernet 0/0  
ip address 192.168.12.1 255.255.255.0  
ip nat inside  
!  
interface FastEthernet 1/0  
ip address 200.198.12.1 255.255.255.0  
ip nat outside  
!  
ip nat inside source static tcp 192.168.12.3 80 200.198.12.1 80
```

For details, see the “Configuring a local server” section.

### 13.2.4 TCP Load Balancing

A virtual host address is defined in the following configuration so that all TCP connections to this virtual host from external networks will be processed by multiple real hosts for load balancing. **Realhosts** defines a real host address pool, while ACL 1 defines the IP address of the virtual host. Traffic from hosts on an external network must be routed to this virtual host. The following configuration applies only to TCP traffic. Note that an extended ACL must be configured to match destination IP addresses.

```
!  
interface FastEthernet 0/0  
ip address 10.10.10.1 255.255.255.0  
ip nat inside  
!  
interface FastEthernet 1/0  
ip address 200.198.12.1 255.255.255.0  
ip nat outside  
!  
ip nat pool realhosts 10.10.10.2 10.10.10.3 netmask 255.255.255.0 type rotary  
ip nat inside destination list 100 pool realhosts  
!  
access-list 100 permit ip any host 10.10.10.100  
!
```

Whether correct NAT entries can be created can be checked by looking up the NAT mapping table.

```
Qtech# sh ip nat translations
Pro Inside global Inside local Outside local   Outside global
tcp 10.10.10.100:23 10.10.10.2:23 100.100.100.100:1178 100.100.100.100:1178
tcp 10.10.10.100:23 10.10.10.3:23 200.200.200.200:1024 200.200.200.200:1024
```

### 13.2.5 Load balancing among multiple outside interfaces

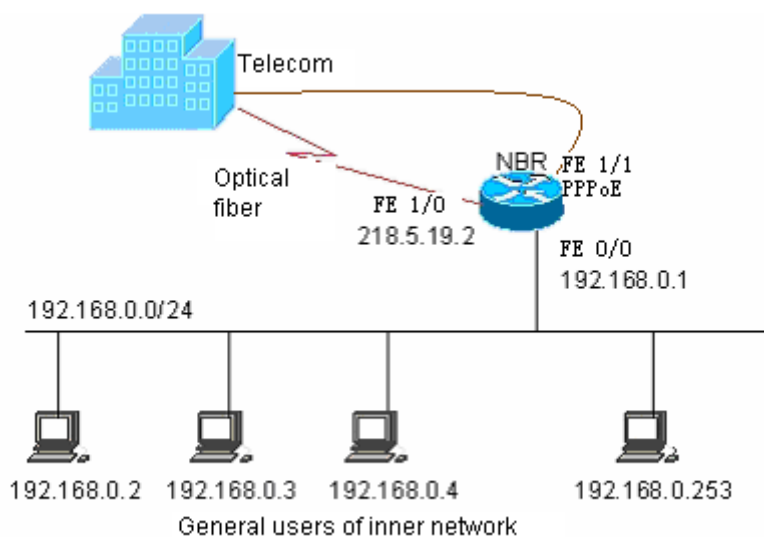
If several WAN ports of a device are used as outside interfaces, load is balanced among these WAN ports by bandwidth. When one WAN port is faulty, the load will be automatically routed to other normal ports. By default, the load is distributed according to global destination addresses of NAT. In the following example, load is balanced between two WAN ports of a RSR series router.

96) Interface GigabitEthernet 0/0 connects to a telecom network.

97) Interface GigabitEthernet 0/1 connects to the education network.

The topology is as follows:

Figure 39



The configuration is as follows:

```
!
# Configure an ACL to allow internal network users to access internet.
access-list 99 permit 192.168.0.0 0.0.0.255

# Configure GigabitEthernet 0/2 to connect to the internal network..
interface GigabitEthernet 0/2
ip nat inside
ip address 10.29.0.253 255.255.255.0
!

# Configure a static IP address for WAN port 0 which connects to the telecom network.
interface GigabitEthernet 0/0
ip nat outside
ip address 218.4.53.238 255.255.255.0
!

# WAN port 1 connects to the education network.
interface GigabitEthernet 0/1
ip nat outside
ip address 172.16.253.18 255.255.255.0
!
```

# Configure a NAT address pool. NAT provides multiple Outside ports. If GigabitEthernet 0/0 is configured as the Outside port, the IP address of the port is set to 218.4.53.238; if GigabitEthernet 0/1 is configured as the Outside port, the IP address of the port is set to 172.16.253.18.

```
ip nat pool setup_build_pool prefix-length 24
address 61.155.18.17 61.155.18.18 match interface GigabitEthernet 0/0
address 210.28.160.100 210.28.160.110 match interface GigabitEthernet 0/1
```

# Enable internal source address translation of NAT

```
ip nat inside source list 99 pool nbr_setup_build_pool
```

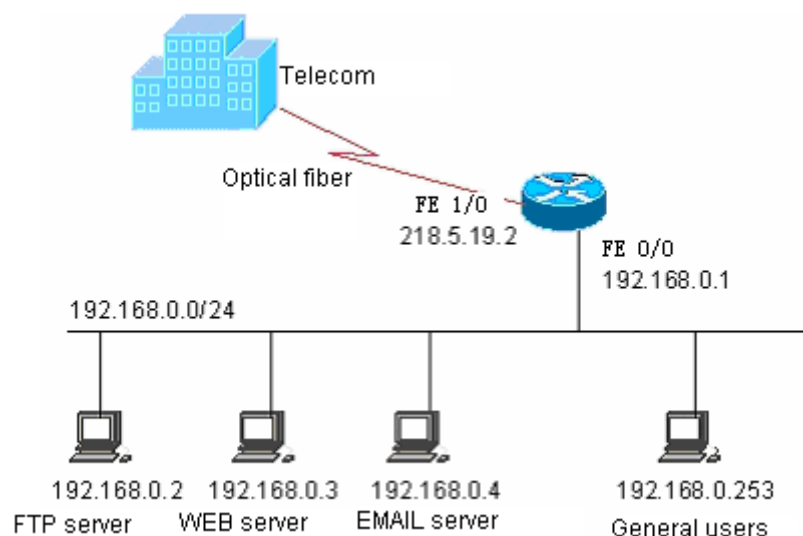
# Configure that traffic is routed to two WAN ports by default.

```
ip route 0.0.0.0 0.0.0.0 FastEthernet 1/0 202.101.98.1
ip route 0.0.0.0 0.0.0.0 dialer 1
!
```

### 13.2.6 Configuring a local server

To configure a local server means to map one or more hosts to a network access server (NAS), so that users on the WAN can access desired services. As shown in Figure , three servers (an FTP server, a web server, and an E-mail server) are deployed on the internal network. It is expected that hosts on the WAN can access the three servers and common users of the internal network can access Internet by using the gateway as a NAS. For Qtech products, static NAT is used for server access and dynamic NAT is used for Internet access.

Figure 40 Configuring a local server



To realize these functions, static NAT needs to be configured.

# Enter privileged user mode

```
Qtech> enable
```

# Enter global configuration mode

```
Qtech# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

# Enter WAN port 0 configuration mode

```
Qtech(config)#interface fastethernet 1/0
```

# Configure the IP address of the WAN port

```
Qtech(config-if)# ip address 218.5.19.2 255.255.255.0
```

# Configure the WAN port as the connection-sharing Internet access port

```
Qtech(config-if) # ip nat outside
```

```
# Enable the WAN port
```

```
Qtech(config-if) # no shut
```

```
# Return to common user mode
```

```
Qtech(config-if) # end
```

```
Qtech#
```

```
# The system prompts that the link to the WAN port is Up.
```

```
%LINK CHANGED: Interface FastEthernet 1/0, changed state to up
```

```
%LINE PROTOCOL CHANGE: Interface FastEthernet 1/0, changed state to UP
```

```
Qtech# config terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
# Enter LAN port configuration mode
```

```
Qtech(config) # interface fastethernet 0/0
```

```
# Configure the IP address of the LAN port
```

```
Qtech(config-if) # ip address 192.168.0.1 255.255.255.0
```

```
# Configure the LAN port as the connection-sharing internet access port
```

```
Qtech(config-if) # ip nat inside
```

```
# Enable the LAN port
```

```
Qtech(config-if) # no shut
```

```
Qtech(config-if) # end
```

```
Qtech#
```

```
%LINK CHANGED: Interface FastEthernet 0/0, changed state to up
```

```
%LINE PROTOCOL CHANGE: Interface FastEthernet 0/0, changed state to UP
```

```
Qtech# config terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
# Configure default route to access to internet
```

```
Qtech(config) # ip route 0.0.0.0 0.0.0.0 fastethernet 1/0 218.5.19.1
```

```
# Configure a default route for Internet access
```

```
Qtech(config) # ip route 0.0.0.0 0.0.0.0 fastethernet 1/0 218.5.19.1
```

```
# Configure an ACL for NAT application
```

```
Qtech(config) # access-list 1 permit any
```

```
# Configure a connection sharing rule to allow common internal users to access Internet over a device
```

```
Qtech(config) # ip nat inside source list 1 interface fastethernet 1/0
```

```
# Configure static mapping of the FTP server
```

```
Qtech(config) # ip nat inside source static tcp 192.168.0.2 20 218.5.19.2 20
```

```
Qtech(config) # ip nat inside source static tcp 192.168.0.2 21 218.5.19.2 21
```

```
# Configure static mapping of the web server
```

```
Qtech(config) # ip nat inside source static tcp 192.168.0.3 80 218.5.19.2 80
```

```
# Configure static mapping of the E-mail server
```

```
Qtech(config) # ip nat inside source static tcp 192.168.0.4 25 218.5.19.2 25
```

```
Qtech(config) # ip nat inside source static tcp 192.168.0.4 110 218.5.19.2 110
```

```
Qtech(config) # end
```

```
Qtech#
```

```
Qtech# config terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
# Configure a password for Telnet access
```



```
Qtech(config)# line vty 0 4
Qtech(config-line)# password remoteuser
Qtech(config-line)# end
Qtech#
Qtech# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)# enable secret private
```

#### # Configure a device name

```
Qtech(config)# host QTECH
QTECH(config)# end
QTECH#
```

#### # Save the configuration

```
QTECH# write
Building configuration...
[OK]
QTECH#
```

#### # Verify the configuration

```
QTECH# show running-config
Building configuration...
Current configuration:
!
!
hostname NBR
!
!
!
access-list 1 permit any
!
!
interface FastEthernet 0/0
ip address 192.168.0.1 255.255.255.0
ip nat inside
!
interface FastEthernet 1/0
ip address 218.5.19.2 255.255.255.0
ip nat outside
!
ip nat inside source list 1 interface FastEthernet 1/0
ip nat inside source static tcp 192.168.0.4 110 218.5.19.2 110
ip nat inside source static tcp 192.168.0.4 25 218.5.19.2 25
ip nat inside source static tcp 192.168.0.3 80 218.5.19.2 80
ip nat inside source static tcp 192.168.0.2 21 218.5.19.2 21
ip nat inside source static tcp 192.168.0.2 20 218.5.19.2 20
!
ip route 0.0.0.0 0.0.0.0 FastEthernet 1/0 218.5.19.1
!
line con 0
line vty 0 4
password remoteuser
login
!
end
QTECH#
```

### 13.2.7 NAT Configuration in case of multiple VRF instances

The following example shows the NAT implementation when there are multiple VRF instances. An IP address may be found in different VRF instances and needs to be translated into different source IP addresses during NAT. In this case, you must specify the target VRF domain of NAT.

```

access-list 1 permit 192.168.12.0 0.0.0.255

ip vrf 1
ip vrf 2

interface FastEthernet 0/0
ip vrf forward 1
ip address 192.168.12.1 255.255.255.0
ip nat inside
!
interface FastEthernet 0/1
ip vrf forward 1
ip address 100.168.12.200 255.255.255.0
ip nat outside
!
interface FastEthernet 1/0
ip vrf forward 2
ip address 192.168.12.1 255.255.255.0
ip nat inside
!
interface FastEthernet 1/1
ip vrf forward 2
ip address 200.168.12.200 255.255.255.0
ip nat outside
!
ip nat pool net100 100.168.12.200 100.168.12.200 netmask 255.255.255.0
ip nat pool net200 200.168.12.200 200.168.12.200 netmask 255.255.255.0

ip nat inside source list 1 pool net100 vrf 1
ip nat inside source list 1 pool net200 vrf 2
Whether correct NAT entries can be created can be checked by looking up the
NAT mapping table.
Qtech# show ip nat translations vrf 1
Pro Inside global  Inside local  Outside local  Outside global
tcp 100.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23
Qtech# show ip nat translations vrf 2
Pro Inside global  Inside local  Outside local  Outside global
tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23

```

### 13.2.8 VPN NAT configuration example

On a MPLS network, NAT can be used to implement VRF traversal.

Figure 41



Configure MPLS

```
mpls ip
```

Configure PBR

```

route-map vrfdata permit 10
match ip address 150
set vrf data

```

### Specify an ACL

```
ip access-list extended 100
 10 permit ip 10.0.0.0 0.255.255.255 any
ip access-list extended 150
 10 permit ip any 20.1.1.0 0.0.0.255
```

### Configure VRF domains

```
ip vrf data
 rd 200:1
 route-target both 200:1
ip vrf v1
 rd 100:1
 route-target export 100:1
ip vrf v2
 rd 100:2
 route-target export 100:2
```

### Deploy MPLS on a public network interface

```
interface GigabitEthernet 0/0
 ip nat outside
 ip ref
 ip address 10.3.1.3 255.255.255.0
 label-switching
 mpls ip
 duplex auto
 speed auto
```

### Configure PBR on a private network interface for NAT deployment

```
interface GigabitEthernet 0/1
 ip vrf forwarding v1
 ip nat inside
 ip policy route-map vrfdata
 ip ref
 ip address 10.1.1.1 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet 0/1.1
 encapsulation dot1Q 100
 ip vrf forwarding v2
 ip nat inside
 ip policy route-map vrfdata
 ip address 10.1.1.1 255.255.255.0
```

### Configure the loopback interface for advertising routes

```
interface Loopback 0
 ip ref
 ip address 3.3.3.3 255.255.255.255
router bgp 100
 bgp router-id 3.3.3.3
 bgp log-neighbor-changes
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback 0
address-family ipv4
 neighbor 4.4.4.4 activate
 exit-address-family
address-family vpnv4 unicast
 neighbor 4.4.4.4 activate
 neighbor 4.4.4.4 send-community both
 neighbor 4.4.4.4 route-map hzb out
 exit-address-family
address-family ipv4 vrf data
 maximum-prefix 10000
```

```

network 0.0.0.0
 redistribute connected
 redistribute static
 exit-address-family
address-family ipv4 vrf v1
 maximum-prefix 10000
 redistribute static
 exit-address-family
address-family ipv4 vrf v2
 maximum-prefix 10000
 exit-address-family
router ospf 1
 router-id 3.3.3.3
 network 0.0.0.0 255.255.255.255 area 0
mpls router ldp
 ldp router-id interface Loopback 0 force

```

#### Configure NAT to take effect on VRF data packets

```

ip nat pool abc 100.1.1.1 100.1.1.1 netmask 255.255.255.0
ip nat inside source static 10.1.1.2 100.1.1.1 vrf data

```

#### Specify a blackhole route

```

ip route vrf data 100.1.1.1 255.255.255.255 Null 0

```

### 13.2.9 NAT Static Port Range Mapping

```

interface GigabitEthernet 0/0
 ip nat inside
 ip address 11.1.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet 0/1
 ip nat outside
 ip address 22.2.2.1 255.255.255.0
 duplex auto
 speed auto
!
ip nat inside source static tcp 11.1.1.2 22.2.2.3 port-range 80 100

```

You can check whether the translation record is established correctly by displaying the NAT mapping table.

```

RSR10X#show ip nat translations
Pro Inside global      Inside local          Outside local         Outside global
tcp 22.2.2.3:93        11.1.1.2:93          33.3.3.18:1000       33.3.3.18:1000
tcp 22.2.2.3:82        11.1.1.2:82          33.3.3.7:1005        33.3.3.7:1005
tcp 22.2.2.3:83        11.1.1.2:83          33.3.3.8:1006        33.3.3.8:1006
tcp 22.2.2.3:99        11.1.1.2:99          33.3.3.24:1000       33.3.3.24:1000
tcp 22.2.2.3:84        11.1.1.2:84          33.3.3.9:1007         33.3.3.9:1007
tcp 22.2.2.3:98        11.1.1.2:98          33.3.3.23:1000       33.3.3.23:1000
tcp 22.2.2.3:94        11.1.1.2:94          33.3.3.19:1000       33.3.3.19:1000
tcp 22.2.2.3:87        11.1.1.2:87          33.3.3.12:1010       33.3.3.12:1010
tcp 22.2.2.3:95        11.1.1.2:95          33.3.3.20:1000       33.3.3.20:1000
tcp 22.2.2.3:86        11.1.1.2:86          33.3.3.11:1009       33.3.3.11:1009
tcp 22.2.2.3:81        11.1.1.2:81          33.3.3.6:1004         33.3.3.6:1004
tcp 22.2.2.3:89        11.1.1.2:89          33.3.3.14:1000       33.3.3.14:1000
tcp 22.2.2.3:97        11.1.1.2:97          33.3.3.22:1000       33.3.3.22:1000
tcp 22.2.2.3:91        11.1.1.2:91          33.3.3.16:1000       33.3.3.16:1000
tcp 22.2.2.3:80        11.1.1.2:80          33.3.3.5:1003         33.3.3.5:1003
tcp 22.2.2.3:96        11.1.1.2:96          33.3.3.21:1000       33.3.3.21:1000
tcp 22.2.2.3:85        11.1.1.2:85          33.3.3.10:1008       33.3.3.10:1008
tcp 22.2.2.3:90        11.1.1.2:90          33.3.3.15:1000       33.3.3.15:1000
tcp 22.2.2.3:92        11.1.1.2:92          33.3.3.17:1000       33.3.3.17:1000

```

```
tcp 22.2.2.3:88      11.1.1.2:88      33.3.3.13:1000   33.3.3.13:1000
tcp 22.2.2.3:100     11.1.1.2:100     33.3.3.25:1000   33.3.3.25:1000
```

## 14 CONFIGURING SSH TERMINAL SERVICE

### 14.1 Overview of SSH

A Secure Shell (SSH) connection functions like a Telnet connection, except that all transmissions based on the connection are encrypted. When a user logs in to the device from an insecure network, the SSH feature provides information security guarantee and powerful authentication function to protect the devices from IP spoofing, plain password interception and other kinds of attacks.

Qtech SSH service supports both the IPv4 and IPv6 protocols.

#### SSH Algorithms Supported by Qtech Products

Supported Algorithm	SSH1	SSH2
Signature authentication algorithm	RSA	RSA, DSA
Key exchange algorithm	RSA public key encryption based key exchange algorithm	KEX_DH_GEX_SHA1 KEX_DH_GRP1_SHA1 KEX_DH_GRP14_SHA1
Encryption algorithm	DES, 3DES, Blowfish	DES, 3DES, AES-128, AES-192, AES-256
User authentication algorithm	User password based authentication method	User password based authentication method
Message authentication algorithm	Not supported	MD5, SHA1, SHA1-96, MD5-96
Compression algorithm	NONE	NONE

### 14.2 SSH Configuration

#### 14.2.1 Default SSH Configurations

Item	Default Value
SSH server status	Off
SSH version	Compatible mode (supporting versions 1 and 2)
SSH user authentication timeout period	120s
SSH user re-authentication times	3

#### 14.2.2 Configuring User Authentication

- Considering the SSH connection security, the login without authentication is forbidden. Therefore, in the login authentication of the users, the login authentication mode must have password configured (authentication-free login allowed for telnet).
- The username and password entered every time must be set. If the current authentication mode does not need the username, the username can be entered randomly but the length must be greater than zero.

#### 14.2.3 Enabling SSH Server

The SSH Server is disabled by default. To enable the SSH Server, run the **enable service ssh-server** command in global configuration mode while generating a SSH key.

Command	Description
Qtech# <b>configure terminal</b>	Enters global configuration mode.
Qtech(config)# <b>enable service ssh-server</b>	Enables the SSH Server.
Qtech(config)# <b>crypto key generate {rsa dsa}</b>	Generates a key



**Caution**

To delete a key, use the `crypto key zeroize` command rather than the `[no] crypto key generate` command.

The SSH module does not support hot standby. For products supporting management module hot standby, after the management module is switched over, if the current primary board has no SSH key file, the `crypto key generate` command must be used to regenerate a key in order to use SSH.

### 14.2.4 Shutting Down the SSH Server

To disable the SSH Server, run the `no enable service ssh-server` command in global configuration mode:

Command	Function
Qtech# <b>configure terminal</b>	Enters global configuration mode.
Qtech(config)# <b>no enable service ssh-server</b>	Disables the SSH Server.

### 14.2.5 Configuring the Supported SSH Server Version

By default, the SSHv1 and SSHv2 are compatible. Run the following commands to configure the SSH version.

Command	Function
Qtech# <b>configure terminal</b>	Enters configuration mode.
Qtech(config)# <b>ip ssh version {1   2}</b>	Configures the supported SSH version.
Qtech(config)# <b>no ip ssh version</b>	Restore the default SSH version. By default, SSHv1 and SSHv2 are supported.

### 14.2.6 Configuring SSH User Authentication Timeout Period

By default, the user authentication timeout period of the SSH server is 120 seconds. Run the following commands to configure the SSH user authentication timeout period.

Command	Function
Qtech# <b>configure terminal</b>	Enters configuration mode.
Qtech(config)# <b>ip ssh time-out time</b>	Configures the SSH timeout period (ranging from 1 to 120 seconds).
Qtech(config)# <b>no ip ssh time-out</b>	Restores the default SSH user authentication timeout period to 120 seconds.

### 14.2.7 Configuring SSH Re-authentication Times

This command is used to set the authentication attempts for SSH users requesting connections to prevent illegal actions such as malicious guesswork. By default, three authentication attempts can be made for the SSH Server. In other words, it allows the user to enter the username and password for three times to attempt the authentication. Run the following commands to configure the SSH re-authentication times:

Command	Function
Qtech# <b>configure terminal</b>	Enters configuration mode.
Qtech(config)# <b>ip ssh authentication-retries retry times</b>	Configures SSH re-authentication times (ranging from 0 to 5).
Qtech(config)# <b>no ip ssh authentication-retries</b>	Restores the default SSH re-authentication times to 3.

**Caution**

For details of the preceding commands, see SSH Command Reference Manual.

### 14.2.8 Configuring SSH Public Key Based Authentication

Only the version 2 of the SSH protocol supports public key based authentication. The following commands associate a public key file with a username. When processing client authentication, the server uses a specified public key file according to the username of the client.

Command	Function
Qtech# <b>configure terminal</b>	Enters configuration mode.
Qtech(config)# <b>ip ssh peer test public-key rsa flash:rsa.pub</b>	Configures the RSA public key file that is associated with the username <i>test</i> .
Qtech(config)# <b>ip ssh peer test public-key dsa flash:dsa.pub</b>	Configures the DSA public key file that is associated with the username <i>test</i> .

### 14.2.9 Configuring the SCP Server Function

With the SCP server enabled on a network device, the user can directly download files from the network device and upload local files to the network device. Meanwhile, the user can transfer all interactive data in encrypted text manner, featuring authentication and security.

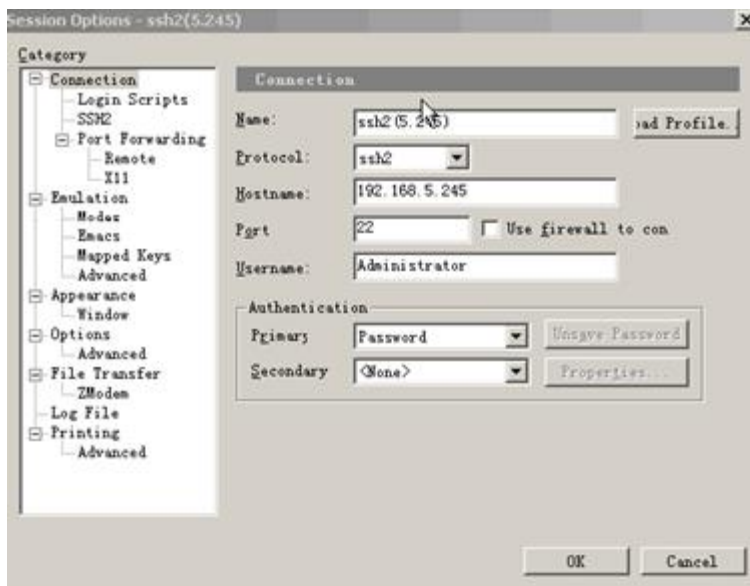
Command	Function
Qtech# <b>configure terminal</b>	Enters configuration mode..
Qtech(config)# <b>ip scp server enable</b>	Enable the SCP server function.
Qtech(config)# <b>no ip scp server enable</b>	Disable the SCP server function.



**Note** For details of the above commands, see *SSH Command Reference Manual*.

## 14.3 Using SSH for Device Management

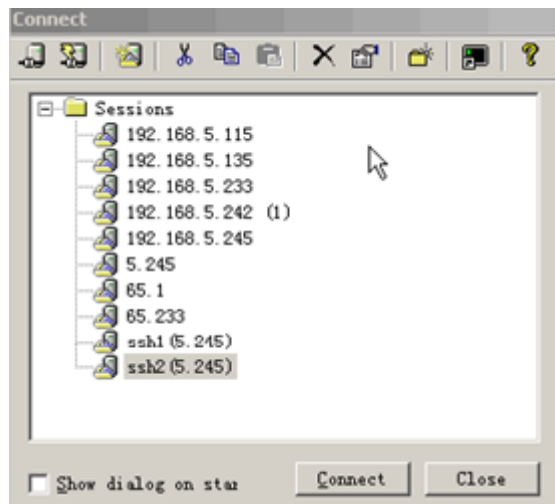
You may use SSH for device management after enabling the SSH Server function that is disabled by default. Since Telnet that comes with the Windows does not support SSH, third-party client software must be used. Currently, the clients with sound forward compatibility include Putty, Linux and SecureCRT. With the client software SecureCRT as an example, the SSH client configuration is described as follows (see the UI below):



As shown in the figure, protocol 2 is used for login, so **SSH2** is selected for **Protocol**. **Hostname** indicates the IP address of the host the user will log in, 192.168.5.245. Port 22 is the default port listened by SSH. **Username** indicates the username, and does not take effect when the device only requires a password. **Authentication**

indicates the authentication mode, and the username/password authentication is supported here. The used password is the same as the password used for Telnet.

Click **OK**. The following dialog box pops up:



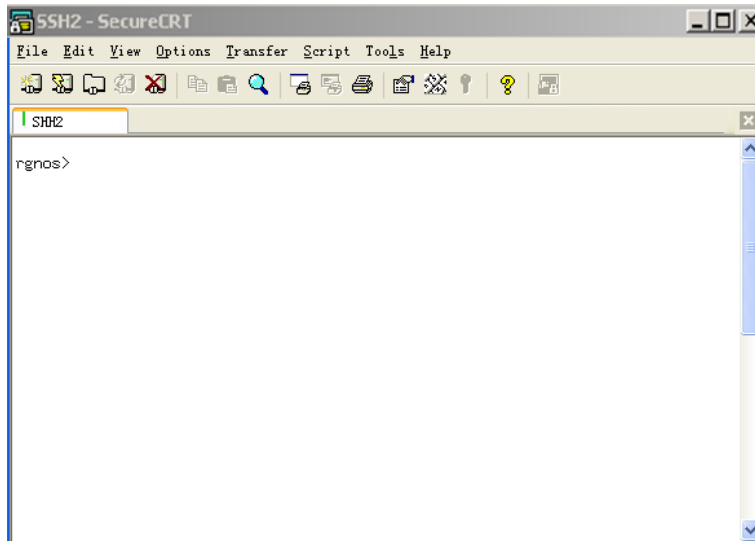
Click **Connect** to log in to the host, as shown below:



Ask the user whose is logging in to the host 192.168.5.245 whether to receive the key from the server. Select **Accept & Save** or **Accept Once**. A dialog box, prompting you to enter a password, pops up as follows:



Enter the Telnet login password. A window pops up as follows:

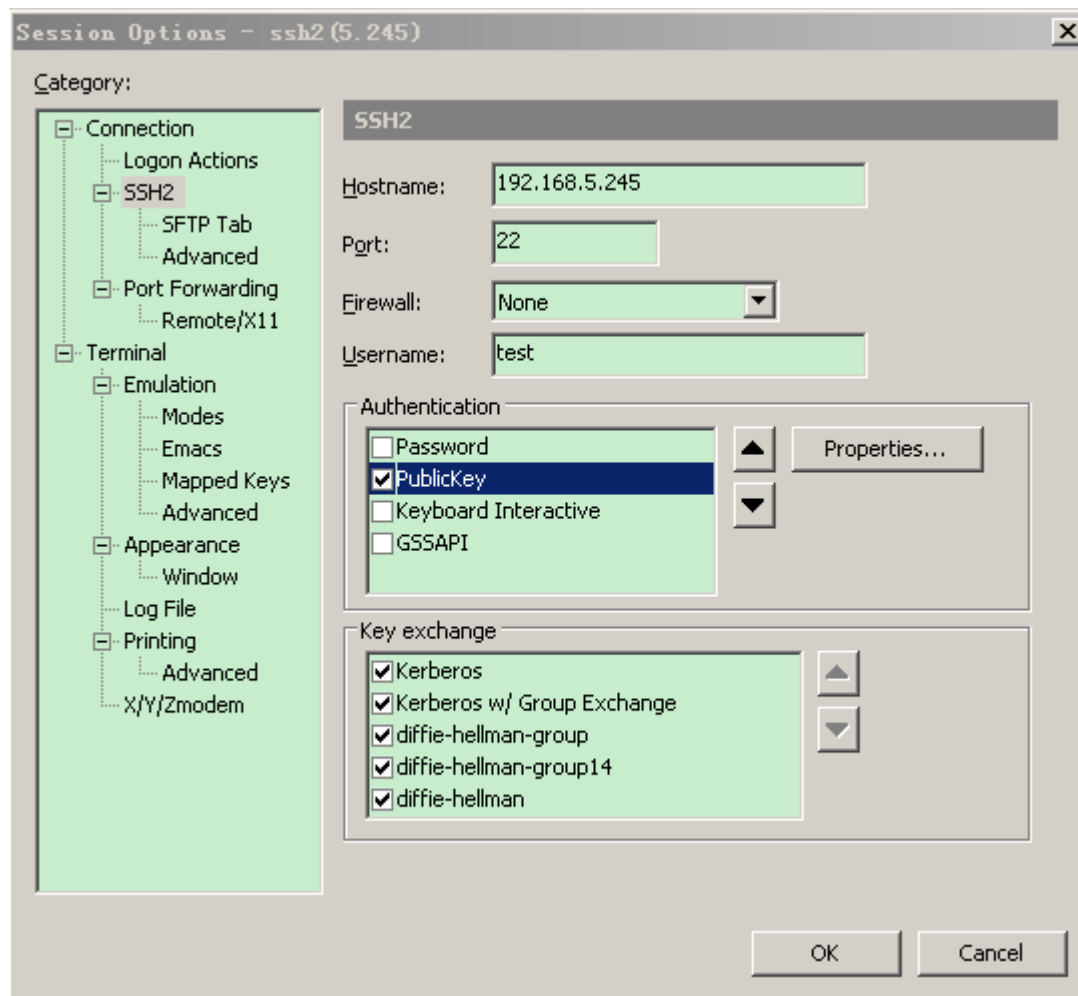


## 14.4 Enabling SSH public key based authentication

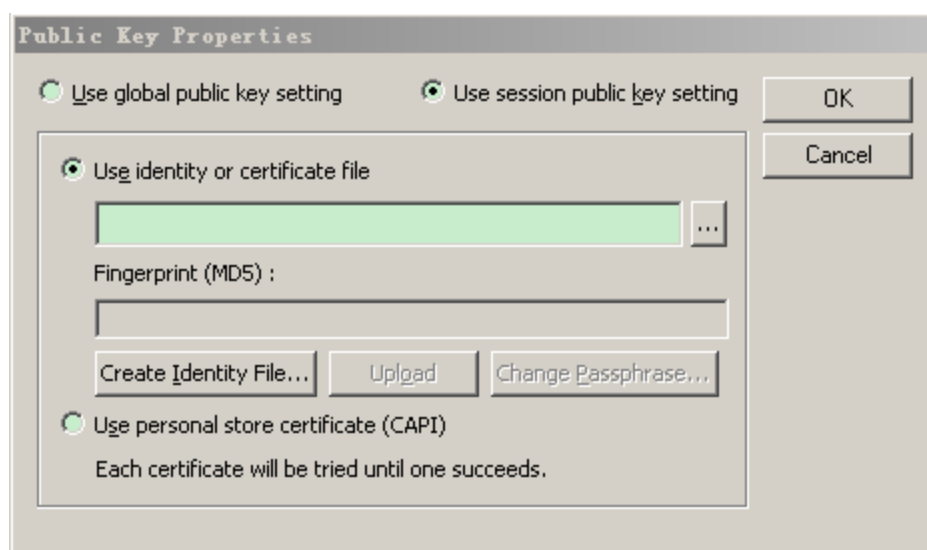
### 14.4.1 Operations on the SSH Client:

To enable SSH public key authentication, generate a key pair ( RSA or DSA ) on the SSH client and put the public key on the SSH server. And then enabling SSH public key based authentication on SSH server. The following section takes client software SecureCRT for an instance to demonstrate how to generate key pair on SSH client.

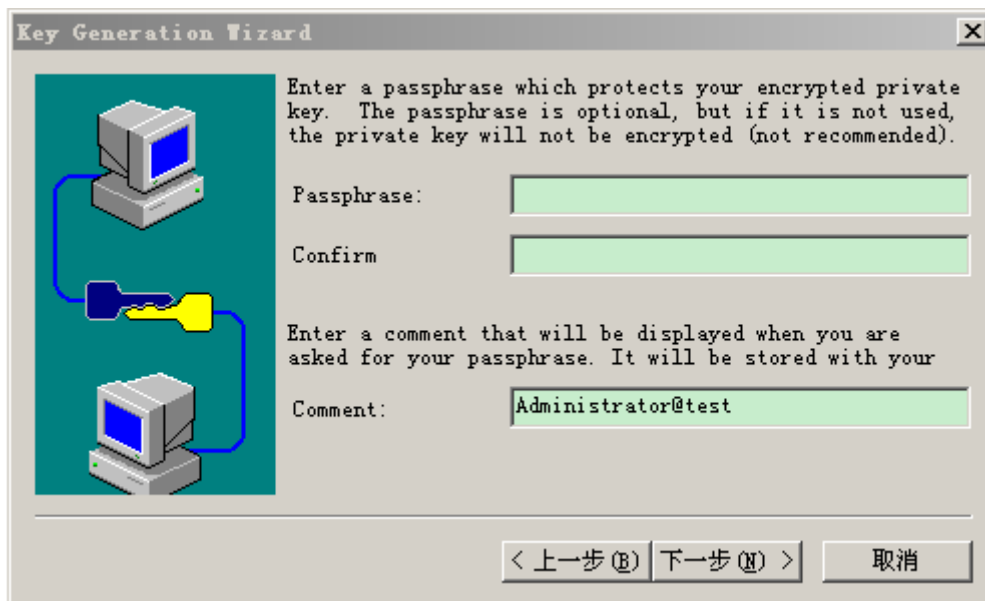
Firstly, click PublicKey in Authentication on Session Option, and then click Properties. as Shown below.



If the key pair is generated before, use the private key (Use identity or certificate file) . Note that this private key must be paired with the public key on the SSH server, otherwise the authentication fails. As shown below.



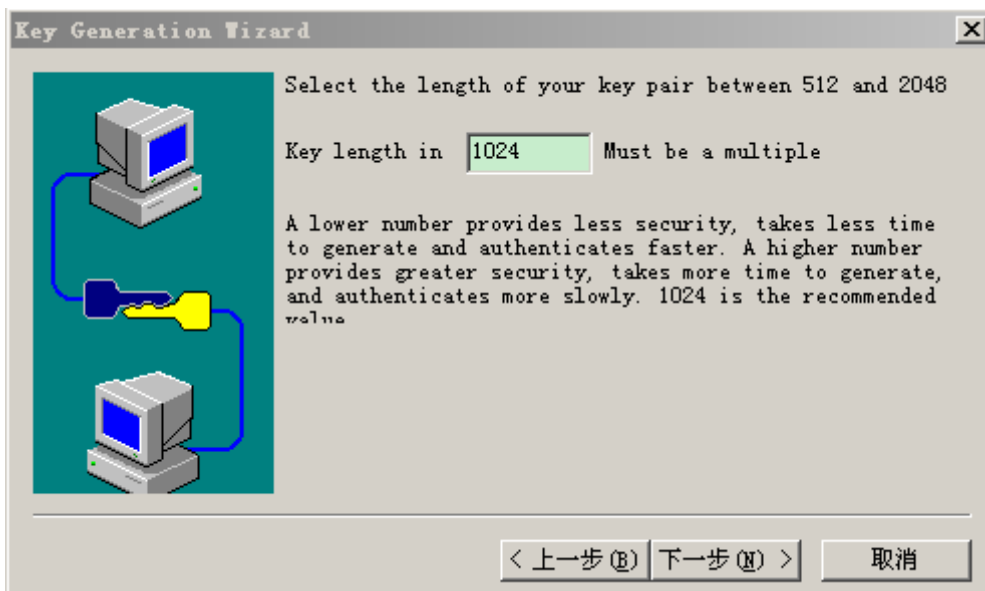
If no key pair is generated before, generate a new key pair. (Optional) set a passphrase for the private key. Once the passphrase is set, you should key in this passphrase for authentication. As shown below.



**Note**

Shaking the mouse when the SSH client is generating the key pair, otherwise the generating rate will be slow.

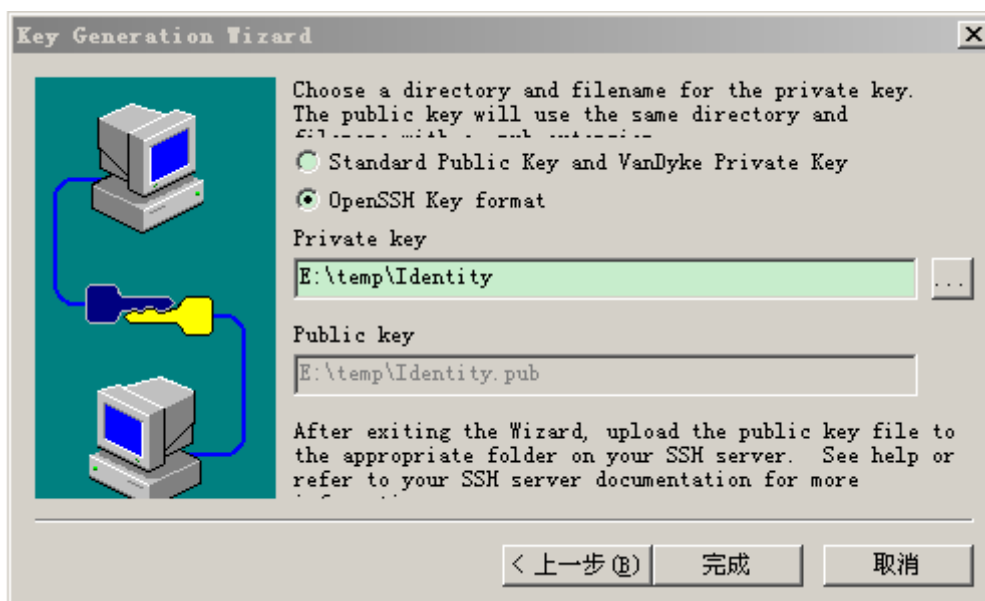
The key files must be stored in OpenSSH key format, otherwise the files cannot be used. If the Putty is adopted as the client software, still the private key is required to turn into the Putty format by puttygen.exe.(Puttygen.exe can generate key pair in OpenSSH format, but Putty cannot use key pair in OpenSSH format directly). However, the public key files generated in OpenSSH format do not need transformation.



**Note**

To guarantee the security of RSA public key based authentication, make sure the key length is longer or equivalent to 768.





#### 14.4.2 Operations on the SSH server

When the key pair is generated on the SSH client, the SSH server (network device) copies the public key files into flash, and associated these public key files with SSH clients' username. Each username can be associated with one RSA public key and one DSA public key. As shown below:

```
Qtech# configure terminal
Qtech(config)# ip ssh peer test public-key rsa flash:rsa.pub
Qtech(config)# ip ssh peer test public-key dsa flash:dsa.pub
```

By doing so, SSH clients can log into network devices through public key based authentication.

### 14.5 Transferring files through SSH

#### 14.5.1 Operation on the SSH server:

SSH transfers files by means of the SCP protocol (Secure Copy). The client can upload files to the network device or download files from the network device through SCP. To realize such function, enable the SCP server function, as shown below.

```
Qtech# configure terminal
Qtech(config)# ip scp server enable
```

By doing so, client can connect server and transfer files through SCP. SCP server use SSH thread. So when a client connects the network device transferring files through SCP, it will takes up a VTY line. ( when using the command show user, you can see the user type is SSH).

#### 14.5.2 Operation on the SSH server:

Both Unix and Linux platform carries SCP command. Taking Ubuntu Linux as an example to demonstrate the use of SCP command, as shown below:

```
Grammar of SCP command:
scp [-1246BCpqrw] [-c cipher] [-F ssh_config] [-i identity_file]
[-l limit] [-o ssh_option] [-P port] [-S program]
[[user@]host1:]file1 [...] [[user@]host2:]file2
Explanation for some options:
```

```
-l : Use SSH version 1 (by default, use SSH version 2);
-2 : Use SSH version 2 (by default);
-C : Specify compressed transmission;
-c : Specify encryption algorithm;
-r : Transmit all files under this content;
-i : Specify key pair;
-l : Limit the transmission rate (measured by Kbits);
For other detailed parameters, see also the scp.0.
```

Take Ubuntu 7.10 as an example to demonstrate file transferring.

The designated user named *test* copies *config.text* file from a network device with an IP address 192.168.195.188 to the local */root*. As shown below:

```
root@dhcpd:~# scp test@192.168.195.188:/config.text /root/config.text
test@192.168.195.188's password:
config.text          100% 1506      1.5KB/s   00:00
Read from remote host 192.168.195.188: Connection reset by peer
```



#### Note

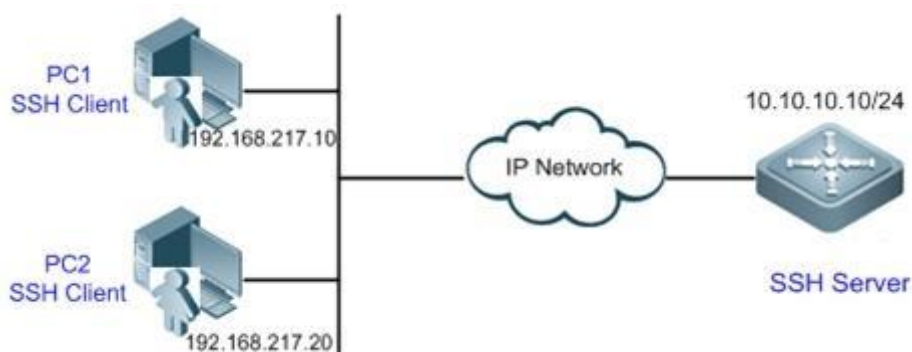
Most options are client related only. And few of these options require support from both client and server. The SCP server on Qtech Networks' devices do not support `-d -p -q -r` options. So when user configuring these options, the device indicates unsupported message.

If no rate limitation (`-l` option) is configured in advance, the CPU usage will rise when the client downloading files from server, and recover after the downloading. The console remains available but other application tasks will be affected.

## 14.6 Typical SSH Configuration Examples

### 14.6.1 Configuring SSH Local Authentication

Figure 42 Networking diagram for SSH local password protection



### 14.6.2 Application Requirements

As shown in Figure , to ensure the security of information exchange, PC1 and PC2 serve as SSH clients from which users will log in to the SSH Server through SSH. The specific requirements are shown below:

- SSH users adopt line password authentication.
- Lines 0 to 4 are activated at the same time. The login password for line 0 is "passzero", and the login password for other four lines is "pass". Any user name can be used.

### 14.6.3 Notes

- Notes on SSH Server configuration are as follows:

- 98) Globally enable SSH Server. By default, SSH Server supports SSHv1 and SSHv2.
- 99) Configure a key. The SSH server will use this key to decrypt the encrypted passwords received from the SSH clients, and compare the plain text with the password stored on the server before returning a message that indicates a successful or failed authentication. SSHv1 uses RSA key, while SSHv2 uses RSA or DSA key.
- 100) Configure the IP address of the Gi 1/1 interface of the SSH server. SSH clients connect to the SSH server through this interface. The routes from SSH clients to the SSH server are reachable.
  - Configurations on SSH Clients:

There are many SSH client software, such as Putty, Linux, OpenSSH and etc. In this example, SecureCRT is used as the SSH client software. For configuration details, see the "Configuration Steps" section.

#### 14.6.4 Configuration Steps

- Configure the SSH Server

Before configuring relevant SSH features, make sure the routes from SSH clients to the SSH server are reachable. The IP addresses of respective interfaces are shown in Figure 6, and the IP address and route configuration are omitted herein.

##### Step 1: Enable SSH Server

```
Qtech(config)# enable service ssh-server
```

##### Step 2: Generate an RSA key

```
Qtech(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
```

##### Step 3: Configure the IP address of Gi 1/1 interface. The client will use this IP address to connect to the SSH server.

```
Qtech(config)#interface gigabitEthernet 1/1
Qtech(config-if- gigabitEthernet 1/1)#ip address 10.10.10.10 255.255.255.0
Qtech(config-if- gigabitEthernet 1/1)#exit
```

##### Step 4: Configure login passwords for lines

! Configure the login password for line 0 as "passzero"

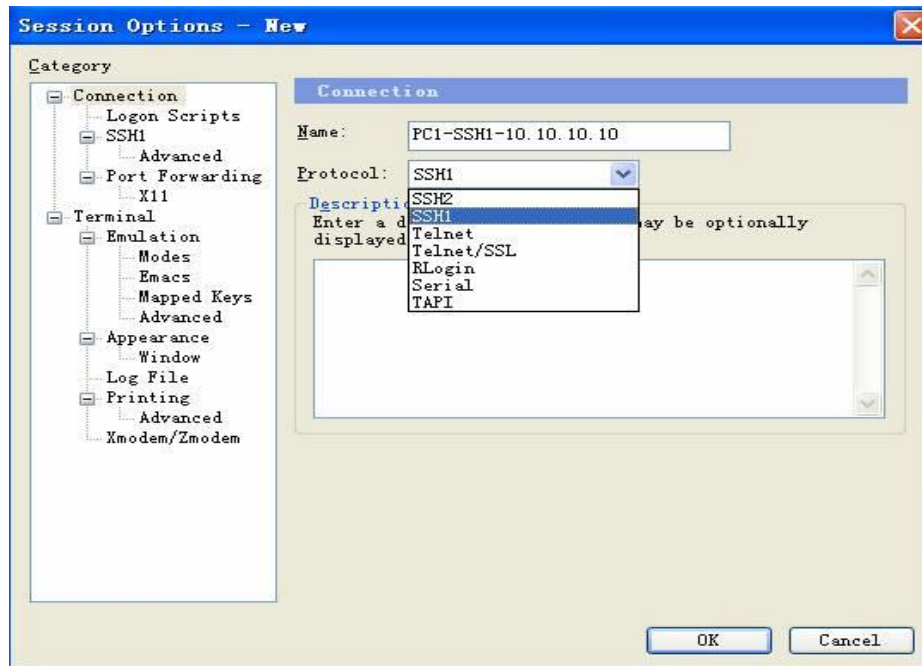
```
Qtech(config)#line vty 0
Qtech(config-line)#password passzero
Qtech(config-line)#privilege level 15
Qtech(config-line)#exit
```

! Configure the login password for lines 1 to 4 as "pass"

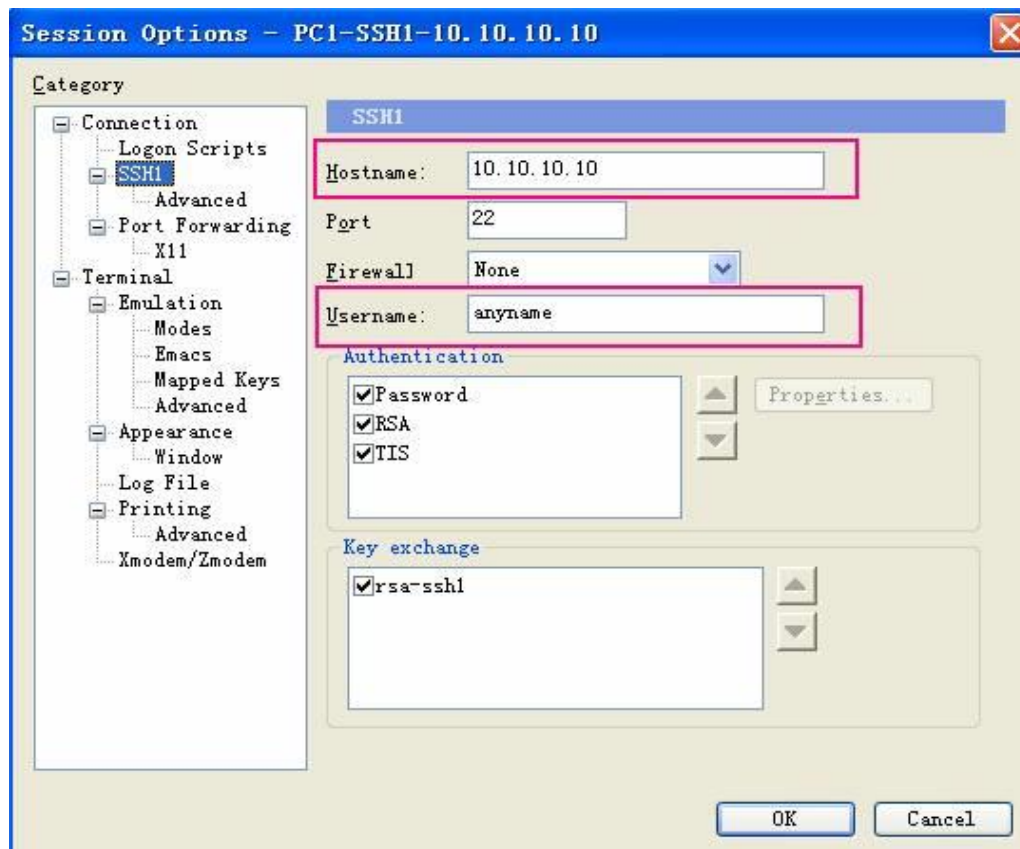
```
Qtech(config)#line vty 1 4
Qtech(config-line)#password pass
Qtech(config-line)#privilege level 15
Qtech(config-line)#exit
```

- Configure SSH Clients (PC1 and PC2)

Start SecureCRT, as shown in the following figure. Use SSH1 for login authentication. Any session name can be specified (here the session name is configured as PC1-SSH1-10.10.10.10).



Configure SSH attributes. The host name is the IP address of the SSH server (10.10.10.10 in this example). Since user name is not required, you can type in any user name in the **User Name** field, but this field cannot be left blank (the user name is **anyname** in this example).



### 14.6.5 Verifying the Configuration

- Verify the SSH Server configuration

Step 1: Run the **show running-config** command to verify the current configuration:

```
Qtech#show running-config
Building configuration...
!
enable secret 5 $1$eyy2$xs28FDw4s2q0tx97
enable service ssh-server
!
interface gigabitEthernet 1/1
 ip address 10.10.10.10 255.255.255.0
 line vty 0
 privilege level 15
 login
 password passzero
 line vty 1 4
 privilege level 15
 login
 password pass
!
end
```

- Verify the configuration of SSH clients

Step 1: Establish a remote connection.

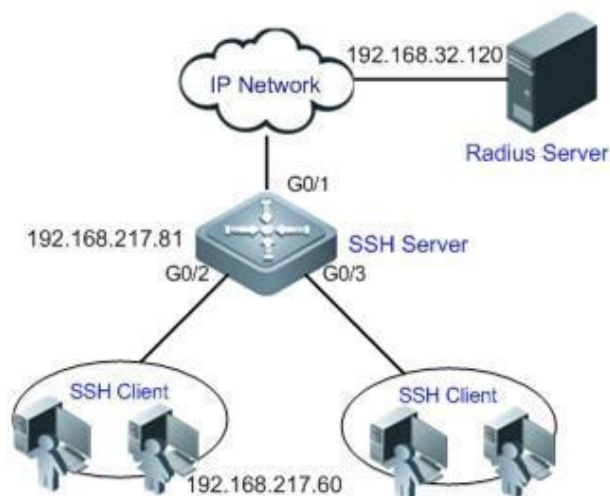
Establish a connection and type in the correct password in order to enter the interface of the SSH Server. The login password for line 0 is "passzero", and the login password for other four lines is "pass".

Step 2: Query the online user.

```
Qtech#show users
Line      User      Host(s)      Idle      Location
  0 con 0
  1 vty 0      idle        00:03:16
  2 vty 1      idle        00:02:16   192.168.217.10
 * 2 vty 1      idle        00:00:00   192.168.217.20
```

## 14.7 Example of Configuring SSH AAA Authentication

Figure 43 Networking diagram for SSH AAA authentication



### 14.7.1 Application Requirements

As shown in Figure 10, to ensure the security of information exchange, PCs serve as SSH clients from which users will log in to the SSH Server through SSH.

To better implement security management, SSH clients adopt AAA authentication. Meanwhile, for stability consideration, two authentication methods are configured in the AAA authentication method list: Radius server authentication and local authentication. Radius server authentication has a higher priority than local authentication unless no response is received during Radius server authentication.

### 14.7.2 Notes

- The routes from SSH clients to the SSH server and the route from the SSH server to the Radius server shall be reachable.
- SSH Server related configuration is complete on the network device. The configuration tips have been described in the previous example, and are not further described herein.
- AAA authentication related configuration is complete on the network device. AAA defines identity authentication and type by creating a method list, which is then applied to the specific service or interface. For details, see the "Configuration Steps" section.

### 14.7.3 Configuration Steps

The routes from SSH clients to the SSH server and the route from the SSH server to the Radius server shall be reachable. Route configuration will not be further described. For details, see the section about route configuration in this manual.

- Configure relevant SSH features on the network device

#### Step 1: Enable SSH Server

```
Qtech(config)# enable service ssh-server
```

#### Step 2: Generate a key

##### ! Generate an RSA key

```
Qtech(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
```

##### ! Generate a DSA key

```
Qtech(config)#crypto key generate dsa
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit DSA keys ...[ok]
```

#### Step 3: Configure the IP address of the device. The clients will use this address to connect to the SSH server.

```
Qtech(config)#interface gigabitEthernet 1/1
Qtech(config-if-gigabitEthernet 1/1)#ip address 192.168.217.81 255.255.255.0
Qtech(config-if-gigabitEthernet 1/1)#exit
```

- Configure AAA authentication on the network device

#### Step 1: Enable AAA on the device

```
Qtech#configure terminal
Qtech(config)#aaa new-model
```



Step 2: Configure information about the Radius server (the shared key used by the SSH server for communicating with the Radius server is "aaaradius")

```
Qtech(config)#radius-server host 192.168.32.120
Qtech(config)#radius-server key aaaradius
```

Step 3: Configure an AAA authentication method list

! Configure a login authentication method list (Radius server authentication followed by local authentication), and the name of the method list is "method".

```
Qtech(config)#aaa authentication login method group radius local
```

Step 4: Apply this method list to the lines

```
Qtech(config)#line vty 0 4
Qtech(config-line)#login authentication method
Qtech(config-line)#exit
```

Step 5: Configure a local user database

! Configure a local user database (configure the user name and password, and bind the user to a privilege level)

```
Qtech(config)#username user1 privilege 1 password 111
Qtech(config)#username user2 privilege 10 password 222
Qtech(config)#username user3 privilege 15 password 333
```

! Configure a password for local Enable authentication

```
Qtech(config)#enable secret w
```

### 14.7.4 Verifying the Configuration

Step 1: Run the **show running-config** command to verify the current configuration:

```
Qtech#show run

aaa new-model
!
aaa authentication login method group radius local
!
username user1 password 111
username user2 password 222
username user2 privilege 10
username user3 password 333
username user3 privilege 15

no service password-encryption
!
radius-server host 192.168.32.120
radius-server key aaaradius
enable secret 5 $1$hbqz$ArCsyqty6yyzpz03
enable service ssh-server
!
interface gigabitEthernet 1/1
 no ip proxy-arp
 ip address 192.168.217.81 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.217.1
!
line con 0
line vty 0 4
 login authentication method
!
end
```

Step 2: Configure the Radius Server. This example describes how to configure the SAM server.

Choose **System Management > Device Management**, and type in 192.168.217.81 as the IP address of the device and the device key **aaaradius**;

Choose **Security Management > Device Management Privilege**, and configure a privilege level for the login user;

Choose **Security Management > Device Administrator**, and type in **user** as the user name and **pass** as the password.

Step 3: Establish a remote SSH connection on the PC.

For details about how to set SSH client software and establish a connection, see the previous example.

Type in **user** as the SSH user and **pass** as the password. The user will log in successfully.

Step 4: Query the online user.

```
Qtech#show users
  Line      User      Host(s)      Idle      Location
  0 con 0           idle        00:00:31
* 1 vty 0      user       idle        00:00:33  192.168.217.60
```

## 15 CONFIGURING IP ACCOUNTING

### 15.1 Understanding IP Accounting

### 15.2 Overview

IP accounting, an easy-to-use traffic management tool, classifies and collects statistics on the traffic passing routers by source IP address and destination IP address. The collected statistics include the number of packets and number of bytes. Traffic accounting and traffic analysis can be implemented on the basis of IP accounting statistics.

### 15.3 Configuring IP Accounting

#### 15.3.1 Enabling IP Accounting

IP accounting is enabled on the inbound or outbound interface. You need to specify an interface and the direction when enabling IP accounting. In addition, you can configure a traffic classification rule while enabling IP accounting. The system will collect statistics on traffic based on the configured rule.

Use the following commands to enable IP accounting.

Command	Function
Qtech> <b>enable</b>	Enters privileged EXEC mode.
Qtech# <b>config terminal</b>	Enters global configuration mode.
Qtech(config)# <b>interface</b> <i>interface-type</i> <i>interface-number</i>	Enters interface configuration mode.
Qtech(config-if)# <b>ip accounting</b> { <b>ingress</b>   <b>egress</b> } <b>list</b> { <i>acl_list_num</i>   <i>acl_list_name</i> }	Enables IP accounting on the interface.
Qtech(config-if)# <b>end</b>	Returns to privileged EXEC mode.
Qtech# <b>copy running-config</b> <b>startup-config</b>	Saves the configuration.

To disable IP accounting on the interface, use the **no ip accounting { ingress | egress }** command in interface configuration mode.

Configuration example

```
Qtech# config terminal
Qtech(config)# interface gigabitEthernet 0/1
Qtech(config-if)# ip accounting ingress list 20 //Enable IP Accounting on the 0/1
interface to classify and collect statistics on incoming traffic based on ACL 20.
Qtech(config-if)# exit
Qtech(config)# interface gigabitEthernet 0/2
Qtech(config-if)# ip accounting egress list 10 //Enable IP Accounting on the 0/2
interface to classify and collect statistics on outgoing traffic based on ACL 10.
Qtech(config-if)# exit
Qtech(config)#
```

#### 15.3.2 Displaying IP Accounting Configuration

Use the **show ip accounting config** command to query IP accounting configuration on an interface. For example:

```
Qtech# show ip accounting config
GigabitEthernet 0/1
ip accounting ingress list 20
```

```
GigabitEthernet 0/1
ip accounting egress list 10
```

### 15.3.3 Displaying IP Accounting Statistics

Use the **show ip accounting interface** *interface-type interface-number* { **ingress** | **egress** } { **interior** | **exterior** } command to query IP accounting statistics on the inbound or outbound interface in privileged, global, or interface mode, with **interior** indicating the statistics matching an ACL rule and **exterior** indicating the statistics not matching the ACL rule.

Command	Function
Qtech> <b>enable</b>	Enters privileged EXEC mode.
Qtech# <b>config terminal</b>	Enters global configuration mode.
Qtech(config)# <b>interface</b> <i>interface-type interface-number</i>	Enters interface configuration mode.
Qtech(config-if)# <b>show ip accounting</b> <i>interface-type interface-number</i> { <b>ingress</b>   <b>egress</b> } { <b>interior</b>   <b>exterior</b> }	Displays IP accounting statistics on the interface.
Qtech(config-if)# <b>end</b>	Returns to privileged EXEC mode.

Configuration example

```
Qtech# config terminal
Qtech(config)# interface gigabitEthernet 0/1
Qtech(config-if)# show ip accounting interface gigabitEthernet 0/1 ingress interior
```

### 15.3.4 Clearing IP Accounting Statistics

Use the **clear ip accounting interface** *interface-type interface-number* { **ingress** | **egress** } command to clear the IP accounting statistics on the specified interface in privileged EXEC mode.

The following example clears IP accounting statistics on the outbound interface.

```
Qtech# clear ip accounting interface gigabitEthernet 0/1 egress
```

## 16 CONFIGURING SDG

### 16.1 Understanding SDG

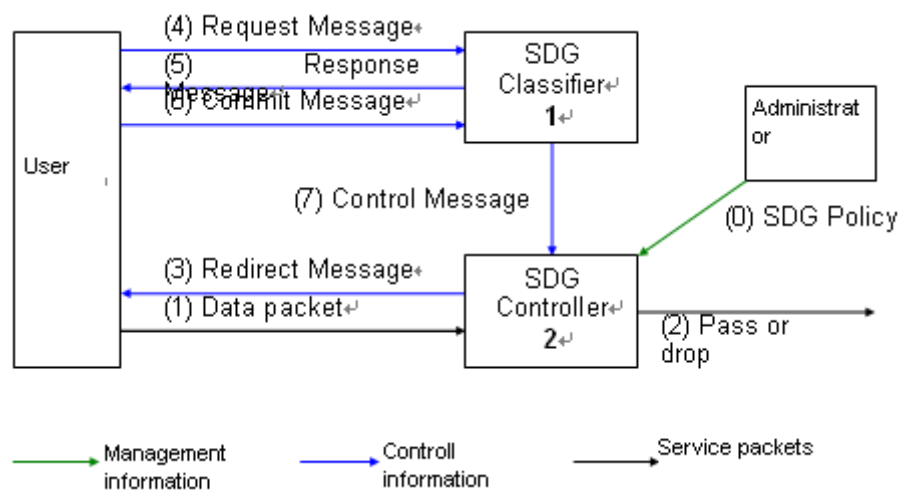
#### 16.1.1 Overview of SDG

To be simple, Security Domain Gateway (SDG) achieves the logical isolation between different security domains. By limiting the user to access only the specified security domain at a time, users can be prevented from accessing different security domains and hence viruses will not spread to other protected domains, or important information will not leak to the insecure domains. SDG has two operating modes: local mode and linked mode.

#### 16.1.2 Working Principle

Working principle of SDG in local mode:

Figure 44



As shown above, the SDG system consists of two parts:

**Classifier:** Through the interaction with users, the classifier determines the current role of each user, and sends this message to the controller. The classifier is realized by means of Web, so that the user does not need to install the client software.

**Controller:** The controller is mainly responsible for receiving the user role message sent by the classifier and applying access control to the traffic sent by the user as per the access permission assigned to such role. In addition, the controller is also responsible for triggering a message prompting the user to reselect a role while accessing an unauthorized domain.

**User:** During the interaction with SDG, the user sends traffic to the controller on one hand and negotiates with the Classifier for role selection on the other hand.

**Administrator:** It is responsible for establishing SDG policies on the controller. Such a policy determines the access permissions of different user roles, implementing "logical isolation". The policy is generally configured through CLI.

The working procedures of SDG are shown below:

**(0):** The administrator establishes a SDG policy according to actual needs, covering the user role, isolated domain and the access control rules applied between user roles and isolated domains.

**(1) → (2):** The Controller receives the traffic sent by the user and applies the access control, so that valid packets can pass and invalid packets failing to trigger "user role selection" will be discarded. A criterion for identifying valid packet depends on an SDG policy: the user role sending this packet is allowed to access the isolated domain.

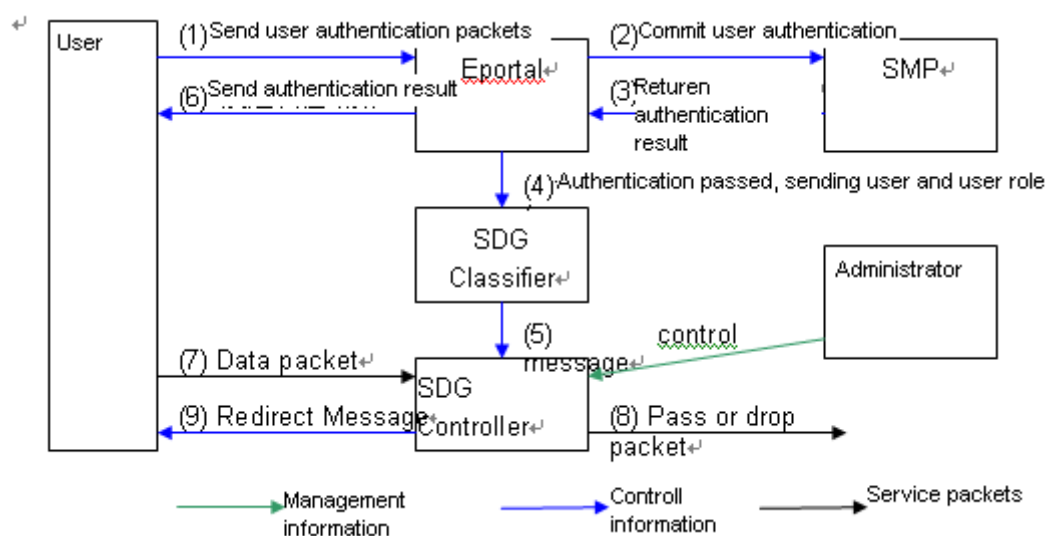
**(1) → (3) → (4):** As for the invalid packets sent by the user, if such packets are capable of triggering "role selection", then the controller will send an Http redirection packet to the user and redirect the user request to the "user role selection" page on the Classifier. One condition for triggering "user role selection" is that the packet must be a valid http request packet.

**(4) → (5) → (6):** The user proactively (or through Controller redirection) sends the "user role selection" request to the Classifier, which will reply to the user (browser) with this page. No matter which role is selected by the user on the page, the selection result will be submitted to the Classifier.

**(7):** The Classifier forwards the user role selection result to the Controller, which will record and use such information as the reference for security check of this user during future access.

Working principle of SDG in linked mode

Figure 45



**Eportal: Eportal server**

**SMP: security authentication server**

Other flows are the same as local mode.

The working procedures of SDG are shown below:

**(0):** The administrator establishes an SDG policy according to actual needs, covering the user role, isolated domain and access control rules applied between user roles and isolated domains.

**(1)→(2):** The user sends authentication packet to Eportal, which will forward the user authentication packet to SMP.

**(3)** MP verifies user information and sends the authentication result to Eportal.

**(4)→(5):** In case of successful authentication, Eportal will send the user and user role to the SDG Classifier, which will update the user role and forward the user role selection result to the Controller. The Controller will record and use such information as the reference for security check of this user during future access.

**(6):** Eportal will send the authentication result to the user, which will reselect the role or send traffic according to the authentication result.

**(7)→(8)→(9):** The SDG Controller matches the user role. If the user role does not match and the redirection condition is met, it will send a redirection packet. The user will reselect the role and send a user authentication packet to the Eportal, or else it will discard the packet. If matched, SDG check is passed.

### 16.1.3 Protocol Specification

N/A



## 16.2 Default Configurations

N/A

## 16.3 Configuring SDG

### 16.3.1 Configuring SDG Mode

While deploying SDG, you can select different SDG operating modes according to users' security needs. The SDG working in local mode is easy to deploy and will be ready to operate after the router is configured. To deploy SDG working in linked mode, you need to add an SMP server. This mode, however, supports user authentication and hence provides higher security.

To configure SDG mode, run the following commands:

Command	Function
Qtech> <b>enable</b>	Enters privileged command mode.
Qtech# <b>config terminal</b>	Enters global configuration mode.
Qtech(config)# <b>ip sdg mode link</b>	Enables SDG linked mode.

### 16.3.2 Configuring the IP Address of the SMP Server

In linked mode, you need to configure the IP address of the SMP server for redirection. The user can also use an SMP URL for redirection.

To configure the IP address of the SMP server, run the following commands:

Command	Function
Qtech> <b>enable</b>	Enters privileged command mode.
Qtech# <b>config terminal</b>	Enters global configuration mode.
Qtech(config)# <b>ip sdg portal ip [url]</b>	Configures the IP address for connecting to the Eport, namely the IP address of the Eportal server .

### 16.3.3 Configuring Aging Time for Offline Users

In linked mode, you need to configure aging time for users. A user is considered offline if the user does not initiate a connection request within the aging time.

To configure aging time for offline users, run the following commands:

Command	Function
Qtech> <b>enable</b>	Enters privileged command mode.
Qtech# <b>config terminal</b>	Enters global configuration mode.
Qtech(config)# <b>ip sdg user-timeout time</b>	Configures aging time for offline users.

### 16.3.4 Configuring Keepalive Duration and Threshold of User Traffic

In association mode, the keepalive duration and threshold of user traffic must be configured. After the keepalive duration and threshold of user traffic are configured, the SDG controller checks whether the user traffic is lower than the configured traffic threshold within the configured keepalive duration. If the user traffic is lower than the configured traffic threshold within the keepalive duration, the user is considered offline. In this case, a trap message is sent to the SMP server to force the user to go offline.

Run the following commands to configure the keepalive duration and threshold of user traffic:

Command	Function
Qtech> <b>enable</b>	Enters the privileged EXEC mode.
Qtech# <b>config terminal</b>	Enters the global configuration mode.
Qtech(config)# <b>ip sdg offline-detect idle-timeout time-out threshold flow-num</b>	Configures the keepalive duration and threshold of user traffic.

### 16.3.5 Configuring DNS Hijacking

In association mode, DNS hijacking must be configured. DNS hijacking is not configured by default and will be immediately enabled once it is configured. When **action** is **drop**, all DNS query packets except Class A DNS query packets are discarded. When **action** is **permit**, all DNS query except class A query packets are forwarded.

Run the following commands to configure DNS hijacking:

Command	Function
Qtech> <b>enable</b>	Enters the privileged EXEC mode.
Qtech# <b>config terminal</b>	Enters the global configuration mode.
Qtech(config)# <b>ip sdg dns-hijack interface loopback num action [ drop   permit ]</b>	Configures DNS hijacking.

### 16.3.6 Configure the Default User

In local mode, add the default user into the specified user group. Upon the first access, the user has the permission to access the specified user group.

To configure the default user, run the following commands:

Command	Function
Qtech> <b>enable</b>	Enters privileged command mode.
Qtech# <b>config terminal</b>	Enters global configuration mode.
Qtech(config)# <b>ip sdg permit-user user-ip user-mask user-group group-name</b>	Adds the default user.
Qtech(config)# <b>no ip sdg permit-user user-ip user-mask user-group group-name</b>	Removes the default user.

### 16.3.7 Configuring SDG Classifiers

To control SDG, you must define SDG classifiers. Each SDG classifier defines a series of user groups (user roles). One user belongs to only one user group at the same time.

The SDG classifier created is applied to SDG policies. When user access violates the SDG policy, the user selection page will be displayed to prompt the user to select a user group.

The user can also take the initiative to access the user selection page to select a user group. The URL of the user selection page is:

"http://" + *device interface address* + "/sdg" + *classifier ID* + ".htm?Qtech\_query\_id=sdg". For example, if the interface address is 192.168.52.52 and the classifier ID is 1, then the corresponding URL is:

http://192.168.52.52/sdg001.htm

To configure SDG classifiers, run the following commands:

Command	Function
Qtech> <b>enable</b>	Enters privileged command mode.
Qtech# <b>config terminal</b>	Enters global configuration mode.
Qtech(config)# <b>ip sdg classifier classifier-id</b>	Configures SDG classifiers and enters SDG classifier command mode.



**Caution** Web server must be enabled in order to generate the user role selection page.

```
Qtech(config)# enable service web-server
```

### 16.3.8 Configuring User Groups

After creating SDG classifiers, run the **user-group** command to configure user groups to be included in this classifier.

To configure user groups, run the following command:

Command	Function
Qtech> <b>enable</b>	Enters privileged command mode.
Qtech# <b>config terminal</b>	Enters global configuration mode.
Qtech(config)# <b>ip sdg classifier classifier-id</b>	Configures SDG classifiers and enters SDG classifier command mode.
Qtech(config)# <b>user-group group-name</b>	Configures the user group included in an SDG classifier.

### 16.3.9 Configuring Static Users

In local mode, add users into the specified user group. The statically configured user will not be changed while the user is selecting a role.

Command	Function
Qtech> <b>enable</b>	Enters privileged command mode.
Qtech# <b>config terminal</b>	Enters global configuration mode.
Qtech(config)# <b>user-group group-name</b>	Configures user groups to be included in an SDG classifier.
Qtech (config-user-group)# <b>user ip</b>	Adds a static user.
Qtech (config-user-group)# <b>no user ip</b>	Removes a static user.

### 16.3.10 Clearing Users in a User Group

In local mode, remove non-static users from a user group; in linked mode, remove all users from a user group.

Command	Function
Qtech> <b>enable</b>	Enters privileged command mode.
Qtech# <b>clear user-group group-name</b>	Removes users from a user group.

### 16.3.11 Configuring SDG Control Policies

A SDG policy can be configured in either inbound or outbound direction of an interface. It consists of one ACL and one SDG classifier. The ACL is used to define the isolation policy, which must be based on the user groups included in the SDG classifier. When user access violates the isolation policy, the user selection page defined in SDG classifier will be displayed to prompt the user to select an appropriate user group.

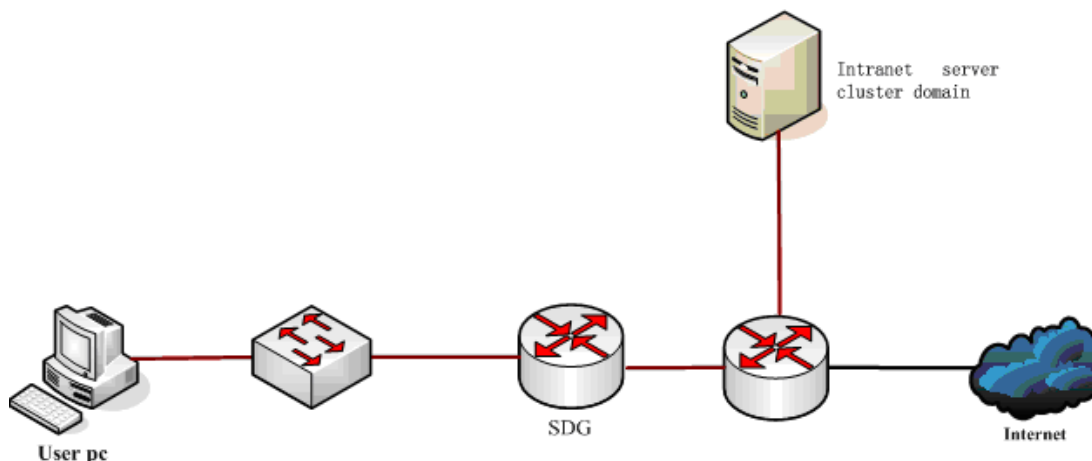
To configure SDG control policies, run the following commands:

Command	Function
Qtech> <b>enable</b>	Enters privileged command mode.
Qtech# <b>config terminal</b>	Enters global configuration mode.
Qtech(config)# <b>interface gigabitEthernet 0/0</b>	Enters interface configuration mode.
Qtech(config-if-gigabitEthernet 0/0)# <b>ip sdg in out access-group acl-no trigger classifier-id</b>	Configures an SDG control policy.

### 16.3.12 Configuration Examples

#### 16.3.12.1 Local mode

Figure 46



As shown above, after transparent bridge mode is enabled on the SDG device, SDG functions can be realized without changing the network structure.

Configuration:

101) Configure SDG to work in local mode

Command	Function
Qtech(config)# ip sdg mode local	Configures SDG to work in local mode.

102) Configure the SMP address for SDG in linked mode

Command	Function
Qtech(config)# ip sdg portal 10.1.1.2 http://xxx.xxx.xxx/eportal	Configure the IP address for connecting to the Eport, namely the IP address of the Eportal server.

103) Create a user group

Define a user group for each user role, including intranet user group (intranet\_user) and internet user group (internet\_user).

Command	Function
Qtech(config)# user-group intranet_user	Configures the intranet user group.
Qtech(config)# user-group internet_user	Configures the internet user group.

104) Configure a static user

In local mode, add a user into the user group

Command	Function
Qtech(config-user-group)#user 192.168.50.18	Adds a user.
Qtech(config-user-group)# no user 192.168.50.18	Removes a user.

105) Create a domain

An intranet server cluster domain (intranet\_site) needs to be defined.

Command	Function
Qtech(config)# network-region intranet_site	Configures an intranet server cluster domain.
Qtech(config-network-region)# network 192.168.0.0 255.255.0.0	Configures all network segments included in the intranet server cluster domain.
.....	

106) Configure an SDG classifier

Define an SDG classifier, which shall include intranet user group (intranet\_user) and internet user group (internet\_user).

Command	Function
Qtech(config)# ip sdg classifier 1	Defines SDG classifier 1.

Qtech(config-sdg-classifier)# <b>user-group</b> <i>intranet_user</i>	Adds intranet_user into the classifier.
Qtech(config-sdg-classifier)# <b>user-group</b> <i>internet_user</i>	Adds internet_user into the classifier.

107) Configure an isolated access policy

Use an ACL to define an isolation policy.

Command	Function
Qtech(config)# <b>ip access-list extend</b> 100	Configures extended ACL 100.
Qtech(config-ext-acl)# <b>permit ip user-group</b> <i>intranet_user</i> <b>network-region</b> <i>intranet_site</i>	Allows intranet users to access intranet servers.
Qtech(config-ext-acl)# <b>deny ip user-group</b> <i>intranet_user</i> <b>any</b>	Prohibits intranet users from accessing other sites.
Qtech(config-ext-acl)# <b>deny ip user-group</b> <i>internet_user</i> <b>network-region</b> <i>intranet_site</i>	Prohibits Internet users from accessing intranet servers.
Qtech(config-ext-acl)# <b>permit ip user-group</b> <i>internet_user</i> <b>any</b>	Allows Internet users to access other sites.

Note: DNS traffic must not be confined. You can create ACEs at the beginning of the ACL to permit DNS traffic.

108) Configure an SDG policy

Configure an SDG policy on the interface. The SDG policy is associated with one ACL and one SDG trigger. HTTP requests violating this ACL will be redirected to the page configured by the SDG trigger.

Command	Function
Qtech(config)# <b>Interface</b> <i>gi 0/0</i>	# Enters Gi 0/0 interface.
Qtech(config-interface)# <b>ip sdg in access-group</b> 100 <b>trigger</b> 1	Configures an SDG policy in the inbound direction and associates the policy with ACL 100 and SDG classifier 1.

109) Enable web-server

Command	Function
Qtech(config)# <b>enable service web-server</b>	The SDG user selection page will only be generated only after web-server is enabled.

110) Enable transparent bridge mode

Command	Function
Qtech(config)# <b>transparent</b>	Enables transparent bridge mode.

Note: Only fast forwarding supports transparent bridge mode

111) Authenticating a user

You can directly type the URL of the SMP server in the address box of a Internet Explorer for authentication, or makes SDG trigger authentication upon denial of access.

## 17 CONFIGURING ANTI-ATTACK FEATURES ON DEVICES

### 17.1 Overview of Device Anti-attack

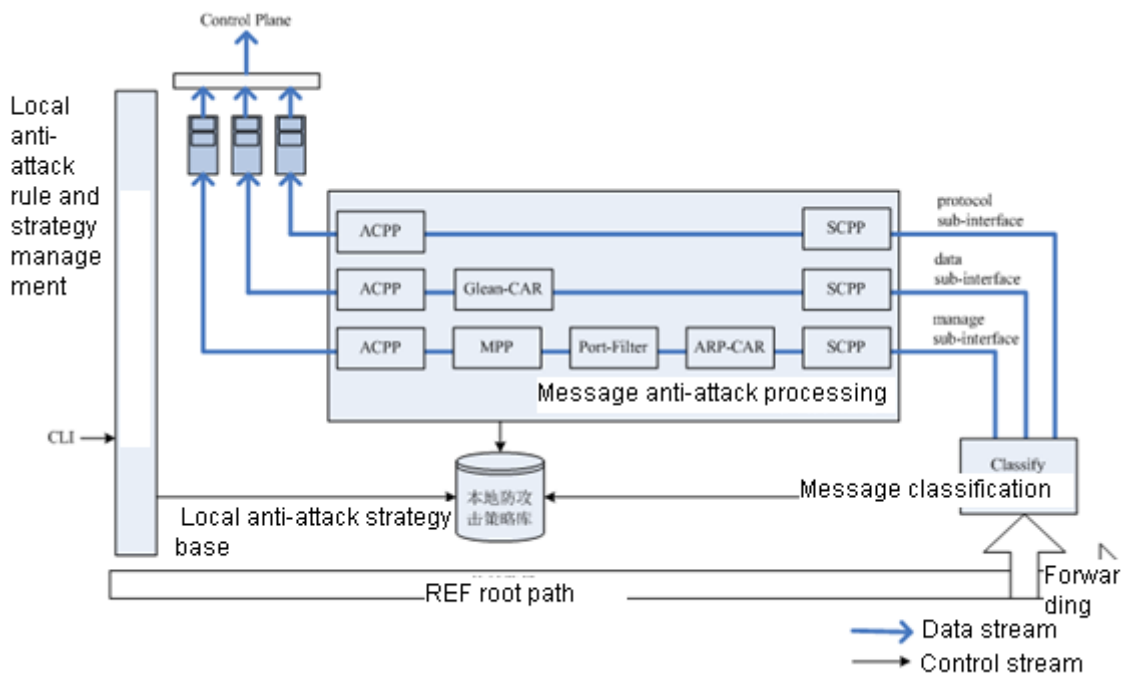
When encountering a network attack or heavy traffic, the device on a complex network may report the following exceptions:

- 112) Extremely high CPU usage;
- 113) Slow response or no response of CLI;
- 114) Loss of link or network control protocol messages, consequently leading to link or network delay variation;
- 115) Unauthorized occupation of bandwidth, resulting in the failure to process important protocol messages.

Such phenomena are due to the difference in processing capacity of control and forwarding planes on one hand and the lack of protection of the control plane on the other hand. The anti-attack module is to classify, filter and rate-limit the data messages that need to be forwarded to the control layer for processing, protecting the key resources of the control plane.

The following figure illustrates the principle and process of device anti-attack:

Figure 47



As shown in the figure, device anti-attack consists of numerous sub-modules:

**Classify:** Identify and classify the data traffic destined for the control plane. There are three categories of traffic including protocol, manage and data. The sub-module sets a base for subsequent rate limiting and filtering.

**Sub-interface:** The three traffic categories correspond to the following three sub-interfaces. The three sub-interfaces and streams through these interfaces are defined as follows:

**Protocol sub-interface:** All protocol control streams sent to the local device, such as link layer protocol messages, routing protocol messages, etc.

**Manage sub-interface:** All management protocol streams sent to the local device, such as FTP, TELNET, SNMP streams, etc. In addition, ARP and ICMP traffic also falls into this category.

**Data sub-interface:** All data streams that cannot be processed by any REF plane.





**Note** The sub-interface in this manual is different from what is usually regarded. It only represents an internal path through which a type of traffic is sent to the control plane, helping you configure anti-attack and process traffic.

**SCPP:** protects the control plane by subdividing traffic. SCPP delivers more delicate rate limiting and protection according to user-defined policies.

**Glean-CAR:** limits the rate of the traffic to the REF plane matching REF Glean adjacency (traffic with a direct route but without a host route matching the destination IP address is diverted to the control plane for destination IP address resolution).

**ARP-CAR:** Since the REF plane cannot complete processing ARP messages, these messages must be forwarded to the control plane. ARP-CAR can limit the rate of ARP messages from each neighbor.

**Port-Filter:** checks whether ports have been enabled for local TCP and UDP messages and filters network traffic for which no local network service is enabled.

**MPP:** Management Plane Protection (MPP) allows administrators to specify one or more interfaces as in-band management interfaces (receiving management messages and forwarding normal service messages). After the MPP function is enabled, only specified in-band management interfaces are allowed to receive the management messages of specified protocol. However, service messages, protocol messages, ARP messages, etc are not affected.

**ACPP:** Aggregate Control Plane Protection (ACPP) limits, on the basis of classification result by Classify, the rate of traffic on protocol sub-interface, manage sub-interface and data sub-interface with default or users' custom-made rate in order to ensure the traffic does not exceed the processing capacity of the control plane and the control plane is protected as a result.

## 17.2 Configuring Device Anti-attack

### 17.2.1 Device Anti-attack Configuration Tasks



**Note** Sub-functions, such as SCPP, Glean-CAR, ARP-CAR, Port-Filter, MPP, and ACPP, are independent from each other. Users may combine and configure them according to their needs and strategies. But it should be noticed that some sub-functions can be applied only to specified sub-interfaces.

### 17.2.2 Entering Control-plane Configuration Mode

All device anti-attack functions are configured in control-plane configuration mode. To enter control-plane configuration mode, run the following command:

Command	Function
Qtech(config)# <b>control-plane { protocol   manage   data }</b>	Enters control-plane configuration mode and accesses corresponding sub-interfaces.

To exit control-plane configuration mode, run the **exit** command.

**17.2.3 Configuring SCPP** SCPP can be used to distinguish and limit the rate of traffic in sub-interfaces according to user-defined policies. Rate limiting is classified into connection limiting and traffic bandwidth limiting. To configure SCPP, run the following commands:

Command	Function
---------	----------

Qtech(config-cp)# <b>scpp list</b> <i>acl_no</i> { <b>bw-rate</b> <i>bw-rate</i>   <b>bw-burst-rate</b> <i>bw-burst-rate</i>   <b>conn-total</b> <i>conn-num</i>   <b>conn-create-rate</b> <i>conn-create-rate</i>   <b>conn-create-burst-rate</b> <i>conn-create-burst-rate</i> }	Configures a SCPP traffic bandwidth limit (unit: pps), a connection limit, etc for the traffic that complies with <b>acl_no</b> strategy on the sub-interface. <i>Acl_no</i> : ACL rule used to select the traffic in need of SCPP processing. <i>Bw-rate</i> : rate limit (unit: pps) <i>Bw-burst-rate</i> : burst rate limit (unit: pps) <i>Conn-num</i> : limit on the total number of connections <i>Conn-create-rate</i> : limit on the rate of connection establishment (unit: connection/s) <i>Conn-create-burst-rate</i> : limit on the burst rate of connection establishment (unit: connection/s)
Qtech(config-cp)# <b>no scpp list</b> <i>acl_no</i>	Deletes configured SCPP rules.

SCPP processing can be applied to traffic on all sub-interfaces.

SCPP is disabled by default and will not be enabled until users configure SCPP rules explicitly.

#### 17.2.4 Configuring Glean-CAR

For traffic that has a direct route but does not have its destination IP address resolved, configure Glean-CAR to limit the rate by using the following commands:

Command	Function
Qtech(config-cp)# <b>glean-car</b> <i>packet_rate_per_group</i>	Configures a rate limit on Glean adjacency traffic initiated by users hashed to the same group <i>Packet_rate_per_group</i> : rate limit (unit: pps)
Qtech(config-cp)# <b>no glean-car</b>	Deletes Glean-CAR rules.

The Glean-CAR function can only be configured on the data sub-interface.

Currently, the hash algorithm extracts the least significant *n* bits (*n* is determined by products) of source address.

It should be noticed that Glean-CAR can limit the rate of Glean adjacency matching traffic initiated by users hashed to the same group. For example, both user of A (192.168.52.57) and user B (192.168.60.57) (with the same hashed result) send traffic to destination host C (172.16.0.5) directly connected to the device. Before ARP messages of host C has been successfully resolved, only a maximum of five messages can be sent by users A and B to the control plane every second for destination IP ARP resolution if `glean-car 5` is configured.

Glean-CAR is enabled by default and the rate limit of Glean adjacency matching traffic initiated by users (source) hashed to the same group is configured at 5 pps.

#### 17.2.5 Configuring ARP-CAR

Run the following commands to configure ARP-CAR on ARP traffic reaching the local device.

Command	Function
Qtech(config-cp)# <b>arp-car</b> <i>packet_rate_per_group</i>	Configures a rate limit of the ARP traffic initiated by users hashed to the same group. <i>Packet_rate_per_group</i> : rate limit (unit: pps)
Qtech(config-cp)# <b>no arp-car</b>	Deletes ARP-CAR rules.

The ARP-CAR function can only be configured on the manage sub-interface.

Currently, the hash algorithm extracts the least significant *n* bits (*n* is determined by products) of source address.

It should be noticed that ARP-CAR can limit the rate of ARP traffic initiated by users hashed to the same group. For example, both user A (192.168.52.57) and user B (192.168.60.57) (with the same hashed result) initiate ARP requests of 192.168.52.1 to the device. If ARP-CAR 5 is configured, only a maximum of five messages can be sent by users A and B to the control plane every second for ARP response.

ARP-CAR is enabled by default and the rate limit of the ARP traffic initiated by users (source) hashed to the same group is configured at 5 pps.

### 17.2.6 Configuring Port-Filter

Run the following commands to configure Port-Filter to filter the transport layer messages that reach the local device yet have no services enabled:

Command	Function
Qtech(config-cp)# <b>port-filter</b>	Enables Port-Filter.
Qtech(config-cp)# <b>no port-filter</b>	Disables Port-Filter.

The Port-Filter function can only be configured on the manage sub-interface.

Port-Filter is disabled by default and will not be enabled until users configure Port-Filter rules explicitly..

### 17.2.7 Configuring MPP

Run the following commands to configure the in-band management interface and the management protocol messages the interface is allowed to receive:

Command	Function
Qtech(config-cp)# <b>management-interface</b> <i>interface</i> <b>allow</b> {ftp   http   https   ssh   snmp   telnet   tftp }	Specifies the in-band management interface and configures the management protocol messages supported by the interface <i>Interface</i> : in-band management interface
Qtech(config-cp)# <b>no management-interface</b> <i>interface</i>	Deletes the specified in-band management interface. The MPP function will be disabled if all in-band management interfaces are deleted.

The MPP sub-function can only be configured on the manage sub-interface.

A maximum of 16 in-band management interfaces can be configured and each of them can receive several or all management protocol messages.

After the MPP function is enabled, in-band management interfaces can receive specified management protocol messages and other interfaces do not receive management protocol messages.

MPP is disabled by default and will not be enabled until users configure MPP rules explicitly.

### 17.2.8 Configuring ACPP

Run the following commands to configure ACPP for the classisified traffic reaching the control plane:

Command	Function
Qtech(config-cp)# <b>acpp bw-rate</b> <i>rate</i> <b>bw-burst-rate</b> <i>burst-rate</i>	Configures ACPP rules for the traffic on sub-interfaces. <i>Rate</i> : rate limit (unit: pps) <i>Burst-rate</i> : burst rate limit (unit: pps)
Qtech(config-cp)# <b>no acpp</b>	Deletes ACPP rules.

ACPP can be applied to all sub-interfaces.

ACPP is disabled by default and will not be enabled until users configure ACPP rules explicitly.

**17.2.9 Enabling Device Anti-attack with Default Rules** Run the following commands in control-plane configuration mode to configure device anti-attack with default rules:

Command	Function
Qtech(config-cp)# <b>ef-rnfp enable</b>	Enables device anti-attack with default rules.
Qtech(config-cp)# <b>ef-rnfp disable</b>	Disables device anti-attack.

Default device anti-attack rules and strategies are configured according to different products and platforms.

## 17.3 Maintaining Device Anti-attack

### 17.3.1 Maintenance of device anti-attack

To query configurations and statistics of device anti-attack, run the following command:

Command	Function
Qtech# <b>show ef-rnfp { acpp {data   manage   protocol}  scpp {data   manage   protocol}  glean-car   arp-car   port-filter   mpp   all }</b>	Views configurations and statistics of device anti-attack.

You can use the **show ef-rnfp { acpp {data | manage | protocol}| scpp {data | manage | protocol}| glean-car | arp-car | port-filter | mpp | all }** command to query configurations and statistics of sub-functions, or the **show ef-rnfp all** command to query the configurations and statistics of available anti-attack functions.

## 17.4 Typical Device Anti-Attack Configuration Example

The following example shows the typical configuration of device anti-attack:

```
Qtech# config
//Enter control-plane configuration mode and protocol sub-interface
Qtech(config)# control-plane protocol
// Configure ACPP to set the traffic rate to 500 pps and burst traffic rate to 600 pps on the protocol sub-interface
Qtech(config-cp)# acpp bw-rate 500 bw-burst-rate 600
//Enter control-plane configuration mode and data sub-interface
Qtech(config)# control-plane data
// Configure ACPP to set the traffic rate to 500 pps and burst traffic rate to 600 pps on the data sub-interface
Qtech(config-cp)# acpp bw-rate 500 bw-burst-rate 600
// Configure Glean-CAR, allowing 10 messages from a source to match Glean adjacency per second
Qtech(config-cp)# glean-car 10
//Enter control-plane configuration mode and manage sub-interface
Qtech(config)# control-plane manage
// Configuring ACPP to set the traffic rate to 500 pps and burst traffic rate to 600 pps on the manage sub-interface
Qtech(config-cp)# acpp bw-rate 500 bw-burst-rate 600
// Configure ARP-CAR allowing 10 messages from a source to match Glean adjacency per second
Qtech(config-cp)# arp-car 10
// Enable Port-Filter
Qtech(config-cp)# port-filter
//Configure MPP rules by specifying gi0/0 interface as the in-band management interface and only allowing it to receive Telnet and SNMP messages
Qtech(config-cp)# management-interface gi0/0 allow telnet snmp
```

## 18 CONFIGURING RPL

### 18.1 Understanding RPL

#### 18.1.1 Overview

Reverse path limited (RPL) enables packets to be sent and returned along the same path, ensuring that these packets are not discarded by firewalls that do not allow one-way connection.

When establishing a flow table, a router buffers the inbound port No. of the first packet. Reply packets of a data flow are matched to the flow table preferentially and are forwarded through the inbound port. (Both the routing table and policy-based routing table are not used preferentially, which is similar to the state-based forwarding mechanism of firewalls.)

#### 18.1.2 Basic Concept

RPL

#### 18.1.3 Work Principle

The source port for obtaining a packet is used as the outbound port for replying to the packet.

#### 18.1.4 Typical Application

Figure 4 Networking topology for a terminal to access the server by traversing the firewall

Figure 48



## 18.2 Configuring RPL

### Default Configuration

The following table describes the default configuration of RPL.

Feature	Default Setting
RPL	Disabled.

#### 18.2.1 Configuring RPL

Command	Function
Qtech(config-GigabitEthernet 0/0)# <b>ip reverse-path</b> [ <b>access-list</b> ] [ <i>acl_id</i> ]	Enables RPL. The value range of <i>acl_id</i> is as follows: 1 to 99 (IP standard access list) 100 to 199 (IP extended access list) 1300 to 1999 (IP standard access list, expanded range) 2000 to 2699 (IP extended access list, expanded range)
Qtech(config-GigabitEthernet 0/0)# <b>no ip reverse-path</b>	Disables RPL.

**Caution**

Before enabling RPL on a subinterface, ensure that the subinterface and its peer subinterface are interconnected and the MAC address of the peer subinterface is learnt by this subinterface. If not, the one-way audio failure will occur. You can ping the IP address of the peer subinterface, or use the **shutdown** command to disable the primary interface of the subinterface and then use the **no shutdown** command to enable the primary interface. The preceding restriction does not apply when RPL is configured on other interfaces.

This command is supported by routers only.

**Configuration example** # Enable RPL.

This example shows how to enable RPL on an interface.

```
Qtech#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)#interface gigabitethernet 0/0/0
Qtech(config-if)# ip reverse-path
Qtech(config-if)#exit
Qtech(config)#end
```

### 18.3 Displaying Device Configurations

Use the following command to show device configurations.

Command	Function
show running-config	Displays device configurations.

## 18.4 Configuration Examples

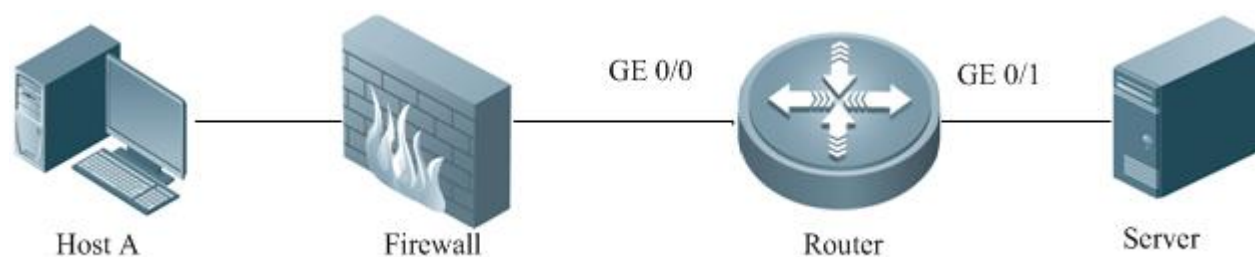
### 18.4.1 RPL Configuration Example

#### Networking requirements

Terminals of a network need to traverse the firewall to access the server.

#### Networking topology

Figure 49 Networking topology for a terminal to access the server through the router and firewall



#### Configuration Tips

- The router and host A is interconnected.
- IP forwarding is enabled on GE 0/0 and GE 0/1.
- Routes to host A are not required on the router.

#### Configuration Steps

Enter configuration commands in interface mode to configure RPL.

```
Qtech#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)#interface gigabitethernet 0/0/0
Qtech(config-if)# ip reverse-path
```



```
Qtech(config-if) #exit  
Qtech(config) #end
```

### Verification

Run the **show running-config** command on the router. **ip reverse-path** is displayed for GE 0/0. Ping the IP address of the server from host A. The server can be successfully pinged.