Network Management and Monitoring

QSR-1920, QSR-2920, QSR-3920

www.qtech.ru

Оглавление

1. NETWORK TEST AND FAULT DIAGNOSIS 7
1.1. Overview 7
1.2. Network Test and Fault Diagnosis Application 7
1.2.1. Ping Function 7
1.2.2. Traceroute Function 12
1.2.3. System Debugging Function 14
1.2.4. Monitoring and Maintaining of Network Test and Fault Diagnosis 15
1.3. Typical Configuration Example of Network Test and Fault Diagnosis 15
1.3.1. Ping Application 15
1.3.2. Traceroute Application 16
2. KEEPALIVE GATEWAY 18
2.1. Overview 18
2.2. Gateway Keepalive Function Configuration 18
2.2.1. Configure Gateway Keepalive Function 18
2.2.2. Monitoring and Maintaining of Gateway Keepalive 19
2.3. Typical Configuration Example of Gateway Keepalive 20
2.3.1. Configure Gateway Keepalive 20
3. SLA 23
3.1. Overview 23
3.2. SLA Function Configuration 23
3.2.1. Enable RTR 24
3.2.2. Configure RTR Entity 25
3.2.3. Configure RTR Entity Group 41
3.2.4. Configure RTR Responder 42
3.2.5. Configure RTR Scheduler 43
3.2.6. Configure Pausing Scheduling Entity 43
3.2.7. Configure Restoring Scheduling Entity 44
3.2.8. SLA Monitoring and Maintaining 45
3.3. SLA Typical Configuration Example 45
3.3.1. Configure ICMP-echo Entity to Detect Basic Network Communication 45
3.3.2. Configure ICMP-path-echo Entity to Detect Network Communication 49
3.3.3. Configure ICMP-path-jitter Entity to Detect Network Communication 52
3.3.4. Configure VoIP-jitter Entity to Detect Network Transmitting VoIP Packets 55
3.3.5. Configure UDP-echo Entity to Detect Network Transmitting UDP Packets 59
3.3.6. Configure Detection Interface Traffic of FLOW-statistics Entity 61
3.3.7. Configure LSP-ping Entity to Detect Communication in MPLS Network 65

3.3.8. Configure LSP-ping Entity with VRF Option to Detect Communication in MPLS L3VPN Network 68
3.3.9. Configure TRACK to Link with ICMP-echo 71
3.3.10. Configure ICMPv6-echo Entity to Detect Basic Network Communication 73
3.3.11. Configure TRACK to Link with ICMPv6-echo 77
3.3.12. Configure Bandwidth-measure Entity to Detect Bandwidth 79
4. NTP 83
4.1. Overview 83
4.2. NTP Function Configuration 84
4.2.1. Configure NTP Basic Functions 84
4.2.2. Configure NTP Optional Parameters 87
4.2.3. Configure NTP Authentication Function 90
4.2.4. Configure NTP Access Control 95
4.2.5. NTP Monitoring and Maintaining 96
4.3. NTP Typical Configuration Example 96
4.3.1. Configure NTP IPv4 Server and Client 96
4.3.2. Configure NTP IPv4 Server and Multi-level Clients 98
4.3.3. Configure NTP Server and Client with MD5 Authentication 100
4.3.4. Configure NTP IPv4 Peer Mode 101
4.3.5. Configure NTP Broadcast Mode 103
4.3.6. Configure NTP IPv6 Server and Client 105
4.3.7. Configure NTP IPV6 Peer Mode 107
5. IPFIX 110
5.1. Overview 110
5.2. IPFIX Function Configuration 110
5.2.1. Configure IPFIX Statistics Function 111
5.2.2. Configure IPFIX Sampling Function 112
5.2.3. Configure IPFIX Packet Attribute 113
5.2.4. Configure IPFIX Flow Template Attribute 115
5.2.5. IPFIX Monitoring and Maintaining 116
5.3. IPFIX Typical Configuration Example 116
5.3.1. Configure Basic Functions of IPFIX IPv4 Flow Exporting in Standard Mode 116
5.3.2. Configure Basic Functions of IPFIX IPv6 Flow Exporting in Standard Mode 118
5.3.3. Configure Basic Functions of IPFIX MPLS Flow Exporting in Standard Mode 120
5.3.4. Configure Basic Functions of IPFIX IPv4 Flow Exporting in extended Mode 122
5.3.5. Configure Basic Functions of IPFIX IPv6 Flow Exporting in extended Mode 124
5.3.6. Configure Basic Functions of IPFIX MPLS Flow Exporting in Extended Mode 126

6. LLDP 129
6.1. Overview 129
6.1.1. Overview of LLDP Protocol 129
6.1.2. TLV Type Information 129
6.1.3. LLDP Work Mechanism 133
6.2. LLDP Function Configuration 134
6.2.1. Configure LLDP Basic Functions 134
6.2.2. Configure LLDP Work Mode 136
6.2.3. Configure TLV Permitted by LLDP to Release 137
6.2.4. Configure LLDP Parameters 139
6.2.5. LLDP Monitoring and Maintaining 142
6.3. LLDP Typical Configuration Example 143
6.3.1. Configure LLDP Basic Functions 143
7. SNMP 147
7.1. Overview 147
7.2. SNMP Function Configuration 150
7.2.1. Configure SNMP Basic Functions 150
7.2.2. Configure SNMPv1/v2 152
7.2.3. Configure SNMPv3 153
7.2.4. Configure SNMP Proxy Forwarding 156
7.2.5. Configure SNMP Trap 157
7.2.6. SNMP Monitoring and Maintaining 158
7.3. SNMP Typical Configuration Example 159
7.3.1. Configure SNMP v1/v2c Proxy Server 159
7.3.2. Configure SNMP v3 Proxy Server 161
7.3.3. Configure SNMP v3 Trap Notify 162
7.3.4. Configure SNMP v3 inform Notify 163
7.3.5. Configure SNMP v3 Proxy Forwarding 165
8. RMON 168
8.1. Overview 168
8.2. RMON Function Configuration 169
8.2.1. Enable RMON Function 169
8.2.2. Configure RMON Alarm Group 169
8.2.3. Configure RMON Extended Alarm Group 170
8.2.4. Configure RMON Event Group 171
8.2.5. Configure RMON History Event 172
8.2.6. Configure RMON Statistics Group 173

8.2.7. RMON Monitoring and Maintaining 173
8.3. RMON Typical Configuration Example 174
8.3.1. Configure RMON Basic Functions 174
9. PORT MIRROR 178
9.1. Overview 178
9.1.1. Introduction to Port Mirror 178
9.1.2. Basic Concepts 178
9.2. SPAN Function Configuration 179
9.2.1. Configure Local Port Mirror 179
9.2.2. Port Mirror Monitoring and Maintaining 180
9.3. Typical Configuration Example of Port Mirror 180
9.3.1. Configure Port Mirror 180
10. PACKET CAPTURE 182
10.1. Overview 182
10.2. Packet Capture Function Configuration 182
10.2.1. Configure Packet Capture Profile 183
10.2.2. Configure Interface Packet Capture Profile 187
10.2.3. Configure System Directory of Packet Capture File 188
10.2.4. Enable Interface Capture Packet Mode 188
10.2.5. Packet Capture Monitoring and Maintaining 189
10.3. Typical Configuration Example of Packet Capture Tool 189
10.3.1. Local Mode of Packet Capture Tool 189
10.3.2. FTP Mode of Packet Capture Tool 191
Note: 192
10.3.3. Mirror Mode of Packet Capture Tool 192
11. CWMP 194
11.1. Overview 194
11.2. CWMP Function Configuration 195
11.2.1. Configure CWMP basic function 196
11.2.2. Configure CWMP Authentication and Encryption Function 202
11.2.3. Configure CWMP Extended Function 204
11.2.4. CWMP Monitoring and Maintaining 205
11.3. CWMP Typical Configuration Example 206
11.3.1. Configure CWMP Authentication Function 206
11.3.2. Configure Source IP Address specified by CWMP 207
11.3.3. Configure CWMP Link Backup 209

12. NETCONF 212
12.1. Overview 212
12.2. NETCONF Basic Function Configuration 212
12.2.1. Configure NETCONF Server Functions 212
12.2.2. NETCONF Monitoring and Maintaining 214
12.3. NETCONF Typical Configuration Example 214
12.3.1. Configure NETCONF Server 214
13. EDP 219
13.1. Overview 219
13.2. EDP Function Configuration 224
13.2.1. Configure EDP Basic Functions 225
13.2.2. Configure Other EDP Functions 227
13.2.3. Configure EDPS Function 228
13.2.4. EDP Monitoring and Maintaining 230
13.3. EDP Typical Configuration Example 231
13.3.1. Configure EDP Basic Functions 231
14. BSM 233
14.1. Overview 233
14.2. BSM Function Configuration 233
14.2.1. Configure BSM Basic Functions 233
14.2.2. Configure BSM Deterioration 236
14.2.3. BSM Monitoring and Maintaining 237
14.3. BSM Typical Configuration Example 237
14.3.1. Configure Basic Function of BSM Link Measuring 237
15. EASY 4G 240
15.1. Overview 240
15.2. Easy 4G Function Configuration 240
15.2.1. Configure Easy 4G Basic Functions 240
15.2.2. Easy 4G Monitoring and Maintaining 241
15.3. Easy 4G Typical Configuration Example 241
15.3.1. Configure Easy 4G Typical Application 241
16. ОБЩАЯ ИНФОРМАЦИЯ 247
16.1. Замечания и предложения 247
16.2. Гарантия и сервис 247
16.3. Техническая поддержка 247

1. NETWORK TEST AND FAULT DIAGNOSIS

1.1. Overview

With the network test and fault diagnosis tool, we can check the network connection status and diagnose the system fault. In daily maintenance, when it is necessary to check the network connection, we can use the ping function and traceroute function. We can open the system debugging information to diagnose the system fault.

1.2. Network Test and Fault Diagnosis Application

Table 1-1 Application list of network test and fault diagnosis

Application Function	
Ping function	ping
	Interactive ping
	grouping
Traceroute function	traceroute
	Interactive traceroute
System debugging function	System debugging

1.2.1. Ping Function

The ping function is used to check the network connection status and whether the host is reachable. The ping function sends the ICMP echo request packet to the host and waits for the ICMP echo response, used to judge whether the destination is reachable. Ping can test the turnaround time from the source to the destination.

Configuration Condition

None

Ping

Table 1-2 ping

Step	Command	Description
Check whether the specified destination address is reachable	ping [vrf vrf-name] {[ip host-name | ip-address] | [ipv6 host-name | ipv6-address] | host-name | ip-address | ipv6-address } [-l packet-length] [-w wait-time] [-n packet-number | -t] [-s src-ip-address]	Mandatory

Interactive ping

Table 1-3 Interactive ping

Step	Command	Description
Enter the ping interactive mode	**ping** [**vrf** *vrf-name*]	Mandatory In the privileged user mode, execute the command to enter the ping interactive mode.
Configure the network protocol type	**Protocol** [**ip**]: [**ip** | **ipv6**]	Optional By default, Use the IPv4 protocol.
Configure the destination IP address or host name	**Target IP address or hostname**: { *ipv6-address* | *ip-address* | *host-name* }	Mandatory
Configure the times of sending the ICMP request packet	**Repeat count** [**5**]: [*repeat-count*]	Optional By default, send for 5 times.
Configure the length of the ICMP request packet	**Datagram size** [**76**]: [*datagram-size*]	Optional The packet length is the size of the whole IP packet. By default, the packet length is 76 bytes.

Step	Command	Description
Configure the timeout for waiting for the ICMP response	**Timeout in seconds** [**2**]: [*timeout*]	Optional By default, time out for 2s.
Enable the extended option	**Extended commands** [**no**]: [**yes** | **no**]	Optional After enabling the extended option, the configuration command of the extended option is available. By default, do not enable the extended option.
Configure the extended option, the source IP address or egress interface of the ICMP request packet	**Source address or interface:** { *ip-address* | *ipv6-address* | *interfacename* }	Optional After enabling the extended option, the command can be configured. By default, do not specify the source address and egress interface of the request packet.
Configure the extended selection, the service type of the ICMP request packet	**Type of service** [**0**]: [*tos*]	Optional Only IPv4 protocol supports the command. After enabling the extended option, the command can be configured. By default, the TOS value is 0.
Configure the extended option, setting not permitting the fragment	**Set DF bit in IP header?** [**no**]: [**yes** | **no**]	Optional Only IPv4 protocol supports the command. After enabling the extended option, the command can be configured. By default, do not set the DF flag, permitting fragment.

Step	**Command**	**Description**
Configure the extended option, validating the data content of the response packet	**Validate reply data?** [**no**]:[**yes** | **no**]	Optional Only IPv4 protocol supports the command. After enabling the extended option, the command can be configured. By default, do not validate the data content.
Configure the extended option, the data content of the ICMP request packet	**Data pattern** [**abcd**]: [*data-pattern*]	Optional After enabling the extended option, the command can be configured. Only IPv4 protocol supports the command. By default, the data content profile is “abcd”.
Configure the extended option, loose source route option, strict source route option, record route, record timestamp, display details	**Loose, Strict, Record, Timestamp, Verbose**[**none**]: [**l | s**] [**r / t / v**]	Optional After enabling the extended option, the command can be configured. Only IPv4 protocol supports the command. By default, do not configure the extended option.
Enable scanning the sent ICMP request packet	**Sweep range of sizes** [**no**]: [**yes** | **no**]	Optional Only IPv4 protocol supports the command. By default, scanning the sent packet is disabled.

Step	Command	Description
Configure the start value of the scanning	**Sweep min size** [**36**]: [*min-szie*]	Optional Only IPv4 protocol supports the command. After enabling scanning the sent packet, the command can be configured. By default, the start value of the scanning is 36.
Configure the end value of the scanning	**Sweep max size** [**18024**]: [*max-size*]	Optional Only IPv4 protocol supports the command. After enabling scanning the sent packet, the command can be configured. By default, the end value of the scanning is 18024
Configure the scanning incremental value	**Sweep interval** [**1**]: [*interval*]	Optional Only IPv4 protocol supports the command. After enabling scanning the sent packet, the command can be configured. By default, the scanning incremental value is 1.

Groupping

Table 1-4 groupping

Step	Command	Description
Send multiple groups of ICMP request packets, checking whether the destination address is reachable	**groupping** [**vrf** *vrf-name*] { *hostname* | *ip-address* } [**-l** packet-length] [**-g** *packet-group*] [**-w** *wait-time*] [**-n** *packet-number*] [**-t**]	Mandatory

Note:

- When pinging the destination host name, first configure the DNS function. Otherwise, ping fails. For DNS configuration, refer to "DNS Configuration" in "IP Network Protocol Configuration".
- For the ping mpls function, refer to "MPLS OAM Configuration".

1.2.2. Traceroute Function

The traceroute function is used to view the gateways passed by the packet from the source to the destination. It is mainly used to check whether the destination is reachable and analyze the faulty network node. The executing process of traceroute is: First send one IP packet with TTL 1 to the destination host; the first-hop gateway drops the packet and returns one ICMP timeout error packet. In this way, traceroute gets the first gateway address in the path. And then traceroute sends one packet with TTL 2. In this way, get the address of the second-hop gateway. Continue the process until reaching the destination host. The UDP port number of the traceroute packet is the port number of the destination that cannot be used by any application program. After the destination receives the packet, return one error packet of the port unreachable. In this way, get all gateway addresses on the path.

Configuration Condition

None

Traceroute

Table 1-5 traceroute

Step	Command	Description
View the gateways passed by the packet from the source to the destination	**traceroute** [**vrf** *vrf-name*] {{**ip** *host-name* | *ip-address*} | {**ipv6** *host-name* | *ipv6-address*} | *host-name* | *ip-address* | *ipv6-address* } [-f start-ttl] [-w wait-time] [-m max-ttl]	Mandatory

Interactive traceroute

Table 1-6 Interactive traceroute

Step	Command	Description
Enter the traceroute interactive mode	**traceroute** [**vrf** *vrf-name*]	Mandatory In the privileged user mode, execute the command to enter the traceroute interactive mode.

Step	Command	Description
Configure the network protocol type	**Protocol** [**ip**]:[**ip** | **ipv6**]	Optional By default, Use the IPv4 protocol.
Configure the destination IP address or host name	**Target IP address or hostname**: { *ip-address* | *ipv6-address* | *host-name* }	Mandatory
Configure the source IP address or egress interface of the traceroute packet	**Source address or interface**: { *ip-address* | *ipv6-address* | *interface-name* }	Optional By default, do not specify the source IP address or egress interface of the packet
Configure the timeout for waiting for each detection packet response	**Timeout in seconds** [**3**]: *timeout*	Optional By default, time out after 3s.
Configure the times of sending the detection packet with the same TTL value	**Probe count** [**3**]: *probe-count*	Optional By default, send for three times.
Configure the minimum TTL value of the detection packet	**Minimum Time to Live** [**1**]: *min-ttl*	Optional By default, the minimum TTL value is 1.
Configure the maximum TTL value of the detection packet	**Maximum Time to Live** [**30**]: *max-ttl*	Optional By default, the maximum TTL value is 30.
Configure the destination UDP port number of the detection packet	**Port Number** [**33434**]: *port-number*	Optional By default, the destination port number is 33434.

Step	Command	Description
Configure the extended option, loose source route option, strict source route option, record route, record timestamp, display details	**Loose, Strict, Record, Timestamp, Verbose**[**none**]: [**l | s**] [**r / t / v**]	Optional Only IPv4 protocol supports the command. By default, do not configure the option.

Note:

- For the traceroute mpls function, refer to “MPLS OAM Configuration”.

1.2.3. System Debugging Function

To help the user diagnose the problem, the most function modules of the device provide the debugging function.

The debugging function has two switch controls:

- The debugging switch of the module, controlling whether to generate the debugging information of the module
- The output switch of the screen, controlling whether to output the debugging information to the terminal

Configuration Condition

None

System Debugging

Table 1-7 System debugging

Step	Command	Description
Open the output switch of the remote login system debugging screen	**terminal monitor**	Optional The remote login includes telnet, ssh and so on. By default, the switch is closed.
Open the output switch of the system debugging screen of the console platform	**configure terminal**	By default, the switch is opened.
Exit the global configuration mode	**exit**	-

Step	Command	Description
Open the debugging switch of the system function module	**debug** { **all** | *module-name* [*option*] }	Optional By default, all debugging switches of the system function modules are closed.

Note:

- The debugging information can be displayed on the terminal only after configuring **debug** module-name option, **terminal monitor** or **logging console** at the same time.
- The generating and output of the debugging information affect the system performance, so when it is necessary, had better use the **debug** module-name option command to open the specified debugging switch. The **debug all** command opens all debugging switches, so we had better not use. After debugging ends, close the corresponding debugging switch in time or use the **no debug all** command to close all debugging switches.

1.2.4. Monitoring and Maintaining of Network Test and Fault Diagnosis

Table 1-8 Monitoring and maintaining of the system test and fault diagnosis

Command	Description
show debugging	Display the function module information of the opened debugging switch in the system.

1.3. Typical Configuration Example of Network Test and Fault Diagnosis

1.3.1. Ping Application

Network Requirement

- Device1 fails to use telnet to log into Device3 and we need to confirm whether the route between Device1 and Device3 is reachable.

Network Topology

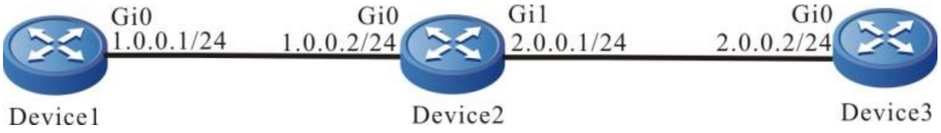


Figure 1-1 ping application networking

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted)

Step 2: Use the ping command to view whether the route between Device1 and Device3 is reachable.

#View whether Device1 and Device3 can ping each other..

```
Device1#ping 2.0.0.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2.0.0.2 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

Step 3: Use the ping command to view whether the route between Device1 and Device2 is reachable.

#View whether Device1 and Device2 can ping each other..

```
Device1#ping 1.0.0.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

Step 4: Use the ping command to view whether the route between Device2 and Device3 is reachable.

#View whether Device2 and Device3 can ping each other..

```
Device2#ping 2.0.0.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2.0.0.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

From the above result, we can see that Device1 and Device2 can communicate with each other, Device2 and Device3 can communicate with each other, and the problem appears between Device1 and Device3. Later, we can check the route configuration, or use the **debug ip icmp** command to view whether the packet content is correct. We also can use traceroute described in the next section to confirm the faulty network node.

1.3.2. Traceroute Application

Network Requirement

- Device1 fails to use telnet to log into Device3 and we need to confirm whether the route between Device1 and Device3 is reachable. If the route is unreachable, we need to confirm the fault of the network node.

Network Topology

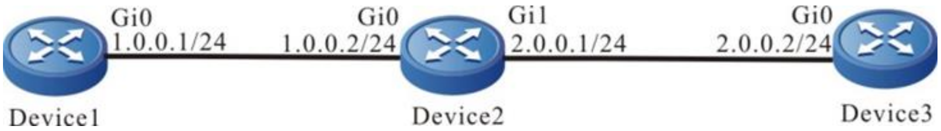


Figure 1-2 Traceroute application networking

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted)

Step 2: Use the **traceroute** command to view whether the route between Device1 and Device3 is reachable.

# View whether Device1 and Device3 can ping each other.

```
Device1#traceroute  2.0.0.2
Type escape sequence to abort.
Tracing the route to 2.0.0.2 , min ttl = 1, max ttl = 30 .

 1  1.0.0.2    0 ms    0 ms    0 ms
 2  *  *      *
 3  *  *      *
 4  *  *      *
 5  *  *      *
 6
```

From the above result, the traceroute packet sent by Device1 can reach Device2. The traceroute packet from Device2 cannot reach Device3. Later, we need to check the route configuration between Device2 and Device3 and line, or use the **debug ip icmp** command to view whether the packet content is correct. We also can use ping described in the last section to detect the connection between Device2 and Device3.

2. KEEPALIVE GATEWAY

2.1. Overview

keepalive gateway sets the Ethernet interface to send the keepalive packet to the specified gateway address, used to monitor the reachability of the destination gateway. When the gateway is unreachable, close the interface IP protocol layer.

After configuring the keepalive gateway on one interface, the interface regularly sends the ARP request packet to the configured gateway address. When the interface does not receive the ARP response packet for successive N times (N is the retry times configured for the user), close the interface IP protocol layer. Until receiving the ARP response packet again, enable the interface IP protocol layer.

2.2. Gateway Keepalive Function Configuration

Table 2-1 Gateway keepalive function configuration list

Configuration Task	
Configure the keepalive gateway function	Configure the keepalive gateway basic function
	Configure the sending parameters of the keepalive packet

2.2.1. Configure Gateway Keepalive Function

Configuration Condition

None

Configure Gateway Keepalive Basic Function

Table 2-2 Configure the gateway keepalive basic function

Step	**Command**	**Description**
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the gateway keepalive	**keepalive gateway** *ip-address* [*interval* { **sec** *interval* | **msec** *interval* }] [*retry retry-count*]	Mandatory By default, do not enable the gateway keepalive function.

Configure Sending Parameters of Keepalive Packet

When configuring the sending parameters of the keepalive packet, we can control the sending rate of the gateway keepalive packet. When the sending rate of the keepalive packet reaches the configured value, pause for the configured time and then continue to send the keepalive packets.

Table 2-3 Configure the sending parameters of the keepalive packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the sending rate of the keepalive packet	**keepalive gateway disperse** [**pkt-rate** *packet-rate*] [**pause-time** *pause-time*]	Optional By default, the maximum sending rate of the keepalive packet is 100pps and the time of pausing sending the keepalive packet is 100ms.

Note:

- Usually, the network equipment has speed limitation for the ARP packet. If there are too many gateway keepalive packets sent at the same time, some keepalive packet may be dropped, seriaouly resulting in the gateway keepalive flapping. You can discretize the sending of the keepalive packet by configuring the sending parameter of the gateway keepalive packet, removing the flapping caused by the speed limitation of the ARP packet when configuring lots of gateway keepalive packets.

2.2.2. Monitoring and Maintaining of Gateway Keepalive

Table 2-4 Monitoring and maintaining of gateway keepalive

Command	Description
clear keepalive gateway statistics [*interface-name*]	Clear the receiving and sending statistics information of the gateway keepalive
show keepalive gateway [*interface-name*]	View the interface enabled with the gateway keepalive and its configuration
show keepalive gateway disperse	View the sending parameter configuration of the gateway keepalive packet
show keepalive gateway statistics [*interface-name*]	View the statistics information of the gateway keepalive

2.3. Typical Configuration Example of Gateway Keepalive

2.3.1. Configure Gateway Keepalive

Network Requirements

- All devices run the OSPF protocol to perform the route interacting.
- The data flow from Device1 to the 201.0.0.0/24 segment first selects the lonk from Switch to Device3.
- The link across Switch between Device1 and Device 3 uses the gateway keepalive function. When Switch fails or Switch link fails, the gateway keepalive fast detects the fault and modifies the interface status to down. After OSPF feels the status change of the interface, switch the route to Device2 for communication.

Network Topology

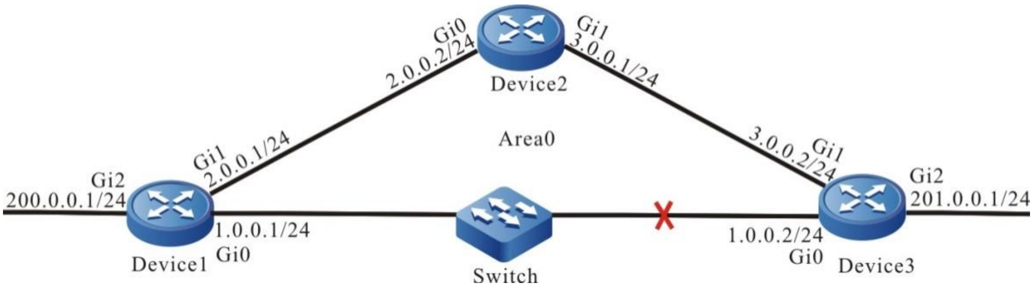


Figure 2-1 Networking of configuring the gateway keepalive

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted)

Step 2: Configure the OSPF process.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
```

```
Device3(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 201.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#View the route table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M -
Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C  1.0.0.0/24 is directly connected, 00:01:28, gigabitethernet0
C  2.0.0.0/24 is directly connected, 03:45:55, gigabitethernet1
O  3.0.0.0/24 [110/2] via 2.0.0.2, 03:44:52, gigabitethernet1
         [110/2] via 1.0.0.2, 00:00:36, gigabitethernet0
C  200.0.0.0/24 is directly connected, 43:03:36, gigabitethernet2
O  201.0.0.1/32 [110/2] via 1.0.0.2, 00:00:36, gigabitethernet0
```

# The data flow from Device1 to the segment 201.0.0.0/24 first selects Device3.

Note:

- The viewing method of Device2 and Device3 is the same as that of Device1, so the viewing process is omitted here.

Step 3: Configure the gateway keepalive.

#Configure Device1.

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#keepalive gateway 1.0.0.2
Device1(config-if-gigabitethernet0)#exit
```

#Configure Device3.

```
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#keepalive gateway 1.0.0.1
Device3(config-if-gigabitethernet0)#exit
```

#View the gateway keepalive information of Device1.

```
Device1#show keepalive gateway
interface gigabitethernet0 gateway 1.0.0.2 time 10s retry 3 remain 3 now UP
```

#View the gateway keepalive information of Device3.

```
Device3#show keepalive gateway
interface gigabitethernet0 gateway 1.0.0.1 time 10s retry 3 remain 3 now UP
```

Step 4: Check the result.

#After Switch fails or Switch link fails, the gateway keepalive fast detects the fault and modifies the interface gigabitethernet0 status to down.

```
Devie1#show keepalive gateway
interface gigabitethernet0 gateway 1.0.0.2 time 10s retry 3 remain 0 now DOWN

Device1#show ip interface gigabitethernet0
gigabitethernet0 is down
 Internet address(es):
  1.0.0.2/24
 Joined group address(es):
  224.0.0.1
 recently lineproto up: 00:40:13 ago
 recently lineproto down: 00:00:41 ago
```

#After OSPF feels the status change of the interface gigabitethernet0, switch the route to Device2 for communication.

```
Device1#show ip ospf interface gigabitethernet 0
gigabitethernet0 is down, line protocol is down
 OSPF is enabled, but not running on this interface

Device1#show ip  route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M -
Management
     D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   2.0.0.0/24 is directly connected, 03:59:32, gigabitethernet1
O   3.0.0.0/24 [110/2] via 2.0.0.2, 03:58:29, gigabitethernet1
C   200.0.0.0/24 is directly connected, 43:17:13, gigabitethernet2
O   201.0.0.1/32 [110/3] via 2.0.0.2, 00:07:00, gigabitethernet1
```

#We can see that the data flow from Device1 to the segment 201.0.0.1/24 first selects the route across Device2.

3. SLA

3.1. Overview

SLA (Service Level Agreements) calculates the related parameters according to the packet transmission and outputs the report at last. SLA, also called RTR (Response Time Reporter), is one network detection and monitoring tool. SLA regularly sends the packets of the specified protocol to detect and monitor the network communication. SLA can diagnose different network applications and output the test result by configuring different types of RTR entities and adjusting.

SLA basic concepts:

- RTR Entity: RTR Entity is one universal concept and not related with the specific type of RTR entity. The current RTR entity types of the system include: ICMP-echo entity, ICMPv6-echo entity, ICMP-path-echo entity, ICMP-path-jitter entity, and UDP-echo entity used to detect the network communication; the VoIP-jitter entity used to detect the VoIP packets transmitted via the network; the FLOW-statistics entity used to detect the interface traffic; the LSP-ping entity used to detect the MPLS network communication; the Bandwidth-measure entity used to detect the interface bandwidth.
- RTR Group: One RTR entity group is the set of one or multiple RTR entities;
- RTR responder: The RTR responder is configured at the destination, mainly used to set up the connection with the source and respond the detection packet sent by the source. Most entities do not need to configure the responder, but when using the UDP-echo entity, VoIP-jitter entity and Bandwidth-measure entity, we should configure the responder.
- RTR Schedule: If only configuring the RTR entity or RTR entity group, we cannot detect, but should initiate the scheduling so that the detection can be completed.

3.2. SLA Function Configuration

Table 3-1 SLA function configuration list

Configuration Task	
Enable RTR	Enable RTR
Configure the RTR entity	Create the RTR entity
	Configure the ICMP-echo entity
	Configure the ICMPv6-echo entity
	Configure the ICMP-path-echo entity
	Configure the ICMP-path-jitter entity
	Configure the VoIP-jitter entity

Configuration Task	
	Configure the UDP-echo entity
	Configure the FLOW-statistics entity
	Configure the LSP-ping entity
	Configure the Bandwidth-measure entity
	Configure the common configuration of the entity
Configure the RTR entity group	Configure the RTR entity group
Configure the RTR responder	Configure the RTR responder
Configure the RTR schedule	Configure the RTR schedule
Configure pausing scheduling the entity	Configure pausing scheduling the entity
Configure restoring scheduling the entity	Configure restoring scheduling the entity

3.2.1. Enable RTR

In the configuration tasks of RTR, first enable RTR so that the configuration of the other functions can take effect.

Configuration Condition

None

Enable RTR

Table 3-2 Enable RTR

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-

Step	Command	Description
Enable RTR	**rtr enable**	Mandatory By default, do not enable RTR.

3.2.2. Configure RTR Entity

Configuration Condition

Before configuring the RTR entity, first complete the following task:

- Enable RTR.

Create RTR Entity

One entity corresponds to one type of detection. After creating the RTR entity and entering the entity configuration mode, we can configure the parameters of the entity.

Table 3-3 Create the RTR entity

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create the RTR entity	**rtr** *entity-id entity-type*	Mandatory

Configure ICMP-echo Entity

The ICMP-echo entity is to detect the network communication. It regularly sends the ICMP echo request packet to one destination address in the network, so as to get the delay and packet loss of the packet transmission from the detection end to the destination end. In one detection period, as long as the ICMP-echo entity receives one ICMP echo request response packet, the entity status is reachable.

The general network devices all support ping, so the entity can take effect in detecting the network communication. With the rich scheduling policies and log recording function, we can let the network administrator get to know the network communication status and history information in time and reduce inputting the common ping command frequently at the same time.

Table 3-4 Configure the ICMP-echo entity

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-

Step	Command	Description
Enter the ICMP-echo entity configuration mode	**rtr** *entity-id* [**icmpecho**]	-
Configure the detection attribute	**set** [**vrf** *vrf-name*] *target-ip-address* [*npacket*] [*data-size*] [*timeout*] [*frequency-value*] [**extend** *source-ip-address* [*tos*] [*set-DF*] [*verify-data*]]	Mandatory By default, do not configure the detection attribute of the entity.
Configure the rtt value as a criterion to determine whether an entity is reachable	**status-care rtt**	Optional By default, do not use the rtt value to judge whether an entity is reachable.
Configure the pktloss value as a criterion to determine whether an entity is reachable	**status-care pktloss**	Optional By default, do not use the pktloss value to judge whether an entity is reachable.
Configure the common configuration of the entity	Refer to “Configure Common Configuration of the Entity”	Optional

Note:

- The scheduling interval (frequency-value) of the ICMP-echo entity needs to meet the following requirement: scheduling interval > npacket * timeout
- If configuring the scheduler for the entity, the age time of the scheduler should be larger than the scheduling interval of the entity.

Configure ICMPV6-echo Entity

The ICMPv6-echo entity is to detect the network communication. It regularly sends the ICMPv6 echo request packet to one destination address in the network, so as to get the delay and packet loss of the packet transmission from the detection end to the destination end. In one detection period, as long as the ICMPv6-echo entity receives one ICMPv6 echo request response packet, the entity status is reachable.

The general network devices all support ping, so the entity can take effect in detecting the network communication. With the rich scheduling policies and log recording function, we can let the network administrator get to know the network communication status and history information in time and reduce inputting the common ping command frequently at the same time.

Table 3-5 Configure the ICMPV6-echo entity

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the ICMPv6-echo entity configuration mode	**rtr** *entity-id* [**icmpv6echo**]	-
Configure the detection attribute	**set** [**vrf** *vrf-name*] *target-ip-address* [*npacket*] [*data-size*] [*timeout*] [*frequency-value*] [**extend** *source-ip-address* [*tos*] [*verify-data*]]	Mandatory By default, do not configure the detection attribute of the entity.
Configure the rtt value as a criterion to determine whether an entity is reachable	**status-care rtt**	Optional By default, do not use the rtt value to judge whether an entity is reachable.
Configure the pktloss value as a criterion to determine whether an entity is reachable	**status-care pktloss**	Optional By default, do not use the pktloss value to judge whether an entity is reachable.
Configure the common configuration of the entity	Refer to “Configure Common Configuration of the Entity”	Optional

Note:

- The scheduling interval (frequency-value) of the ICMPv6-echo entity needs to meet the following requirement: scheduling interval > npacket * timeout
- If configuring the scheduler for the entity, the age time of the scheduler should be larger than the scheduling interval of the entity.

Configure ICMP-path-echo Entity

The ICMP-path-echo entity is to detect the network communication. It regularly sends the ICMP echo request packet to one destination address in the network, so as to get the delay and packet loss of the packet transmission from the detection end to the destination end, as well as the delay and packet loss between the detection end and the intermediate devices from the detection end to the destination. In one detection period, as long as the ICMP-path-echo entity receives one ICMP echo request response packet, the entity status is reachable.

The general network devices all support ping, so the entity can take effect in detecting the network communication. With the rich scheduling policies and log recording function, we can let the network administrator get to know the network communication status (for example, which network device on the path has serious delay) and history information in time.

Table 3-6 Configure the ICMP-path-echo entity

Step	Command	Description
Enter the system configuration mode	**configure terminal**	-
Enter the ICMP-path-echo entity configuration mode	**rtr** *entity-id* [**icmp-path-echo**]	-
Configure the detection attribute	**set dest-ipaddr** *target-ip-address* [**source-ipaddr** *source-ip-address*]	Mandatory
Configure the loose source route selection	**lsr-path** [*hop-ip-address-list* | **none**]	Optional By default, do not configure the loose source route selection.
Configure only detecting the network status from the source to the destination	**targetOnly** [**true | false**]	Optional By default, if targetOnly is true, only detect the network status from the source to the destination. If targetOnly is false, detect the network status from the source to the destination hop by hop.
Configure whether to verify the content of the response packet	**verify-data** [**true | false**]	Optional By default, do not verify the data content.
Configure the common configuration of the entity	Refer to “Configure Common Configuration of the Entity”	Optional

Configure ICMP-path-jitter Entity

The ICMP-path-jitter entity is to detect the network communication. It regularly sends the ICMP echo request packet to one destination address in the network, so as to get the delay, jitter, and packet loss of the packet transmission from the detection end to the destination end, as well as the delay, jitter and packet loss between the detection end and the intermediate devices from the detection end to the destination. In one detection period, as long as the ICMP-path-jitter entity receives one ICMP echo request response packet, the entity status is reachable.

The general network devices all support ping, so the entity can take effect in detecting the network communication. With the rich scheduling policies and log recording function, we can let the network administrator get to know the network communication status (for example, which network device on the path has serious delay) and history information in time.

Table 3-7 Configure the ICMP-path-jitter entity

Step	Command	Description
Enter the system configuration mode	**configure terminal**	-
Enter the ICMP-path-jitter configuration mode	**rtr** *entity-id* [**icmp-path-jitter**]	-
Configure the detection attribute	**set dest-ipaddr** *target-ip-address* [*pkt-number*] [*pkt-interval*] [**source-ipaddr** *source-ip-address*]	Mandatory
Configure the IP address of the loose source route selection	**lsr-path** [*hop-ip-address-list* | **none**]	Optional By default, do not configure the loose source route selection.
Configure only detecting the network status from the source to the destination	**targetOnly** [**true** | **false**]	Optional By default, if targetOnly is true, only detect the network status from the source to the destination. If targetOnly is false, detect the network status from the source to the destination hop by hop.
Configure the jitter threshold and over-limit rule	**threshold-jitter** *jitter* **direction** { **be | se** }	Optional By default, the jitter threshold is 6000ms and the over-limit rule is be.
Configure whether to verify the content of the response packet	**verify-data** [**true | false**]	Optional By default, do not verify the data content.

Step	Command	Description
Configure the common configuration of the entity	Refer to “Configure Common Configuration of the Entity”	Optional

Note:

- When the over-limit rule is be and the actual value is larger than or equal to the threshold, it judged as over-limit; when the over-limit rule is se and the actual value is smaller than or equal to the threshold, it is judged as over-limit.

Configure VoIP-jitter Entity

The VoIP-jitter entity is the RTR entity used to measure the transmission quality of the VoIP packet in the general IP network.

The VoIP-jitter entity can simulate the G.711 A Law, G.711 mu Law, and G.729A codec or the customized codes to send the UDP packet with the corresponding rate, packet interval and size from the source device to the destination device, measure the turnaround time, uni-directional packet loss and uni-directional delay of the packet, and calculates the ICPIF value based on the statistics information. At last, estimate the MOS value according to the ICPIF value. In the detection period, as long as the VoIP-jitter entity receives one detection response packet, the status of the entity is reachable.

Table 3-8 Configure the VoIP-jitter entity

Step	Command	Description
Enter the system configuration mode	**configure terminal**	-
Enter the VoIP-jitter configuration mode	**rtr** *entity-id* [**jitter**]	Mandatory If the entity already exists, directly enter the entity configuration mode.
Configure the detection attribute	**set dest-ipaddr** *target-ip-address* **dest-port** *target-port* { **g711alaw** | **g711ulaw** | **g729a** | **user_defined** *packet-size packet-number packet-interval schedule-interval* } [**source-ipaddr** *source-ip-address*] [**source-port** *source-port*]	Mandatory

Step	Command	Description
Configure the uni-directional delay threshold from the source to the destination and over-limit rule	**threshold-sd-delay** *sd-delay* **direction** { **be | se** }	Optional By default, the sd delay threshold is 5000ms and the over-limit rule is be.
Configure the uni-directional jitter threshold from the source to the destination and over-limit rule	**threshold-sd-jitter** *sd-jitter* **direction** { **be** | **se** }	Optional By default, the sd jitter threshold is 6000ms and the over-limit rule is be.
Configure the packet loss threshold and over-limit rule from the source to the destination	**threshold-sd-pktloss** *sd-packet* **direction** { **be** | **se** }	Optional By default, the sd packet loss threshold is 60000 and the over-limit rule is be.
Configure the uni-directional delay threshold from the destination to the source and over-limit rule	**threshold-ds-delay** *ds-delay* **direction** { **be** | **se** }	Optional By default, the ds delay threshold is 5000ms and the over-limit rule is be.
Configure the uni-directional jitter threshold from the destination to the source and over-limit rule	**threshold-ds-jitter** *ds-jitter* **direction** { **be** | **se** }	Optional By default, the ds unit-directional jitter threshold is 6000ms and the over-limit rule is be.
Configure the packet loss threshold from the destination to the source and over-limit rule	**threshold-ds-pktloss** *ds-packet* **direction** { **be** | **se** }	Optional By default, the ds packet loss threshold is 60000 and the over-limit rule is be.
Configure the icpif threshold and the over-limit rule	**threshold-icpif** *icpif-value* **direction** { **be** | **se** }	Optional By default, the icpif threshold is 100000000 and the over-limit rule is be.

Step	Command	Description
Configure the mos threshold and the over-limit rule	**threshold-mos** *mos-value* **direction** { **be** | **se** }	Optional By default, the mos threshold is 10000000 and the over-limit rule is be.
Configure the common configuration of the entity	Refer to “Configure Common Configuration of the Entity”	Optional

Note:

- When using the VoIP-jitter entity detection, besides configuring the VoIP-jitter entity, we also need to configure the RTR responder at the destination.
- By default, the VoIP-jitter entity sends many packets, which occupy the network bandwidth, so when configuring the entity exceeds one hour, the shell prompts.
- When the VoIP-jitter entity detects the network transmitting the VoIP packet, the clocks of the source and the destination need to be consistent, so before scheduling the VoIP-jitter entity, we also need to configure the NTP server at the destination and NTP client at the source. After the clocks are synchronized, configure the RTR responder, and at last, configure the scheduler. For the configuration of NTP, refer to the NTP chapter of the configuration manual.

When the over-limit rule is be and the actual value is larger than or equal to the threshold, it judged as over-limit; when the over-limit rule is se and the actual value is smaller than or equal to the threshold, it is judged as over-limit.

Configure UDP-echo Entity

The UDP-echo entity mainly detects the UDP packet transmitted in the IP network. In the entity, we need to specify the destination address and port of the sent packet. We can monitor the transmission of the UDP packet in the IP network by scheduling the entity. In one detection period, as long as the UDP-echo entity receives one detection response packet, the entity status is reachable.

The UDP-echo entity can monitor efficiently to record the turnaround delay, packet loss and other information of the UDP packet in the IP network, even record the monitored history information by logs so that the network administrator can get to know the network communication and fix the fault.

Table 3-9 Configure the UDP-echo entity

Step	Command	Description
Enter the system configuration mode	**configure terminal**	-

Step	Command	Description
Enter the UDP-echo entity configuration mode	**rtr** *entity-id* [**udp-echo**]	Mandatory If the entity already exists, directly enter the entity configuration mode.
Configure the detection attribute	**set dest-ipaddr** *target-ip-address* **dest-port** *target-port* [**source-ipaddr** *source-ip-address*] [**source-port** *source-port*]	Mandatory By default, do not configure the detection attribute of the UDP-echo entity.
Configure the filling content of the packet	**data-pattern** *pad*	Optional By default, the filling content is "ABCD".
Configure the common configuration of the entity	Refer to "Configure Common Configuration of the Entity"	Optional

Note:

- When using the UDP-echo entity detection, besides configuring the UDP-echo entity, we also need to configure the RTR responder at the destination.

Configure FLOW-statistics Entity

The FLOW-statistics entity is to detect the interface traffic and one entity corresponds to one interface. We can monitor the traffic on the interface by scheduling the entity. In one detection period, as long as there are packets passing the interface monitored by the FLOW-statistics entity, the entity status is reachable.

The interval of the FLOW-statistics entity monitoring the interface traffic is 10s-10min. We can record the traffic peak value information on the interface by monitoring, even can record the history information of the traffic statistics during each monitoring, so as to make the network administrator get to know the network communication status and fix the fault.

Table 3-10 Configure the FLOW-statistics entity

Step	Command	Description
Enter the system configuration mode	**configure terminal**	-

Step	Command	Description
Enter the FLOW-statistics entity configuration mode	**rtr** *entity-id* [**flow-statistics**]	Mandatory If the entity already exists, directly enter the entity configuration mode.
Configure the detection attribute	**flow-statistics interface** *interface-name* **interval** *interval*	Mandatory
Configure the traffic threshold received by the interface and the over-limit rule	**threshold-inflow** *flow-value* **direction** { **be** | **se** }	Optional By default, the traffic threshold received by the interface is 200000000bps (bit/s) and the over-limit rule is be.
Configure the threshold of the packets received by the interface and the over-limit rule	**threshold-inpacket** *packet-value* **direction** { **be** | **se** }	Optional By default, the threshold of the packets received by the interface is 200000000 and the over-limit rule is be.
Configure the threshold of the traffic received by the interface and the over-limit rule	**threshold-outflow** *flow-value* **direction** { **be** | **se** }	Optional By default, the traffic threshold sent by the interface is 200000000 bps (bit/s) and the over-limit rule is be.
Configure the threshold of the packets received by the interface and over-limit rule	**threshold-outpacket** *packet-value* **direction** { **be** | **se** }	Optional By default, the threshold of the packets received by the interface is 200000000 and the over-limit rule is be.
Configure the common configuration of the entity	Refer to “Configure Common Configuration of the Entity”	Optional

Note:

- When the over-limit rule is be and the actual value is larger than or equal to the threshold, it judged as over-limit; when the over-limit rule is se and the actual value is smaller than or equal to the threshold, it is judged as over-limit.

Configure LSP-ping Entity

The LSP-ping entity is used to detect and maintain the fault in the MPLS network. LSP-ping provides one mechanism to detect the end-to-end LSP connection and the consistency of the control layer and data layer. The detected LSP type includes the LSP set up by LDP, BGP, and RSVP-TE. In one detection period, the LSP-ping entity status is reachable as long as receiving one echo response packet.

Table 3-11 Configure the LSP-ping entity

Step	Command	Description
Enter the system configuration mode	**configure terminal**	-
Enter the LSP-ping entity configuration mode	**rtr** *entity-id* [**lsp-ping**]	Mandatory If the entity already exists, directly enter the entity configuration mode.
Configure the detection attribute	**set fec** { **ipv4** *prefix-address prefix-mask-length* | **traffic-eng tunnel** *tunnel-interface-number* | **vrf** *vrf-name* **ipv4** *prefix-address prefix-mask-length* }	Mandatory By default, do not configure the detection attributes of the LSP-ping entity.
Configure the EXP field value in the MPLS label of the echo request packet	**exp** *exp-bits*	Optional By default, the value of the EXP field is 0.
Configure the sending interval of the echo request packets	**interval** *interval-value*	Optional By default, the sending interval of the echo request packet is 0ms.
Configure the repeat sending times of the echo request packets in one scheduling	**repeat** *repeat-count*	Optional By default, the repeat sending times of the echo request packets in one scheduling is 5.

Step	Command	Description
Configure the echo request packet length	**request-packet-size** *packet-size*	Optional By default, the echo request packet length is 120 bytes.
Configure the TTL value of the outer label of the echo request packet	**ttl** *ttl-value*	Optional By default, the TTL value of the outer label of the echo request packet is 255.
Configure the common configuration of the entity	Refer to "Configure Common Configuration of the Entity"	Optional

Configure Bandwidth-measure Entity

The Bandwidth-measure entity is an RTR entity used to measure network bandwidth. At present, the bandwidth detection module supports point-to-point links, and the source and destination must be L3 physical interfaces, rather than logical interfaces such as sub interfaces and loopback interfaces.

When the client requests bandwidth detection, it will send the bandwidth detection parameters to the server. The server determines whether other bandwidth detection tasks are running. If so, it returns that bandwidth detection is not allowed.

The client of the Bandwidth-measure entity sends a detection request to the server and tells the server some parameters of the detection through the TLV message. After the server responds, it starts to send the detection packet. The server calculates the bandwidth value according to the number of packets received per unit time, and notifies the detection result to the client through the TLV message.

Table 3-12 Configure the Bandwidth-measure entity

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter Bandwidth-measure entity configuration mode	**rtr** *entity-id* [**bandwidth-measure**]	Mandatory If the entity already exists, directly enter the entity configuration mode.

Step	Command	Description
Configure the detection attributes	**set** *target-ip-addresss target-port* {*measure-time*}	Mandatory By default, do not configure the detection attribute of the bandwidth-measure entity.
Configure the common configuration of the entity	Refer to "Configure Common Configuration of the Entity"	Optional

Note:

- When using bandwidth measure entity detection, in addition to configuring the bandwidth measure entity, you also need to configure the RTR transponder at the destination.

Configure Common Configuration of Entities

Table 3-13 Configure the common configuration of the entities

Step	Command	Description
Configure the alarm type	**alarm-type** [**log** | **log-and-trap** | **trap** | **none**]	Optional By default, the alarm mode is none, that is, do not alarm. The entity not supporting the command: Bandwidth-measure entity
Configure the number of the saved history records	**number-of-history-kept** *history-number*	Optional By default, save one history record.
Configure the period of saving the history records	**periods** *periods*	Optional By default, after each scheduling ends, save one history record. The entity not supporting the command: Bandwidth-measure entity

Step	Command	Description
Configure the timeout	**timeout** *timeout*	Optional By default, the timeout is: ICMP-path-echo entity 5000ms ICMP-path-jitter entity 5000ms VoIP-jitter entity 50000ms UDP-echo entity 5000ms LSP-ping entity 2s Bandwidth-measure entity 1s The entity not supporting the command: ICMP-echo entity ICMPv6-echo entity FLOW-statistics entity
Configure the TOS value of the packet	**tos** *tos-value*	Optional By default, the TOS value is 0. The entity not supporting the command: ICMP-echo entity ICMPv6-echo entity LSP-ping entity FLOW-statistics entity Bandwidth-measure entity
Configure the VRF attribute of the entity	**vrf** *vrf-name*	Optional By default, do not configure the VRF attribute of the entity. The entities not supporting the command: ICMP-echo entity ICMPv6-echo entity LSP-ping entity FLOW-statistics entity

Step	Command	Description
Configure the scheduling interval of the entity	**frequency** *seconds*	Optional By default, the scheduling interval is: ICMP-path-echo entity 60s ICMP-path-jitter entity 60s UDP-echo entity 60s LSP-ping entity 20s Bandwidth-measure entity 1 minute The entities not supporting the command: ICMP-echo entity ICMPv6-echo entity VoIP-jitter entity FLOW-statistics entity
Configure the length of the detection packet	**request-data-size** *data-size*	Optional By default, the length of the detection packet: ICMP-path-echo entity 70 bytes ICMP-path-jitter entity 70 bytes UDP-echo entity 16 bytes Bandwidth-measure entity 1400 bytes The entities not supporting the command: ICMP-echo entity ICMPv6-echo entity VoIP-jitter entity LSP-ping entity FLOW-statistics entity

Step	Command	Description
Configure the packet loss threshold and the over-limit rule	**threshold-pktloss** *pktloss* **direction** { **be | se** }	Optional By default, the packet loss threshold: ICMP-echo entity 150 ICMPv6-echo entity 150 ICMP-path-echo entity 1 ICMP-path-jitter entity 100 UDP-echo entity 1 LSP-ping entity 200000000 The over-limit rule is be. The entities not supporting the command: VoIP-jitter entity FLOW-statistics entity Bandwidth-measure entity
Configure the bi-directional delay threshold and the over-limit rule	**threshold-rtt** *rtt* **direction** { **be | se** }	Optional By default, the bi-directional delay threshold is: ICMP-echo entity 9000ms ICMPv6-echo entity 9000 ms ICMP-path-echo entity 9000ms ICMP-path-jitter entity 9000ms VoIP-jitter entity 9000ms UDP-echo entity 9000ms LSP-ping entity 9000ms The over-limit rule is be. The entities not supporting the command: FLOW-statistics entity Bandwidth-measure entity

Note:

- If the RTR entity already exists and the entity is in the un-scheduled state, execute the **rtr** *entity-id* command to enter the entity configuration mode directly.

- When the over-limit rule is be and the actual value is larger than or equal to the threshold, it judged as over-limit; when the over-limit rule is se and the actual value is smaller than or equal to the threshold, it is judged as over-limit.
- The scheduling interval of the ICMP-path-echo entity needs to meet the following requirement: scheduling interval > timeout.
- The scheduling interval of the ICMP-path-jitter entity needs to meet the following requirement: scheduling interval > timeout; timeout needs to meet the following requirement: timeout > pkt-number * pkt-interval; For the pkt-number parameter and the pkt-interval parameter, refer to the set command of the ICMP-path-echo entity.
- The scheduling interval of the UDP-echo entity needs to meet the following requirement: scheduling interval > timeout + 5.
- The scheduling interval of the LSP-ping entity needs to meet the following requirement: scheduling interval >= (interval + timeout)*repeat + 5.

3.2.3. Configure RTR Entity Group

One RTR entity group is the set of one or multiple RTR entity groups. One RTR entity can belong to multiple RTR entity groups and the group cannot become the member of the group. One group can only contain one member once. The RTR entity group is identifies by the group ID uniquely and the group name is automatically generated by the system.

The RTR entity group is mainly to schedule one RTR set. The scheduling for the RTR entity group is equivalent to the scheduling for all RTR entities in the RTR entity group. The detection result is saved in the history records of the RTR entity.

Configuration Condition

Before configuring the RTR entity group, first complete the following task:

- Enable RTR.

Configure RTR Entity Group

Table 3-14 Configure the RTR entity group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the configuration mode of the RTR entity group	**rtr group** *group-id*	Mandatory If the RTR entity group does not exist, automatically create the entity group.
Add the members in the RTR entity group	**member** *entity-list*	Optional By default, the RTR entity group does not contain any member.

Step	Command	Description
Configure the options of the RTR entity group	**option** { **or** | **and** }	Optional By default, the status option of the RTR entity group is and (when all entities in the group are reachable, the group status can be reachable)
Configure the scheduling interval between the members in the RTR entity group	**interval** *interval*	Optional By default, the scheduling interval of the members in the group is 0s.
Configure the RTR entity group to generate the scheduler automatically	**group probe**	Optional By default, do not configure the RTR entity group to generate the scheduler automatically.

Note:

- One VoIP-jitter entity or UDP-echo entity cannot be added to multiple groups for scheduling. Otherwise, the scheduling result may be wrong.
- The calculation method for the scheduling interval of the RTR entity group is as follows: scheduling interval = the maximum of all member scheduling intervals + (member quantity - 1) * scheduling interval between the members.
- The members of the RTR entity group do not support the Bandwidth-measure entity member.

3.2.4. Configure RTR Responder

The RTR responder is mainly used to set up the connection with the source end and respond the detection packets sent by the source end, so as to ensure that the detection result is correct. The VoIP-jitter entity, the UDP-echo entity, and the Bandwidth-measure entity need to set up the connection with the destination end, so we should configure the RTR responder at the destination end.

Configuration Condition

Before configuring the RTR responder, first complete the following task:

- Enable RTR.

Configure RTR Responder

Table 3-15 Configure the RTR responder

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the RTR responder	**rtr responder**	Mandatory By default, do not configure the RTR responder.

3.2.5. Configure RTR Scheduler

The RTR scheduler is the policy of the scheduling detection for the RTR entity or group. The RTR scheduler can take one entity member as the object and also can take one RTR entity group as the object, but cannot take the group and entity as the object together. The RTR scheduler is identified by the schedule ID uniquely and not related with the RTR entity type, but the scheduling interval should consider the attributes of the scheduled RTR entity or the members in the RTR entity group. The RTR scheduler provides rich scheduling policies and can select to schedule at once or start to schedule after some time, even can set the absolute time of starting the scheduling. Besides, the scheduler can automatically demise after the set scheduling times and also can always exist.

Configuration Condition

Before configuring the RTR scheduler, first complete the following task:

- Configure the desired RTR entity or RTR entity group

Configure RTR Scheduler

Table 3-16 Configure the RTR scheduler

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the RTR scheduler, scheduling one entity or group	**rtr schedule** *schedule-id* { **entity** *entity-id* | **group** *group-id* } **start** { *hh*:*mm* [:*ss*] *date month year* | **after** *hh*:*mm* [:*ss*] | **now** } **ageout** *ageout-time* **life** { **forever** | *life-time* **repeat** *repeat-times* }	Mandatory By default, do not configure the RTR scheduler.

Note:

- The age time of the RTR scheduler should be larger than the scheduling interval of the scheduling object. Otherwise, after one scheduling, the scheduler is deleted because of aging and timeout.

3.2.6. Configure Pausing Scheduling Entity

For the entity being scheduled, we can configure pausing scheduling the entity.

Configuration Condition

Before configuring pausing scheduling the entity, first complete the following task:

- The entity is being scheduled

Configure Pausing Scheduling Entity

Table 3-17 Configure pausing scheduling the entity

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure pausing scheduling the entity	**rtr** *entity-id* **halt**	Optional By default, do not pause the scheduling entity.

Note:

- Only one entity can configure **rtr halt**. If the entity is the member of the RTR entity group, we cannot configure **rtr halt.**
- After configuring **rtr halt** and if still not configuring **rtr resume** before the scheduling period ends, the scheduler of scheduling the entity is deleted because of aging and timeout.
- **Bandwidth-measure** entity does not support the function.

3.2.7. Configure Restoring Scheduling Entity

For the entity paused scheduling, we can configure restoring scheduling the entity.

Configuration Condition

Before configuring restoring scheduling the entity, first complete the following task:

- The entity is in the paused scheduling state

Configure Restoring Scheduling Entity

Table 3-18 Configure restoring scheduling the entity

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure restoring scheduling the entity	**rtr** *entity-id* **resume**	Optional

Note:

- **Bandwidth-measure** entity does not support the function

3.2.8. SLA Monitoring and Maintaining

Table 3-19 SLA Monitoring and Maintaining

Command	Description
show rtr entity [*entity-id*]	Display the RTR entity information
show rtr group [*group-id*]	Display the information of the RTR entity group
show rtr history *entity-id*	Display the history record information of the specified RTR entity
show rtr schedule [*schedule-id*]	Display the information of the RTR scheduler

3.3. SLA Typical Configuration Example

3.3.1. Configure ICMP-echo Entity to Detect Basic Network Communication

Network Requirement

- Use the ICMP-echo entity on Device1, detecting the basic communication of the network from Device1 to Device3.

Network Topology

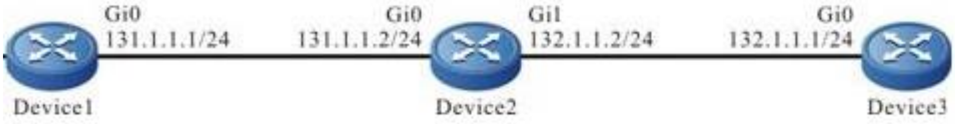


Figure 3-1 Networking of configuring ICMP-echo entity

Configuration Steps

Step 1: Configure the IP address and route of the interface, making Device1 and Device3 communicate with each other. (Omitted)

Step 2: Configure the ICMP-echo entity and add the attribute parameters.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmpecho
Device1(config-rtr-icmpecho)#set 132.1.1.1 5 70 2 12 extend 131.1.1.1 0 TRUE FALSE
Device1(config-rtr-icmpecho)#alarm-type log
Device1(config-rtr-icmpecho)#number-of-history-kept 255
Device1(config-rtr-icmpecho)#threshold-pktLoss 10 direction be
Device1(config-rtr-icmpecho)#threshold-rtt 1000  direction be
```

```
Device1(config-rtr-icmpecho)#exit
```

#View the ICMP-echo entity parameters.

```
Device1#show rtr entity 1
-------------------------------------------------------------
ID:1          name:IcmpEcho1        Created:TRUE
***************type:ICMPECHO***************
CreatedTime:WED OCT 31 14:49:31 2012
LatestModifiedTime:WED OCT 31 14:53:53 2012
Times-of-schedule:0
TargetIp:132.1.1.1
Transmit-packets:5
Totally-send-packets:0
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceIp:131.1.1.1     tos:0   DF(DON'T FRAG):TRUE    Verify-data:FALSE
In-scheduling:FALSE
Schedule frequency:12(s)
Status:DEFAULT
```

The result shows that the entity parameters are consistent with the configuration..

In-scheduling: FALSE indicates that the entity is not scheduled.

Status: DEFAULT indicates that the entity status is DEFAULT.

Note:

- When the entity is not scheduled, the status is DEFAULT; when the entity is scheduled and if the entity is reachable, the status is REACHABLE; if the entity is unreachable, the status is UNREACHABLE.

Step 3: Schedule the defined ICMP-echo entity and define the attribute parameters of the scheduling.

#Configure Device1

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life forever
```

Step 4: Check the result.

1. When the network connectivity from Device1 to Device3 is normal:

#View the entity status.

```
Device1#show rtr entity 1
------------------------------------------------------------
ID:1          name:IcmpEcho1        Created:TRUE
****************type:ICMPECHO****************
CreatedTime:WED OCT 31 14:49:31 2012
LatestModifiedTime:WED OCT 31 14:53:53 2012
Times-of-schedule:1
Time-of-last-schedule:WED OCT 31 14:54:07 2012
TargetIp:132.1.1.1
Transmit-packets:5
Totally-send-packets:5
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceIp:131.1.1.1    tos:0   DF(DON'T FRAG):TRUE    Verify-data:FALSE
In-scheduling:TRUE
multi-notify:OFF
Schedule frequency:12(s)
Status:REACHABLE
```

In-scheduling: TRUE indicates that the entity is being scheduled;

Status: REACHABLE indicates that the entity status is reachable, that is, the network connection from Device1 to Device3 is normal.

2. When the network connectivity from Device1 to Device3 is faulty:

The alarm mode is configured as log, so when the network is disconnected, print the alarm information on the device, as follows:

```
%SLA-4:Rtr 1 (ICMPECHO) rtt [9000ms] was exceeded(>=) threshold [1000ms].
```

#View the entity status.

```
Device1#show rtr entity 1
```

```
-------------------------------------------------------------
ID:1        name:IcmpEcho1      Created:TRUE
***************type:ICMPECHO***************
CreatedTime:WED OCT 31 14:49:31 2012
LatestModifiedTime:WED OCT 31 14:53:53 2012
Times-of-schedule:4
Time-of-last-schedule:WED OCT 31 14:54:43 2012
TargetIp:132.1.1.1
Transmit-packets:5
Totally-send-packets:20
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceIp:131.1.1.1    tos:0   DF(DON'T FRAG):TRUE    Verify-data:FALSE
In-scheduling:TRUE
Schedule frequency:12(s)
Status:UNREACHABLE
```

In-scheduling: TRUED indicates that the entity is being scheduled;

Status: UNREACHABLE indicates that the entity status is unreachable, that is, the network connection from Device1to Device3 is unreachable.

#View the history record content.

```
Device1#show rtr history 1
-------------------------------------------------------------
ID:1   Name:IcmpEcho1  CurHistorySize:4      MaxHistorysize:255
History recorded as following:
WED OCT 31 14:54:46 2012
     PktLoss:5       ,Rtt:invalid
WED OCT 31 14:54:32 2012
     PktLoss:0       ,Rtt:11      (ms)
WED OCT 31 14:54:20 2012
     PktLoss:0       ,Rtt:2       (ms)
```

```
WED OCT 31 14:54:07 2012
        PktLoss:0        ,Rtt:2        (ms)
```

In the history records, record the packet loss and delay of each scheduling; if Rtt is invalid, it indicates that there is fault in the network and the network is reachable.

3.3.2. Configure ICMP-path-echo Entity to Detect Network Communication

Network Requirement

- Use the ICMP-path-echo entity on Device1, detecting the path network communication from Device1 to Device3.

Network Topology

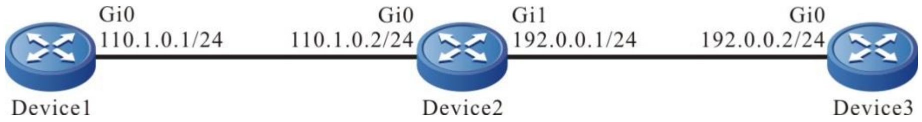


Figure 3-2 Networking of configuring the ICMP-path-echo entity

Configuration Steps

Step 1: Configure the IP address and route of the interface, making Device1, Device2, and Device3 communicate with each other. (Omitted)

Step 2: Configure the ICMP-path-echo entity and add the attribute parameters.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmp-path-echo
Device1(config-rtr-icmppathecho)#set dest-ipaddr 192.0.0.2 source-ipaddr 110.1.0.1
Device1(config-rtr-icmppathecho)#number-of-history-kept 255
Device1(config-rtr-icmppathecho)#targetOnly false
Device1(config-rtr-icmppathecho)#exit
```

# View the ICMP-path-echo entity parameters.

```
Device1#show rtr entity 1
-------------------------------------------------------------
ID:1          name:IcmpPathEcho1          Created:TRUE
***************type:ICMPPATHECHO***************
CreatedTime:WED OCT 24 10:18:02 2012
LatestModifiedTime:WED OCT 24 10:19:09 2012
Times-of-schedule:0
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:1 (each hop)
Request-data-size:70
```

```
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:FALSE
Status:DEFAULT
-------------------------------------------------------------
```

The result shows that the entity parameters are consistent with the configuration..

In-scheduling: FALSE indicates that the entity is not scheduled.

Status: DEFAULT indicates that the entity status is DEFAULT.

Step 3: Schedule the defined ICMP-path-echo entity and define the attribute parameters of the scheduling.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life 600 repeat 10
```

Step 4: Check the result.

#View the entity status.

```
Device1#show rtr entity 1
-------------------------------------------------------------
ID:1        name:IcmpPathEcho1           Created:TRUE
***************type:ICMPPATHECHO***************
CreatedTime:WED OCT 24 10:18:02 2012
LatestModifiedTime:WED OCT 24 10:19:09 2012
Times-of-schedule:1
Time-of-last-schedule:WED OCT 24 10:20:01 2012
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:1 (each hop)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
```

```
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:TRUE
Status:REACHABLE
```

In-scheduling: TRUE indicates that the entity is being scheduled.

Status: REACHABLE indicates that the entity status is reachable, that is, the network connection from Device1to Device3 is normal.

#View the history record content.

```
Device1#show rtr history 1
-----------------------------------------------------------------
ID:1    Name:IcmpPathEcho1
History of hop-by-hop:
 110.1.0.2      PktLoss:0       ,Rtt:2        (ms)
 192.0.0.2      PktLoss:0       ,Rtt:1        (ms)
History of record from source to dest:
CurHistorySize:1       MaxHistorysize:255
WED OCT 24 10:20:01 2012
        PktLoss:0       ,Rtt:1        (ms)
```

In the history records, record the packet loss and delay of each scheduling.

#Wait for some time and after scheduling for 10 times, view the entity status.

```
Device1#show rtr entity 1
-----------------------------------------------------------------
ID:1          name:IcmpPathEcho1            Created:TRUE
***************type:ICMPPATHECHO***************
CreatedTime:WED OCT 24 10:18:02 2012
LatestModifiedTime:WED OCT 24 10:19:09 2012
Times-of-schedule:10
Time-of-last-schedule:WED OCT 24 10:29:01 2012
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:1 (each hop)
Request-data-size:70
Timeout:5000(ms)
```

```
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:FALSE
Status:DEFAULT
```

After scheduling for 10 times, the scheduling stops and the entity status is DEFAULT.

3.3.3. Configure ICMP-path-jitter Entity to Detect Network Communication

Network Requirement

- Use the ICMP-path-jitter entity on Device1, detecting the path network communication from Device1 to Device3.

Network Topology

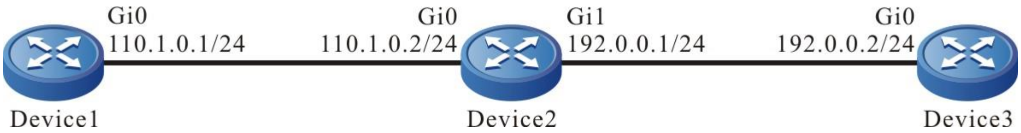


Figure 3-3 Networking of configuring the ICMP-path-jitter entity

Configuration Steps

Step 1: Configure the IP address and route of the interface, making Device1, Device2, and Device3 communicate with each other. (Omitted)

Step 2: Configure the ICMP-path-jitter entity and add the attribute parameters.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmp-path-jitter
Device1(config-rtr-icmppathjitter)#set dest-ipaddr 192.0.0.2 10 20 source-ipaddr 110.1.0.1
Device1(config-rtr-icmppathjitter)#number-of-history-kept 255
Device1(config-rtr-icmppathjitter)#targetOnly false
Device1(config-rtr-icmppathjitter)#exit
```

#View the ICMP-path-jitter entity parameters.

```
Device1#show rtr entity 1
-----------------------------------------------------------------
ID:1        name:IcmpPathJitter1        Created:TRUE
```

```
****************type:ICMPPATHJITTER****************
CreatedTime:WED OCT 24 10:54:31 2012
LatestModifiedTime:WED OCT 24 10:56:12 2012
Times-of-schedule:0
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:10 (each hop)
Packets-interval:20(ms)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktLoss: 200000000  direction:be
Threshold-of-jitter:6000(ms) direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:FALSE
Status:DEFAULT
---------------------------------------------------------------
```

The result shows that the entity parameters are consistent with the configuration..

In-scheduling: FALSE indicates that the entity is not scheduled.

Status: DEFAULT indicates that the entity status is DEFAULT.

Step 3: Schedule the defined ICMP-path-jitter entity and define the attribute parameters of the scheduling.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life foreve
```

Step 4: Check the result.

#View the entity status.

```
Device1#show rtr entity 1
---------------------------------------------------------------
ID:1          name:IcmpPathJitter1          Created:TRUE
****************type:ICMPPATHJITTER****************
```

```
CreatedTime:WED OCT 24 10:54:31 2012
LatestModifiedTime:WED OCT 24 10:56:12 2012
Times-of-schedule:4
Time-of-last-schedule:WED OCT 24 11:00:25 2012
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:10 (each hop)
Packets-interval:20(ms)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktLoss: 200000000 direction:be
Threshold-of-jitter:6000(ms) direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:TRUE
Status:REACHABLE
--------------------------------------------------------------
```

In-scheduling: TRUE indicates that the entity is being scheduled.

Status: REACHABLE indicates that the entity status is reachable, that is, the network connection from Device1to Device2 is normal.

#View the history record content.

```
Device1#show rtr history 1
--------------------------------------------------------------
ID:1    Name:IcmpPathJitter1
History of hop-by-hop:
 110.1.0.2    PktLoss:0       Rtt:1       (ms),Jitter:0       (ms)
 192.0.0.2    PktLoss:0       Rtt:0       (ms),Jitter:0       (ms)
History of record from source to dest:
CurHistorySize:4      MaxHistorysize:255
WED OCT 24 11:00:25 2012
     PktLoss:0       ,Rtt:1       (ms),Jitter:0       (ms)
WED OCT 24 10:59:25 2012
```

```
        PktLoss:0        ,Rtt:0        (ms),Jitter:0        (ms)
WED OCT 24 10:58:25 2012
        PktLoss:0        ,Rtt:0        (ms),Jitter:0        (ms)
WED OCT 24 10:57:25 2012
        PktLoss:0        ,Rtt:0        (ms),Jitter:0        (ms)
--------------------------------------------------------------
```

In the history records, record the packet loss, delay and jitter of each scheduling.

3.3.4. Configure VoIP-jitter Entity to Detect Network Transmitting VoIP Packets

Network Requirement

- Use the VoIP-jitter entity on Device1 and detect the network transmitting VoIP packets from Device1 to Device3

Network Topology

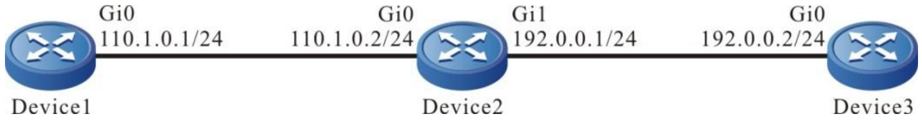


Figure 3-4 Networking of configuring the VoIP-jitter entity

Configuration Steps

Step 1: Configure the IP address and route of the interface, making Device1 communicate with Device3. (Omitted)

Step 2: Configure ntp and synchronize the clock.

#Configure Device3.

```
Device3#configure terminal
Device3(config)#ntp master
```

#Configure Device1.

```
Device1(config)#ntp server 192.0.0.2
```

#View that Device3 becomes the clock server successfully and prompt that the clock is synchronized.

```
Device3#show ntp status
Current NTP status information
Clock is synchronized, stratum 8, reference is 127.127.8.10
reference time is D4321EF4.7BBBBB68 (08:01:56.483 Wed Oct 24 2012)
```

#View that Device1 becomes the clock client successfully, prompt that the clock is synchronized and display the server address.

```
Device1#show ntp status
Current NTP status information
Clock is synchronized, stratum 9, reference is 192.0.0.2
reference time is D43222C1.91110F31 (08:18:09.566 Wed Oct 24 2012)
```

Step 3: Configure responder on Device3 as the responder end.

#Configure Device3

```
Device3(config)#rtr enable
Device3(config)#rtr responder
```

Step 4: Configure the VoIP-jitter entity on Device1 and add the attribute parameters.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 jitter
Device1(config-rtr-jitter)#set dest-ipaddr 192.0.0.2 dest-port 1234 g711alaw source-ipaddr 110.1.0.1 source-port 1234
Device1(config-rtr-jitter)#number-of-history-kept 255
Device1(config-rtr-jitter)#exit
```

#View the entity parameter.

```
Device1#show rtr entity 1
------------------------------------------------------------
ID:1        name:Jitter1        Created:TRUE
****************type:JITTER****************
CreatedTime:WED OCT 24 16:02:32 2012
LatestModifiedTime:WED OCT 24 16:02:58 2012
Times-of-schedule:0
Entry-state:Pend
TargetIp:192.0.0.2    targetPort:1234
Codec:G.711 A-Law     Packet-size:172 Packet-number:1000
Packet-transmit-interval:20(ms)
frequency:60(s)
SourceIp:110.1.0.1    Soure-port:1234
TimeOut:50000(ms)
Alarm-type:none
Threshold-of-dsDelay:5000(ms) direction:be
Threshold-of-dsJitter:6000(ms) direction:be
Threshold-of-dsPktLoss:200000000 direction:be
Threshold-of-sdDelay:5000(ms) direction:be
Threshold-of-sdJitter:6000(ms) direction:be
Threshold-of-sdPktLoss:200000000 direction:be
Threshold-of-rtt:9000(ms) direction:be
```

```
Threshold-of-mos:10000000 direction:be
Threshold-of-icpif:100000000 direction:be
Number-of-history-kept:255
Periods:1
Status:DEFAULT
---------------------------------------------------------------
```

The result shows that the entity parameters are consistent with the configuration..

Status: DEFAULT indicates that the entity status is DEFAULT.

Step 5: Schedule the defined VoIP-jitter entity and define the attribute parameters of the scheduling.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life 600 repeat 10
```

Step6: Check the result.

#View the entity status.

```
Device1#show rtr entity 1
---------------------------------------------------------------
ID:1          name:Jitter1          Created:TRUE
****************type:JITTER****************
CreatedTime:WED OCT 24 16:02:32 2012
LatestModifiedTime:WED OCT 24 16:06:02 2012
Times-of-schedule:3
Time-of-last-schedule:WED OCT 24 16:08:29 2012
Entry-state:Transmit
TargetIp:192.0.0.2      targetPort:1234
Codec:G.711 A-Law      Packet-size:172 Packet-number:1000
Packet-transmit-interval:20(ms)
frequency:60(s)
SourceIp:110.1.0.1      Soure-port:1234
TimeOut:50000(ms)
Alarm-type:none
Threshold-of-dsDelay:5000(ms) direction:be
Threshold-of-dsJitter:6000(ms) direction:be
Threshold-of-dsPktLoss:200000000 direction:be
Threshold-of-sdDelay:5000(ms) direction:be
Threshold-of-sdJitter:6000(ms) direction:be
Threshold-of-sdPktLoss:200000000 direction:be
```

```
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-mos:10000000 direction:be
Threshold-of-icpif:100000000 direction:be
Number-of-history-kept:255
Periods:1
Status:REACHABLE
------------------------------------------------------------
```

Entry-state: Transmit indicates that the entity is being scheduled.

Status: REACHABLE indicates that the entity status is reachable and the network from Device1 to Device3 transmits the VoIP packets normally.

#View the history record contents.

```
Device1#show rtr history 1
------------------------------------------------------------
ID:1    Name:Jitter1    CurHistorySize:3       MaxHistorysize:255
History recorded as following:
WED OCT 24 16:08:46 2012
    SdPktLoss:0        ,DsPktLoss:0        ,Rtt:185      (ms),
    SdDelay:14       (ms),DsDelay:178      (ms),SdJitter:8         (ms),DsJitter:183
(ms),
    Mos:5.000000        ,icpif:0.000000
WED OCT 24 16:07:45 2012
    SdPktLoss:0        ,DsPktLoss:0        ,Rtt:14       (ms),
    SdDelay:16     (ms),DsDelay:7      (ms),SdJitter:10     (ms),DsJitter:13     (ms),
    Mos:5.000000        ,icpif:0.000000
WED OCT 24 16:06:46 2012
    SdPktLoss:0        ,DsPktLoss:0        ,Rtt:17       (ms),
    SdDelay:16     (ms),DsDelay:9      (ms),SdJitter:11     (ms),DsJitter:13     (ms),
    Mos:5.000000        ,icpif:0.000000
------------------------------------------------------------
```

In the history records, record the uni-directional packet loss, turnaround delay, uni-directional delay, and uni-directional jitter of each scheduling.

Note:

- Before configuring the VoIP-jitter entity, we need to configure the NTP service to realize the network clock synchronization and configure the **rtr responder** command at the destination end as the responder. Note that if the clock is not synchronized or not configuring the responder end, the scheduling result is wrong.

3.3.5. Configure UDP-echo Entity to Detect Network Transmitting UDP Packets

Network Requirement

- Use the UDP-echo entity on Device1 and detect the network transmitting UDP packets from Device1 to Device3

Network Topology

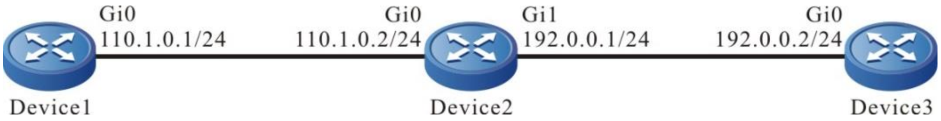


Figure 3-5 Networking of configuring the UDP-echo entity

Configuration Steps

Step 1: Configure the IP address and route of the interface, making Device1 communicate with Device3. (Omitted)

Step 2: Configure responder on Device3 as the responder end.

#Configure Device3

```
Device3#configure terminal
Device3(config)#rtr enable
Device3(config)#rtr responder
```

Step 3: Configure the UDP-echoentity on Device1 and add the attribute parameters.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 udpecho
Device1(config-rtr-udpecho)#set dest-ipaddr 192.0.0.2 dest-port 1001 source-ipaddr
110.1.0.1 source-port 1001
Device1(config-rtr-udpecho)#number-of-history-kept 255
Device1(config-rtr-udpecho)#frequency 10
Device1(config-rtr-udpecho)#exit
```

#View the entity parameter.

```
Device1#show rtr entity 1
-----------------------------------------------------------------
ID:1          name:UdpEcho1          Created:TRUE
****************type:UDPECHO****************
CreatedTime:WED OCT 24 16:36:45 2012
LatestModifiedTime:WED OCT 24 16:37:44 2012
Times-of-schedule:0
```

```
Entry-state:Pend
TargetIp:192.0.0.2    TargetPort:1001
SourceIp:110.1.0.1    SourePort:1001
TimeOut:5000(ms)
request-data-size:16
Frequecy:10(s)
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
Status:DEFAULT
---------------------------------------------------------------
```

The result shows that the entity parameters are consistent with the configuration..

Status: DEFAULT indicates that the entity status is DEFAULT.

Step 4: Schedule the defined UDP-echo entity and define the attribute parameters of the scheduling.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life forever
```

Step 5: Check the result.

#View the entity status.

```
Device1#show rtr entity 1
---------------------------------------------------------------
ID:1         name:UdpEcho1        Created:TRUE
***************type:UDPECHO***************
CreatedTime:WED OCT 24 16:36:45 2012
LatestModifiedTime:WED OCT 24 16:37:44 2012
Times-of-schedule:5
Time-of-last-schedule:WED OCT 24 16:39:50 2012
Entry-state:Pend
TargetIp:192.0.0.2    TargetPort:1001
SourceIp:110.1.0.1    SourePort:1001
TimeOut:5000(ms)
request-data-size:16
Frequecy:10(s)
```

```
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Data-pattern:ABCD
Number-of-history-kept:255
Periods:1
Status:REACHABLE
-----------------------------------------------------------------
```

Status: REACHABLE indicates that the entity status is reachable, that is, the network from Device1 to Device2 can transmits the UDP packets normally.

#View the history record content.

```
Device1#show rtr history 1
-----------------------------------------------------------------
ID:1    Name:UdpEcho1   CurHistorySize:5      MaxHistorysize:255
History recorded as following:
WED OCT 24 16:39:54 2012
    PktLoss:0       ,Rtt:1       (ms)
WED OCT 24 16:39:44 2012
    PktLoss:0       ,Rtt:1       (ms)
WED OCT 24 16:39:33 2012
    PktLoss:0       ,Rtt:2       (ms)
WED OCT 24 16:39:23 2012
    PktLoss:0       ,Rtt:2       (ms)
WED OCT 24 16:39:13 2012
    PktLoss:0       ,Rtt:2       (ms)
-----------------------------------------------------------------
```

In the history records, record the packet loss and delay of each scheduling.

Note:

- Before configuring the UDP-echo entity, we need to configure the rtr responder command at the destination end as the responder. If the responder end is not configured, the scheduling result is wrong.

3.3.6. Configure Detection Interface Traffic of FLOW-statistics Entity

Network Requirement

- Use the FLOW-statistics entity on Device1, detecting the traffic of the interface gigabitethernet0.

Network Topology

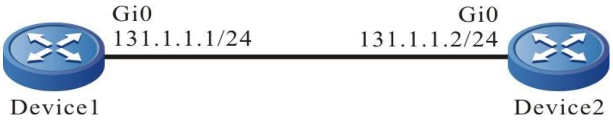


Figure 3-6 Networking of configuring the FLOW-statistics entity

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Configure the FLOW-statistics entity on Device1 and add the attribute parameters.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 flow-statistics
Device1(config-rtr-flowsta)#flow-statistics interface gigabitethernet0 interval 60
Device1(config-rtr-flowsta)#number-of-history-kept 255
Device1(config-rtr-flowsta)#exit
```

#View the entity parameters.

```
Device1#show rtr entity 1
--------------------------------------------------------------
ID:1          name:flow-statistics1          Created:TRUE
****************type:FLOWSTATISTICS****************
CreatedTime:THU OCT 25 09:57:43 2012
LatestModifiedTime:THU OCT 25 09:58:03 2012
Times-of-schedule:0
Alarm-type:none
Threshold-of-inputPkt:200000000 direction:be
Threshold-of-inputFlow:200000000 direction:be
Threshold-of-outputPkt:200000000 direction:be
Threshold-of-outputFlow:200000000 direction:be
Interface:gigabitethernet0
Statistics-interval:60(s)
Number-of-history-kept:255
Periods:1
Status:DEFAULT
--------------------------------------------------------------
```

The result shows that the entity parameters are consistent with the configuration.

Status: DEFAULT indicates that the entity status is DEFAULT.

Step 3: Schedule the defined FLOW-statistics entity and define the attribute parameters of the scheduling.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life 600 repeat 10
```

Step 4: Check the result.

1. When there is the received data traffic on the interface gigabitethernet0:

#View the entity status.

```
Device1#show rtr entity 1
------------------------------------------------------------------
ID:1          name:flow-statistics1          Created:TRUE
****************type:FLOWSTATISTICS****************
CreatedTime:THU OCT 25 09:57:43 2012
LatestModifiedTime:THU OCT 25 09:58:03 2012
Times-of-schedule:2
Time-of-last-schedule:THU OCT 25 10:02:11 2012
Alarm-type:none
Threshold-of-inputPkt:200000000 direction:be
Threshold-of-inputFlow:200000000 direction:be
Threshold-of-outputPkt:200000000 direction:be
Threshold-of-outputFlow:200000000 direction:be
Interface:gigabitethernet0
Statistics-interval:60(s)
Number-of-history-kept:255
Periods:1
Status:REACHABLE
------------------------------------------------------------------
```

Status: REACHABLE indicates that the entity status is reachable, that is, there are packets entering and leaving the gigabitethernet0 interface.

2. When there is no egress or ingress data traffic on the interface gigabitethernet0.

#View the entity status.

```
Device1#show rtr entity 1
------------------------------------------------------------------
ID:1          name:flow-statistics1          Created:TRUE
****************type:FLOWSTATISTICS****************
CreatedTime:THU OCT 25 09:57:43 2012
```

```
LatestModifiedTime:THU OCT 25 09:58:03 2012
Times-of-schedule:5
Time-of-last-schedule:THU OCT 25 10:05:11 2012
Alarm-type:none
Threshold-of-inputPkt:200000000 direction:be
Threshold-of-inputFlow:200000000 direction:be
Threshold-of-outputPkt:200000000 direction:be
Threshold-of-outputFlow:200000000 direction:be
Interface:gigabitethernet0
Statistics-interval:60(s)
Number-of-history-kept:255
Periods:1
Status:UNREACHABLE
------------------------------------------------------------
```

Status: UNREACHABLE indicating when there is egress or ingress traffic on the interface gigabitethernet0, the entity status is un-reachable.

#View the history record content.

```
Device1#show rtr history 1
------------------------------------------------------------
ID:1         Name:flow-statistics1  CurHistorySize:5     MaxHistorysize:255
History recorded as following:
THU OCT 25 10:05:11 2012
     Input pkt:0        (packets/s),Input flow:0        (bits/s),
     Output pkt:0       (packets/s),Output flow:0       (bits/s)
THU OCT 25 10:04:11 2012
     Input pkt:209      (packets/s),Input flow:214000   (bits/s),
     Output pkt:0       (packets/s),Output flow:0       (bits/s)
THU OCT 25 10:03:11 2012
     Input pkt:8460     (packets/s),Input flow:8663000  (bits/s),
     Output pkt:0       (packets/s),Output flow:0       (bits/s)
THU OCT 25 10:02:11 2012
     Input pkt:8460     (packets/s),Input flow:8663000  (bits/s),
     Output pkt:0       (packets/s),Output flow:0       (bits/s)
THU OCT 25 10:01:12 2012
     Input pkt:6456     (packets/s),Input flow:6610000  (bits/s),
     Output pkt:0       (packets/s),Output flow:0       (bits/s)
------------------------------------------------------------
```

In the history records, record the rate of entering and leaving the interface gigabitethernet0 during each scheduling in details (based on the quantity and based on bit).

Note:

- The reachability of the FLOW-statistics entity can be defined as: The entity is being scheduled. As long as there is traffic at the IN or OUT direction, the entity status is REACHEABLE; if there is no traffic, the entity status is UNREACHABLE.

3.3.7. Configure LSP-ping Entity to Detect Communication in MPLS Network

Network Requirement

- In the MPLS network, use the LSP-ping entity on PE1, detecting the network communication from PE1 to PE2.

Network Topology

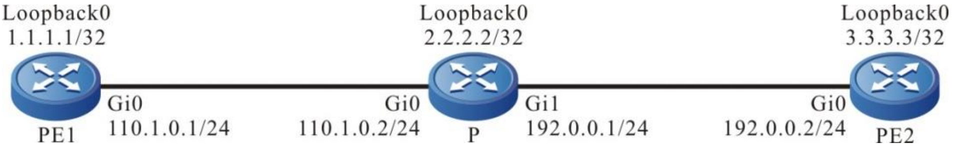


Figure 3-7 Networking of configuring the LSP-ping entity

Configuration Steps

Step 1: Configure the IP address of the interface; PE1, P and PE2 form the MPLS network; in the MPLS network, run the IGP routing protocol and LDP; set up one LSP from PE1 to PE2 for FEC 3.3.3.3/32. (omitted; for the configuration of the MPLS environment, refer to MPLS configuration document)

Step 2: Configure the LSP-ping entity on PE1 and add the attribute parameters.

#Configure Device.

```
PE1#configure terminal
PE1(config)#rtr enable
PE1(config)#rtr 1 lsp-ping
PE1(config-rtr-lsp-ping)#set fec ipv4 3.3.3.3 32
PE1(config-rtr-lsp-ping)#number-of-history-kept 255
PE1(config-rtr-lsp-ping)#exit
```

#View the entity parameters.

```
PE1#show rtr entity 1
---------------------------------------------------------------
ID:1          name:LspPing1          Created:TRUE
****************type:LSPPING****************
CreatedTime:THU OCT 25 14:02:22 2012
LatestModifiedTime:THU OCT 25 14:05:28 2012
Times-of-schedule:0
LDP IPv4 prefix:3.3.3.3  mask length:32
Echo request time out:2(s)
Echo request ttl:255
Echo request size:120(byte)
Echo request exp:0
Echo request send interval:0(ms)
Echo request repeat count:5
Schedule frequency:20(s)
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-packet-loss:200000000 direction:be
Number-of-history-kept:255
Periods:1
Total count of echo request need to send:0
Total count of echo request actually sent:0
Total count of echo reply received:0
Total count of valid echo reply received:0
In-scheduling:FALSE
Status:DEFAULT
--------------------------------------------------------------
```

The result shows that the entity parameters are consistent with the configuration.

In-scheduling: FALSE indicates that the entity is not scheduled.

Status: DEFAULT indicates that the entity status is DEFAULT.

Step 3: Schedule the defined LSP-ping entity, defining the attribute parameters of the scheduling.

#Configure PE1.

```
PE1(config)#rtr schedule 1 entity 1 start now ageout 100 life forever
```

Step 4: Check the result.

#View the entity status.

```
PE1#show rtr entity 1
--------------------------------------------------------------
ID:1          name:LspPing1          Created:TRUE
****************type:LSPPING****************
CreatedTime:THU OCT 25 14:02:22 2012
LatestModifiedTime:THU OCT 25 14:07:2 2012
Times-of-schedule:4
Time-of-last-schedule:THU OCT 25 14:13:51 2012
```

```
LDP IPv4 prefix:3.3.3.3  mask length:32
Echo request time out:2(s)
Echo request ttl:255
Echo request size:120(byte)
Echo request exp:0
Echo request send interval:0(ms)
Echo request repeat count:5
Schedule frequency:20(s)
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-packet-loss:200000000 direction:be
Number-of-history-kept:255
Periods:1
Total count of echo request need to send:120
Total count of echo request actually sent:120
Total count of echo reply received:120
Total count of valid echo reply received:120
In-scheduling:TRUE
Status:REACHABLE
--------------------------------------------------------------
```

In-scheduling: TRUE indicates that the entity is being scheduled.

Status: REACHABLE indicates that the entity status is reachable, that is, the MPLS network connection from Device1 to Device3 is normal.

#View the history record content.

```
PE1#show rtr history 1
--------------------------------------------------------------
ID:1    Name:LspPing1   CurHistorySize:4       MaxHistorysize:255
History recorded as following:
THU OCT 25 14:07:11 2012
        PktLoss:0         ,Rtt:0         (ms)
THU OCT 25 14:06:51 2012
        PktLoss:0         ,Rtt:0         (ms)
THU OCT 25 14:06:31 2012
        PktLoss:0         ,Rtt:0         (ms)
THU OCT 25 14:06:12 2012
        PktLoss:0         ,Rtt:0         (ms)
--------------------------------------------------------------
```

In the history records, record the packet loss and delay of each scheduling.

3.3.8. Configure LSP-ping Entity with VRF Option to Detect Communication in MPLS L3VPN Network

Network Requirement

- In the MPLS L3VPN network, use the LSP-ping entity with the VRF option on PE1, detecting the network communication from PE1 to CE2.

Network Topology

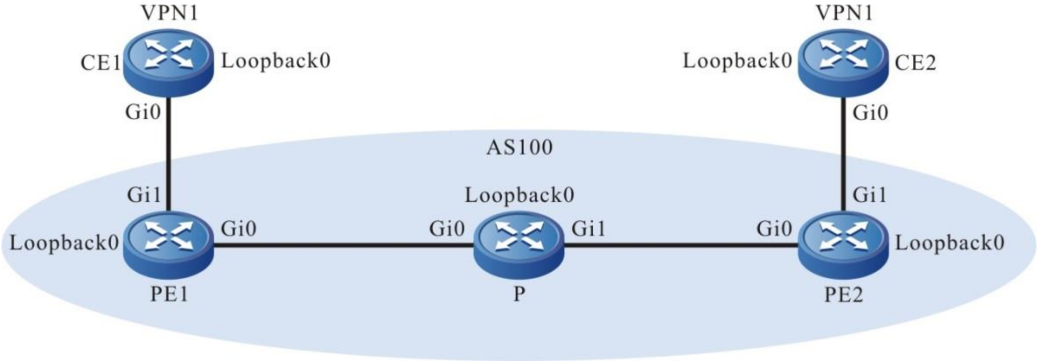


Figure 3-8 Networking of configuring the LSP-ping entity with the VRF option

Device	Interface	IP address	Device	Interface	IP address
CE1	Gi0	95.1.1.2/16	PE2	Gi0	92.1.1.2/16
	Loopback0	5.5.5.5/32		Gi1	90.1.1.1/16
PE1	Gi0	93.1.1.1/16		Loopback0	75.75.75.75/32
	Gi1	95.1.1.1/16	CE2	Gi0	90.1.1.2/16
	Loopback0	90.90.90.90/32		Loopback0	8.8.8.8/32
P	Gi0	93.1.1.2/16			
	Gi1	92.1.1.1/16			
	Loopback0	11.11.11.11/32			

Configuration Steps

Step 1: Configure the IP address of the interface; CE1, PE1, P and PE2, CE2 form the MPLS L3VPN network; CE1 and CE2 can communicate with each other; VRF is 1 on PE1. (omitted; for the configuration of the MPLS L3VPN environment, refer to the configuration document of MPLS route)

Step 2: Configure the LSP-ping entity with the VRF option on PE1 and add the attribute parameters.

#Configure PE1.

```
PE1#configure terminal
PE1(config)#rtr enable
PE1(config)#rtr 1 lsp-ping
PE1(config-rtr-lsp-ping)#set fec vrf 1 ipv4 8.8.8.8
PE1(config-rtr-lsp-ping)#number-of-history-kept 255
PE1(config-rtr-lsp-ping)#exit
```

#View the entity parameters.

```
PE1#show rtr entity 1
-----------------------------------------------------------------
ID:1          name:LspPing1          Created:TRUE
****************type:LSPPING****************
CreatedTime:MON NOV 05 09:39:40 2012
LatestModifiedTime:MON NOV 05 09:39:59 2012
Times-of-schedule:0
VPN IPv4 prefix:8.8.8.8  mask length:32  VRF name:1
Echo request time out:2(s)
Echo request ttl:255
Echo request size:120(byte)
Echo request exp:0
Echo request send interval:0(ms)
Echo request repeat count:5
Schedule frequency:20(s)
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-packet-loss:200000000 direction:be
Number-of-history-kept:255
Periods:1
Total count of echo request need to send:0
Total count of echo request actually sent:0
Total count of echo reply received:0
Total count of valid echo reply received:0
In-scheduling:FALSE
Status:DEFAULT
```

The result shows that the entity parameters are consistent with the configuration.

In-scheduling: FALSE indicates that the entity is not scheduled.

Status: DEFAULT indicates that the entity status is DEFAULT.

Step 3: Schedule the defined LSP-ping entity, defining the attribute parameters of the scheduling.

#Configure PE1.

```
PE1(config)#rtr schedule 1 entity 1 start now ageout 100 life forever
```

Step 4: Check the result.

#View the entity status.

```
PE1#show rtr entity 1
--------------------------------------------------------------
CreatedTime:MON NOV 05 09:39:40 2012
LatestModifiedTime:MON NOV 05 09:39:59 2012
Times-of-schedule:3
Time-of-last-schedule:MON NOV 05 09:41:13 2012
VPN IPv4 prefix:8.8.8.8  mask length:32  VRF name:1
Echo request time out:2(s)
Echo request ttl:255
Echo request size:120(byte)
Echo request exp:0
Echo request send interval:0(ms)
Echo request repeat count:5
Schedule frequency:20(s)
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-packet-loss:200000000 direction:be
Number-of-history-kept:255
Periods:1
Total count of echo request need to send:15
Total count of echo request actually sent:15
Total count of echo reply received:15
Total count of valid echo reply received:15
In-scheduling:TRUE
Status:REACHABLE
--------------------------------------------------------------
```

In-scheduling: TRUE indicates that the entity is being scheduled.

Status: REACHABLE indicates that the entity status is reachable, that is, the MPLS L3VPN network connection from PE1 to CE2 is normal.

#View the history record content.

```
PE1#show rtr history 1
---------------------------------------------------------------
ID:1    Name:LspPing1   CurHistorySize:3      MaxHistorysize:255
History recorded as following:
MON NOV 05 09:41:13 2012
        PktLoss:0        ,Rtt:0        (ms)
MON NOV 05 09:40:53 2012
        PktLoss:0        ,Rtt:0        (ms)x
MON NOV 05 09:40:33 2012
        PktLoss:0        ,Rtt:0        (ms)
---------------------------------------------------------------
```

In the history records, record the packet loss and delay of each scheduling.

3.3.9. Configure TRACK to Link with ICMP-echo

Network Requirement

- TRACK links with SLA. Judge the validity of the static route on Device1 via the entity status.

Network Topology

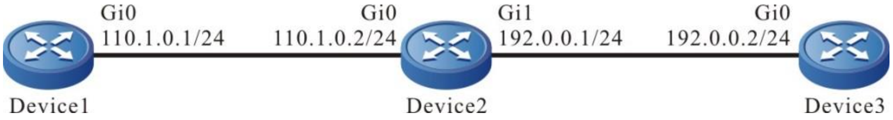


Figure 3-9 Networking of configuring TRACK to link with SLA

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted)

Step 2: Configure the ICMP-echo entity on Device1 to detect the network connectivity from Device1 to Device2, and add the entity to the entity group.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmpecho
Device1(config-rtr-icmpecho)#set 110.1.0.2 5 70 2 12 extend 110.1.0.1 0 true false
Device1(config-rtr-icmpecho)#number-of-history-kept 255
Device1(config-rtr-icmpecho)#exit
Device1(config)#rtr group 1
Device1(config-rtr-group)#member 1
```

```
Device1(config-rtr-group)#exit
```

Step 3: Define TRACK and associate with LSA.

#Configure Device1.

```
Device1(config)#track 1
Device1(config-track)#rtr 1
```

Step 4: Add the static route and associate TRACK.

#Configure Device1.

```
Device1(config)#ip route 192.0.0.0 255.255.255.0 110.1.0.2 track 1
```

Step 5: Schedule the entity group and check the validity of the static route.

#Configure Device1.

```
Device1(config)#rtr schedule 1 group 1 start now ageout 100 life forever
```

Step 6: Check the result.

1. When the network connectivity from Device1 to Device2 is normal:

#View the entity group status.

```
Device1#show rtr group 1
---------------------------------------------
ID:1         name:rtrGroup1       Members schedule interval:0
Option: AND     Status:REACHABLE
*****************************
type:SINGLE     Entity Id :1
The status of the entity group is REACHEABLE.
#In the route table of Device1, view the route of the segment 192.0.0.0/24.
Device1#show ip route 192.0.0.0
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

S   192.0.0.0/24 [1/10] via 110.1.0.2, 00:00:09, gigabitethernet0
```

The result displays that there is the route to the segment 192.0.0.0/24, indicating that when the status of the entity group is RECHABLE, judge that the associated static route is valid.

2. When the network connectivity from Device1 to Device2 is faulty:

#View the status of the entity group:

```
Device1#show rtr group 1
---------------------------------------------
ID:1         name:rtrGroup1       Members schedule interval:0
Option: AND     Status:UNREACHABLE
******************************
type:SINGLE     Entity Id :1
The status of the entity group is UNREACHEABLE.
```

#In the route table of Device1, view the route of the segment 192.0.0.0/24.

```
Device1#show ip route 192.0.0.2
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M -
Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
```

The result displays that there is no route to the segment 192.0.0.0/24, indicating that when the status of the entity group is UNREACHABLE, judge that the associated static route is invalid.

3.3.10. Configure ICMPv6-echo Entity to Detect Basic Network Communication

Network Requirement

- Use the ICMPv6-echo entity on Device1, detecting the basic communication of the network from Device1 to Device3.

Network Topology

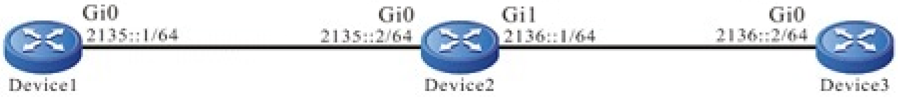


Figure 3-10 Networking of configuring ICMPv6-echo entity

Configuration Steps

Step 1: Configure the IPv6 address and route of the interface, making Device1 and Device3 communicate with each other. (Omitted)

Step 2: Configure the ICMP-echo IPv6 entity and add the attribute parameters.

#Cofigure Device1.

```
Device1#configure terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmpv6echo
```

```
Device1(config-rtr-icmpv6echo)#set 2136::2 5 70 2 12 extend 2135::1 0 TRUE
Device1(config-rtr-icmpv6echo)#alarm-type log
Device1(config-rtr-icmpv6echo)#number-of-history-kept 255
Device1(config-rtr-icmpv6echo)#threshold-pktLoss 10 direction be
Device1(config-rtr-icmpv6echo)#threshold-rtt 1000  direction be
Device1(config-rtr-icmpv6echo)#exit
```

#View ICMP-echo ipv6 entity parameters.

```
Device1#show rtr entity 1
-------------------------------------------------------------
ID:1          name:Icmpv6Echo1              Created:TRUE
***************type:ICMPV6ECHO***************
CreatedTime:Tue Sep 17 10:05:52 2019
LatestModifiedTime:Tue Sep 17 10:21:06 2019
Times-of-schedule:0
TargetIpv6:2136::2
Transmit-packets:5
Totally-send-packets:0
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceIpv6:2135::1     tos:0   Verify-data:TRUE
In-scheduling:FALSE
Schedule frequency:12(s)
Status:DEFAULT
-------------------------------------------------------------
```

The result shows that the entity parameters are consistent with the configuration..

In-scheduling: FALSE indicates that the entity is not scheduled.

Status: DEFAULT indicates that the entity status is DEFAULT.

Note:

- When the entity is not scheduled, the status is DEFAULT; when the entity is scheduled and if the entity is reachable, the status is REACHABLE; if the entity is unreachable, the status is UNREACHABLE.

Step 3: Schedule the defined ICMPv6-echo entity and define the attribute parameters of the scheduling.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 20 life forever
```

Step 4: Check the result.

1. When the network connectivity from Device1 to Device3 is normal:

#View the entity status.

```
Device1#show rtr entity 1
----------------------------------------------------------------
ID:1          name:Icmpv6Echo1             Created:TRUE
****************type:ICMPV6ECHO****************
CreatedTime:Tue Sep 17 10:05:52 2019
LatestModifiedTime:Tue Sep 17 10:21:06 2019
Times-of-schedule:2
Time-of-last-schedule:Tue Sep 17 10:24:08 2019
TargetIpv6:2136::2
Transmit-packets:5
Totally-send-packets:10
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceIpv6:2135::1     tos:0   Verify-data:TRUE
In-scheduling:TRUE
Schedule frequency:12(s)
Status:REACHABLE
----------------------------------------------------------------
```

In-scheduling: TRUE indicates that the entity is being scheduled;

Status: REACHABLE indicates that the entity status is reachable, that is, the network connection from Device1 to Device3 is normal.

2. When the network connectivity from Device1 to Device3 is faulty:

The alarm mode is configured as log, so when the network is disconnected, print the alarm information on the device, as follows:

```
%SLA-4:Rtr 1 (ICMPV6ECHO) rtt [9000ms] was exceeded(>=) threshold [1000ms].
```

#View the entity status.

```
Device1#show rtr entity 1
--------------------------------------------------------------
ID:1          name:Icmpv6Echo1             Created:TRUE
***************type:ICMPV6ECHO***************
CreatedTime:Tue Sep 17 10:05:52 2019
LatestModifiedTime:Tue Sep 17 10:21:06 2019
Times-of-schedule:21
Time-of-last-schedule:Tue Sep 17 10:28:08 2019
TargetIpv6:2136::2
Transmit-packets:5
Totally-send-packets:105
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceIpv6:2135::1      tos:0   Verify-data:TRUE
In-scheduling:TRUE
Schedule frequency:12(s)
Status:UNREACHABLE
--------------------------------------------------------------
```

In-scheduling: TRUED indicates that the entity is being scheduled;

Status: UNREACHABLE indicates that the entity status is unreachable, that is, the network connection from Device1to Device3 is unreachable.

#View the history record content.

```
Device1#show rtr history 1
--------------------------------------------------------------
ID:1    Name:Icmpv6Echo1       CurHistorySize:4       MaxHistorysize:255
History recorded as following:
Tue Sep 17 10:24:42 2019
        PktLoss:5         ,Rtt:invalid
Tue Sep 17 10:24:29 2019
```

```
          PktLoss:1       ,Rtt:400      (ms)
Tue Sep 17 10:24:17 2019
          PktLoss:0       ,Rtt:1       (ms)
Tue Sep 17 10:24:05 2019
          PktLoss:0       ,Rtt:0       (ms)
-------------------------------------------------------------
```

In the history records, record the packet loss and delay of each scheduling; if Rtt is invalid, it indicates that there is fault in the network and the network is reachable.

3.3.11. Configure TRACK to Link with ICMPv6-echo

Network Requirement

- TRACK links with icmpv6-echo. Judge the validity of the static route on Device1 via the entity status.

Network Topology

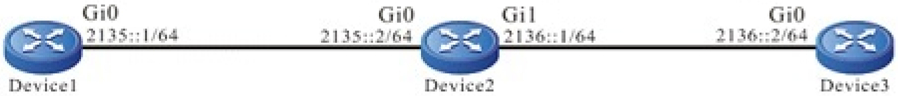


Figure 3-11 Networking of configuring TRACK to link with ICMPv6-echo

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted)

Step 2: Configure the ICMPv6-echo entity on Device1 to detect the network connectivity from Device1 to Device2, and add the entity to the entity group.

#Configure Device1.

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmpv6echo
Device1(config-rtr-icmpv6echo)# set 2135::2 5 70 2 12 extend 2135::1 0 FALSE
Device1(config-rtr-icmpv6echo)#number-of-history-kept 255
Device1(config-rtr-icmpv6echo)#exit
Device1(config)#rtr group 1
Device1(config-rtr-group)#member 1
Device1(config-rtr-group)#exit
```

Step 3: Define TRACK and associate with LSA.

#Configure Device1.

```
Device1(config)#track 1
Device1(config-track)#rtr 1
Device1(config-track)#exit
```

Step 4: Add the static route and associate TRACK.

#Configure Device1.

```
Device1(config)#ipv6 route 2136::/64 2135::2 track 1
```

Step 5: Schedule the entity group.

#Configure Device1.

```
Device1(config)#rtr schedule 1 group 1 start now ageout 20 life forever
```

Step 6: Check the result.

1. When the network connectivity from Device1 to Device2 is normal:

#View the entity group status.

```
Device1#show rtr group 1
-----------------------------------------------
ID:1          name:rtrGroup1        Members schedule interval:0
Option: AND     Status:REACHABLE
*****************************
type:SINGLE     Entity Id :1
```

The status of the entity group is REACHEABLE.

#In the route table of Device1, view the route of the segment 2136::/64.

```
Device1#show ipv6 route 2136::/64
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

S   2136::/64 [1/0]
     via 2135::2 [0], 00:50:17, gigabitethernet0
```

The result displays that there is the route to the segment 2136::/64, indicating that when the status of the entity group is RECHABLE, judge that the associated static route is valid.

2. When the network connectivity from Device1 to Device2 is faulty:

#View the status of the entity group:

```
Device1#show rtr group 1
-----------------------------------------------
ID:1          name:rtrGroup1        Members schedule interval:0
Option: AND     Status:UNREACHABLE
*****************************
type:SINGLE     Entity Id :1
```

The status of the entity group is UNREACHEABLE.

#In the route table of Device1, view the route of the segment 2136::/64.

```
Device1#show ipv6 route 2136::/64
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management
```

The result displays that there is no route to the segment 2136::/64, indicating that when the status of the entity group is UNREACHABLE, judge that the associated static route is invalid.

3.3.12. Configure Bandwidth-measure Entity to Detect Bandwidth

Network Requirement

- The Bandwidth-measure entity is used on Device1 to detect the bandwidth of the interconnection link between interface Device1 and Device2.

Network Topology

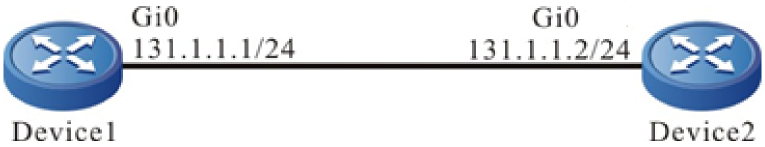


Figure 3-12 Networking of configuring Bandwidth-measure entity

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted)

Step 2: Configure the bandwidth measure entity on Device1 and add attribute parameters.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 bandwidth-measure
Device1(config-rtr-bwmeas)#set 131.1.1.2 55555
Device1(config-rtr-bwmeas)#number-of-history-kept 255
Device1(config-rtr-bwmeas)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#rtr enable
Device2(config)#rtr responser
```

#View the entity parameters.

```
Device1#show rtr entity 1
--------------------------------------------------------------
ID:1          name: BandwidthMeas1          Created:TRUE
***************type: BANDWIDTHMEAS***************
```

```
CreatedTime:Tue May 28 11:00:50 2019
LatestModifiedTime:Tue May 28 11:01:02 2019
Times-of-schedule:0
Entry-state:Pend
TargetIp:131.1.1.2     TargetPort:55555
TimeOut:1(s)
Request-data-size:1400
Measure-time:3(s)
Frequency:1(min)
Number-of-history-kept:255
----------------------------------------------------------
```

The results show that the entity parameters are consistent with the configuration.

State: Pend indicates that the entity state is Pend.

Step 3: Call the defined Bandwidth-measure entity and define the attribute parameters of scheduling.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life 600 repeat 10
```

Step 4: Check the result.

#View the entity status.

```
Device1#show rtr entity 1
----------------------------------------------------------
ID:1          name:BandwidthMeas1           Created:TRUE
****************type:BANDWIDTHMEAS****************
CreatedTime:Tue May 28 11:08:50 2019
LatestModifiedTime:Tue May 28 11:09:02 2019
Times-of-schedule:2
Time-of-last-schedule:Tue May 28 11:16:47 2019
Entry-state:Pend
TargetIp: 131.1.1.2     TargetPort:55555
TimeOut:1(s)
Request-data-size:1400
Measure-time:3(s)
Frequency:1(min)
Number-of-history-kept:255
----------------------------------------------------------
```

State: the status is still Pend, and Times-of-schedule indicates the number of the executed schedulings. You can view the scheduling results through the history.

#View history content.

```
Device1#show rtr history 1
---------------------------------------------------------------
ID:1   Name:BandwidthMeas1    CurHistorySize:2      MaxHistorysize:255
History recorded as following:
Tue May 28 11:16:47 2019
    Status:Success
    Result:983(M)
    Path:131.1.1.1(gigabitethernet0)-->131.1.1.2(gigabitethernet0)
    BW-Data:983 983 983 983 983
Tue May 28 11:15:47 2019
    Status:Success
    Result:983(M)
    Path:131.1.1.1(gigabitethernet0)-->131.1.1.2(gigabitethernet0)
    BW-Data:983 983 983 983 983
---------------------------------------------------------------
```

Status: indicates the connection status with the peer end, and Success indicates that the detection is successful.

Result: average bandwidth.

Path: local IP address, interface and peer IP address and interface.

BW-Data: data detected for 5 times within the detection time.

#View the bandwidth value of interface gigabitethernet0 of Device1.

```
Device1#show interface gigabitethernet 0
gigabitethernet0:
  line protocol is up
  Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
  Type: ETHERNET_CSMACD
  Internet address: 131.1.1.1/24
  Broadcast address: 131.1.1.255
  Metric: 0, MTU: 1500, BW: 1000000 Kbps, DLY: 10 usec, VRF: global
  Reliability 255/255, Txload 65/255, Rxload 1/255
  Ethernet address is 001f.ce20.77e4
  Last clearing of "show interface" counters is 0 hour 0 minute 5 seconds ago
  input rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
  output rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
  2 packets received; 2 packets sent
```

```
172 bytes received; 172 bytes sent
0 multicast packets received
0 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
Unknown protocol 0
   line status up: speed 1000M, duplex full, media-type copper
   rxframe:2, rxBroadcast:0, rxMulticast:0, rxOctets:172
   rxPause:0, rxCrcErr:0, rxOctErr:0, rxtxLenErr:0
   txframe:2, txBroadcast:0, txMulticast:0, txOctets:172
   txPause:0, jabbers:0, collisions:0, CarrierSenseErrors:0
   InDiscards:0, InErrors:0, OutDiscards:0, OutErrors:0
```

It can be seen that the interface bandwidth is 1000M, which is consistent with the detection results.

Note:

- Before scheduling, the Bandwidth-measure entity needs to configure the rtr responder command at the destination as the response end.
- Currently, only bandwidth detection between directly-connected networks is supported.

4. NTP

4.1. Overview

NTP (Network Time Protocol) is the standard Internet protocol used to synchronize the time in Internet. NTP is to synchronize the device time to the standard time. Currently, the adopted time standard is UTC (Universal Time Coordinated).

The design of NTP fully considers the complexity of the time synchronization on Internet. NTP provides the strict, practical, and valid mechanism, applicable to the Internet environments with various scales and speeds. NTP not only corrects the present time, but also continuously tracks the time change and can adjust automatically, even the network fails, it can maintain the time stability. The network cost generated by NTP is small and has the measures of ensuring the network security. The measures can make NTP get the reliable and correct time synchronization on Internet.

In the actual application, select the appropriate NTP work mode according to the network deployment, so as to meet the network clock synchronization requirement in different environments. NTP supports the following three work modes:

- Client/server mode

In the client/server mode, the client sends the clock synchronization packet with Mode field 3 (client mode) to the server. After receiving the packet, the server automatically works in the server mode and sends the response packet with Mode field 4 (server mode). After receiving the response packet, the client synchronizes the system clock. In the mode, the client can synchronize the clock from the server, while the server cannot synchronize the clock from the client.

- Peer mode

In the peer mode, the active peer and passive peer first interact the NTP packet with the Mode field 3 (client mode) and 4 (server mode). And then, the active peer sends the clock synchronization packet with the M ode field 1 (the active peer mode) to the passive peer. After receiving the packet, the passive peer automatically works in the passive peer mode and sends the clock synchronization packet with the Mode field 2 (passive peer mode). In this way, the peer mode is set up. In the mode, the active peer and the passive peer synchronize the clock mutually. If the clocks of the two parties are already synchronized, be subject to the clock with smaller layers.

- Broadcast mode

In the broadcast mode, the broadcast server periodically sends the clock synchronization packet with the Mode field 5 (broadcast server mode) to the broadcast address 255.255.255.255, and the broadcast client monitors the broadcast packet from the broadcast server. When the broadcast client receives the first broadcast packet, the broadcast client and broadcast server interact the NTP packet with the Mode field 3 (client mode) and 4 (server mode), so as to get the network delay of the broadcast client and broadcast server. And then, the broadcast client continues to monitor the broadcast packet and synchronizes the system clock according to the received broadcast packet.

4.2. NTP Function Configuration

Table 4-1 NTP function configuration list

Configuration Task	
Configure the NTP basic functions	Configure the NTP client/server mode
	Configure the NTP peer mode
	Configure the NTP broadcast mode
Configure the NTP optional parameters	Configure the NTP reference clock
	Configure the source interface of the NTP packet
	Configure the receiving and sending control of the NTP packet
	Configure the number of the NTP dynamic sessions
Configure the NTP authentication functions	Configure the NTP client/server authentication
	Configure the NTP peer authentication
	Configure the NTP broadcast authentication
Configure the NTP access control	Configure the NTP access control

4.2.1. Configure NTP Basic Functions

Configuration Condition

Before configuring the NTP basic functions, first complete the following task:

- Configure the network layer address of the interface, making the network layer between the NTP clock service requester and clock service provider reachable.
- The NTP clock service provider enables NTP.

Configure NTP Client/Server Mode

When using the NTP client/server mode, do not need special configuration on the server, but it is necessary to ensure that the serve clock is synchronized and the clock layers of the server are smaller than the clock layers of the client.

Perform the following configuration on the NTP client.

Table 4-2 Configure the NTP client

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Specify the NTP server	**ntp server** [**vrf** *vrf-name*] { *ip-address* | **ipv6** *ipv6-address* | *domain-name* } [**version** *version-number* | **key** *key-number* | **source** *interface-name*]*	Mandatory By default, do not specify the NTP server.

Note:

- The *ip-address* parameter is one unicast address, but cannot be the broadcast address, multicast address or IP address of the local device.
- *ipv6-address* parameter is a global unicast address or Link-Local address, and cannot be a multicast address.
- After specifying the source interface of sending the client packet through **source** *interface-name*, the primary IP address or the first global unicast IPv6 address of the interface will be set as the source IP address of sending the client packet. If the configured server address is IPv6 Link-local address, the source interface must be specified.
- You can specify multiple servers by configuring the **ntp server** or **ntp server ipv6** command multiple times, and you can specify up to 64 servers (the sum of IPv4 + IPv6 + domain names).

Configure NTP Peer Mode

When using the NTP peer mode, do not need special configuration on the passive peer, but it is necessary to ensure that the passive peer can receive and send the NTP packet. You can enable NTP by configuring the **ntp enable (ipv6)** command on the passive peer or any NTP command in “4.2.1 Configure NTP Basic Functions”.

Perform the following configuration on the NTP active peer.

Table 4-3 Configure the NTP active peer

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Specify the NTP passive peer	**ntp peer** [**vrf** *vrf-name*] { *ip-address* | **ipv6** *ipv6-address* | *domain-name* } [**version** *version-number* | **key** *key-number* | **source** *interface-name*] *	Mandatory By default, do not specify the NTP passive peer.

Note:

- The *ip-address* parameter is one unicast address, but cannot be the broadcast address, multicast address or IP address of the local device.
- *ipv6-address* parameter is a global unicast address or Link-Local address, and cannot be a multicast address.
- After specifying the source interface of sending the active peer packet through **source** *interface-name*, the primary IP address or the first global unicast IPv6 address of the interface will be set as the source IP address of sending the active peer packet. If the configured peer address is IPv6 Link-local address, the source interface must be specified.
- You can specify passive peers by configuring the **ntp peer** or **ntp peer ipv6** command multiple times, and you can specify up to 64 passive peers (the sum of IPv4 + IPv6 + domain names).

Configure NTP Broadcast Mode

When using the NTP broadcast mode, the broadcast server and broadcast client both need to be configured and it is necessary to ensure that the clock of the broadcast server is synchronized and the clock layers are smaller than the clock layers of the broadcast client. It is necessary to specify one interface for sending the NTP broadcast packet on the broadcast server and one interface for receiving the NTP broadcast packet on the broadcast client, so the configuration of the broadcast mode can only be performed in the specific interface mode.

Perform the following configuration on the NTP broadcast client.

Table 4-4 Configure the NTP broadcast client

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-

Step	Command	Description
Enable the NTP broadcast client on the interface	**ntp broadcast client**	Mandatory By default, the interface does not enable the NTP broadcast client.

Perform the following configuration on the NTP broadcast server.

Table 4-5 Configure the NTP broadcast server

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Enable the NTP broadcast server on the interface	**ntp broadcast-server** [**key** *key-number* | **version** *version-number*]*	Mandatory By default, the interface does not enable the NTP broadcast server.

4.2.2. Configure NTP Optional Parameters

Configuration Condition

None

Clock NTP Reference Clock

NTP can synchronize the system time via the following two modes:

- Synchronize with the local clock, that is, adopt the local clock as the NTP reference clock
- Synchronize with the other clock source in network, that is, use any of the previous mentioned three NTP work modes.

Table 4-6 Configure the local clock as the NTP reference clock

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the local clock as the NTP reference clock	**ntp master** [*stratum-number*]	Mandatory By default, do not configure the local clock as the NTP reference clock.

Note:

- After configuring the local clock as the NTP reference clock, NTP cannot synchronize the clock from the other clock source in the network.
- After configuring the local clock as the NTP reference clock, the local device can serve as the clock source to synchronize the other device in the network. Please use the configuration carefully, so as to avoid the clock error of other device in the network.

Configure Source Interface of the NTP Packet

If the source interface of the NTP packet is configured and when the device actively sends the NTP packet, select the master IP address of the specified source interface as the source IP address of the packet.

Table 4-7 Configure the source interface of the NTP packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the source interface of the NTP packet	**ntp source** *interface-name*	Mandatory By default, do not configure the source interface of the NTP packet.

Note:

- If using the **ntp server** or **ntp peer** command to specify the source interface, first use the source interface specified by the **ntp server** or **ntp peer** command.
- If **ntp broadcast** is configured in the interface mode, the source interface of the NTP broadcast packet is the interface configured with the above command.
- If the source interface of the specified NTP packet is in the down state, restore the primary address of the default routing interface or the source address of the first global unicast address encapsulating NTP to send packets.

If the source interface of the specified NTP packet has no configured address and is in the up state, but there is no corresponding IPv4 or IPv6 address, restore the primary address of the default routing interface or the source address of the first global unicast address encapsulating NTP to send packets.

Configure Receiving and Sending Control of NTP Packet

By default, the device will not receive and send all NTP packets. You can configure the receiving and sending control of the NTP packet to enable receiving and sending the NTP packet.

Table 4-8 Configure the receiving and sending control of the NTP packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable receiving and sending the NTP packet	**ntp enable [ipv6]**	Mandatory By default, prohibit receiving and sending the NTP packet.

Note:

- After configuring the command **no ntp enable**, it will prohibit receiving and sending all IPv4 NTP packets. If configuring the command **ntp enable**, enable receiving and sending IPv4 NTP packets.
- After configuring the command **no ntp enable ipv6**, prohibit receiving and sending all IPv6 NTP packets. If configuring the command **ntp enable ipv6**, enable receiving and sending IPv6 NTP packets.

Configure Number of NTP Dynamic Sessions

Set the maximum number of NTP dynamic connections allowed locally by configuring the number of NTP dynamic sessions.

Table 4-9 Configure the number of NTP dynamic sessions

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the maximum number of NTP dynamic connections permitted locally	**ntp max-dynamic-sessions** *number*	Mandatory By default, the number of the permitted dynamic NTP sessions is 100.

4.2.3. Configure NTP Authentication Function

In the network with high requirement for the security, when running the NTP protocol, it is necessary to enable the authentication function. Authenticate the packet interacted by the NTP clock service requester and clock service provider to ensure that the clock service requester is synchronized with the valid time, improving the network security.

Configuration Condition

To configure the NTP authentication function, first complete the following task:

- Configure the network layer address of the interface, making the network layer between the NTP clock service requester and clock service provider reachable.
- The NTP clock service provider enables NTP.

Configure NTP Client/Server Authentication

When configuring the NTP client/server authentication, it is necessary to enable the authentication function on the client and server, configure the authentication key, set the authentication key as the trusted key, and specify the key associated with the server on the client.

Perform the following configuration on the NTP client.

Table 4-10 Configure the NTP client authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the NTP authentication function	**ntp authenticate**	Mandatory By default, do not enable the NTP authentication function.

Step	Command	Description
Configure the authentication key	**ntp authentication-key** *key-number* **md5 {0** *plain-key* **| 7** *cipher-key***}**	Mandatory By default, do not configure the authentication key.
Configure the specified key as the trusted key	**ntp trusted-key** *key-number*	Mandatory By default, do not specify the trusted key.
Specify the key associated with the server	**ntp server** [**vrf** *vrf-name*] { *ip-address* | *domain-name* | **ipv6** *ipv6-address* } [**version** *version* | **source** *interface-name*] **key** *key-number*	Mandatory

Perform the following configuration on the NTP server.

Table 4-11 Configure the NTP server authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the NTP authentication function	**ntp authenticate**	Mandatory By default, do not enable the NTP authentication function.
Configure the authentication key	**ntp authentication-key** *key-number* **md5 {0** *plain-key* **| 7** *cipher-key***}**	Mandatory By default, do not configure the authentication key.

Step	Command	Description
Specify the key as the trusted key	**ntp trusted-key** *key-number*	Mandatory By default, do not specify the trusted key.

Note:

- The server and client need to be configured with the same authentication key.

Configure NTP Peer Authentication

When configuring the NTP peer authentication, it is necessary to enable the authentication function on the active peer and passive peer, configure the authentication key, set the authentication key as the trusted key, and specify the key associated with the passive peer on the active peer.

Perform the following configuration on the NTP active peer.

Table 4-12 Configure the NTP active peer authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the NTP authentication function	**ntp authenticate**	Mandatory By default, do not enable the NTP authentication function.
Configure the authentication key	**ntp authentication-key** *key-number* **md5 {0** *plain-key* **| 7** *cipher-key***}**	Mandatory By default, do not configure the authentication key.
Specify the key as the trusted key	**ntp trusted-key** *key-number*	Mandatory By default, do not specify the trusted key.

Step	Command	Description
Specify the key associated with the passive peer	**ntp peer** [**vrf** *vrf-name*] *ip-address* | *domain-name* | **ipv6** *ipv6-address* [**version** *version* | **source** *interface-name*] **key** *key-number*	Mandatory

Perform the following configuration on the NTP passive peer.

Table 4-13 Configure the NTP passive peer authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the NTP authentication function	**ntp authenticate**	Mandatory By default, do not enable the NTP authentication function.
Configure the authentication key	**ntp authentication-key** *key-number* **md5 {0** *plain-key* **| 7** *cipher-key***}**	Mandatory By default, do not configure the authentication key.
Specify the key as the trusted key	**ntp trusted-key** *key-number*	Mandatory By default, do not specify the trusted key

Note:

- The active peer and passive peer need to be configured with the same authentication key.

Configure NTP Broadcast Authentication

When configuring the NTP broadcast authentication, it is necessary to enable the authentication function on the broadcast client and broadcast server, configure the authentication key, set the authentication key as the trusted key, and specify the key associated with the broadcast server.

Perform the following configuration on the NTP broadcast client.

Table 4-14 Configure the NTP broadcast client authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the NTP authentication function	**ntp authenticate**	Mandatory By default, do not enable the NTP authentication function.
Configure the authentication key	**ntp authentication-key** *key-number* **md5 {0** *plain-key* **| 7** *cipher-key***}**	Mandatory By default, do not configure the authentication key.
Specify the key as the trusted key	**ntp trusted-key** *key-number*	Mandatory By default, do not specify the trusted key.

Perform the following configuration on the NTP broadcast server.

Table 4-15 Configure the NTP broadcast server authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the NTP authentication function	**ntp authenticate**	Mandatory By default, do not enable the NTP authentication function.

Step	Command	Description
Configure the authentication key	**ntp authentication-key** *key-number* **md5 {0** *plain-key* **| 7** *cipher-key***}**	Mandatory By default, do not configure the authentication key.
Specify the key as the trusted key	**ntp trusted-key** *key-number*	Mandatory By default, do not specify the trusted key.
Enter the interface configuration mode	**interface** *interface-name*	-
Specify the key associated with the broadcast server	**ntp broadcast-server** [**version** *version-number*] **key** *key-number*	Mandatory

Note:

- The broadcast server and broadcast client need to be configured with the same authentication key.

4.2.4. Configure NTP Access Control

Configuration Condition

To configure the NTP access control, first complete the following task:

- Configure the ACL associated with the access control

Configure NTP Access Control

NTP can limit the access for the local NTP server by associating with ACL.

Table 4-16 Configure the NTP access control

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the NTP access control	**ntp access-control list** *access-list-name*	Mandatory By default, do not configure the NTP access control.

4.2.5. NTP Monitoring and Maintaining

Table 4-17 NTP Monitoring and Maintaining

Command	Description
show ntp associations [ipv6]	Display the NTP session information
show ntp status	Display the NTP status information
snmp-server enable traps ntp [stratum-change | sync-lost | sync-success]*	Enable the Trap function of NTP

4.3. NTP Typical Configuration Example

4.3.1. Configure NTP IPv4 Server and Client

Network Requirements

- Device1 is the NTP server and Device2 is the NTP client.
- Device1 and Device2 are interconnected via their interface gigabitethernet 0 and the route is reachable.
- The NTP server is the clock source and the client gets the clock from the server.

Network Topology

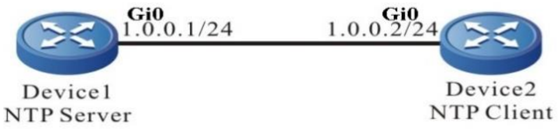


Figure 4-1 Networking of configuring NTP server and client

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted)

Step 2: Configure the NTP server Device1.

#Enable NTP IPv4 of Device1, configure Moscow time zone, local clock and number of layers is 3.

```
Device1#configure terminal Device1(config)#ntp enable
Device1(config)#clock timezone MOSCOW 3
Device1(config)#ntp master 3
Device1(config)#exit
```

Step 3: Configure Device2 as the NTP client2.

#Enable the NTP IPV4 of Device2, and configure the time zone as the Moscow time zone.

```
Device2#configure terminalDevice2(config)#ntp enable
Device2(config)#clock timezone MOSCOW 3
```

#Specify the NTP server Device1 and the IP address is 1.0.0.1.

```
Device2(config)#ntp server 1.0.0.1
Device1(config)#exit
```

Step 4: Check the result.

#Execute the **show ntp status** command on the client Device2, and view the clock synchronization status, indicating that the client and NTP server Device1 are synchronized and the clock layers is 4, larger than Device1.

```
Device2#show ntp status
Current NTP status information
 NTP ipv4 is enabled
 NTP ipv6 is disabled
Clock is synchronized, stratum 4, reference is 1.0.0.1
reference time is D442EB0E.432F29BD (01:49:02.262 Tue Nov 06 2012)
```

#Execute the **show clock** command to view the device clock on the client Device2.

```
Device2#show clock


MOSCOW(UTC+03:00) TUE NOV 06 09:49:30 2012
```

4.3.2. Configure NTP IPv4 Server and Multi-level Clients

Network Requirement

- Device1 is the NTP server; Device2 and Device3 are the NTP client.
- Device2 are interconnected with Device1 and Device 3 via the interface gigabitethernet 0, gigabitethernet 1; the route is reachable.
- Device1 provides the clock for Device2; Device2 provides the clock for Device3.

Network Topology

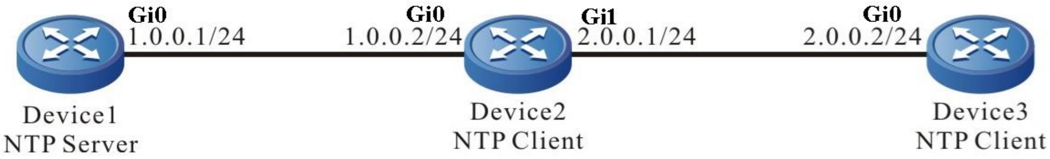


Figure 4-2 Networking of configuring the NTP server and multi-level clients

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted)

Step 2: Configure the NTP server Device1.

#Enable NTP IPv4 of Device1, configure the time zone as Moscow time zone, local clockas reference clock, and number of layers as 3.

```
Device1#configure terminal
Device1(config)#ntp enable
Device1(config)#clock timezone MOSCOW 3
Device1(config)#ntp master 3
Device1(config)#exit
```

Step 3: Configure the NTP client Device2.

#Enable the NTP IPV4 of Device2, and configure the time zone as the Moscow time zone.

```
Device2#configure terminal
Device2(config)#ntp enable
Device2(config)#clock timezone MOSCOW 3
```

#Specify the NTP server Device1 and the IP address is 1.0.0.1.

```
Device2(config)#ntp server 1.0.0.1
```

Step 4: Configure the NTP client Device3.

#Enable the NTP IPV4 of Device3, and configure the time zone as the Moscow time zone.

```
Device3#configure terminal
```

```
Device3(config)#ntp enable
Device3(config)#clock timezone MOSCOW 3
```

#Specify the NTP server Device2 and the IP address is 2.0.0.1.

```
Device3(config)#ntp server 2.0.0.1
```

Step 5: Check the result, viewing the clock synchronization information on Device2 and Device3.

#Execute the **show ntp status** command on the client Device2, and view the clock synchronization status, indicating that the clock layers of Device2 is 1 larger than Device1 and it is 4, indicating that the client Device2 is already synchronized with the server Device1.

```
Device2#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
Clock is synchronized, stratum 4, reference is 1.0.0.1
reference time is D44CC35E.BAA6A190 (13:02:22.729 Tue Nov 13 2012)
```

#Execute the **show clock** command to view the device clock on the client Device2.

```
Device2#show clock

MOSCOW(UTC+03:00) TUE NOV 13 21:02:24 2012
```

#Execute the **show ntp status** command on the client Device3, and view the clock synchronization status, indicating that the clock layers of Device3 is 1 larger than Device2 and it is 5, indicating that the client Device3 is already synchronized with the server Device2.

```
Device3#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
Clock is synchronized, stratum 5, reference is 2.0.0.1
reference time is D44CC365.5CC8C4C8 (13:02:29.362 Tue Nov 13 2012)
```

#Execute the **show clock** command to view the device clock on the client Device3.

```
Device3#show clock

MOSCOW(UTC+03:00) TUE NOV 13 21:02:36 2012
```

4.3.3. Configure NTP Server and Client with MD5 Authentication

Network Requirements

- Device1 is the NTP server; Device2 is the NTP client; both adopt the MD5 algorithm authentication.
- Device1 and Device2 are interconnected via their interface gigabitethernet 0; the route is reachable.
- NTP server is the clock source and the client gets the clock from the server.

Network Topology

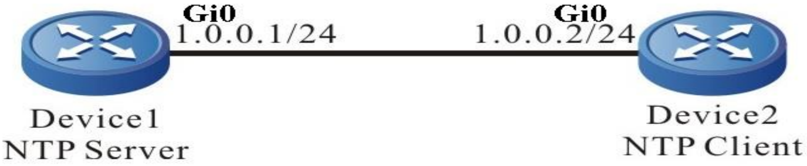


Figure 4-3 Networking of configuring the NTP server and client with MD5 authentication

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted)

Step 2: Configure the NTP server.

#Enable NTP IPv4 of Device1, configure the time zone as Moscow time zone, local clockas reference clock, and number of layers as 3.

```
Device1#configure terminal
Device1(config)#ntp enable
Device1(config)#clock timezone MOSCOW 3
Device1(config)#ntp master 3
Device1(config)#exit
```

#Enable the authentication.

```
Device1(config)#ntp authenticate
```

#Configure the authentication key serial number as 1, algorithm as MD5 and key as admin.

```
Device1(config)#ntp authentication-key 1 md5 0 admin
```

#Configure the key 1 be trusted.

```
Device1(config)#ntp trusted-key 1
```

Step 3: Configure the NTP client.

#Enable the NTP IPV4 of Device2, and configure the time zone as the Moscow time zone.

```
Device2#configure terminal
Device2(config)#ntp enable
Device2(config)#clock timezone MOSCOW 3
```

#Specify the NTP server for the client and the IP address is 1.0.0.1.

```
Device2(config)#ntp server 1.0.0.1
```

#Enable the authentication.

```
Device2(config)#ntp authenticate
```

#Configure the authentication key serial number as 1, algorithm as MD5 and key as admin.

```
Device2(config)#ntp authentication-key 1 md5 0 admin
```

#Configure the key 1 be trusted.

```
Device2(config)#ntp trusted-key 1
```

Step 4: Check the result.

#Execute the **show ntp status** command on the client Device2, and view the clock synchronization status, indicating that the clock layers of Device2 is 1 larger than Device1 and it is 4, indicating that the client Device3 is already synchronized with the server Device1.

```
Device2#show ntp status
Current NTP status information
NTP ipv4 is enabled
 NTP ipv6 is disabled
Clock is synchronized, stratum 4, reference is 1.0.0.1
reference time is D442ECE1.8BB7B219 (01:56:49.545 Tue Nov 06 2012)
```

#Execute the **show clock** command to view the device clock on the client Device2.

```
Device2#show clock


MOSCOW(UTC+03:00) TUE NOV 06 09:56:52 2012
```

Caution:

- The authentication serial numbers of the NTP client and server should be the same and the keys should be the same.

4.3.4. Configure NTP IPv4 Peer Mode

Network Requirements

- Device1, Device2, and Device3 are interconnected via their interfaces; the route is reachable.
- Device1 sets the local clock as the reference clock and the number of the layers is 3.
- Device2 is the NTP client; set Device1 to the NTP server.
- Device3 sets Device2 as the peer, Device3 is the active peer, and Device2 is the passive peer.

Network Topology

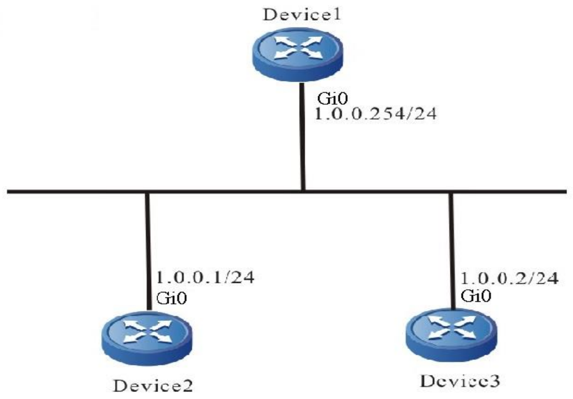


Figure 4-4 Networking of configuring the NTP peer mode

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Enable NTP IPv4 of Device1, configure the time zone as Moscow time zone, local clockas reference clock, and number of layers as 3.

```
Device1#configure terminal
Device1(config)#ntp enable
Device1(config)#clock timezone MOSCOW 3
Device1(config)#ntp master 3
Device1(config)#exit
```

Step 3: Device2 specifies Device1 as the NTP server.

#Enable the NTP IPV4 of Device2, and configure the time zone as the Moscow time zone.

```
Device2#configure terminal
Device2(config)#ntp enable
Device2(config)#clock timezone MOSCOW 3
```

#Specify the IP address of the NTP server as 1.0.0.254.

```
Device2(config)#ntp server 1.0.0.254
```

Step 4: Device3 sets Device2 as the peer.

#Enable the NTP IPV4 of Device3, and configure the time zone as the Moscow time zone.

```
Device3#configure terminal
Device3(config)#ntp enable
Device3(config)#clock timezone MOSCOW 3
```

#Specify the IP address of the NTP peer as 1.0.0.1.

```
Device3(config)#ntp peer 1.0.0.1
```

Step 5: Check the result.

#Execute the **show ntp status** command on the client Device2 and view the clock synchronization status information.

```
Device2#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
Clock is synchronized, stratum 4, reference is 1.0.0.254
reference time is D8E9785D.221F1F5 (03:09:17.8 Tue Apr 28 2015)
```

The layers of Device2 clock is 4, larger than Device1 by 1, and the reference clock server address is 1.0.0.254, indicating that the client Device2 is already synchronized with the server Device1.

#Execute the **show clock** command to view the device clock on the client Device2.

```
Device2#show clock


MOSCOW(UTC+03:00) TUE APR 28 11:10:36 2015
```

#Execute the **show ntp status** command on the active peer Device3 and view the clock synchronization status information.

```
Device3#show ntp status
Current NTP status information
 NTP ipv4 is enabled
 NTP ipv6 is disabled
Clock is synchronized, stratum 5, reference is 1.0.0.1
reference time is D8E9795C.29835CC9 (03:13:32.162 Tue Apr 28 2015)
```

The layers of Device3 clock is 5, larger than Device2 by 1, and the reference clock server address is 1.0.0.1, indicating that the active peer Device3 is already synchronized with the passive peer Device2.

#Execute the **show clock** command to view the device clock on client Device3.

```
Device3#show clock


MOSCOW(UTC+03:00) TUE APR 28 11:16:19 2015
```

4.3.5. Configure NTP Broadcast Mode

Network Requirements

- Device1, Device2, and Device3 are interconnected via their interfaces; the route is reachable.
- Device1 sets the local clock as the reference clock and the number of the layers is 3.
- Device1 is the NTP broadcast server and sends the NTP broadcast packet from the interface gigabitethernet0.

- Device2 and Device3 are the NTP broadcast client, monitoring the NTP broadcast packet on their interface gigabitethernet0.

Network Topology

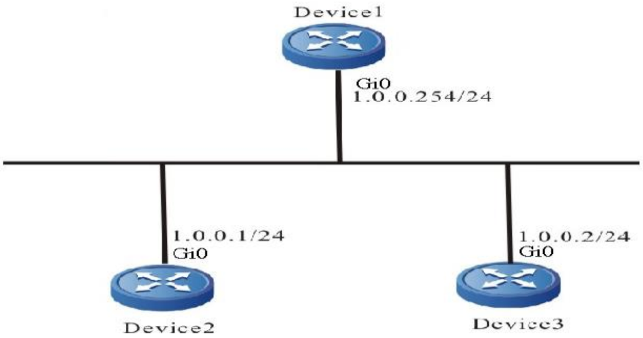


Figure 4-5 Networking of configuring the NTP broadcast mode

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Device1 sets the local clock as the reference clock and the number of the layers is 3; configure Device1 as the NTP broadcast server, sending the NTP broadcast packet from the interface gigabitethernet0.

#Enable NTP IPv4 of Device1, configure the time zone as Moscow time zone, local clockas reference clock, and number of layers as 3.

```
Device1#configure terminal
Device1(config)#ntp enable
Device1(config)#clock timezone MOSCOW 3
Device1(config)#ntp master 3
Device1(config)#exit
```

#Configure Device1 as the NTP broadcast server, sending the NTP broadcast packet from the interface gigabitethernet0.

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ntp broadcast-server
```

Step 3: Configure Device2 as the NTP broadcast client, monitoring the NTP broadcast packet on the interface gigabitethernet0.

```
Device2#configure terminal
Device2(config)#ntp enable
Device2(config)#clock timezone MOSCOW 3
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ntp broadcast-client
```

Step 4: Configure Device3 as the NTP broadcast client, monitoring the NTP broadcast packet on the interface gigabitethernet0.

```
Device3#configure terminal
Device3(config)#ntp enable
Device3(config)#clock timezone MOSCOW 3
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#ntp broadcast-client
```

Step 5: Execute the **show ntp status** command on the client Device2 and view the clock synchronization status information.

```
Device2#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
Clock is synchronized, stratum 4, reference is 1.0.0.254
reference time is D8E97C99.5110D9FE (03:27:21.316 Tue Apr 28 2015)
```

The number of Device2 clock layers is 4, larger than Device1 by 1, and the reference clock server address is 1.0.0.254, indicating that the client Device2 is already synchronized with the server Device1.

#Execute the show clock command to view the device clock on the client Device2.

```
Device2#show clock
MOSCOW(UTC+03:00) TUE APR 28 11:27:22 2015
```

#Execute the **show ntp status** command on the active peer Device3 and view the clock synchronization status information.

```
Device3#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
Clock is synchronized, stratum 4, reference is 1.0.0.254
reference time is D8E97CAC.78F42CA6 (03:27:40.472 Tue Apr 28 2015)
```

The layers of Device3 clock is 4, larger than Device1 by 1, and the reference clock server address is 1.0.0.254, indicating that the active peer Device3 is already synchronized with the server Device1.

#Execute the **show clock** command to view the device clock on client Device3.

```
Device3#show clock
MOSCOW(UTC+03:00) TUE APR 28 11:27:41 2015
```

4.3.6. Configure NTP IPv6 Server and Client

Network Requirements

- Device1 is the NTP server and Device2 is the NTP client.

- Device1 and Device2 are interconnected via their interface gigabitethernet 0 and the route is reachable.
- The NTP server is the clock source and the client gets the clock from the server.

Network Topology

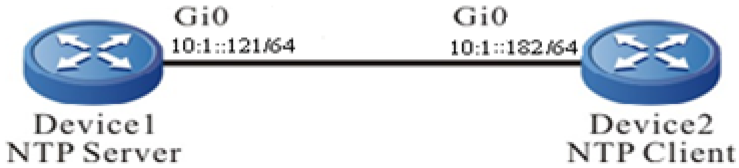


Figure 4-6 Networking of configuring NTP IPv6 server and client

Configuration Steps

Step 1: Configure the IPv6 address of the interface. (Omitted)

Step 2: Configure the NTP server Device1.

#Enable NTP IPv6 of Device1, configure Moscow time zone, local clock and number of layers is 3.

```
Device1#configure terminal
Device1(config)#ntp enable ipv6
Device1(config)#clock timezone MOSCOW 3
Device1(config)#ntp master 3
Device1(config)#exit
```

Step 3: Configure Device2 as the NTP client2.

#Enable the NTP IPV6 of Device2, and configure the time zone as the Moscow time zone.

```
Device2#configure terminal
Device2(config)#ntp enable ipv6
Device2(config)#clock timezone MOSCOW 3
```

#Specify the NTP server Device1 and the IPv6 address is 10:1::121.

```
Device2(config)#ntp server ipv6 10:1::121
Device2(config)#exit
```

Step 4: Check the result.

#Execute the **show ntp status** command on the client Device2, and view the clock synchronization status, indicating that the client and NTP server Device1 are synchronized and the clock layers is 4, larger than Device1.

```
Device2#show ntp status
Current NTP status information
 NTP ipv4 is disabled
NTP ipv6 is enabled
Clock is synchronized, stratum 4, reference is 10:1::121
```

```
reference time is D442EB0E.432F29BD (01:49:02.262 Tue Nov 06 2012)
```

#Execute the **show clock** command to view the device clock on the client Device2.

```
Device2#show clock
MOSCOW(UTC+03:00) TUE NOV 06 09:49:30 2012
```

4.3.7. Configure NTP IPV6 Peer Mode

Network Requirements

- Device1, Device2, and Device3 are interconnected via their interfaces; the route is reachable.
- Device1 sets the local clock as the reference clock and the number of the layers is 3.
- Device2 is the NTP client; set Device1 to the NTP server.
- Device3 sets Device2 as the peer, Device3 is the active peer, and Device2 is the passive peer.

Network Topology

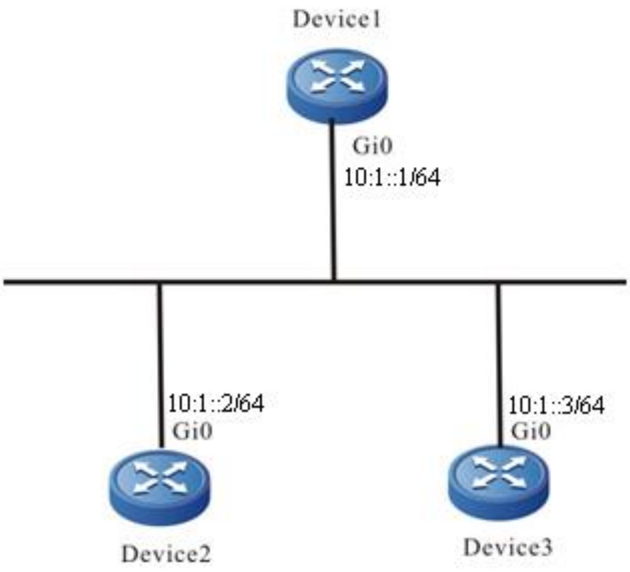


Figure 4-7 Networking of configuring the NTP IPv6 peer mode

Configuration Steps

Step 1: Configure the IPv6 address of the interface. (omitted)

Step 2: Enable NTP IPv6 of Device1, configure the time zone as Moscow time zone, local clockas reference clock, and number of layers as 3.

```
Device1#configure terminal
Device1(config)#ntp enable ipv6
Device1(config)#clock timezone MOSCOW 3
Device1(config)#ntp master 3
```

Step 3: Device2 specifies Device1 as the NTP server.

#Enable the NTP IPV6 of Device2, and configure the time zone as the Moscow time zone.

```
Device2#configure terminal
Device2(config)#ntp enable ipv6
Device2(config)#clock timezone MOSCOW 3
```

#Specify the IPv6 address of the NTP server as 10:1::1.

```
Device2(config)#ntp server ipv6 10:1::1
```

Step 4: Device3 sets Device2 as the peer.

#Enable the NTP IPV6 of Device3, and configure the time zone as the Moscow time zone.

```
Device3#configure terminal
Device3(config)#ntp enable ipv6
Device3(config)#clock timezone MOSCOW 3
```

#Specify the IPv6 address of the NTP peer as 10:1::2.

```
Device3(config)#ntp peer ipv6 10:1::2
```

Step 5: Check the result.

#Execute the **show ntp status** command on the client Device2 and view the clock synchronization status information.

```
Device2#show ntp status
Current NTP status information
NTP ipv4 is disabled
NTP ipv6 is enabled
Clock is synchronized, stratum 4, reference is 10:1::1
reference time is D8E9785D.221F1F5 (03:09:17.8 Tue Apr 28 2015)
```

The layers of Device2 clock is 4, larger than Device1 by 1, and the reference clock server address is 10:1::1, indicating that the client Device2 is already synchronized with the server Device1.

#Execute the **show clock** command to view the device clock on the client Device2.

```
Device2#show clock
MOSCOW(UTC+03:00) TUE APR 28 11:10:36 2015
```

#Execute the **show ntp status** command on the active peer Device3 and view the clock synchronization status information.

```
Device3#show ntp status
Current NTP status information
NTP ipv4 is disabled
 NTP ipv6 is enabled
Clock is synchronized, stratum 5, reference is 10:1::2
reference time is D8E9795C.29835CC9 (03:13:32.162 Tue Apr 28 2015)
```

The layers of Device3 clock is 5, larger than Device2 by 1, and the reference clock server address is 10:1::2, indicating that the active peer Device3 is already synchronized with the passive peer Device2.

#Execute the **show clock** command to view the device clock on client Device3.

```
Device3#show clock
MOSCOW(UTC+03:00) TUE APR 28 11:16:19 2015
```

5. IPFIX

5.1. Overview

IPFIX (IP Flow Information Export) completes the measuring and exporting of the device flow information and is one technology of providing the packet statistics based on the flow. The packets entering the device define the flow according to the source IP address, destination IP address, source port number, destination port number, protocol number, output interface, and input interface. The same tuple is identified as one flow. The information recorded by the flow also can be sent to NMS (Network Management Station) via the UDP packet for the traffic analysis software to analyze. The network manager can complete the analysis and monitoring of the traffic passing the device by analyzing the statistics information recorded by the flow.

At present, QTECH ipfix function provides two modes. The standard mode adopts the standard cflow V9 to collect and export flow data, which can be connected with the NetFlow server; The extended mode is based on the session. It does not distinguish the interface direction, supports the flow compression function, and can only connect with QTECH ICC server.

5.2. IPFIX Function Configuration

Table 5-1IPFIX function configuration list

Configuration Task	
Configure the IPFIX statistics function	Configure the IPFIX function version
	Configure the interface to enable the IPFIX statistics function of the standard mode
	Configure the interface to enable the IPFIX statistics function of the extended mode
Configure the IPFIX sampling function	Configure the IPFIX sampling interval
Configure the IPFIX packet attribute	Configure the destination address and port number of the IPFIX packet
	Configure the source interface of the IPFIX packet
	Configure the interval of sending the IPFIX compression packet
	Configure containing the length of MPLS label stack when calculating MPLS packet load length

Configuration Task	
Configure the IPFIX packet attribute	Configure the period of exporting the IPFIX active flow log
Configure the IPFIX flow template attributes	Configure the update period of the IPFIX flow template time

5.2.1. Configure IPFIX Statistics Function

Enable the IPFIX flow statistics function on the interface and measure the traffic information on the interface.

Configuration Condition

None

Configure IPFIX Function Version

Table 5-2 Configure the IPFIX work mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the IPFIX work mode	**ipfix version { standard | extended }**	Optional By default, the standard mode is enabled.

Note:

- standard mode: netflow v9 mode defined by RFC, which can be connected to common servers.
- extended mode: regardless of direction, it is no longer required to configure the access direction of data flow under the interface, but can only be connected with the supporting flow collection platform of QTECH.

Configure the Interface to Enable IPFIX Statistics Function in Standard Mode

Table 5-3 Configure the interface to enable the IPFIX statistics function in the standard mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Enable the IPFIX statistics function of the interface	**ipfix** {**ip**| **ipv6| mpls** } { **egress** | **ingress** }	Mandatory By default, the IPFIX statistics function is disabled on the interface.

Configure the Interface to Enable IPFIX Statistics Function in extended Mode

Table 5-4 Configure the interface to enable the IPFIX statistics function in the extended mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Enable the IPFIX statistics function of the interface	**ipfix apply** { **ip | ipv6 | mpls }**	Mandatory By default, the IPFIX statistics function is disabled on the interface.

5.2.2. Configure IPFIX Sampling Function

Enable the IPFIX sampling interval on the interface and count the traffic information on the interface according to the sampling interval. The sampling function is not supported in extended mode and will not take effect after configuration.

Configuration Condition

Before configuring the IPFIX sampling statistics function, complete the following task first:

- Enable the IPFIX statistics function on the interface

Configure IPFIX Sampling Function

Table 5-5 Configure IPFIX sampling function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Enable the IPFIX statistics function of the interface	**ipfix** { **ip | ipv6 | mpls**} **sampler** *value*	Mandatory By default, the sampling interval is 1.

5.2.3. Configure IPFIX Packet Attribute

After the device enables the IPFIX flow statistics function, IPFIX measures the traffic information of the interface. After the flow is aged, the device encapsulates the flow information in the IPFIX packet and sends to NMS.

Configuration Condition

None

Configure Destination Address of IPFIX Packet

Configure the destination IP address and destination port number of the IPFIX packet. If the destination address of the IPFIX packet is not configured, the device does not send the IPFIX packet.

Table 5-6 Configure the destination address of the IPFIX packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the destination IP address and port number of the IPFIX packet	**ipfix destination** [**vrf** *vrf-name*] {*ip-address* | **ipv6** *ipv6-address*} *port-number*	Mandatory We can configure two ipv4 destination addresses and two ipv6 destination addresses at most. By default, do not configure the destination IP address and port number of the IPFIX packet.

Configure Source Interface of IPFIX Packet

Configure the source interface of the IPFIX packet. After the configuration, the source address of the IPFIX packet is the configured interface IP address.

Table 5-7 Configure the source interface of the IPFIX packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the source interface of the IPFIX packet	**ipfix source** *interface-name*	Optional By default, the source address of the IPFIX packet is the IP address of the egress interface of the packet.

Configure the Interval of Sending IPFIX Compression Packet

Configure the interval of sending the IPFIX compression packet.

Table 5-8 Configure the interval of sending the IPFIX compression packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the interval of sending the IPFIX compression packet	**ipfix compress timers** *period*	Optional By default, send the compression packet every 30s.

Configure Containing MPLS Label Stack Length when Calculating mpls Packet Load Length

Configure containing the MPLS label stack length when calculating the mpls packet load length.

Table 5-9 Configure containing the MPLS label stack length when calculating the mpls packet load length

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the MPLS label stack length when calculating the mpls packet load length	**ipfix mpls flow length**	Optional By default, the IPFIX packet contains the MPLS label stack length.

Configure the Period of Exporting IPFIX Active Flow Logs

Configure the period of exporting the IPFIX active flow logs.

Table 5-10 Configure the period of exporting the IPFIX active flow logs

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the period of exporting the IPFIX active flow logs	**ipfix timeout active** *minutes*	Optional By default, the period of exporting the active flow logs is 5 minutes.

5.2.4. Configure IPFIX Flow Template Attribute

The flow template on NMS has the life period. After timeout, the flow template will be deleted and as a result, the subsequent flow information cannot be resolved. Therefore, the device needs to send the flow template to NMS periodically. The user can configure how many minutes to send the flow template once.

Configuration Condition

None

Configure Time Update Period of IPFIX Flow Template

Configure the time update period of the PFIX flow template.

Table 5-11 Configure the time update period of the IPFIX flow template

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the time update period of the IPFIX flow template	**ipfix template flow refresh timers** *period*	Optional By default, the update period of the IPFIX flow template is 5 minutes.

5.2.5. IPFIX Monitoring and Maintaining

Table 5-12 IPFIX monitoring and maintaining

Command	Description
clear ipfix { ip | ipv6 } flow	Clear the IPFIX statistics information
show ipfix { **ip | ipv6 } flow** [**proto** *protocol*] [**src-ip** *srcaddr*] [**dst-ip** *dstaddr*] [**src-port** *srcport*] [**dst-port** *dstport*]	Display the flow statistics information

5.3. IPFIX Typical Configuration Example

5.3.1. Configure Basic Functions of IPFIX IPv4 Flow Exporting in Standard Mode

Network Requirements

- Run the traffic analysis software on NMS; Device and NMS route are reachable;
- Enable IPFIX to measure the data flow of the interface gigabitethernet1 on Device and send the statistics result to NMS.

Network Topology

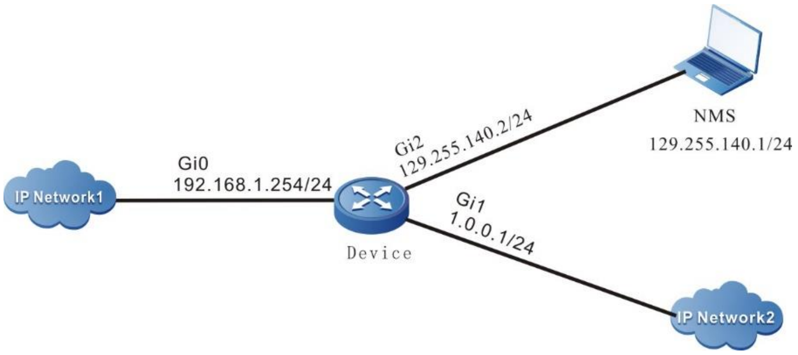


Figure 5-1 Networking of configuring the basic functions of the IPFIX IPv4 flow exporting in standard mode

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Configure IPFIX.

#Configure Device.

On the interface gigabitethernet1, enable IPFIX and measure all data flow of the IPv4 flow received and sent from the interface.

```
Device(config)#interface gigabitethernet1
Device(config-if-gigabitethernet1)#ipfix ip ingress
Device(config-if-gigabitethernet1)#ipfix ip egress
Device(config-if-gigabitethernet1)#exit
```

Configure the destination address and destination port number of the IPFIX packet (that is, NMS address and port number).

```
Device(config)#ipfix destination 129.255.140.1 9996
```

Step 3: Check the result.

#View the Conn table entry of Device.

```
Device#show connection ipv4 table
IPV4 connection table
Protocol  Source:port           Destination:port/other   State        Lifetime  Vrf
--------  ---------------------    ---------------------    ------------- --------
--------
OTHER(253)[10.2.2.10]:0          [192.168.1.1]:0         rawip-open    30       global
TCP       [10.2.2.10]:1024      [192.168.1.1]:1024       tcp-est       3600     global
UDP       [10.2.2.10]:1024       [192.168.1.1]:1024       udp-open      30       global
ICMP      [10.2.2.10]:0         [192.168.1.1]:0          icmp          60       global
```

#View the IPFIX statistics information of Device.

```
Device#show ipfix ip flow
Protocol  SRC:SP                           DST:DP                          INIFPKTS
INIFBYTES     OUTIFPKTS     OUTIFBYTES    DIR
--------  ---------------------           ---------------------           -----
--------  -------------  -------------  -------------  ---
253     [10.2.2.10]:0                [192.168.1.1]:0                3411812      375299320
0             0             0
253     [10.2.2.10]:0                [192.168.1.1]:0                3411812      375299320
0             0             1
6       [10.2.2.10]:1024             [192.168.1.1]:1024             3411812      375299320
0             0             0
6       [10.2.2.10]:1024             [192.168.1.1]:1024             3411812      375299320
0             0             1
17      [10.2.2.10]:1024             [192.168.1.1]:1024             3411812      375299320
0             0             0
17      [10.2.2.10]:1024             [192.168.1.1]:1024             3411812      375299320
0             0             1
1       [10.2.2.10]:0                [192.168.1.1]:0                3411812      375299320
0             0             0
1       [10.2.2.10]:0                [192.168.1.1]:0                3411812      375299320
0             0             1
```

We can see that the device measures the data flow received and sent by the interface gigabitethernet1 and sends the statistics result to NMS.

#NMS can monitor all data flow received and sent by the interface gigabitethernet1 of Device.

5.3.2. Configure Basic Functions of IPFIX IPv6 Flow Exporting in Standard Mode

Network Requirements

- Run the traffic analysis software on NMS; Device and NMS route are reachable;
- Enable IPFIX to measure the IPv6 data flow of the interface gigabitethernet1 on Device and send the statistics result to NMS.

Network Topology

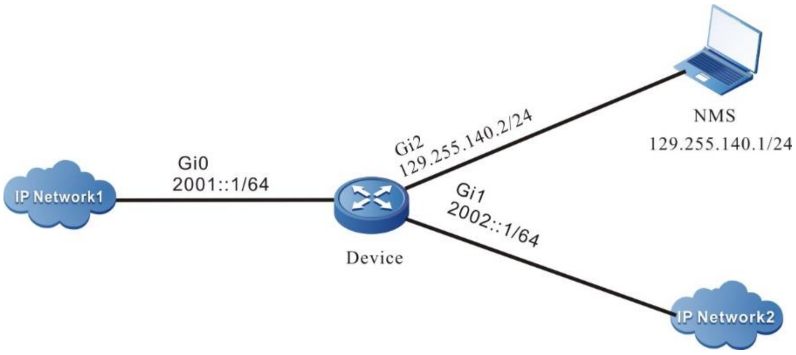


Figure 5-2 Networking of configuring the basic functions of the IPFIX IPv6 flow exporting in standard mode

Configuration Steps

Step 1: Configure the IPv6 address of the interface. (omitted)

Step 2: Configure IPFIX.

#Configure Device.

On the interface gigabitethernet1, enable IPFIX and measure all data flow of the IPv6 flow received and sent from the interface.

```
Device#configure terminal
Device(config)#interface gigabitethernet1
Device(config-if-gigabitethernet1)#ipfix ipv6 ingress
Device(config-if-gigabitethernet1)#ipfix ipv6 egress
Device(config-if-gigabitethernet1)#exit
```

Configure the destination address and destination port number of the IPFIX packet (that is, NMS address and port number).

```
Device(config)#ipfix destination 129.255.140.1 9996
```

Step 3: Check the result.

#View the Conn table entry of Device.

```
Device#show connection ipv6 table
IPV6 connection table
Protocol  Source:port                       Destination:port/other                State
Lifetime    Vrf
-------- ---------------------              ---------------------                     -
------------ -------- --------
OTHER(59) [10::10]:0                          [2001::2]:0                          rawip-
open     30       global
TCP       [10::10]:1024                     [2001::2]:1024                         rawip-
open     30       global
UDP       [10::10]:1024                     [2001::2]:1024                         rawip-
open     30       global
ICMPV6    [10::10]:0                          [2001::2]:0                          rawip-
open     30       global
```

#View the IPFIX statistics information of Device.

```
Device#show ipfix ipv6 flow
Protocol  SRC:SP                            DST:DP                               INIFPKTS
INIFBYTES     OUTIFPKTS     OUTIFBYTES    DIR
-------- ---------------------           ---------------------              -----
-------- ------------- ------------- ------------- ---
59       [10::10]:0                  [2001::2]:0                  2088179      229699690
0           0           0
```

```
59      [10::10]:0                [2001::2]:0              2088179     229699690
0         0         1
6       [10::10]:1024             [2001::2]:1024           2088179     229699690
0         0         0
6       [10::10]:1024             [2001::2]:1024           2088179     229699690
0         0         1
17      [10::10]:1024             [2001::2]:1024           2088179     229699690
0         0         0
17      [10::10]:1024             [2001::2]:1024           2088179     229699690
0         0         1
58      [10::10]:0                [2001::2]:0              2088179     229699690
0         0         0
58      [10::10]:0                [2001::2]:0              2088179     229699690
0         0         1
```

We can see that the device measures the IPv6 data flow received and sent by the interface gigabitethernet1 and sends the statistics result to NMS.

#NMS can monitor all IPv6 data flow received and sent by the interface gigabitethernet1 of Device.

5.3.3. Configure Basic Functions of IPFIX MPLS Flow Exporting in Standard Mode

Network Requirements

- IP Network1 and IP Network2 act as the CE end of MPLS L3VPN.
- Run the traffic analysis software on NMS; the P device and NMS route are reachable;
- Enable IPFIX to measure the data flow of the interface gigabitethernet1 on the P device and send the statistics result to NMS.

Network Topology

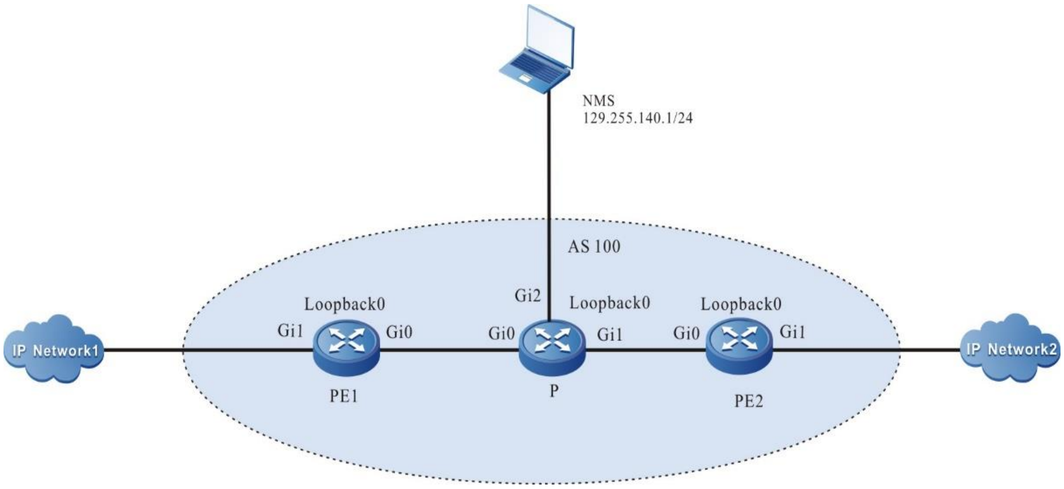


Figure 5-3 Networking of configuring the basic functions of the IPFIX MPLS flow exporting in standard mode

Device	Interface	IP Address	Device	Interface	IP Address
PE1	Gi0	93.1.1.2/24	P	Gi2	129.255.140.2/24
	Gi1	94.1.1.1/24		Loopback0	11.11.11.11/32
	Loopback0	22.22.22.22/32	PE2	Gi0	92.1.1.1/24
P	Gi0	93.1.1.1/24		Gi1	90.1.1.1/24
	Gi1	92.1.1.2/24		Loopback0	33.33.33.33/32

Configuration Steps

Step 1: Configure the IP address of each interface and the network environment of MPLS L3VPN. (omitted. For the specific configuration of MPLS L3VPN environment, refer to MPLS configuration document.)

Step 2: Configure IPFIX.

Enable IPFIX on the interface gigabitethernet1 of the P device to count all MPLS data flows received and sent from the interface.

```
P#configure terminal
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#ipfix mpls ingress
P(config-if-gigabitethernet1)#ipfix mpls egress
P(config-if-gigabitethernet1)#exit
```

Configure the destination address and destination port number of the ipfix packet on the P device (i.e. the address and port number of NMS).

```
P(config)#ipfix destination 129.255.140.1 9996
```

Step 3: Check the result.

#View the Conn statistics information of the P device.

```
P#show connection ipv4 table
IPV4 connection table
Protocol  Source:port           Destination:port/other   State        Lifetime  Vrf
```

```
-------- ---------------------   ---------------------   ------------- ------
-- --------
OTHER(253)[100.0.0.1]:0         [110.0.0.1]:0         rawip-open    30      global
TCP     [100.0.0.1]:1024        [110.0.0.1]:1024      rawip-open    30      global
UDP     [100.0.0.1]:1024        [110.0.0.1]:1024      rawip-open    30      global
ICMP    [100.0.0.1]:0           [110.0.0.1]:0         rawip-open    30      global
```

#View the IPFIX statistics information of the P device.

```
P#show ipfix ip flow
Protocol  SRC:SP                     DST:DP                INIFPKTS     INIFBYTES
OUTIFPKTS   OUTIFBYTES   DIR

-------- ---------------------          ---------------------     ------------
- ------------- ------------- ------------- ---
253      [100.0.0.1]:0               [110.0.0.1]:0           3411812      375299320     0
0          0
253      [100.0.0.1]:0               [110.0.0.1]:0           3411812      375299320     0
0          1
6       [100.0.0.1]:1024            [110.0.0.1]:1024          3411812      375299320     0
0          0
6       [100.0.0.1]:1024            [110.0.0.1]:1024          3411812      375299320     0
0          1
17      [100.0.0.1]:1024            [110.0.0.1]:1024          3411812      375299320     0
0          0
17      [100.0.0.1]:1024            [110.0.0.1]:1024          3411812      375299320     0
0          1
1       [100.0.0.1]:0               [110.0.0.1]:0           3411812      375299320     0
0          0
1       [100.0.0.1]:0               [110.0.0.1]:0           3411812      375299320     0
0          1
```

We can see that the P device measures the MPLS data flow received and sent by the interface gigabitethernet1 and sends the statistics result to NMS.

#NMS can monitor all MPLS data flow received and sent by the interface gigabitethernet1 of the P device.

5.3.4. Configure Basic Functions of IPFIX IPv4 Flow Exporting in extended Mode

Network Requirements

- Run the traffic analysis software on NMS; Device and NMS route are reachable;
- Enable IPFIX to measure the data flow of the interface gigabitethernet0 and gigabitethernet1on Device and send the statistics result to NMS.

Network Topology

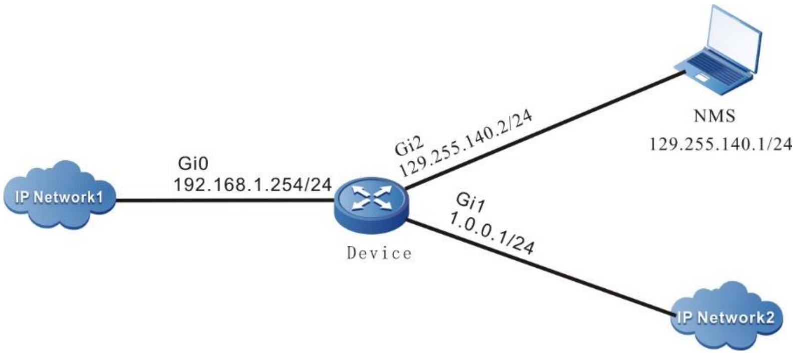


Figure 5-4 Networking of configuring the basic functions of the IPFIX IPv4 flow exporting in extended mode

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Configure IPFIX.

#Configure Device.

On the interface gigabitethernetg 0 and igabitethernet1, enable IPFIX and measure all data flow of the IPv4 flow received and sent from the interface.

```
Device(config)#ipfix version extended
Would you want to change ipfix version ?(y/n)y
Device(config)#interface gigabitethernet0
Device(config-if-gigabitethernet0)#ipfix apply ip
Device(config-if-gigabitethernet0)#exit
Device(config)#interface gigabitethernet1
Device(config-if-gigabitethernet1)#ipfix apply ip
Device(config-if-gigabitethernet1)#exit
```

Configure the destination address and destination port number of the IPFIX packet (that is, NMS address and port number).

```
Device(config)#ipfix destination 129.255.140.1 9996
```

Note:

- In the extended mode, it is necessary to enable the corresponding ipfix on both the ingress and egress interfaces.

Step 3: Check the result.

#View the Conn statistics information of Device.

```
Device#show connection ipv4 table
IPV4 connection table
Protocol  Source:port           Destination:port/other   State        Lifetime  Vrf
--------  ---------------------  ---------------------  ------------- --------
  --------
```

```
OTHER(253)[10.2.2.10]:0        [192.168.1.1]:0        rawip-open    30      global
TCP      [10.2.2.10]:1024      [192.168.1.1]:1024     tcp-est      3600     global
UDP      [10.2.2.10]:1024      [192.168.1.1]:1024      udp-open     30       global
ICMP     [10.2.2.10]:0         [192.168.1.1]:0        icmp        60       global
```

#View the IPFIX statistics information of Device.

```
Device#show ipfix ip flow
Protocol  SRC:SP                              DST:DP                              INIFPKTS
INIFBYTES     OUTIFPKTS     OUTIFBYTES     DIR

-------- ---------------------          ---------------------           -----
-------- ------------- ------------- ------------- ---
253      [10.2.2.10]:0                 [192.168.1.1]:0                 3411812     375299320
3411812       375299320
6        [10.2.2.10]:1024              [192.168.1.1]:1024              3411812     375299320
3411812       375299320
17       [10.2.2.10]:1024              [192.168.1.1]:1024              3411812     375299320
3411812       375299320
1        [10.2.2.10]:0                 [192.168.1.1]:0                 3411812     375299320
3411812       375299320
```

We can see that the device measures the data flow and sends the statistics result to NMS.

#NMS can monitor the exported flow on Device.

Note:

- In the extended mode, the direction is not distinguished, and the bi-directional flows with the same five tuples are combined into a flow log

5.3.5. Configure Basic Functions of IPFIX IPv6 Flow Exporting in extended Mode

Network Requirements

- Run the traffic analysis software on NMS; Device and NMS route are reachable;
- Enable IPFIX to measure the IPv6 data flow of the interface gigabitethernet0 and gigabitethernet1on Device and send the statistics result to NMS.

Network Topology

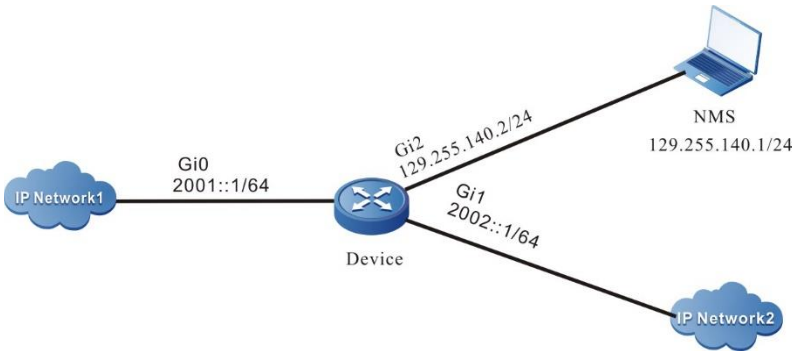


Figure 5-5 Networking of configuring the basic functions of the IPFIX IPv6 flow exporting in extended mode

Configuration Steps

Step 1: Configure the IPv6 address of the interface. (omitted)

Step 2: Configure IPFIX.

#Configure Device.

On the interface gigabitethernetg 0 and igabitethernet1, enable IPFIX and measure all IPv6 data flow of the IPv4 flow received and sent from the interface.

```
Device#configure terminal
Device(config)#ipfix version extended
Would you want to change ipfix version ?(y/n)y
Device(config)#interface gigabitethernet0
Device(config-if-gigabitethernet0)#ipfix apply ipv6
Device(config-if-gigabitethernet0)#exit
Device(config)#interface gigabitethernet1
Device(config-if-gigabitethernet1)#ipfix apply ipv6
Device(config-if-gigabitethernet1)#exit
```

Configure the destination address and destination port number of the IPFIX packet (that is, NMS address and port number).

```
Device(config)#ipfix destination 129.255.140.1 9996
```

Note:

- In the extended mode, it is necessary to enable the corresponding ipfix on both the ingress and egress interfaces.

Step 3: Check the result.

#View the Conn statistics information of Device.

```
Device#show connection ipv6 table
IPV6 connection table
Protocol Source:port                    Destination:port/other            State
Lifetime  Vrf
--------- ---------------------          ---------------------              -
------------ -------- --------
OTHER(59) [10::10]:0                     [2001::2]:0                     rawip-
open     30       global
TCP      [10::10]:1024                  [2001::2]:1024                   rawip-
open     30       global
UDP      [10::10]:1024                  [2001::2]:1024                   rawip-
open     30       global
ICMPV6    [10::10]:0                     [2001::2]:0                     rawip-
open     30       global
```

#View the IPFIX statistics information of Device.

```
Device#show ipfix ipv6 flow
Protocol  SRC:SP                              DST:DP                              REQPKTS
REQBYTES      RESPKTS      RESBYTES      DIR
--------  ---------------------          ---------------------          -----
--------  -------------  -------------  -------------  ---
59       [10::10]:0                  [2001::2]:0                 2088179      229699690
2088179       229699690
6       [10::10]:1024               [2001::2]:1024              2088179      229699690
2088179       229699690
17       [10::10]:1024               [2001::2]:1024              2088179      229699690
2088179       229699690
58       [10::10]:0                  [2001::2]:0                 2088179      229699690
2088179       229699690
```

We can see that the device measures the IPv6 data flow and sends the statistics result to NMS.

#NMS can monitor the all IPv6 flows received and sent by Device.

Note:

- In the extended mode, the direction is not distinguished, and the bi-directional flows with the same five tuples are combined into a flow log.

5.3.6. Configure Basic Functions of IPFIX MPLS Flow Exporting in Extended Mode

Network Requirements

- IP Network1 and IP Network2 act as the CE end of MPLS L3VPN.
- Run the traffic analysis software on NMS; the P device and NMS route are reachable;
- Enable IPFIX to measure the data flow of the interface gigabitethernet0 and gigabitethernet1 on the P device and send the statistics result to NMS.

Network Topology

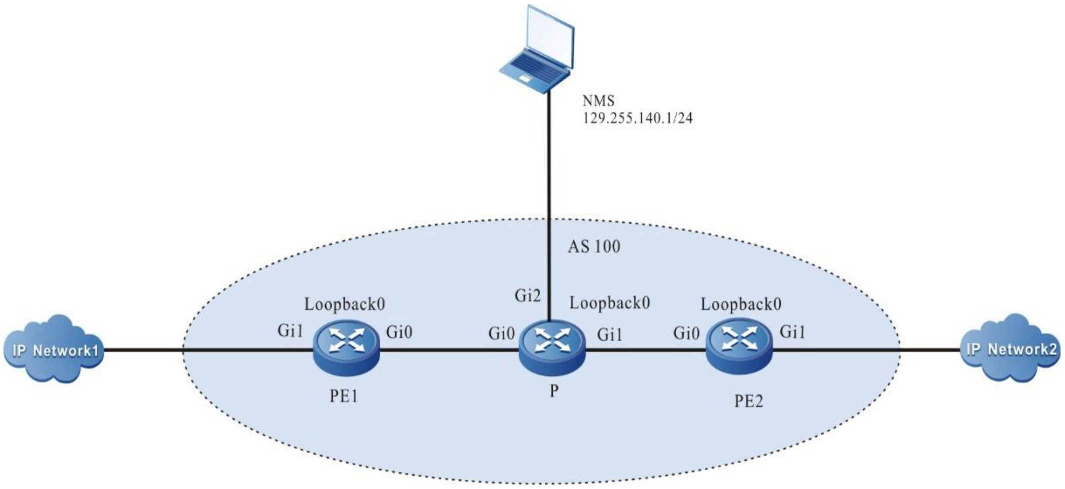


Figure 5-6 Networking of configuring the basic functions of the IPFIX MPLS flow exporting in extended mode

Device	Interface	IP Address	Device	Interface	IP Address
PE1	Gi0	93.1.1.2/24	P	Gi2	129.255.140.2/24
	Gi1	94.1.1.1/24		Loopback0	11.11.11.11/32
	Loopback0	22.22.22.22/32	PE2	Gi0	92.1.1.1/24
P	Gi0	93.1.1.1/24		Gi1	90.1.1.1/24
	Gi1	92.1.1.2/24		Loopback0	33.33.33.33/32

Configuration Steps

Step 1: Configure the IP address of each interface and the network environment of MPLS L3VPN. (omitted. For the specific configuration of MPLS L3VPN environment, refer to MPLS configuration document.)

Step 2: Configure IPFIX.

Enable IPFIX on the interface gigabitethernet0 and gigabitethernet1 of the P device to count all MPLS data flows received and sent from the interface.

```
P#configure terminal
P(config)#ipfix version extended
Would you want to change ipfix version ?(y/n)y
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#ipfix apply mpls
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#ipfix apply mpls
P(config-if-gigabitethernet1)#exit
```

Configure the destination address and destination port number of the ipfix packet on the P device (i.e. the address and port number of NMS).

```
P(config)#ipfix destination 129.255.140.1 9996
```

Note:

- In the extended mode, it is necessary to enable the corresponding ipfix on both the ingress and egress interfaces.

Step 3: Check the result.

#View the Conn statistics information of the P device.

```
P#show connection ipv4 table
IPV4 connection table
Protocol  Source:port           Destination:port/other   State       Lifetime  Vrf
--------  ---------------------    ---------------------    ------------- --------  --------
OTHER(253)[100.0.0.1]:0          [110.0.0.1]:0          rawip-open    30      global
TCP       [100.0.0.1]:1024       [110.0.0.1]:1024       rawip-open    30      global
UDP       [100.0.0.1]:1024       [110.0.0.1]:1024       rawip-open    30      global
ICMP      [100.0.0.1]:0          [110.0.0.1]:0          rawip-open    30      global
```

#View the IPFIX statistics information of the P device.

```
P#show ipfix ip flow
Protocol  SRC:SP                         DST:DP                         INIFPKTS
INIFBYTES    OUTIFPKTS    OUTIFBYTES    DIR
--------  ---------------------          ---------------------          -----
--------  -------------  -------------  -------------  ---
253     [100.0.0.1]:0                [110.0.0.1]:0                3411812      375299320
3411812       375299320
6       [100.0.0.1]:1024             [110.0.0.1]:1024             3411812      375299320
3411812       375299320
17      [100.0.0.1]:1024             [110.0.0.1]:1024             3411812      375299320
3411812       375299320
1       [100.0.0.1]:0                [110.0.0.1]:0                3411812      375299320
3411812       375299320
```

We can see that the P device measures the MPLS data flow and sends the statistics result to NMS.

#NMS can monitor the exported MPLS flow of the P device.

Note:

- In the extended mode, the direction is not distinguished, and the bi-directional flows with the same five tuples are combined into a flow log

6. LLDP

6.1. Overview

6.1.1. Overview of LLDP Protocol

LLDP (Link Layer Discovery Protocol) is the link layer protocol defined in the IEEE 802.1ab standard. It organizes the information of the local device to TLV (Type/Length/Value), encapsulates in LLDPDU (Link Layer Discovery Protocol Data Unit) and sends to the direct-connected neighbor device. Meanwhile, it saves the LLDPDU received from the neighbor device in the standard MIB (Management Information Base) mode. With LLDP, the device can save and manage its own and direct-connected neighbor device information for the network management system to query and judge the link communication status.

6.1.2. TLV Type Information

TLV that LLDP can encapsulate includes the basic TLV, organization-defined TLV and MED (Media Endpoint Discovery) TLV. Basic TLV is a group of TLV regarded as the basis of the network device management. Organization defined TLV and MED TLV is the TLV defined by the standard organization and other institutions, used to strengthen the management for the network devices. We can configure whether to release in LLDPDU according to the actual demand.

Basic TLV

In basic TLV, there are several types of TLV, which are mandatory for realizing the LLDP function, that is, should release in LLDPDU, as shown in the following table.

Table 6-1 Description of the basic TLV

TLV Type	Description	Whether to release
End of LLDPDU TLV	Indicate LLDPDU end	Yes
Chassis ID TLV	The MAC address of the sending device	Yes
interface ID TLV	Used to identify the port of the LLDPDU sending end; when the device does not send MED TLV, the content is the port name; when selecting to send MED TLV, the content is the MAC address of the port.	Yes
Time To Live TLV	The live time of the local device information on the neighbor device	Yes

TLV Type	Description	Whether to release
interface Description TLV	The description character string	No
System Name TLV	The device name	No
System Description TLV	The system description	No
System Capabilities TLV	The main functions of the system and which functions can be enabled	No
Management Address TLV	Management address, corresponding interface number and oid (object identifier). The management address can be a manually configured IP address; If not configured, select the primary IP address of the management port of the device; If the management interface is not configured, for the L2 Ethernet interface, select the primary IP address that the interface allows to pass through the VLAN; For the L3 Ethernet interface, select its configured IP address; If no IP address is configured above, the management address value is not supported. The TLV is sent by default.	Yes

TLV Defined by Organization

TLV defined by the organization includes TLV defined by 802.1 Organization and TLV defined by 802.3 Organization, as shown in the following table.

Table 6-2 Description of the TLV defined by the 802.1 organization

TLV Type	Description	Whether to release
Port VLAN ID TLV	Port VLAN ID	No
Port And Protocol VLAN ID TLV	Port protocol VLAN ID	No
VLAN Name TLV	Port VLAN name	No
Protocol Identity TLV	The protocol type supported by the port. The local device does not support sending protocol identity TLV, but can receive this type of TLV	No

Table 6-3 Description of the TLV defined by the 802.3 organization

TLV Type	Description	Whether to release
MAC/PHY Configuration/Status TLV	The rate and duplex status of the port, whether the port rate auto negotiation is supported, whether the auto negotiation function is enabled, and the current rate and duplex status	No
Power Via MDI TLV	Power supply capability of the port	No
Link Aggregation TLV	Whether the port supports link aggregation and whether to enable link aggregation	No
Maximum Frame Size TLV	The maximum frame length supported is the MTU (max transmission unit) configured by the port	No

MED TLV

The MED TLV information is as shown in the following table.

Table 6-4 The description of MED TLV

TLV Type	Description	Whether to release
LLDP-MED Capabilities TLV	The MED device type of the device and the LLDP MED TLV type that can be encapsulated in LLDPDU	No
Hardware Revision TLV	The hardware version of the device	No
Firmware Revision TLV	The firmware version of the device	No
Software Revision TLV	The software version of the device	No
Serial Number TLV	The serial number of the device	No
Manufacturer Name TLV	The manufacturer of the device	No
Model Name TLV	The module name of the device	No
Asset ID TLV	The asset ID of the device for directory management and asset tracking	No
Location Identification TLV	The location ID information of the connected device, used by the other devices in the application based on the location	No
Network Policy TLV	VLAN ID of the port, supported applications (such as voice and video), priority of applications, policies used, etc	No

6.1.3. LLDP Work Mechanism

LLDP Work Mode

The port includes the following four LLDP work modes:

- RxTx: send and receive LLDPDU;
- Tx: only send LLDPDU;
- Rx: only receive LLDPDU;
- Disable: do not send or receive LLDPDU.

LLDP Sending Mechanism

The LLDP sending mechanism:

- When the port works in the RxTx or Tx mode, regularly send LLDPDU to the neighbor device according to the sending period of the LLDP packet;
- After the port enables the polling function, regularly poll whether the LLDP concerned configuration in the local device changes. If the configuration changes, send LLDPDU at once. To prevent the frequent change of the local information from causing lots of the sent LLDPDU, it is necessary to delay and wait for some time and then continue to send the next LLDPDU when sending one LLDPDU every time.
- When some configuration related with the local device LLDP changes (for example, select the released TLV type), or if finding the configuration change after enabling the polling function, enable the fast sending mechanism, that is, immediately send the LLDPDU of the specified quantity continuously, and then restore the normal LLDP packet sending period.
- When the global LLDP function is disabled or the port enabled with LLDP executes shutdown, adds to the aggregation group, and disables the LLDP, as well as restarts the device, send one LLDPDU with CLOSE TLV to inform the neighbor device.

LLDP Receiving Mechanism

When the port works in the RxTx or Rx mode, check the validity of the received LLDPDU and the carried TLV. After passing the validity check, save the neighbor information to the local device and set the age time of the neighbor information at the local device according to the TTL (Time To Live) carried in LLDPU. If the TTL value in the received LLDPDU is 0, age the neighbor information at once. The storing capability of the LLDP protocol for the neighbor is limited. Currently, one port of the device supports the information of 200 neighbors at most. The device can store 1000 neighbors at most. If the neighbors reach the threshold, more neighbor advertising packets are dropped and cannot be saved.

6.2. LLDP Function Configuration

Table 6-5 LLDP function configuration list

Configuration Task	
Configure the LLDP basic functions	Enable the global LLDP function
	Enable the interface LLDP function
Configure the LLDP work mode	Configure the LLDP work mode
Configure the TLV that LLDP permits to release	Configure the basic TLV permitted to release
	Configure the organization-defined TLV permitted to release
	Configure the MED TLV permitted to release
Configure the LLDP parameters	Configure the neighbor live time
	Configure the delay of sending packets
	Configure the sending period of packets
	Configure the number of the packets sent fast
	Configure the re-initializing delay
	Configure the period of checking the LLDP configuration

6.2.1. Configure LLDP Basic Functions

Enable the global LLDP function and port LLDP function at the same time so that LLDP can work normally. The local device gets the neighbor device information by interacting LLDPDU with other device.

Configuration Condition

None

Enable Global LLDP Function

Table 6-6 Enable the global LLDP function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the global LLDP function	**lldp run**	Mandatory By default, do not enable the global LLDP function.

Enable Port LLDP Function

Table 6-7 Enable the port LLDP function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2/L3 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the l2/l3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the port LLDP function	**lldp enable**	Mandatory By default, the interface does not enable the LLDP function.

6.2.2. Configure LLDP Work Mode

Configuration Condition

None

Configure LLDP Work Mode

The user can set different work modes according to the role of the device in the network. If it is the seed device (the center device collected by network topology), it is suggested to configure the LLDP work mode as Rx. Otherwise, it is suggested to configure the LLDP work mode as Tx.

Table 6-8 Configure the LLDP work mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2/L3 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the l2/l3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the LLDP work mode as Rx	**lldp receive**	Optional By default, LLDP work mode is RxTx. LLDP work mode is decided by the command **lldp receive** and **lldp transmit** together.
Configure the LLDP work mode as Tx	**lldp transmit**	
Configure the LLDP work mode as RxTx	**lldp receive-transmit**	

6.2.3. Configure TLV Permitted by LLDP to Release

The neighbor device can get to know the details of the local device by releasing TLV.

Configuration Condition

None

Configure Basic TLV Permitted by LLDP to Release

The user can release different basic TLVs according to the actual application demand.

Table 6-9 Configure the basic TLV permitted by LLDP to release

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2/L3 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the l2/l3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the basic TLV LLDP permits to release	**lldp tlv-select** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** } }	Optional By default, permit to release all basic TLVs.

Configure Organization-defined TLV LLDP Permits to Release

The user can release different organization-defined TLVs according to the actual application demand.

Table 6-10 Configure the organization-defined TLV LLDP permits to release

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2/L3 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the l2/l3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the organization-defined TLV LLDP permits to release	**lldp tlv-select { dot1-tlv { all | port-vlan-id | protocol-vlan-id | vlan-name } | dot3-tlv { all | link-aggregation | mac-physic | max-frame-size | power } }**	Optional By default, permit to release all organization-defined TLVs.

Configure MED TLV LLDP Permits to Release

The user can release different MED TLVs according to the actual application demand.

Table 6-11 Configure the MED TLV LLDP permits to release

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2/L3 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the l2/l3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the MED TLV LLDP permits to release	**lldp med-tlv-select** { **all** | **capability** | **location-id elin-address** *phonenum* | **network-policy** | **inventory** }	Optional By default, do not permit to release all MED TLVs.

Note:

- The interface types supporting the LLDP protocol include Ethernet main interface, Ethernet sub interface, L2 Ethernet interface, and Ethernet link aggregation port.

6.2.4. Configure LLDP Parameters

Configuration Condition

None

Configure Neighbor Life Time

Specify the life time of the local device information on the neighbor device by configuring the neighbor TTL so that the neighbor device can delete the local device information after the TTL of the local device arrives.

Table 6-12 Configure the neighbor life time

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the life time of the local device on the neighbor device	**lldp holdtime** *holdtime-value*	Optional By default, the life time of the local device on the neighbor device is 120s.

Configure the Delay of Sending Packets

Configuring the delay of sending packets can prevent the frequent change of the local information from causing lots of LLDPDU to be sent.

Table 6-13 Configure the delay of sending packets

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the delay of sending the LLDP packets	**lldp transmit-delay** *transmit-delay-value*	Optional By default, the delay of sending the LLDP packets is 2s.

Configure Packet Sending Period

The local device regularly sends the LLDP packet to the neighbor device by configuring the period of sending the packets so that the information of the local device on the neighbor device is not aged.

Table 6-14 Configure the period of sending packets

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the period of sending the LLDP packets	**lldp transmit-interval** *transmit-interval-value*	Optional By default, the period of sending the LLDP packets is 30s.

Configure Fast Sent Packet Quantity

When some LLDP configuration of the local device (for example, select the released TLV type) changes, or when the polling mechanism finds that the LLDP concerned configuration information in the local device changes after enabling the polling function, to make other devices discover the change of the local device as soon as possible, enable the fast sending mechanism, that is, continuously send the LLDPDUs of the specified quantity (it is 3 by default) at once, and then restore the normal sending period.

Table 6-15 Configure the fast sent packet quantity

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the number of the fast sent packets	**lldp fast-count** *fast-count-value*	Optional By default, the number of the fast sent packets is 3.

Configure Re-initializing Delay

When the port work mode changes, re-initialize the port protocol status machine. To prevent the frequent change of the port work mode from re-initializing the port protocol status machine continuously, we can configure the re-initializing delay of the port.

Table 6-16 Configure the re-initializing delay

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the re-initializing delay	**lldp reinit** *reinit-value*	Optional By default, the re-initializing delay is 2s.

Configure LLDP Configuration Check Period

To inform the neighbor device in time after the LLDP configuration changes, we can configure the period of checking the LLDP configuration.

Table 6-17 Configure the period of checking the LLDP configuration

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2/L3 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the l2/l3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the polling function and configure the polling period	**lldp check-change-interval** *check-change-interval-value*	Optional By default, the polling function is disabled.

6.2.5. LLDP Monitoring and Maintaining

Table 6-18 LLDP Monitoring and Maintaining

Command	Description
clear lldp neighbors [**interface** *interface-name* | **link-aggregation** *link-aggregation-id*]	Clear the neighbor information
show lldp neighbors [**detail** | **interface** *interface-name* [**detail**] | **link-aggregation** *link-aggregation-id* [**detail**]]	Display the neighbor information
show lldp neighbors oui [**interface** *interface-name* | **link-aggregation** *link-aggregation-id*]	Display neighbor OUI address information and write Voice-VLAN OUI table entry status

Command	Description
clear lldp statistics	Clear the LLDP packet statistics information
show lldp statistics { **interface** *interface-name* | **link-aggregation** *link-aggregation-id* }	Display the received and sent LLDP packet statistics information of the specified port
show lldp	Display the LLDP global configuration information
show lldp interface *interface-name*	Display the LLDP work mode of the specified port and the polling period of checking the LLDP configuration change
show lldp link-aggregation *link-aggregation-id*	Display the LLDP working mode of the specified aggregation group and the polling cycle for checking LLDP configuration changes
show lldp tlv-select [**interface** *interface-name* | **link-aggregation** *link-aggregation-id*]	Display the basic TLV and organization-defined TLV configuration information
show lldp voice neighbors [**detail** | **interface** *interface-name* [**detail**] | **link-aggregation** *link-aggregation-id* [**detail**]]	Display the voice neighbor information

6.3. LLDP Typical Configuration Example

6.3.1. Configure LLDP Basic Functions

Network Requirement

- Configure the LLDP function on Device1, Device2 and Device3, realizing the link-layer neighbor discovery.

Network Topology

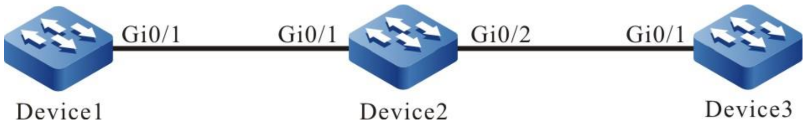


Figure 6-1 Networking of configuring the LLDP basic functions

Configuration Steps

Step 1: Enable the LLDP function on Device.

# Enable the LLDP function on Device1.

```
Device1#configure terminal
Device1(config)#lldp run
```

#Enable the LLDP function on Device2.

```
Device2#configure terminal
Device2(config)#lldp run
```

#Enable the LLDP function on Device3.

```
Device3#configure terminal
Device3(config)#lldp run
```

Step 2: Configure the LLDP function on the interface.

#Enable the LLDP function on port gigabitethernet0 of Device1.

```
Device1(config)#interface gigabitethernet 0
Device1(config-if-gigabitethernet0)#lldp enable
Device1(config-if-gigabitethernet0)#exit
```

#Enable the LLDP function on interface gigabitethernet0/1/0, gigabitethernet0 of Device2.

```
Device2(config)#interface gigabitethernet 0/1/0
Device2(config-if-gigabitethernet0/1/0)#lldp enable
Device2(config-if-gigabitethernet0/1/0)#exit
Device2(config)#interface gigabitethernet 0
Device2(config-if-gigabitethernet0)#lldp enable
Device2(config-if-gigabitethernet0)#exit
```

#Enable the LLDP function on port gigabitethernet0 of Device3.

```
Device3(config)#interface gigabitethernet 0
Device3(config-if-gigabitethernet0)#lldp enable
Device3(config-if-gigabitethernet0)#exit
```

Step 3: Check the result.

#View the neighbor information on Device1.

```
Device1#show lldp neighbors

1 neighbor entries in system
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
```

```
Index    Local Intf          Hold-time  Capability    Peer Intf          Device ID
1       gigabitethernet 0/1    120        B,R          gigabitethernet0/1   Device2
```

Device1 discovers neighbor Device2.

#View the details information of Device1 neighbor.

```
Device1#show lldp neighbors detail
```

Neighbor 1:

1. Basic information

```
Chassis ID                    : ccd8.1f11.c0af
Interface ID                  : gigabitethernet0/1
Interface Description         : gigabitethernet0/1
System Name                   : Device2
System Description            : MyPower (R) Operating System Software Copyright (C)
2020 QTECH Communication
                                Technology Co.,Ltd.All Rights Reserved.
Time Remaining                : 113 seconds
System Capabilities           : B,R
Enabled Capabilities          : B,R
Management Addresses          : Not Supported
```

2. 802.1 organizationally information

```
Port VLAN ID                  : 1
Port And Protocol VLAN ID     : 0
VLAN Name Of VLAN 1           : DEFAULT
```

3. 802.3 organizationally information

```
Auto Negotiation              : Supported, Enabled
PMD Auto Negotiation Advertised : 10BASE-T,10BASE-TFD,100BASE-TX,100BASE-
TXFD,1000BASE-TFD,
Media Attachment Unit Type    : 1000BaseTFD,
Port Class                    : PD
PSE Power                     : Not Supported, Disabled
PSE Pairs Control Ability     : No
Power Pairs                   : 0
Power Class                   : 0
Link Aggregation              : Supported, Disabled
Link Aggregation ID           : 0
Max Translate Unit            : 2048
```

4. MED organizationally information

```
Capabilities                  : Not Supported
```

```
Class Type                : Not Supported
Application Type             : Not Supported
Policy                  : Not Supported
VLAN Tagged                 : Not Supported
VLAN ID                   : Not Supported
L2 Priority               : Not Supported
DSCP Value                 : Not Supported
Location ID               : Not Supported
Power Type                 : Not Supported
Power Source                 : Not Supported
Power Priority              : Not Supported
Power Value                 : Not Supported
HardwareRev                  : Not Supported
FirmwareRev                  : Not Supported
SoftwareRev                 : Not Supported
SerialNum                  : Not Supported
Manufacturer Name                : Not Supported
Model Name                  : Not Supported
Asset Tracking Identifier    : Not Supported
-----------------------------------------------
```

Total entries displayed: 1

Note:

- For viewing the neighbor information of Device2 and Device3, refer to Device1.

7. SNMP

7.1. Overview

SNMP (Simple Network Management Protocol) is one standard protocol of managing Internet. It ensures that the management information can be transmitted between Network Managing Station and managed device SNMP agent. It is convenient for the system administrator to manage the network system.

SNMP is one application layer protocol in the client/server mode. It mainly includes three parts:

- NMS (Network Managing Station)
- SNMP agent
- MIB (Management Information Base)

The structure set of all managed objects maintained by the device is called MIB. The managed objects are organized according to the hierarchical tree structure. MIB defines the network management information got by one device. To be consistent with the standard network management protocol, each device should use the format defined in MIB to display the information. One subset of IOS ASN.1 defines the syntax for MIB. Each MIB uses the tree structure defined in ASN.1 to organize all available information. Each piece of information is one node with punctuation and each node contains one object ID and one short text description.

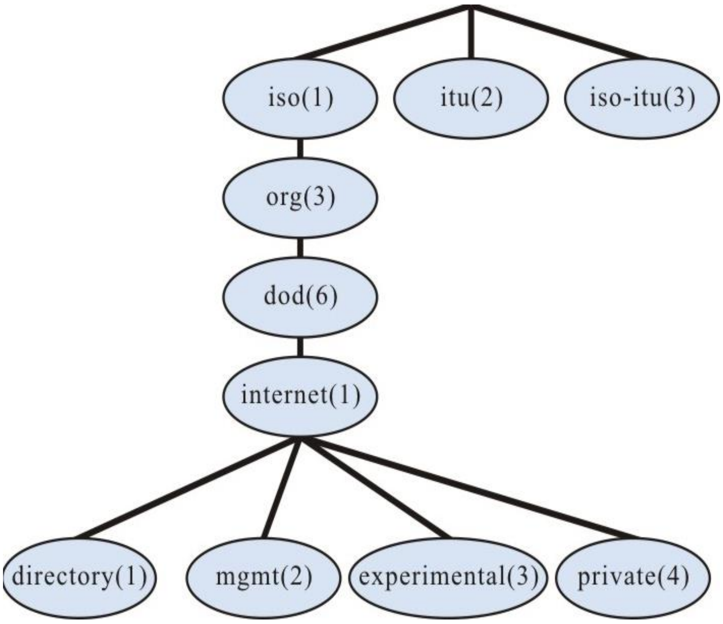


Figure 7-1 ASN.1 tree diagram of network management

SNMP protocol versions include SNMPv1, SNMPv2, and SNMPv3.

- SNMPv1: The first version of the SNMP protocol. The disadvantages: security problem, bandwidth waste, no communication capability between managers, the protocol only provides the limited operations;
- SNMPv2: It makes some improvement on the basis of SNMPv1, making the functions stronger and the security better;
- SNMPv3: original identity, information integrality and some aspects of re-transmission protect, content confidentiality, authorization and process control, the remote configuration and management capability needed by the above three capabilities;

Therefore, the development of SNMPv3 is centralized on two targets, that is, provide the workable security platform at the enhanced architecture and maintain the consistency of the network management system.

The SNMP protocol mainly includes the following operations:

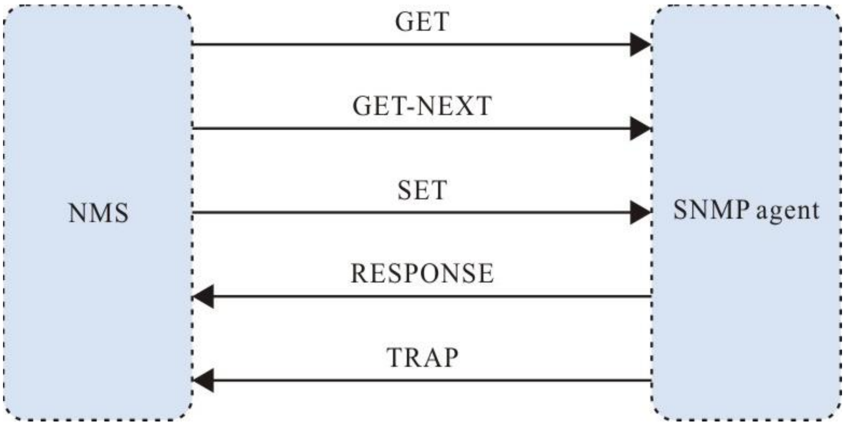


Figure 7-2 SNMP management operation diagram

- Get-request: SNMP network work station gets one or multiple parameters from the SNMP agent.
- Get-next-request: SNMP network work station gets the next parameter of one or multiple parameters from the SNMP agent.
- Get-bulk: SNMP network work station gets the batch parameters from the SNMP agent.
- Set-request: SNMP network work station sets one or multiple parameters of the SNMP agent.
- Get-response: SNMP agent returns one or multiple parameters and it is the responding operation of the SNMP agent for the above three operations.
- Trap: The packet sent by the SNMP agent actively, informing that something happens to the SNMP network work station.

SNMPv1 and SNMPv2 use the authentication name to check whether to have the right to use the MIB object, so only when the authentication name of the network work station is consistent with one authentication name defined in the device, we can manage the device.

The authentication name has the following two attributes:

- Read-only: The read authority of the authorized network work station for all MIB objects of the device;
- Read-write: The read and write authority of the authorized network work station for all MIB objects of the device.

SNMPv3 determines which security mechanism to be adopted to process the data by the security model and the security level. There are three security models: SNMPv1, SNMPv2c, and SNMPv3.

Table 7-1 Supported security model and security level

Security Model	**Security Level**	**Authentication**	**Encryption**	**Description**
SNMPv1	NoAuthNoPriv	Authentication name	None	Confirm the data validity via the authentication name.
SNMPv2c	NoAuthNoPriv	Authentication name	None	Confirm the data validity via the authentication name.
SNMPv3	NoAuthNoPriv	User name	None	Confirm the data validity via the user name.
SNMPv3	AuthNoPriv	MD5/SHA/SM3	None	Use HMAC-MD5/HMAC-SHA/SM3 data authentication mode.
SNMPv3	AuthPriv	MD5/SHA/SM4	DES/AES/SM4	Use the HMAC-MD5/HMAC-SHA/SM3 data authentication mode and CBC-DES/CFB-AES-128/CBC-SM4 data encryption mode.

7.2. SNMP Function Configuration

Table 7-2 SNMP function configuration list

Configuration Task	
Configure the SNMP basic functions	Enable the SNMP service
	Configure the MIB view
	Configure the manager contact information
	Configure the physical location information of the device
Configure SNMPv1/v2	Configure the SNMP community name
Configure SNMPv3	Configure the SNMP user group
	Configure the SNMP user
	Configure SNMP advertising
	Configure SNMP agent forwarding
Configure SNMP Trap	Configure SNMP Trap

7.2.1. Configure SNMP Basic Functions

Configuration Condition

None

Enable SNMP Service

If the device is enabled with the SNMP service, the device can manage and configure via the SNMP network management software.

Table 7-3 Enable the SNMP service

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the SNMP service	**snmp-server start**	Mandatory By default, the SNMP service is disabled.

Configure MIB View

Use the view-based access control model to judge whether the associated management object of one operation is permitted by the view. Only the management objects permitted by the view can be permitted to access.

Table 7-4 Configure the MIB view

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the MIB view	**snmp-server view** *view-name oid-string* { **include** | **exclude** }	Mandatory By default, the SNMP view name is Default.

Configure Manager Contact Information

The manager contact information is one information node in the SNMP protocol. The network management software can get the information via SNMP.

Table 7-5 Configure the manager contact mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the manager contact information	**snmp-server contact** *contact-line*	Mandatory

Configure Device Physical Location Information

The device physical location information is one information node in the SNMP protocol. The network management software can get the information via SNMP.

Table 7-6 Configure the physical location information of the device

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the physical location information of the device	**snmp-server location** *location*	Mandatory

7.2.2. Configure SNMPv1/v2

Configuration Condition

Before configuring SNMPv1/v2, first complete the following task:

- Configure the link-layer protocol, ensuring the normal communication of the link layer
- Configure the IP address of the interface, making the network layer of the neighboring nodes reachable

Create SNMP Community Name

SNMPv1/SNMPv2c adopts the security scheme based on the community name. SNMP community name can be regarded as the password between NMS and SNMP proxy, that is to say, SNMP proxy only accepts the management operations of the same community name and the SNMP from different community name is not responded and is dropped directly.

Table 7-7 Configure the community name

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the community name of the SNMP proxy	**snmp-server community** *community-name* [**view** *view-name*] { **ro** | **rw** } [*access-list-number* | *access-list-name* | **ipv6** *access-list-number*]	Mandatory By default, the community name is public.

7.2.3. Configure SNMPv3

Configuration Conditions

Before configuring SNMPv3, first complete the following task:

- Configure the link-layer protocol, ensuring the normal communication of the link layer
- Configure the IP address of the interface, making the network layer of the neighboring nodes reachable

Create SNMP User Group

During controlling, we can associate some user with one group. The users of one group have the same access authority.

- We can configure one group to associate with the view. There are three kinds of views, that is, read-only view, write view and notify view.
- We can configure the security level of the group, configuring whether to need the authentication and encryption.

Table 7-8 Create the SNMP user group

Step	**Command**	**Description**
Enter the global configuration mode	**configure terminal**	-
Create the SNMP user group	**snmp-server group** *group-name* **v3** { **authnopriv** | **authpriv** | **noauth** } [**notify** *notify-view* | **read** *read-view* | **write** *write-view*]	Mandatory **Authnopriv:** authenticate, but not encrypt **Authpriv:** authenticate and encrypt **Noauth:** not authenticate or encrypt

Create SNMP User

Perform the security management via the user-based security model. The network work station can communicate with the SNMP proxy only after using the valid user. The valid user needs to be configured.

For SNMPv3, we also can specify the security level, authentication algorithm (MD5 or SHA or SM3), authentication password, encryption algorithm (DES or AES or SM4), and encryption password.

Table 7-9 Configure the user

Step	**Command**	**Description**
Enter the global configuration mode	**configure terminal**	-
Create the SNMP user	**snmp-server user** *user-name group-name* [**remote** *ip-address port-num*] **v3** [**auth** { **md5** | **sha**| **SM3** } *password* [**encrypt** [**des** | **aes | SM4**] *password*]] {**access** *access-list-number* | access-list-name | ***Ipv6*** *access-list-number*}	Mandatory

Note:

- Configure the SNMPv3 user based on the user security model (USM), save the authentication and encryption information of each user. Note that only after configuring the authentication protocol, we can configure the encryption protocol.
- For the remote user (the so-called remote is relative to the local SNMPv3 entity. If the local SNMPv3 entity needs to communicate with other SNMPv3 entity, the other SNMPv3 entity is called remote SNMPv3 entity. This is mentioned in notify and proxy), we also need to specify the IP address and UDP port number of the remote user. When configuring the remote user, we should configure the engineID of the remote SNMP entity of the user first. Besides, each user should correspond with one group so that we can map one security model and security name to one group name via the view-based access control.
- When configuring the auto proxy forwarding and we may not know the IP address of the delegated device, we only need to input 0.0.0.0 at ip-address. Besides, the auto proxy forwarding should be combined with the keepalive mechanism.

Configure SNMP Notify

SNMPv3 notify configuration contains the following several kinds:

- SNMPv3 notify configuration: Configure the SNMPv3 notify and specify the type of the notify message as inform;
- SNMPv3 notify filter configuration: Notify filter means the filter used to determine whether one notify message should be sent to one destination address.
- SNMPv3 notify address map table configuration: Associate the notify address with one filter table.

Table 7-10Configure the notify

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the SNMP notify	**snmp-server notify notify** *notify-name taglist* **inform**	Mandatory
Configure the SNMP notify filter	**snmp-server notify filter** *filter-name oid-subtree* { **exclude** | **include** }	Mandatory Exclude: Filter out the notifications of all objects in the MIB sub tree. Include: Inform all objects in the MIB sub tree.

Step	Command	Description
Configure the SNMP address parameters	**snmp-server AddressParam** { *address-name* | **paramIn** } **v3** *user-name* { **noauth** | **authpriv** | **authnopriv** }	Mandatory
Configure the SNMP notify filter map table	**snmp-server notify profile** *filter-name address-param*	Mandatory *filter-name*: Specify the notify filter name to be mapped *address-param*: Specify the address parameter name to be mapped.

7.2.4. Configure SNMP Proxy Forwarding

If the network work station cannot directly access the managed SNMP proxy, the intermediate device needs to support the proxy forwarding. Currently, only SNMPv3 supports the proxy forwarding.

Table 7-11 Configure the proxy forwarding

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the SNMP remote engine ID	**snmp-server engineID remote** *ip-address port-num* [**vrf** *vrf-name*] *engine-id* [*group-name*]	Mandatory Configure the engine ID of the SNMP entity needing the proxy forwarding
Configure the SNMP address parameters	**snmp-server AddressParam** [*address-name* | **paramIn**] **v3** *user-name* { **noauth** | **authpriv** | **authnopriv** }	Mandatory

Step	**Command**	**Description**
Configure the SNMP notify address	**snmp-server TargetAddress** *target-name ip-address port-num address-param taglist time-out retry-num*	Mandatory
Configure the SNMP proxy forwarding	**snmp-server proxy** *proxy-name* { **inform** | **trap** | **read** | **write** } { *engineId* | **auto** } *engineId address-param target-addr* [*context-name*]	Mandatory

7.2.5. Configure SNMP Trap

Trap is the information SNMP proxy actively sends to the network work station, used to report some specified events. Trap packets include general Trap and customized Trap. The general trap contains Authentication, Linkdown, Linkup, Coldstart, and Warmstart; the customized Trap is output according to the requirements of the modules.

Table 7-12 Configure Trap

Step	**Command**	**Description**
Enter the global configuration mode	**config terminal**	-
Enable the trap of the link interface down or up	**snmp-server enable traps snmp** [**linkup** | **linkdown**]	Mandatory By default, SNMP Trap is disabled.
Enter the interface configuration mode	**interface** *interface-type interface-num*	Mandatory
Configure the trap of the interface status change	**snmp trap link-status**	Mandatory

Step	Command	Description
Configure the Trap target host	**snmp-server host** { *ip-address* | *host-name* } **traps** {**community** *community-name* **version** { **1 | 2** } **| user** *username* **authnopriv | authpriv | noauth version 3** }[**port** *portname* **| vrf** *vrf-name*]	Mandatory It is necessary to specify ip-address as the IP address of the network work station.
Configure the source address of the Trap packet	**snmp-server trap-source** *ip-address*	Optional

Note:

Usually, there is much Trap information, so it occupies the device resources, affecting the device performance. Therefore, it is suggested to enable the Trap function of the specified module as desired, but do not need to enable the Trap of all modules.

7.2.6. SNMP Monitoring and Maintaining

Table 7-13 SNMP monitoring and maintaining

Command	Description
show snmp-server	View the SNMP protocol packet statistics information
show snmp-server AddressParams	View the SNMP proxy address parameter information
show snmp-server community	View the SNMP proxy community information
show snmp-server contact	View the device manager contact
show snmp-server context	View the SNMPv3 context
show snmp-server engineGroup	Display the information of the SNMP proxy engine group

Command	Description
show snmp-server engineID	Display the information of the SNMP proxy engine ID
show snmp-server group	View the SNMP proxy user group information
show snmp-server Host	Display the information of the SNMP proxy trap host
show snmp-server location	View the location information of the device
show snmp-server notify filter	Display the information of the SNMP proxy notify filter
show snmp-server notify notify	Display the information of the SNMP proxy notify
show snmp-server notify profile	Display the associated information of the SNMP proxy notify
show snmp-server proxy	View the SNMP proxy forwarding information
show snmp-server reg-list	View the module information of the SNMP registered MIB
show snmp-server TargetAddress	View the SNMP proxy address entry information
show snmp-server user	View the SNMP user information
show snmp-server view	View the SNMP view information

7.3. SNMP Typical Configuration Example

7.3.1. Configure SNMP v1/v2c Proxy Server

Network Requirements

- Device is the SNMP Agent device and the route with the NMS server is reachable.

- NMS monitors and manages Device via SNMP v1 or SNMP v2c; when Device fails, it actively reports to NMS.

Network Topology

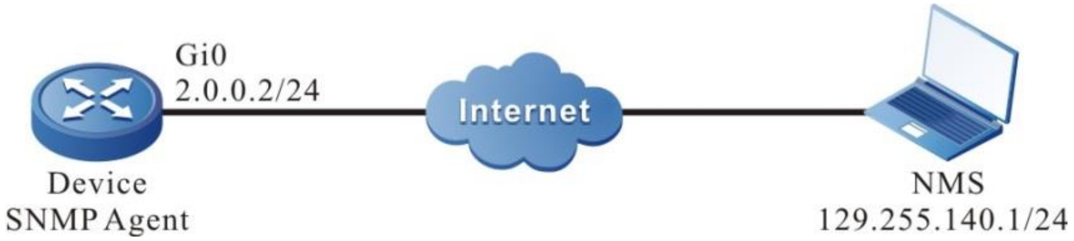


Figure 7-3 Networking of configuring SNMP v1/v2c proxy server

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted)

Step 2: Enable the SNMP proxy on Device and configure the SNMP community name.

#Configure Device.

Enable the SNMP proxy; configure the node view name as public, read-only community name as public and read-write community name as private.

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view public 1.3.6.1 include
Device(config)#snmp-server community public view default ro
Device(config)#snmp-server community private view default rw
```

Step 3: Configure Device to send the Trap packets to the network work station (NMS) actively and use the community name public.

#Configure Device.

```
Device(config)#snmp-server enable traps
Device(config)#snmp-server host 129.255.140.1 traps community public version 2
```

Note:

- The SNMP version specified in the **snmp-server host** command should be consistent with the SNMP version running on NSM.

Step 4: Configure NMS.

#On the NMS using SNMP v1/v2c, we need to set “read-only community name” and “read-write community name”. Besides, we also need to set “timeout” and “re-try times”. The user queries and configures the device via the NMS.

Note:

- When using the read-only community name, the user can only query the device via NMS.
- When using the read-write community name, the user can query and configure the device via NMS.

Step 5: Check the result.

#NMS can query and configure some parameters of Device via the MIB node. NMS can receive various Trap information from Device, such as interface up, down of Device, the route change caused by the network oscillation. Device will generate the corresponding Trap information and send to NMS.

7.3.2. Configure SNMP v3 Proxy Server

Network Requirements

- Device is the SNMP Agent device and the route with the NMS server is reachable.
- NMS manages Device via SNMPv3.

Network Topology

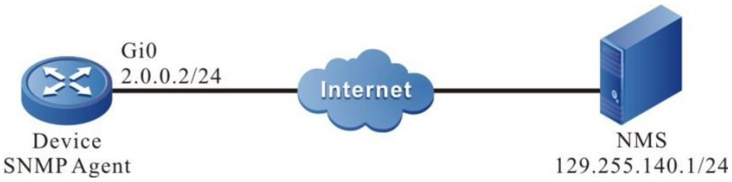


Figure 7-4 Networking of configuring the SNMP v3 proxy server

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted).

Step 2: Enable the SNMP proxy on Device and configure the SNMPv3 basic information.

#Configure Device.

Enable the SNMP proxy; configure the node view name as public and it can access all objects in the node 1.3.6.1.

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view public 1.3.6.1 include
```

Configure the user group as public and security level as authpriv; the read-write view and notify view both use public; configure the user name as public, belonging to the user group public, authentication algorithm as MD5, authentication password as admin, encryption algorithm as DES and encryption password as admin.

```
Device(config)#snmp-server group public v3 authpriv read public write public notify public
Device(config)#snmp-server user public public v3 auth md5 admin encrypt des admin
```

Configure the text name as public.

```
Device(config)#snmp-server context public
```

Step 3: Configure NMS.

#On the NMS using SNMP v3, we need to set the user name and select the security level. According to different security levels, we need to set the authentication algorithm, authentication password, encryption algorithm, encryption password and so on. Besides, we also need to set “timeout” and “re-try times”. The user queries and configures the device via the NMS.

Step 4: Check the result.

# On NMS, we can query and set some parameters of Device via the MIB node.

7.3.3. Configure SNMP v3 Trap Notify

Network Requirements

- Device is the SNMP Agent device and the route with the NMS server is reachable.
- NMS monitors Device via SNMPv3. When Device fails or has something wrong, it actively reports to NMS.

Network Topology

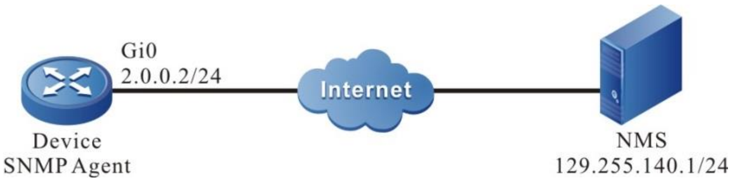


Figure 7-5 Networking of configuring SNMPv3 trap notify

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted).

Step 2: Enable the SNMP agent on Device and configure the SNMPv3 basic information.

#Configure Device.

Enable the SNMP agent; configure the node view name as default and it can access all objects in the node 1.3.6.1.

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default 1.3.6.1 include
```

Configure the user group as public and the security level as authpriv, both the read-write view and notify view use default; configure the user name as public, belonging to the user group public, authentication algorithm is MD5, authentication password is Admin, encryption algorithm is DES, and the encryption password is Admin.

```
Device(config)#snmp-server group public v3 authpriv read default write default
notify default
```

```
Device(config)#snmp-server user public public v3 auth md5 Admin encrypt des
Admin
```

Configure Device to send all Trap information.

```
Device(config)#snmp-server enable traps
```

Step 3: Configure Device to send the SNMP v3 trap packet to NMS.

#Configure Device.

Configure SNMP v3 trap user name as public on NSM, and the security level as authpriv.

```
Device(config)# snmp-server host 129.255.140.1 traps user public authpriv version 3
```

Step 4: Configure NMS.

#On NMS, it is necessary to configure the user name and password consistent with the SNMP Agent, run the network management software and monitor the UDP port 162.

Step 5: Check the result.

#NMS can receive various Trap information from Device, such as interface up, down of Device, the route change caused by the network oscillation. Device generates the corresponding Trap information and sends to NMS.

7.3.4. Configure SNMP v3 inform Notify

Network Requirements

- Device is the SNMP Agent device and the route with the NMS server is reachable.
- NMS monitors Device via SNMPv3. When Device fails or has something wrong, it actively reports to NMS.

Network Topology

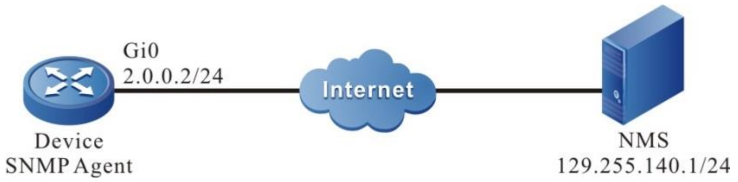


Figure 7-6 Networking of configuring SNMPv3 inform notify

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted).

Step 2: Enable the SNMP proxy on Device and configure the SNMPv3 basic information.

#Configure Device.

Enable the SNMP proxy; configure the node view name as default and it can access all objects in the node 1.3.6.1.

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default 1.3.6.1 include
```

Configure the user group as group1 and security level as authpriv; the read-write view and notify view both use default.

```
Device(config)#snmp-server group group1 v3 authpriv read default write default
notify default
```

Step 3: Configure Device to send notify message to NMS.

#Configure Device.

Configure the IP address and enginID of the remote user, that is, NMS.

```
Device(config)#snmp-server engineID remote 129.255.140.1 162 bb87654321
```

Configure the remote user name as re-user1, belonging to the user group group1, authentication algorithm as MD5, authentication password as admin, encryption algorithm as DES and encryption password as admin.

```
Device(config)#snmp-server user user1 group1 remote 129.255.140.1 162 v3 auth md5
admin encrypt des admin
```

Configure the local address parameter name as param-user1; configure the target address name as target-user1; use the address parameter param- user1; the target address list name is target-user1.

```
Device(config)#snmp-server AddressParam param-user1 v3 user1  authpriv
Device(config)#snmp-server TargetAddress target-user1  129.255.140.1 162 param-
user1 tag-user1 10 3
```

Configure the notify entity as notify- user1; configure the filter entity of notify as filter- user1, containing the notify of all objects in the node 1.3.6.1; configure the notify configuration table, and let the filter entity fileter-user1 associate with the address parameter param-user1.

```
Device(config)#snmp-server notify notify notify-user1 tag-user1  inform
Device(config)#snmp-server notify filter filter-user1 1.3.6.1 include
Device(config)#snmp-server notify profile filter-user1 param-user1
```

Step 4: Configure NMS.

#On NMS, do not need to configure, but just need to run the network management software and monitor the UDP port 162.

Step 5: Check the result.

#NMS can receive various Trap information from Device, such as interface up, down of Device, the route change caused by the network oscillation. Device generates the corresponding Trap information and sends to NMS.

7.3.5. Configure SNMP v3 Proxy Forwarding

Network Requirements

- The route from Device2 to NMS server is reachable.
- Device2 is the proxy device Agent; Device1 is the delegated device.
- On Device1 and Device2, run SNMPv3.
- On NMS, run SNMPv3. NMS manages Device1 and Device2 via SNMP v3.

Network Topology

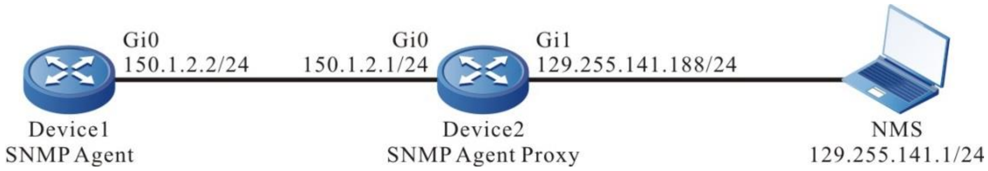


Figure 7-7 Networking of configuring the SNMP v3 proxy forwarding

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted).

Step 2: On the proxy device Device2, enable the SNMP proxy and configure the SNMPv3 basic information.

#Configure Device2.

Enable the SNMP proxy; configure the node view name as default and it can access all objects in the node 1.3.6.1.

```
Device2#configure terminal
Device2(config)#snmp-server start
Device2(config)#snmp-server view default 1.3.6.1 include
```

Configure the user group as group-local and security level as noauth; the read-write view and notify view both use default; configure the user name as user1, belonging to the user group group-local, authentication algorithm as MD5, authentication password as proxy, encryption algorithm as DES and encryption password as proxy.

```
Device2(config)#snmp-server group group-local v3 noauth read default write default notify default
Device2(config)#snmp-server user user1 group-local v3 auth md5 proxy encrypt des proxy
```

Step 3: On the delegated device Device1, enable the SNMP proxy and configure the SNMP view.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#snmp-server start
Device1(config)#snmp-server view default 1.3.6.1 include
```

Step 4: Configure the information of the delegated device on the proxy device Device2.

#Configure Device2.

Configure the IP address and enginID of the delegated device.

```
Device2(config)#snmp-server engineID remote 150.1.2.2 161 800016130300017a000137
```

Configure the user group of the delegated device as group-user, security level as authpriv; both the read-view and notify view use default.

```
Device2(config)#snmp-server group group-user v3 authpriv read default write default notify default
```

Configure the user name as re-user, belonging to the user group group-user, authentication algorithm as MD5, authentication password as proxy, encryption algorithm as DES and encryption password as proxy.

```
Device2(config)#snmp-server user re-user group-user remote 150.1.2.2 161 v3 auth md5 proxy encrypt des proxy
```

Configure the local address parameter name as plocal and remote address parameter name as puser; configure the target address name as tuser and use the address parameter puser.

```
Device2(config)#snmp-server AddressParam plocal v3 user1 authpriv
Device2(config)#snmp-server AddressParam puser v3 re-user authpriv
Device2(config)#snmp-server TargetAddress tuser 150.1.2.2 161 puser taguser 10 2
```

Configure the proxy forwarding name as proxy-re-user, the operation authority as WRITE, the enginID of the delegated device as 800016130300017a000137, the used address parameter plocal, the used target address tuser; configure the context name as proxyuser.

```
Device2(config)#snmp-server proxy proxy-re-user WRITE 800016130300017a000137 plocal tuser proxyuser
Device2(config)#snmp-server context proxyuser
```

#View the enginID information of Device2.

```
Device2#show snmp-server engineID
Local  engine ID: 800016130300000000052fd
IPAddress: 150.1.2.2.0.161 remote engine ID: 800016130300017a000137
```

Note:

- The enginID of the remote device should be consistent with the delegated device. The enginID of the device can be viewed via the **show snmp-server engineID** command.
- The monitoring protocol of the delegated device is UDP and the port is 161.

Step 5: Perform the related configuration of SNMPv3 on the delegated device Device1.

#Configure Device1.

Configure the user group as g1 and security level as authpriv; the read-write view and notify view both use default; configure the user name as re-user, authentication algorithm as MD5, authentication password as proxy, encryption algorithm as DES and encryption password as proxy.

```
Device1(config)#snmp-server group g1 v3 authpriv read default write default notify default
Device1(config)#snmp-server user re-user g1 v3 auth md5 proxy encrypt des proxy
Device1(config)#snmp-server context proxyuser
```

Step 6: Configure NMS.

#SNMP v3 adopts the authentication and encryption security mechanism. On the NMS, we need to set the user name and select the security level. According to different security levels, we need to set the authentication algorithm, authentication password, encryption algorithm, encryption password and so on. Besides, we also need to set “timeout” and “re-try times”. The user can query and configure the device via the NMS. When it is necessary to query or configure the delegated device, we also need to set the enginID of the proxy forwarding as the enginID of the delegated device on NMS.

Step 8: Check the result.

#On NMS, we can query and set some parameters of Device2 and Device1 via the MIB node.

8. RMON

8.1. Overview

One important function of the network management is to monitor the element performances of the network. In the traditional SNMP network management mode, the initiative of the management is mainly mastered by the network management station. Usually, the network management work station regularly polls the data of the device and then measures and analyzes in the network management system, so as to get the desired information of the administrator. In this mode, the network management work station needs to send and receive lots of packets to the network devices. When there are many devices in the network, it causes the additional load for the network. Meanwhile, the network blocking and other factors take various accidents to the running of the network management system. As for this, we put forward the RMON (Remote Network Monitoring) concept.

The realizing of RMON still needs the supporting of the SNMP protocol. In fact, it is one group of MIBs, distributed in MIB-2, and the object ID is 1.3.6.1.2.1.16. Compared with other general MIB, RMON adds the calculation at Agent during realizing, that is, put the processing, such as performance statistics in the device. This realizes the distributed processing in the whole network, reducing the disadvantages brought by the polling of the network management work station.

RMON needs to realize lots of calculation functions, so the previous RMON proxy (also called Probe) is acted by a special device, distributed in the network to monitor the corresponding target. With the improvement of the processing capability of the network device, RMON is gradually integrated to the network devices, so as to realize the RMON requirement high-efficiently. However, this also puts forward higher performance requirement for the network devices, after all, the calculations of RMON occupy lots of system resources, reducing the system performance. This is also the additional cost brought by the management, so RMON is mainly realized in the hardware with the network processing capability, such as switching chip.

RMON MIB has 10 groups:

- statistics: Measure all Ethernet interfaces of the device, such as broadcast and conflict;
- history: Record the samples of the periodical statistics information that is taken out from the statistics group;
- alarm: Permit the administration Console user to configure the sampling interval and alarm when the values of any counters or integers (recorded by the RMON proxy) exceed the threshold value;
- host: Include the input/output traffics of various types of hosts adhering to the subnet;
- hostTopN: Contain the stored statistics information of hosts, some parameters in the host tables of these hosts are the highest;
- matrix: Indicate the error and utilization information in the form of matrix, so that the operator can use any address pair to search for information;
- filter: Permit the monitor to monitor the packets matched with the filter;
- event: Present the table of all events generated by the RMON proxy;
- tokenRing: Maintain the statistic and configuration information of a subnet which is a token ring

8.2. RMON Function Configuration

Table 8-1 RMON function configuration list

Configuration Task	
Enable the RMON function	Enable the RMON function
Configure the RMON alarm group	Configure the RMON alarm instance
Configure the RMON event group	Configure the RMON trigger event
Configure the RMON history group	Configure the RMON history group instance
Configure the RMON statistics group	Configure the RMON statistics management function

8.2.1. Enable RMON Function

Configuration Condition

None

Enable RMON Function

Enabling RMON is to provide the related resource for the RMON monitoring function. The sources can take effect only after configuring the RMON monitoring group function.

Table 8-2 Enable the RMON function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the RMON function	**rmon**	Mandatory By default, do not enable the RMON function.

8.2.2. Configure RMON Alarm Group

RMON alarm group function means to configure multiple alarms and each alarm monitors one alarm instance. Within the sampling interval, when the alarm instance data value changes and exceeds the increasing threshold or the decreasing threshold, trigger the alarm event. According to the processing mode defined by the alarm event group, process the alarms. When the data value exceeds the threshold continuously, alarm only for the first exceeding.

Configuration Condition

Before configuring the RMON alarm group, first complete the following task:

- Enable the SNMP proxy function
- Enable the TRAP function of RMON in SNMP

Configure RMON Alarm Instance

Table 8-3 Configure the RMON alarm instance

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the RMON function	**rmon**	Optional
Configure the RMON alarm group	**rmon alarm** *alarm-num OID interval* { **absolute | delta** } **risingthreshold** *rising-threshold* [*rising-event*] **fallingthreshold** *falling-threshold* [*falling-event*] [**owner** *owner*]	Mandatory By default, the alarm trigger event group is 1. By default, the owner of the alarm group is config.

8.2.3. Configure RMON Extended Alarm Group

RMON extended alarm group can calculate the alarm variables, and then compares the calculation result with the set threshold to achieve more abundant alarm functions.

Configuration Condition

Before configuring the RMON alarm group, first complete the following task:

- Enable the SNMP proxy function
- Enable the TRAP function of RMON in SNMP
- Configure one statistics group

Configure the RMON Alarm Example

Table 8-4 Configure the RMON alarm example

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable RMON function	**rmon**	Optional
Configure one statistics group	**rmon statistics ethernet** *statistics-num OID* [**owner** *owner*]	Mandatory By default, the owner of the statistics group is config.
Configure the RMON alarm group	**rmon prialarm** *alarm-num WORD interval* { **absolute** | **delta** } **risingthreshold** *rising-threshold* [*rising-event*] **fallingthreshold** *falling-threshold* [*falling-event*] **entrytype forever** [**owner** *owner*]	Mandatory By default, the owner of the alarm group is config.

8.2.4. Configure RMON Event Group

Configuring the RMON event group function means to configure multiple events, defining the event serial number and processing mode of each event. The event has the following several processing modes: The event is recorded in the log; the event sends the TRAP message to the network management system; record the event in the log and send the TRAP message to the network management system, but do not process.

Configuration Condition

Before configuring the RMON event group, first complete the following task:

- Enable the SNMP proxy function
- Enable the TRAP function of RMON in SNMP

Configure RMON Trigger Event

RMON trigger event is mainly used to process the events when the RMON alarm happens.

Table 8-5 Configure the RMON trigger event

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the RMON function	**rmon**	Optional
Configure the RMON event group	**rmon event** *event-num* [**description** *event-description* | **log** *max-num* | **owner** *owner* | **trap** *communit*]	Mandatory By default, the owner of the event group is config.

8.2.5. Configure RMON History Event

Configuring RMON history group function means to configure multiple history groups. RMON history group stores the subnet data got by sampling with fixed interval. The group comprises the history control table and history data. The control table defines the sampled subnet interface serial number, the sampling interval, and hot much data to sample each time, while the data table is used to store the data got during the sampling.

Configuration Condition

Before configuring the RMON history group, first complete the following task:

- Enable the SNMP proxy function

Configure RMON History Group Instance

RMON history group mainly configures the monitor object of the history control table, sampling interval, hot much data to sample, and so on.

Table 8-6 Configure the RMON history group instance

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the RMON function	**rmon**	Optional
Configure the RMON history group	**rmon history control** *history-num OID buckets-num* [**interval** *interval*] [**owner** *owner*]	Mandatory By default, the sampling interval is 1800s. By default, the owner of the history group is config.

8.2.6. Configure RMON Statistics Group

Configuring the RMON statistics group function is to configure the monitor object as the statistics information of the Ethernet interface. The statistics group provides one table and each row of the table indicates the statistics information of one subnet. The network administrator can get various statistics information of one segment from the table (the traffic of one segment, the distributing of various types of packets, various types of error packets, the number of collisions and so on).

Configuration Condition

Before configuring the RMON statistics group, first complete the following task:

- Enable the RMON function
- Enable the SNMP proxy function

Configure Statistics Management Function

Table 8-7 Configure RMON statistics management function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the RMON function	**rmon**	Mandatory
Configure the RMON statistics group	**rmon statistics ethernet** *statistics-num OID* [**owner** *owner*]	Mandatory By default, the owner of the statistics group is config.

8.2.7. RMON Monitoring and Maintaining

Table 8-8 RMON Monitoring and Maintaining

Command	Description
show rmon alarm	Display the RMON alarms configured in the device
show rmon alarm supportVariable	Display the monitor objects supported in the device
show rmon event	Display the RMON event configured in the device
show rmon history { **control | ethernet** *control-num* }	Display the RMON history group configured in the device

Command	Description
show rmon prialarm	Display the configured RMON extended alarms in the device
show rmon statistics ethernet	Display the RMON statistics group configured in the device

8.3. RMON Typical Configuration Example

8.3.1. Configure RMON Basic Functions

Network Requirements

- Device is the RMON proxy device and the route with the NMS server is reachable;
- Monitor and manage the event groups, alarm groups, history groups and statistics groups of RMON via NMS.

Network Topology

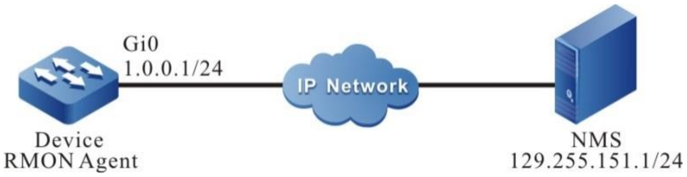


Figure 8-1 Networking of configuring the RMON basic functions

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted)

Step 2: Configure the SNMP proxy.

#Enable the SNMP proxy, and configure the node view node as default and read-only community name as public.

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default 1.3.6.1 include
Device(config)#snmp-server community public view default ro
```

#Enable the SNMP Trap function and configure the destination address and the used community name of the Trap packet.

```
Device(config)#snmp-server enable traps
Device(config)#snmp-server host 129.255.151.1 traps community public
```

Step 3: Configure the RMON event group, alarm group, history group and statistics group of Device.

#Enable the RMON proxy.

```
Device(config)#rmon
```

#Configure the serial number of the event group as 1 and record the ingress packets of port gigabitethernet0.

Device(config)#rmon event 1 description gigabitethernet0_in_octes log 100 trap public

#Configure the alarm event group; the monitor object is ifInOctets.1; configure the sampling of the relative value; the sampling interval is 10s. Configure the increasing and decreasing threshold as 100; configure the triggered event of reaching the threshold value as event1.

```
Device(config)#rmon alarm 1 ifInOctets.1 10 delta risingthreshold 100 1
fallingthreshold 100 1 owner 1
```

#Configure the RMON statistics group.

```
Device(config)#rmon statistics ethernet 1 ifIndex.1
```

#Configure the RMON history group.

```
Device(config)#rmon history control 1 ifIndex.1 10
```

Note:

- The corresponding port of the instance index ifInOctets.1 is gabitethernet0 on the device.
- The remote monitored object instance index needs to be read from the interface table ifEntry of MIB-2.

Step 4: Configure NMS.

#On NMS using SNMP v1/v2c, we need to set “Read-only community name”, “timeout” and “Retry times”.

Step 5: Check the result.

#View the RMON event group entry configuration of Device.

```
Device#show rmon event
Event 1 is active, owned by config
Description : gigabitethernet_0_in_octes
Event firing causes: log and trap, last fired at 11:38:07


Current log entries:
     logIndex        logTime          Description
------------------------------------------------------------------
        1          11:38:07       gigabitethernet_0_in_octes
```

#Configure the RMON alarm entry configuration of Device.

```
Device#show rmon alarm
Alarm 1 is active, owned by 1
Monitoring variable: ifInOctets.1,     Sample interval: 10 second(s)
Taking samples type: delta,     last value was 4225
```

```
Rising threshold :   100,      assigned to event: 1
Falling threshold :  100,      assigned to event: 1
```

#Configure RMON statistics group entry configuration of Device.

```
Device#show rmon statistics ethernet
------------------------------
Ethernet statistics table information:
     Index: 1
     Data Source: ifIndex.1
     Owner: config
     Status: Valid
------------------------------
 ifIndex.1 statistics information:
------------------------------
 DropEvents:0
 Octets: 26962295
 Pkts:252941
 BroadcastPkts:156943
 MulticastPkts:62331
 CRCAlignErrors:51
 UndersizePkts:0
 OversizePkts:0
 Fragments:0
 Jabbers:0
 Collisions:0
 Pkts64Octets:167737
 Pkts65to127Octets:47962
 Pkts128to255Octets:22497
 Pkts256to511Octets:9967
 Pkts512to1023Octets:4032
 Pkts1024to1518Octets:745
```

#View the RMON history group entry configuration of Device.

```
Device#show rmon history control
----------------------------------
RMON history control entry index: 1
     Data source: IfIndex.1
     Buckets request: 10
     Buckets granted: 2
```

```
          Interval: 1800
          Owner: config
          Entry status: Valid
      ----------------------------------
```

#NMS can query the History, Event and Statistics information in Device via MIB.

NMS can receive the Trap information of the Alarm event from Device. For example, when the ingress traffic change rate of the monitor interface is larger than the increasing threshold or smaller than the decreasing threshold, Device generates the corresponding Trap information and sends to NMS.

9. PORT MIRROR

9.1. Overview

9.1.1. Introduction to Port Mirror

Port mirror is one management mode used to monitor the data flow of the device port, including local port mirror, remote port mirror, and encapsulated remote port mirror. Currently, QTECH router only supports the local port mirror.

9.1.2. Basic Concepts

Port Mirror Session

Port mirror session means to mirror the data flow of one or multiple monitor ports on the device and send to the destination port. The mirrored data flow can be the input data flow and also can be the output data flow or mirror the input and output data flow at the same time. We can configure port mirror for the disabled port and the port mirror session does not take effect, but as long as the related port is enabled, the port mirror takes effect. There are L2 port mirror sessions and L3 port mirror sessions. They are independent and have no relationship with each other.

Local SPAN

Local SPAN supports the port mirror on one device. All monitor ports and destination ports are on the same device. Local SPAN is to configure L2 port mirror.

L3 Port Mirror

All monitoring ports and destination ports are L3 routing physical ports on the same device.

Traffic Type

Traffic type includes Receive (Rx) (the received traffic of the mirror port, Transmit (Tx) (the forwarded traffic of the mirror port, and Both (the received and forwarded traffic of the mirror port).

Port Mirror Source Port

Port mirror source port is also called monitored port. Its data is monitored for network analysis. The monitored data flow can be at the input direction, output direction or both. It can function in different VLANs. The source port can be general port or aggregation group. One source port can only belong to one port mirror session.

Port Mirror Destination Port

Port mirror destination port can only be one separate actual physical port. One destination port can only be used in one port mirror session.

Note:

- The destination port should not be connected to other device. Otherwise, it may result in the network loop.
- The destination port should be larger than or equal to the bandwidth of the mirror port. Otherwise, there may be packet loss.

9.2. SPAN Function Configuration

Table 9-1 Port mirror function configuration list

Configuration Task	
Configure Local Port Mirror	Configure local port mirror session

9.2.1. Configure Local Port Mirror

Local Port Mirror is used to analyze the data flow of the local device port.

Configuration Condition

None

Configure Local Port Mirror Session

Local Port Mirror session copies the received or forwarded packets of one or multiple source ports and forwards out from the destination port without affecting the normal service forwarding of the source port.

Table 9-2 Configure the local port mirror session

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the source end of Local Port Mirror session	**monitor session** *session-number* **source interface** *interface-list* [**both** | **tx** | **rx**]	Mandatory By default, do not configure the source end of local port mirror session.
Configure the destination end of the local port mirror session	**monitor session** *session-number* **destination interface** *interface-name*	Mandatory By default, do not configure the destination end of the local port mirror session.

Note:

- When configuring the session source end and specifying the port enabled with the mirror as the aggregation group, the specified aggregation group should be already created. If the aggregation group is not created, the configuration fails. Similarly, when configuring the destination end of the session and specifying the forwarding port of the mirror packet as the aggregation group, the specified aggregation group also should be already created. If the aggregation group is not created, the configuration fails.
- One port cannot be the source port and destination port of one session at the same time.

- One port cannot exist in multiple sessions at the same time.

9.2.2. Port Mirror Monitoring and Maintaining

Table 9-3 Port Mirror Monitoring and Maintaining

Command	Description
show monitor session {*session-number* **|** *all* **} [statis]**	Display the mirror statistics of one mirror session or all mirror sessions
clear monitor session {*session-number* **|** *all* **} statis**	Clear the mirror statistics of one mirror session or all mirror sessions

9.3. Typical Configuration Example of Port Mirror

9.3.1. Configure Port Mirror

Network Requirement

- PC1, PC2 and PC3 are connected with Device; PC1 and PC2 communicate with each other via Device.
- Configure local port mirror on Device: the source port is gigabitethernet0, and the destination port is gigabitethernet2, realizing that PC3 monitors the packets received and sent by port gigabitethernet0 of Device.

Network Topology

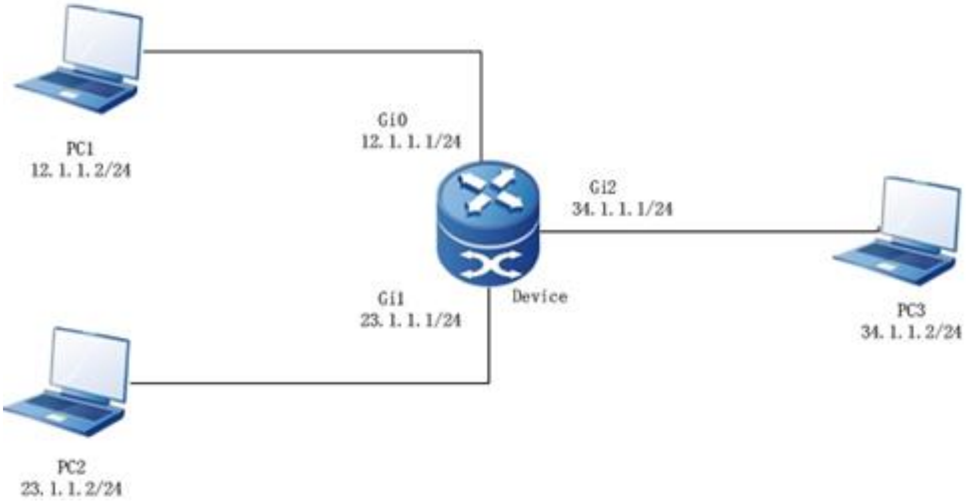


Figure 9-1 Networking of configuring the local port mirror

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the port mirror.

#On Device, configure the local port mirror. The source session port of the mirror is gigabitethernet0, and the destination session port is gigabitethernet2.

```
Device#configure terminal
Device(config)#monitor session 13 source interface gigabitethernet 0 both
Device(config)#monitor session 13 destination interface gigabitethernet 2
```

#On Device, view the session information of the port mirror.

```
Device#show monitor 13 sessio all
Session 1
Type : SPAN Local Session
Destination Interface : gigabitethernet2
Source Interface(both) :
gigabitethernet0
(Source Interface:Total-1, Max-64, Remain-63)
```

Step 3 : Check the result.

#On Device, view the statistics information of the port mirror.

```
Device#show monitor session 13 statis

SPAN statistics on session: 1
---------------------------------------------------
Input-Pkts   Output-Pkts   Drop-Pkts
23556        23556         0
---------------------------------------------------
```

#When PC1 and PC2 communicate with each other, the packets sent and received by port gigabitethernet0 can be got on PC3.

10. PACKET CAPTURE

10.1. Overview

Router packet capture is to capture the packet on the interface to the control plane, encapsulate the packet to the pcap format packet and write into the pcap file, or mirror the captured packet and send to the destination interface. There are three modes for processing the captured packet:

1. Local file mode: Set up the pcap file on the memory of the router, encapsulate the captured packet as the pcap format and write into the file. After the packet is captured, enter the file system packet capture directory of the router, copy the pcap file to the PC remotely, and use the wireshark software on the PC to open the pcap file for the offline analysis.
2. Remote FTP mode: After executing the packet capture command on the router, ftp sets up the packet capture file on the PC remotely, and then, encapsulates the captured packet as the pcap format packet, and writes into the file remotely. After the packet is captured, close the file, and use wireshark to open the file for analyzing the packet offline.
3. Mirror mode: Directly send the captured packet on the interface to the destination interface, and use wireshark and other tools on the directly-connected device of the destination interface to capture the mirrored packet.

10.2. Packet Capture Function Configuration

Table 10-1 Packet capture function configuration list

Configuration Task	
Configure the packet capture profile	Configure the packet capture profile
	Configure the packet capture direction
	Configure the timeout of the packet capture
	Configure the maximum length of the packet capture
	Configure the capture filter parameters of the packet receiving direction
	Configure the capture filter parameters of the packet sending direction
	Configure the maximum limit of the local packet captured file

Configuration Task	
Configure the packet capture profile	Configure the bandwidth limit of the interface packet capture
Configure the interface packet capture profile	Configure the packet capture profile applied on the interface
Configure the packet capture file system directory	Configure the local stored file system directory of the packet capture
Enable the interface packet capture mode	Enable the interface FTP mode to capture the packet
	Enable the interface local file mode to capture the packet
	Enable the interface mirror mode to capture the packet

10.2.1. Configure Packet Capture Profile

Configuration Condition

Before configuring the parameters of the packet capture profile, you need to create the profile.

Configure Packet Capture Profile

Creating one packet capture profile is to provide the personalized filter information for the interface capture packet. If the packet capture profile is not configured, the interface captures the packet according to the default value.

Table 10-2Configure one packet capture profile

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure one packet capture profile	**traffic-capture profile** *profile-name*	Mandatory By default, do not create the profile.

Configure Packet Capture Direction

The packet capture profile can configure three capture direction types, including only sending, only receiving, and both sending and receiving. If not configuring the capture packet direction, configure both sending and receiving by default.

Table 10-3 Configure the packet capture direction

Step	**Command**	**Description**
Enter the global configuration mode	**configure terminal**	-
Configure one packet capture profile	**traffic-capture profile** *profile-name*	Mandatory
Configure the packet capture direction	**direction** {**bidirection** | **rx** | **tx**}	Optional By default, it is bidirection.

Configure the Timeout of Packet Capture

Table10-4 Configure the timeout of the packet capture

Step	**Command**	**Description**
Enter the global configuration mode	**configure terminal**	-
Configure one packet capture profile	**traffic-capture profile** *profile-name*	Mandatory
Configure the timeout of the packet capture	**capture timeout** *value*	Optional By default, the timeout is 60 minutes.

Configure the Maximum Length of the Captured Packet

Table 10-4 Configure the maximum length of the captured packet

Step	**Command**	**Description**
Enter the global configuration mode	**configure terminal**	-
Configure one packet capture profile	**traffic-capture profile** *profile-name*	Mandatory

Step	Command	Description
Configure the maximum length of the captured packet	**packet length** *packet-value*	Optional By default, the maximum length of the captured packet is 65535.

Configure Filter Parameters of Packet Receiving Capture

Table 10-5 Configure the filter parameters of the packet receiving capture

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure one packet capture profile	**traffic-capture profile** *profile-name*	Mandatory
Configure the sampling frequency of the packet receiving capture	**incoming sample one-in-every** *value*	Optional By default, the capturing frequency is 1.
Configure the IP ACL capture filter of the packet receiving	**incoming acl-list {***ip-acl –name* | *ip-acl-num}*	Optional By default, do not configure IP ACL.
Configure the IPv6 ACL capture filter of the packet receiving	**incoming ipv6-acl-list {***ipv6-acl –name* | *ipv6-acl-num}*	Optional By default, do not configure IPv6 ACL.

Configure Capture Filter Parameters of the Packet Sending

Table 10-6 Configure the packet filter parameters of the packet sending capture

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure one packet capture profile	**traffic-capture profile** *profile-name*	Mandatory
Configure the sampling frequency of the packet sending capture	**outgoing sample one-in-every** *value*	Optional By default, the capturing frequency is 1.
Configure the IP ACL capture filter of the packet sending	**outgoing acl-list {***ip-acl –name* | *ip-acl-num}*	Optional By default, do not configure IP ACL.
Configure the IPv6 ACL capture filter of the packet sending	**outgoing ipv6-acl-list {***ipv6-acl –name* | *ipv6-acl-num}*	Optional By default, do not configure IPv6 ACL.

Configure Max. Limit of Local Captured Packet File

Table 10-7 Configure the maximum limit of the local captured packet file

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure one packet capture profile	**traffic-capture profile** *profile-name*	Mandatory
Configure the maximum limit of the local captured packet file	**capture size** *value*	Optional By default, the maximum local captured packet file is 1024KB.

Configure Bandwidth Limit of Interface Capture Packet

Table 10-8 Configure the bandwidth limit of the interface capture packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure one packet capture profile	**traffic-capture profile** *profile-name*	Mandatory
Configure the bandwidth limit of the interface capture packet	**capture bandwidth** *value*	Optional By default, the bandwidth limit of the interface capture packet is 1M.

10.2.2. Configure Interface Packet Capture Profile

After the packet capture profile is created, configure the profile on the specified interface. When enabling the packet capture function in the future, the system automatically capture the packet according to the configured profile parameters of the interface. If no packet capture profile is configured on the interface, the system adopts the default value to capture the packet.

Configuration Condition

Before configuring the packet capture profile on the interface, the packet capture profile need to be already created.

Configure Interface Packet Capture Profile

Table 10-9 Configure the packet capture interface profile

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Ethernet interface configuration mode	**interface** *interface-name*	After entering the interface configuration mode, the subsequent configuration takes effect only on the current interface.
Configure the interface packet capture profile	**traffic-capture apply** *profile-name*	Optional By default, no packet capture profile is configured on the interface.

10.2.3. Configure System Directory of Packet Capture File

In the device, create the memory file system directory with the specified size /tcap. The system is only used to store the captured packet file in the local capture packet mode. After restarting the device, all files in the directory will be cleared. After capturing the packet, be sure to send the captured packet file to the PC remotely.

Configuration Condition

None

Configure System Directory of Packet Capture File

Table 10-10 Configure the system directory of the packet capture file

Step	Command	Description
Distribute the packet capture file system directory	**traffic-capture alloc-ram-device** *device-size*	Optional In the privileged user mode, execute the command. By default, adopt the local mode to capture the packet, and the system automatically distributes 2000KB /tcap file system directory.

10.2.4. Enable Interface Capture Packet Mode

On the specified interface of the routing device, you can enable three packet capture modes, that is, local file mode, remote FTP mode, and mirror mode. After enabling the packet capturing, you can separately stop the packet capturing on the specified interface, and also can globally stop the packet capture on all interfaces.

Configuration Condition

None

Enable Interface FTP Mode to Capture Packets

Table 10-11 Enable the interface FTP mode to capture the packets

Step	Command	Description
Enable the FTP mode to capture the packet on the specified interface	**traffic-capture interface** *interface-name* **ftp** [**vrf** { *vrf-name* }] { *host-ip-address* } { *usrname* } { *password* } { *tcap-filename* } {**start | stop}**	Optional In the privileged user mode, execute the command. By default, do not enable any interface capture packet.

Enable Interface Local File Mode to Capture the Packet

Table 10-12 Enable the interface local file mode to capture the packet

Step	Command	Description
Enable the local file mode to capture the packet on the specified interface	**traffic-capture interface** *interface-name* **local** *tcap-filename* {**delete | start | stop**}	Optional In the privileged user mode, execute the command. By default, do not enable any interface capture packet.

Enable Interface Mirror Mode to Capture Packets

Table 10-13 Enable interface mirror mode to capture the packet

Step	Command	Description
Enable the mirror mode to capture the packet on the specified interface	**traffic-capture interface** *interface-name* **mirror interface** *destination-interface-name* {**start | stop**}	Optional In the privileged user mode, execute the command. By default, do not enable any interface capture packet.

10.2.5. Packet Capture Monitoring and Maintaining

Table 10-14 Packet capture monitoring and maintaining

Command	Description
show traffic-capture profile	Display the parameter information of all configured packet capture profiles
show traffic-capture control	Display the packet capture control structure management information when capturing the packet
show traffic-capture alloc-ram-device	Display whether to distribute the local captured packet memory file system

10.3. Typical Configuration Example of Packet Capture Tool

10.3.1. Local Mode of Packet Capture Tool

Network Requirement

- Device and PC communicate with each other.

- On Device, enable the capture tool local mode to capture the packets passing gi1. And then, enter the Device file system, and copy local.pcap to the PC remotely.

Network Topology

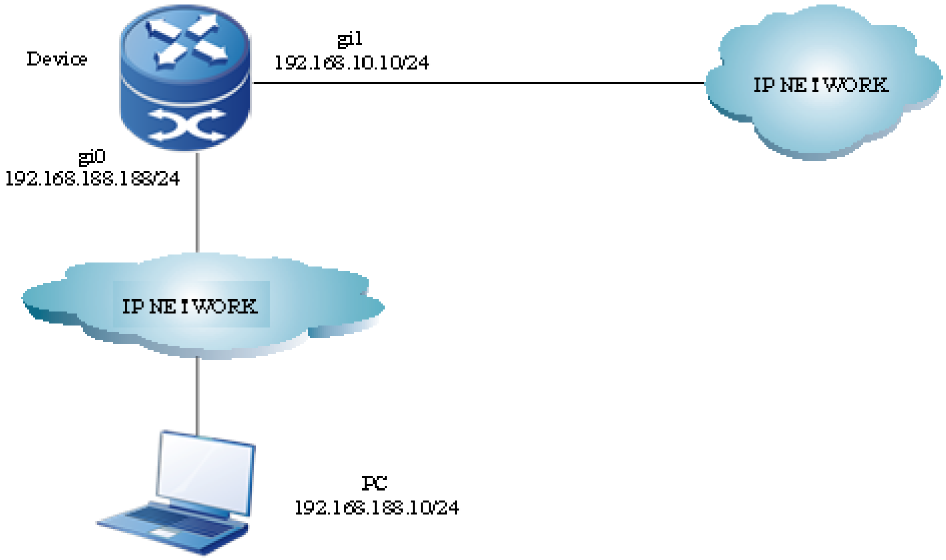


Figure 10-1 Networking of configuring the local mode of the capture tool

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Start the local mode to capture the packet.

#On Device, capture the packets passing the interface gi1 at the local.

```
Device#traffic-capture interface gi1 local local.pcap start
TCAP: 20000KB ram device is created
Starting capture traffic:
```

Step 3: Stop capturing the packet in the local mode.

#On Device, stop capturing the packets of interface gi1 via the packet capture tool.

```
Device#traffic-capture interface gi1 local local.pcap stop
Nov  9 2016 16:24:19.864: [tSshd-sh00]TCAP:Total 1200 bytes copying completed.
```

Step 4: Copy the captured file to the PC remotely.

#On Device, you can see the captured file in the packet capture directory.

```
Device#filesystem
Device(config-fs)#cd /tcap
Device(config-fs)#dir
         size        date        time      name
80            Nov-09-2016  10:42:26  .              <DIR>
0            Nov-09-2016  10:05:54  ..             <DIR>
```

```
1200          Nov-09-2016  10:45:51   local.pcap
Device(config-fs)#copy file-system /tcap/local.pcap ftp 192.168.188.10 admin admin local.pcap
Copying!!
Total 1200 bytes copying completed.
```

Note:

- The packet capture software can use the wireshark and other software. For the using method, refer to wireshark guide document.

10.3.2. FTP Mode of Packet Capture Tool

Network Requirement

- Device and PC communicate with each other.
- On Device, enable the capture tool FTP mode to capture the packets passing gi1. And then, enter the FTP directory in the PC to view the captured file ftp.pcap.

Network Topology

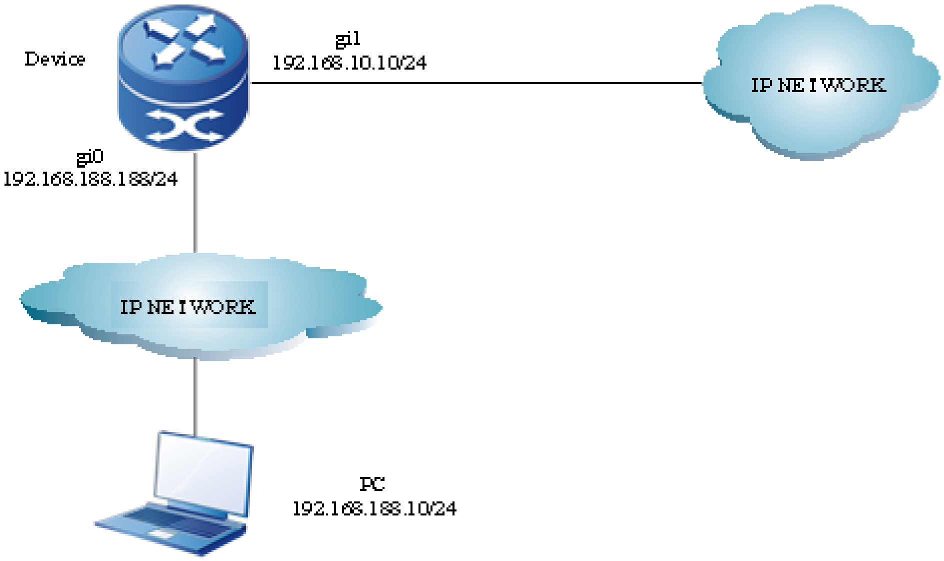


Figure 10-2 Networking of configuring the FTP mode of the capture tool

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Start the FTP mode to capture the packet.

#On Device, capture the packets passing the interface gi1 via the packet capture tool.

```
Device#traffic-capture interface gi1  ftp 192.168.188.10 admin admin ftp.pcap start
Starting capture traffic:
```

Step 3: Stop capturing the packet via the FTP mode.

#On Device, stop capturing the packets of the interface gi1 via the packet capture tool.

```
Device#traffic-capture interface gi1 ftp 192.168.188.10 admin admin ftp.pcap stop
Nov  9 2016 16:24:19.864: [tSshd-sh00]TCAP:Total 112 bytes copying completed.
```

Note:

- The packet capture software can use the wireshark and other software. For the using method, refer to wireshark guide document.

10.3.3. Mirror Mode of Packet Capture Tool

Network Requirement

- Device and PC communicate with each other.
- On Device, enable the mirror mode of the capture tool to capture the packets passing the interface gi1. The PC is directly connected to the mirror destination port via the network port. Open wireshark to capture the packets of the corresponding adapter. The mirror mode does not support WAN interface as the mirror destination port.

Network Topology

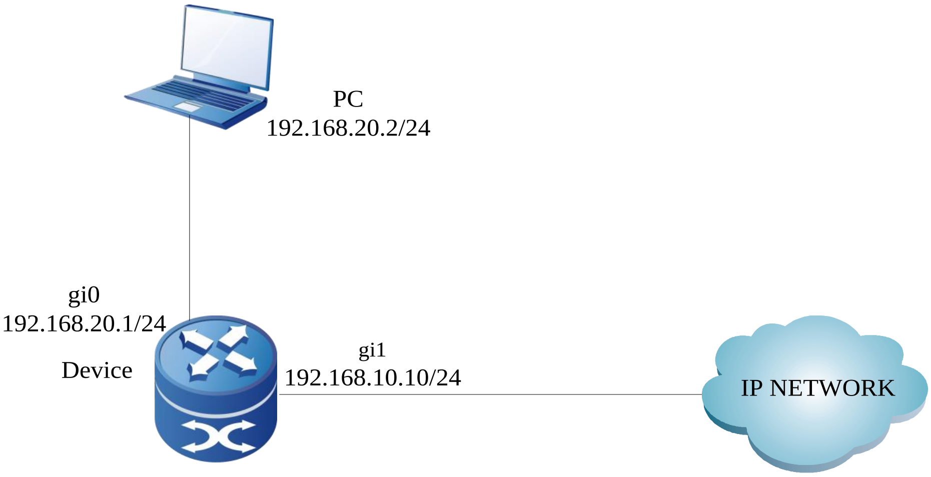


Figure 10-3 Networking of configuring the mirror mode of the capture tool

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Start the mirror mode to capture the packet.

#On Device, capture the packet passing the interface gi1, and mirror the packet to the interface gi0. The interface is directly connected with the PC.

```
Device# traffic-capture interface gi1 mirror interface gi0 start
Starting capture traffic:
```

Step 3: Stop capturing the packets via the mirror mode.

#On Device, stop capturing the packets of the interface gi1, PC is directly connected with gi0 via the network port, and open the packet capture software to capture the packets of the corresponding adapter, that is, the packets passing the interface gi1.

```
Device# traffic-capture interface gi1 mirror interface gi0 stop
```

```
Nov  9 2016 16:25:07.278: [tSshd-sh00]112 Bytes is captured on gigabitethernet1
```

Step 4: Check the result.

On the PC, analyze the captured packets via the packet capture software.

Note:

- The packet capture software can use the wireshark and other software. For the using method, refer to wireshark guide document.
- When capturing packets in the mirror mode, it is recommended that the mirror destination interface uses the network management interface.

11. CWMP

11.1. Overview

CWMP (CPE WAN Management Protocol) is a protocol developed by the BroadBandForum.org to manage and configure the CPE (Customer Premise Equipment), also called TR-069. It defines the general protocol frame, message standard, management mode, and data model to manage the CPE connecting to the carrier's Internet broadband access network.

CWMP can be described as a data frame model, which describes the communication between the device such as broadband router and the ACS (Auto-Configuration Server). It is used to perform the remote centralized configuration and management to the CPE (such as broadband router, switch, Internet gateway device, and STB) from the user side.

CWMP protocol is an application layer protocol above the IP layer. This protocol can be applied widely and has no restrict on the access mode. CPEs based on the following access modes, such as ADSL- (Asymmetrical Dig2wital Subscriber Loop), Ethernet network, and PON (Passive Optical Network), can use this protocol. System architecture based on the TR069 is shown in Figure 11-1. End-to-end architecture of the CWMP protocol has the following features:

1. With elastic connection model, both the CPE and ACS can trigger the connection establishment. This avoids maintaining connection between the CPE and ACS.
2. It can be automatically discovered between the CPE and ACS.
3. ACS can dynamically configure and monitor the CPE.

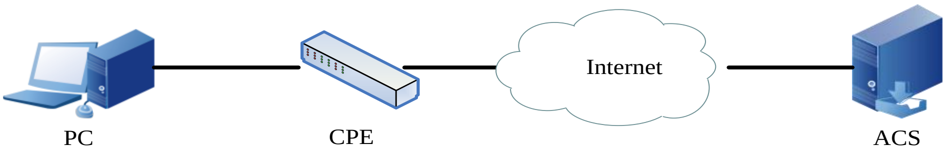


Figure 11-1 CPE and ACS architecture

For the CPE, the CWMP mainly completes the following four aspects of work:

4. Configure the CPE automatically and configure the dynamic service. For the ACS, each CPE can mark itself in the protocol, such as the model and version. According to the set rule, the ACS can send the configuration to a certain CPE or to a group of CPEs. The CPE can automatically request the ACS configuration information when it powers on and the ACS can actively initiate the configuration at any time. Through this function, it can achieve the CPE "zero configuration installation" function or control the service parameter dynamic change from the network side.
5. Manage the version file and configuration file of the CPE. The CWMP provides the management and download to the version file and configuration file in the CPE. The ACS can identify the version number of the user device and determines whether to remote update the software version of the device. The ACS can know whether the update succeeds after update completes. The CPE can backup through uploading the configuration file and recover through downloading the configuration file under the ACS control.

6. Configure remote upgrade to the CPE. It is a function initiated by the ACS to configure the remote upgrade to the CPE. Currently, the ACS performs remote upgrade to the CPE configuration in the hierarchical mode.
7. Achieve the secure management to the device interface. Through the RPC mode defined by the CWM (remote process invoking), it can perform secure management to the device interface, including the disabling, enabling, automatic binding, automatic unbinding, 802.1x interface , and disabling the 802.1x function

Warning:

- Ensure that the device with Flash as 16M will not power off or reboot when upgrading the version using the CWMP and ensure the correctness of the upgrade version. Otherwise, the system may fail to be booted.

11.2. CWMP Function Configuration

Table 11-1 CWMP function configuration list

Configuration Task	
Configure the CWMP basic function	Enter the CWMP configuration mode
	Enable the CWMP proxy
	Configure the ACS server related information
	Configure the WAN device interface
	Configure the CWMP to periodically send the INFORM packet
	Configure the period of the CWMP sending the INFORM packet
	Configure the CWMP file download
	Configure the breakpoint resume function of the CWMP file
	Configure the provision code of the CWMP
Configure the CWMP authentication and encryption function	Configure the CWMP authentication information
	Configure the ACS certificate of the CWMP
	Configure the ACS certificate fingerprint of the CWMP

Configuration Task	
Configure the CWMP extended function	Configure the specified IP address of the CWMP
	Configure the CWMP link backup

11.2.1. Configure CWMP basic function

Configuration Condition

Before configuring the CWMP proxy basic function, first enter the global configuration mode and then configure the CWMP proxy basic function.

Enter CWMP Configuration Mode

For the configuration related to the CWMP proxy, first enter the CWMP proxy configuration mode.

Table 11-2 Enter the CWMP configuration mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the CWMP proxy configuration mode	**cwmp agent**	Mandatory

Enable CWMP Proxy

If the device is enabled with the CWMP proxy function, then the device can interact with the CS through the CWMP proxy to remote configure and manage the device.

Table 11-3 Enable the CWMP proxy

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the CWMP proxy configuration mode	**cwmp agent**	Mandatory
Enable the CWMP proxy	**enable**	Mandatory By default, the CWMP proxy is in the disabled state.

Configure ACS Server Related Information

By configuring the ACS related information, including the connection address of the ACS server, the device can communicate with the ACS server.

Table 11-4 Configure the ACS server related information

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the CWMP proxy configuration mode	**cwmp agent**	Mandatory
Enable the CWMP proxy	**enable**	Mandatory By default, the CWMP proxy is in the disabled state.
Configure ACS related information	**management server url** *url-string*	Mandatory By default, the device is not configured with the ACS related parameter. For the unencrypted mode, *url-string* uses the http protocol. For the encryption mode, *url-string* uses the https protocol.
Configure the user name of the device initiating the connection to the ACS	**management server** *user-name*	Optional By default, the device is not configured with the ACS related parameter. If the user name is not configured on the ACS, do not need to configure the user name.
Configure the user name and corresponding password of the device initiating the connection to the ACS	**management server** *password*	Optional By default, the device is not configured with the ACS related parameter. If the user name and corresponding password are not configured on the ACS, do not need to configure the user name and password.

Configure WAN Device Interface

Specify the interface as the default WAN device interface in the interface mode. If the default WAN device is not specified, it will cause that the CWMP proxy cannot send the Inform packet to connect the ACS server.

Table 11-5 Configure the WAN device interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L3 interface to be used	**interface** *interface-name*	Mandatory It must be configured in the L3 interface mode.
Configure the default WAN device	**cwmp wan default**	Mandatory By default, the WAN device interface of the CWMP proxy is not specified.

Note:

- If the default WAN device is not specified, it may cause that the CWMP cannot send the Inform packet to connect the ACS. It must be clear that the parameter name and the IP address of the WAN device connecting to the Internet in the current system when organizing the Inform packet.
- After an interface is specified as the default WAN device, if the WAN IP address is not configured in the CWMP mode and the interface is configured with the IP address, the connection request URL is generated by using the IP address of the interface.

Configure CWMP to Periodically Send INFORM Packet

By configuring the CWMP to periodically send the Inform packet, the device can periodically send the Inform packet to the ACS. After the ACS receives the Inform packet sent by the device, handle the packet based on the pre-configuration.

Table 11-6 Configure the CWMP to periodically send the INFORM packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the CWMP proxy configuration mode	**cwmp agent**	Mandatory
Enable the CWMP proxy	**enable**	Mandatory By default, the CWMP proxy is disabled.
Configure the CWMP to periodically send the INFORM packet	**enable inform**	Mandatory By default, the function of CWMP periodically sending the INFORM function is enabled.

Configure Period of CWMP Sending INFORM Packet

After configuring the CWMP to periodically send the INFORM packet, you can configure the period of the CWMP proxy sending the Inform packet. The default sending period is 43200s (12h).

Table 11-7 Configure the period of the CWMP sending the INFORM packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the CWMP configuration mode	**cwmp agent**	Mandatory
Enable the CWMP proxy	**enable**	Mandatory By default, the CWMP proxy is disabled.
Configure the CWMP to periodically send the INFORM packet	**enable inform**	Mandatory By default, the function of the CWMP periodically sending the INFORM packet is enabled,

Step	Command	Description
Configure the period of the CWMP sending the INFORM packet	**inform interval** *inform-interval*	Mandatory By default, the interval for the device automatically sending the inform packet is 43200s.

Note:

- After the function of the CWMP proxy sending the Inform packet is configured and the sending period of the Inform packet is not configured, the CWMP sends the Inform packet to the ACS in 43200s (12h) by default.
- After the periodical sending interval of the Inform packet is modified, the modified interval can only take effect when the last interval expires. If you want the modified interval to take effect immediately, you can reboot the CWMP proxy. Wherein, for enable and no enable, refer to the related chapter in the CWMP command manual.

Configure CWMP File Download

When the function of CWMP proxy supporting the file download is required to download the version file and configuration file, configure the CWMP proxy file download function in advance.

Table 11-8 Configure the CWMP file download

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the CWMP proxy configuration mode	**cwmp agent**	Mandatory
Enable the CWMP proxy	**enable**	Mandatory By default, the CWMP proxy is disabled.
Configure the CWMP file download function	**enable download**	Mandatory By default, the file download function of the CWMP is not enabled.

Configure Breakpoint Resume Function of CWMP File

After the CWMP file download function is configured and the CWMP is required to support the breakpoint resume function, you can configure the function.

Table 11-9 Configure the breakpoint resume function of the CWMP file

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the CWMP proxy configuration mode	**cwmp agent**	Mandatory
Enable the CWMP proxy	**enable**	Mandatory By default, the CWMP proxy is disabled.
Configure the CWMP file download function	**enable download**	Mandatory By default, the file download function of the CWMP is not enabled.
Configure the breakpoint resume function of the CWMP file	**enable download resume**	Mandatory By default, the file breakpoint resume function of the CWMP is not enabled.

Note:

- Before the breakpoint resume function of the CWMP file is configured the file download function of the CWMP must be configured. If the file download function is not configured at first, then the file breakpoint resume function will not take effect even if the file resume function is configured.

Configure CWMP Provision Code

This function is used to configure the CWMP provision code which is used to mark the basic service information provided by the CWMP.

Table 11-10 Configure CWMP provision code

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the CWMP proxy configuration mode	**cwmp agent**	Mandatory
Enable the CWMP proxy	**enable**	Mandatory By default, the CWMP proxy is disabled.
Configure the CWMP provision code	**provision code** *provision-code*	Mandatory By default, the CWMP is not configured with the provision code.

11.2.2. Configure CWMP Authentication and Encryption Function

Configuration Condition

Before configuring the CWMP authentication and encryption function, first complete the following task:

- The basic configuration of the CWMP proxy is completed, including the CWMP proxy enabling configuration and the ACS information configuration of the CWMP proxy.
- When configuring the encryption function, prepare the certificate and it requires manual import.

Configure CWMP Authentication Function

When the ACS requires initiating the connection to the device, configure the CWMP proxy to authenticate the connection request sent from the ACS in terms of the security.

Table 11-11 Configure the CWMP authentication function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the CWMP proxy configuration mode	**cwmp agent**	Mandatory
Enable the CWMP proxy	**enable**	Mandatory By default, the CWMP proxy is disabled.
Configure the user name for the CPE authenticating the connection request from the ACS	**connection request username** *user-name*	Mandatory By default, the user name is not configured.
Configure the password for the CPE authenticating the connection request from the ACS	**connection request password** *password*	Mandatory By default, the password is not configured.

Configure CWMP PKI Trust Domain Name

Viewing from the security, when the device connects to the ACS through the HTTPS mode, you need to specify the KPI trust domain name of the CWMP proxy, so as to verify the validity of the ACS certificate.

Table 11-12 Configure the CWMP ACS certificate

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the CWMP proxy configuration mode	**cwmp agent**	Mandatory
Enable the CWMP proxy	**enable**	Mandatory By default, the CWMP proxy is disabled.

Step	Command	Description
Configure the KPI trust domain name of the CWMP proxy	**secure-identity ca**-*name*	Mandatory By default, the CWMP proxy does not have the KPI trust domain name.

11.2.3. Configure CWMP Extended Function

Configuration Condition

Before configuring the CWMP extended function, first complete the following tasks:

- Complete the CWMP basic configurations, including the CWMP proxy enabling configuration, CWMP proxy ACS information configuration.
- Configure the IP address of the interface to enable that the network layers of the neighboring nodes are reachable.
- When the link backup function is required, the interface configured as backup must be normal, including the configured IP address and the interface in the UP state.

Configure CWMP Specified Source IP Address

When the source IP address is configured, the ACS can directly communicate with the specified IP address.

Table 11-13 Configure the source IP address specified by the CWMP

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the CWMP proxy configuration mode	**cwmp agent**	Mandatory
Enable the CWMP proxy	**enable**	Mandatory By default, the CWMP proxy is disabled.
Configure the source IP address specified by the CWMP proxy	**ip source** *ip-address*	Mandatory By default, the source IP address of the packet is not specified when the device establishes link with the ACS and the source IP address of the packet is the packet egress interface.

Configure CWMP link backup

When the link backup function is configured under the interface mode, there is one default WAN interface and others are backup WAN interfaces when the device is configured with multiple WAN interfaces. The IP address of the default WAN interface is used to generate the connection request URL and then send it to the ACS. When the default WAN interface is down, one interface is chosen from the backup WAN interface and is considered as the current WAN interface. Then, its IP address is used to generate the connection request URL,

Table 11-14 Configure the CWMP link backup

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L3 interface requiring setting backup	**interface** *interface-name*	Mandatory
Configure the backup interface of CWMP proxy	**cwmp wan backup**	Mandatory By default, the WAN device backup interface of the CWMP proxy is not specified.

Note:

- Each device can only be configured with one CWMP WAN default interface and one CWMP WAN backup interface.

11.2.4. CWMP Monitoring and Maintaining

Table 11-15 CWMP monitoring and maintaining

Command	Description
show cwmp agent	Display the related information of the CWMP proxy.
show cwmp session	Display the session information of the CWMP proxy.
show cwmp methods	Display the RPC (Remote Procedure Call)) supported by the CWMP proxy
show cwmp parameter all	Display all the parameter names of the CWMP proxy

Command	Description
show cwmp parameter *para-string*	Display the detailed parameter information of the specified CWMP proxy
show cwmp parameter notify { active | **all** | **forceactive** | **passive }**	Display the notified parameter name of the CWMP proxy
show cwmp parameter values [*para-string* | **error**]	Display the detailed parameter information of the specified CWMP proxy

11.3. CWMP Typical Configuration Example

11.3.1. Configure CWMP Authentication Function

Network Requirements

- Device accesses the ACS through the Network and enable the CWMP function on Device. Configure the authentication function both on Device and ACS.
- After the authentication passes, Device will execute the version upgrade, configuration restoration, configuration backup, and configuration upgrade tasks sent by the ACS.

Network Topology

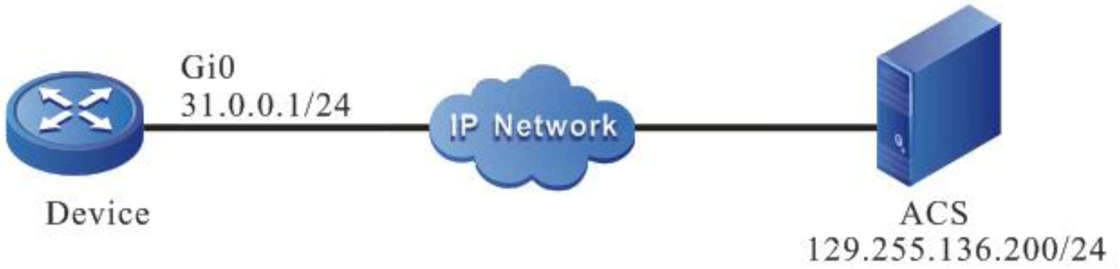


Figure 11-2 Networking of the CWMP authentication function

Configuration Steps

Step 1: Configure the IP address and route of the interface. (Omitted)

Step 2: Configure the CWMP.

#Enable the CWMP proxy and file download function on Device and configure the URL of the ACS.

```
Device#configure terminal
Device(config)#cwmp agent
Device(config-cwmp)#enable
Device(config-cwmp)#management server url
http://129.255.136.200:8080/openacs/acs
Device(config-cwmp)#enable download
Device(config-cwmp)#exit
```

#Configure the gigabitethernet0 interface as the default WAN device.

```
Device(config)#interface gigabitethernet0
Device(config-if-gigabitethernet0)#cwmp wan default
Device(config-if-gigabitethernet0)#exit
```

Step 3: Configure the ACS server.

#Create the fragment template on the ACS and configure both the authentication user name and password as admin. (Omitted)

#Create the configuration upgrade task on the ACS and choose the fragment template to be created. Deliver the configuration task to Device. (Omitted)

Note:

- The ACS sends the authentication user name and password to Device through configuring the upgrade task to ensure that the ACS can pass the Device authentication.

#Create version upgrade task, restoration task, and backup task on the ACS.

Step 4: Check the result.

#Execute the **show running-config** command on Device and it can be viewed that the ACS sends the user name and password of Device.

```
cwmp agent
 management server url http://129.255.136.200:8080/openacs/acs
 connection request username admin
 connection request password admin
 enable download
 enable
 exit
```

#Device can successfully execute the version upgrade task. Configure the restoration task and backup task sent by the ACS.

11.3.2. Configure Source IP Address specified by CWMP

Network Requirements

- Device accesses the ACS through Network and enable the CWMP function on Device.
- Specify the source IP address of the CWMP as 1.0.0.1. enable Device to visit the ACS through the firewall and execute the version upgrade, configuration restoration, and configuration backup tasks sent by the ACS.

Network Topology

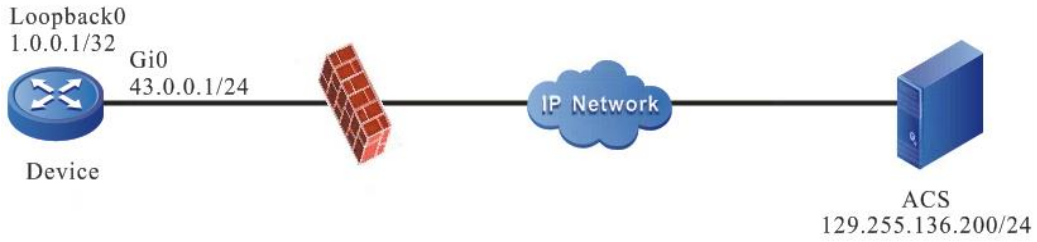


Figure 11-3 Networking of configuring the source IP address specified by the CWMP

Configuration Steps

Step 1: Configure the IP address and router of the interfaces. (Omitted)

Step 2: Configure the CWMP.

# Enable the CWMP proxy and file download function on Device. Configure the URL of the ACS and the source IP address of the CWMP as 1.0.0.1.

```
Device#configure terminal
Device(config)#cwmp agent
Device(config-cwmp)#enable
Device(config-cwmp)#management server url
http://129.255.136.200:8080/openacs/acs
Device(config-cwmp)#enable download
Device(config-cwmp)#ip source 1.0.0.1
Device(config-cwmp)#exit
```

#Configure the Loopback0 interface as the default WAN device.

```
Device(config)#interface loopback 0
Device(config-if-loopback0)#cwmp wan default
Device(config-if-loopback0)#exit
```

Step 3: Configure the firewall.

#The firewall rejects the packet with the source IP address as 43.0.0.1 to pass and allows the packet with the source IP address as 1.0.0.1 to pass.

Step 4: Configure the ACS server.

#Create the version upgrade task and configuration restoration task and configuration backup task on the ACS.

Step 5: Check the result.

#Execute the **show running-config** command on Device and the configured source IP address can be viewed.

```
cwmp agent
 management server url http://129.255.136.200:8080/openacs/acs
```

```
enable download
enable
ip source 1.0.0.1
exit
```

#Device can successfully execute the version upgrade task and configuration restoration task and configuration backup task sent by the ACS.

11.3.3. Configure CWMP Link Backup

Network Requirements

- Device can access the ACS through two links. The gigabitethernet0 interface is selected by priority to communicate with the ACS.
- When the gigabitethernet0 interface is faulty, Device can communicate with the ACS through the gigabitethernet1 interface. When the gigabitethernet0 interface recovers, Device can communicate with the ACS through the gigabitethernet1 interface.

Network Topology

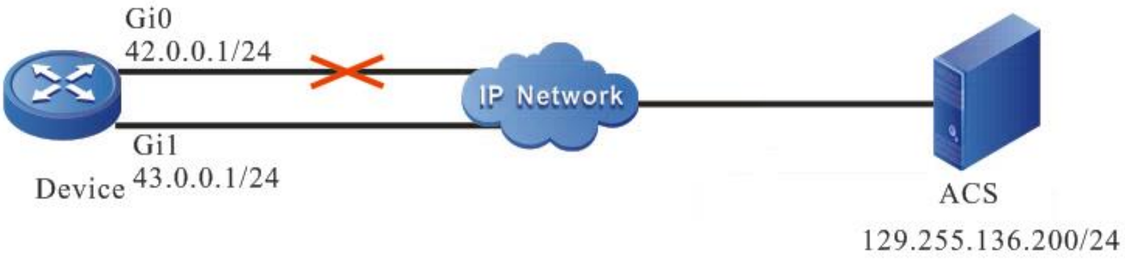


Figure 11-4 Networking of configuring the CWMP link backup

Configuration Steps

Step 1: Configure the IP address and route of the interfaces. (Omitted)

Step 2: Configure the CWMP.

#Enable the CWMP proxy and file download function on Device and configure the URL of the ACS.

```
Device#configure terminal
Device(config)#cwmp agent
Device(config-cwmp)#enable
Device(config-cwmp)#management server url
http://129.255.136.200:8080/openacs/acs
Device(config-cwmp)#enable download
Device(config-cwmp)#exit
```

#Configure the gigabitethernet0 interface as the default WAN interface.

```
Device(config)#interface gigabitethernet0
Device(config-if-gigabitethernet0)#cwmp wan default
Device(config-if-gigabitethernet0)#exit
```

#Configure the gigabitethernet1 interface as the backup WAN device.

```
Device(config)#interface gigabitethernet1
Device(config-if-gigabitethernet1)#cwmp wan backup
Device(config-if-gigabitethernet1)#exit
```

Step 4: Check the result.

#View the CWMP proxy information on Device.

```
Device#show cwmp agent
 Agent status: Enabled
 Periodic Inform: Enabled
 Download files: Enabled
 Inform interval: 43200
 ACS URL: http://129.255.136.200:8080/openacs/acs
 ACS user name:
 ACS user password:
 Connection request URL: http://42.0.0.1:7547/00017A/MyPower-
S4320/00017a136922/cwmp
 Connection request user name:
 Connection request password:
 Default WAN device: vlan2
 Current WAN device: vlan2
 CA certificate: /flash/tr069/ca.pem
```

It can be viewed that the default WAN device is gigabitethernet0 and current WAN device is gigabitethernet0. It can be viewed on the ACS management page that the corresponding IP address of Device is 42.0.0.1.

#When the gigabitethernet0 interface on Device is faulty, view the CWMP proxy information.

```
Device#show cwmp agent
 Agent status: Enabled
 Periodic Inform: Enabled
 Download files: Enabled
 Inform interval: 43200
 ACS URL: http://129.255.136.200:8080/openacs/acs
 ACS user name:
 ACS user password:
 Connection request URL: http://43.0.0.1:7547
 Connection request user name:
 Connection request password:
 Default WAN device: gigabitethernet0
```

```
Current WAN device: gigabitethernet1
Secure identity:
```

It can be viewed that the default WAN device is gigabitethernet0 and current WAN device is gigabitethernet1. It can be viewed on the ACS management page that the corresponding IP address of Device is 43.0.0.1.

#When the gigabitethernet0 interface on Device is recovered, view the CWMP proxy information. It can be viewed that both the default WAN device and the current WAN device is gigabitethernet0. It can be viewed on the ACS management page that the corresponding IP address of Device is 42.0.0.1.

12. NETCONF

12.1. Overview

NETCONF (Network Configuration Protocol) is a kind of network management protocol based on XML. It provides a programmable method to configure and manage network devices. With this protocol, users can set parameters, obtain parameter values, obtain statistical information, etc. NETCONF packet uses the XML format and has powerful filtering ability. Each data item has a fixed element name and location, which makes different devices of the same manufacturer have the same access mode and result presentation mode. The devices of different manufacturers can also get the same effect by mapping XML, which makes it very convenient in the development of the third-party software, it is easy to develop a special customized network management software in the environment of mixing different manufacturers and different devices. With the help of such network management software, using NETCONF function will make the configuration management of network equipment simpler and more efficient.

12.2. NETCONF Basic Function Configuration

Table 12-1 NETCONF basic function configuration list

Configuration Tasks	
Configure the functions of the NETCONF server	Enable the NETCONF server function
	Configure the disconnection timeout of the NETCONF client
	Configure the maximum sessions of NETCONF

12.2.1. Configure NETCONF Server Functions

Configuration Conditions

Before configuring the functions of the NETCONF server, first complete the following tasks:

- Configure the link-layer protocol and ensure the normal communication of the link layer.
- Configure the network-layer address of the interface and ensure that the NETCONF client node is reachable at the network layer.

Enable NETCONF Server Function

Table 12-2 Enable the NETCONF server function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the global NETCONF function	**netconf server enable**	Mandatory By default, the NETCONF function is not enabled.

Configure Timeout Disconnection Function of the NETCONF Client

Table 12-3 Configure the timeout disconnection time of the NETCONF client

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the global NETCONF function	**netconf client idle-time**	Mandatory By default, the timeout disconnection time of the NETCONF client is 3600s.

Configure Max. Sessions of NETCONF

Table 12-4 Configure the maximum number of the NETCONF sessions

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the maximum sessions of NETCONF	**netconf server max-session session-num**	Optional By default, the maximum sessions supported by the NETCONF server is 4.

12.2.2. NETCONF Monitoring and Maintaining

Table 12-5 NETCONF monitoring and maintaining

Command	Description
show netconf session	Display the connected session information of the NETCONF client

12.3. NETCONF Typical Configuration Example

12.3.1. Configure NETCONF Server

Network Requirements

- Device1 and Device2 are NETCONF server devices, communicating with the controller via the unicast route protocol.
- The controller monitors and manages Device1 and Device2 via NETCONF.

Network Topology

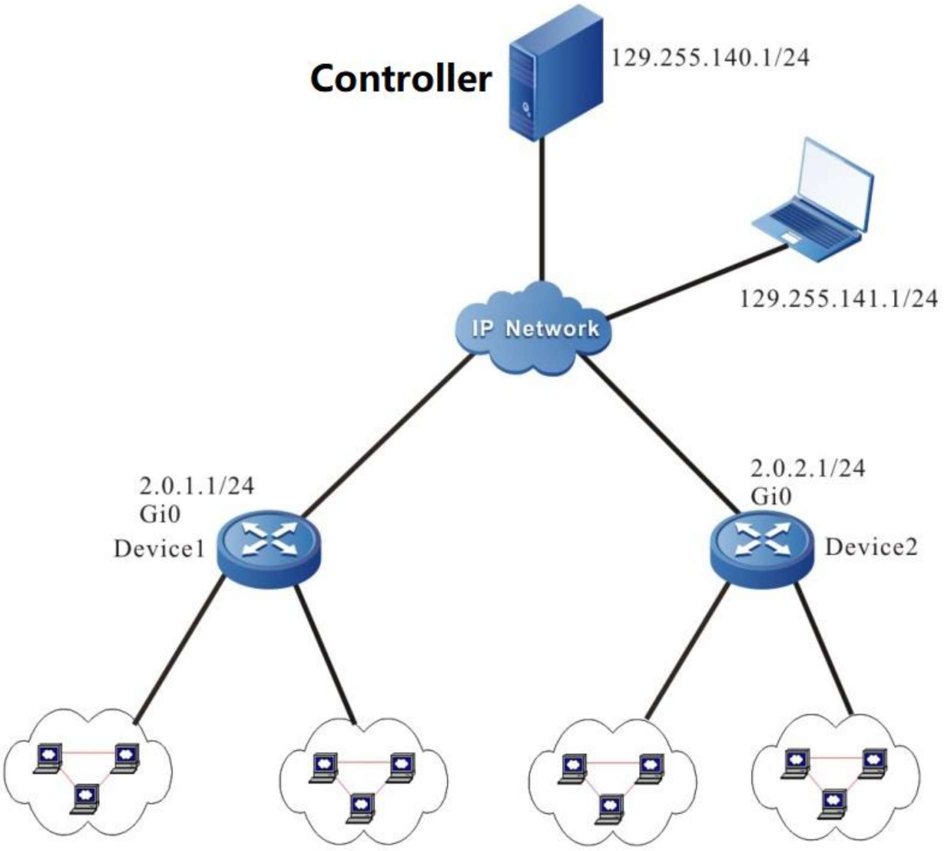


Figure 12-1 Networking of configuring the NETCONF server

Configuration Steps

Set up the NETCONF connection between the controller and device, and then, the controller configures and manages the device via NETCONF. Take Device1 as an example, and the configuration of Device2 is similar.

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Configure the NETCONF user.

#On the device, create Netconf user with user name **admin** and password **admin@123**.

```
Device1#configure terminal
Device1(config)#local-user admin class manager
Device1(config-user-manager-admin)#service-type netconf ftp
Device1(config-user-manager-admin)#password 0 admin@123
Device1(config-user-manager-admin)#privilege 15
Device1(config-user-manager-admin)#exit
```

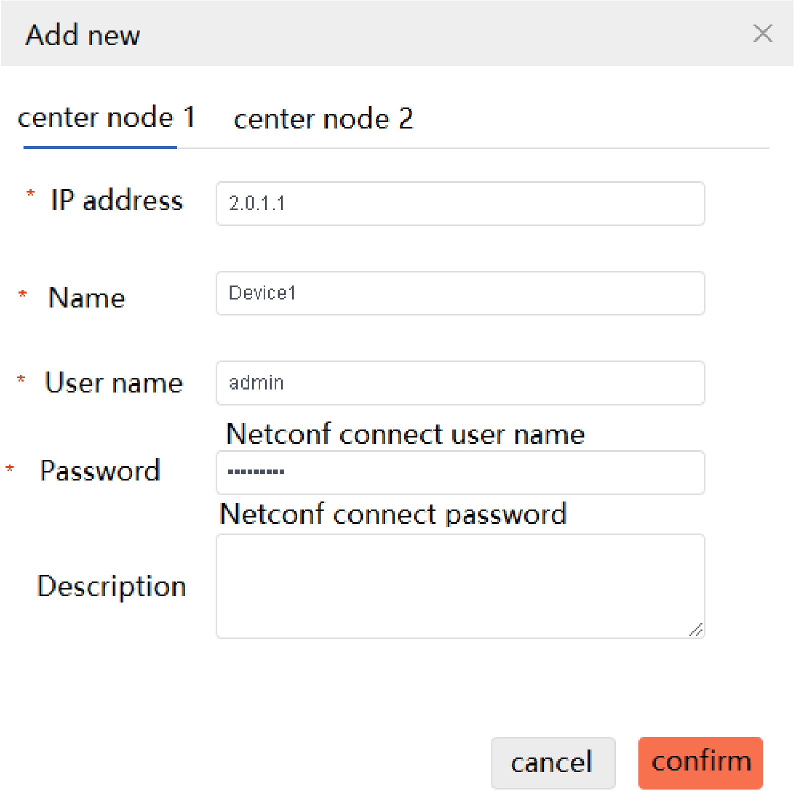
Step 3: Enable the NETCONF server function on the device.

#On the device, enable the NETCONF server function.

```
Device1(config)#netconf server enable
```

Step 4: Configure the controller.

#Open the controller, click "Network Planning", select "Network Discovery", click "Add Node", and configure NETCONF parameters: "IP address", "Name", "Account" and "Password". The configured parameters "IP address", "Account" and "Password" must be consistent with those on the device. Click **OK** to establish normal communication between the device and the controller.



Add new

* IP address: 2.0.1.1

* Name: Device1

* User name: admin

Netconf connect user name

* Password: ••••••••

Netconf connect password

Description:

Figure 12-2 Configure the controller

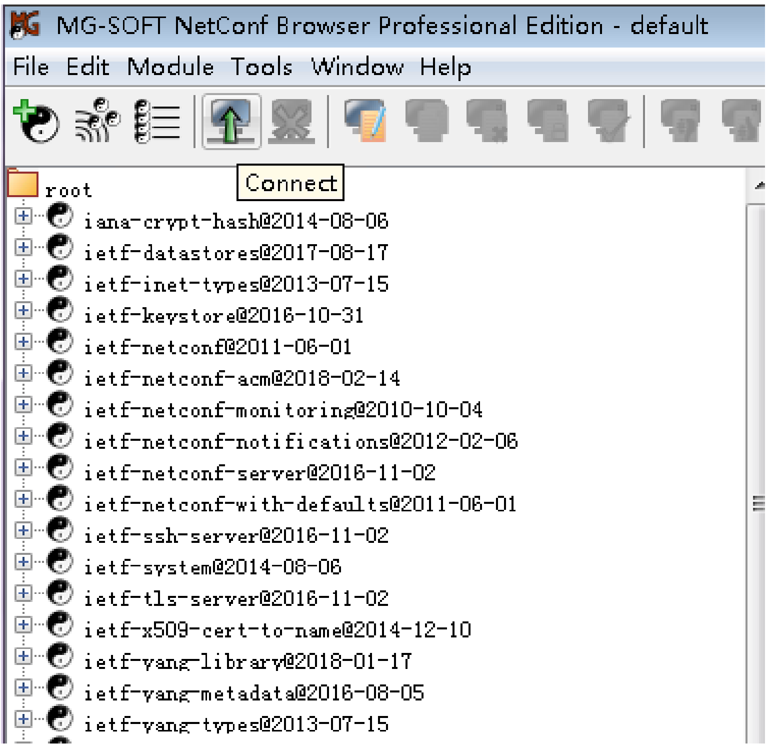
Step 5: Check the result.

#On the device, query the connection set up between the controller and the NETCONF server.

```
Device1#show netconf session
 ------------------
 session id: 1
 transport: SSH
 user name: admin
 source host: 129.255.140.1
 login time: 2019-06-1T20:29:05Z
 in rpcs: 1
 in bad rpcs: 0
 out rpc errors: 0
out notifications: 0
```

Step 6: Configure MG-SOFT NetConf Browser client.

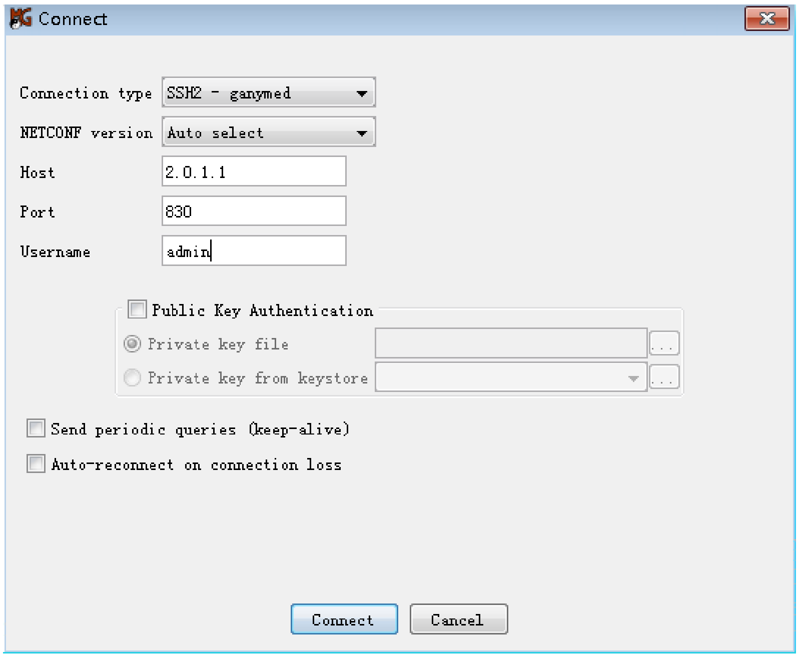
#You can also establish a connection with the device server through the MG-SOFT NetConf Browser software. Open MG-SOFT NetConf Browser software, click "Connect", configure NETCONF parameters: "IP address", "port number" and "account", click "Connect", enter the password, and click "OK". The configured parameters "IP address", "account" and "password" must be consistent with those on the device.



MG-SOFT NetConf Browser Professional Edition - default
File Edit Module Tools Window Help
Connect
root

```
iana-crypt-hash@2014-08-06
ietf-datastores@2017-08-17
ietf-inet-types@2013-07-15
ietf-keystore@2016-10-31
ietf-netconf@2011-06-01
ietf-netconf-acm@2018-02-14
ietf-netconf-monitoring@2010-10-04
ietf-netconf-notifications@2012-02-06
ietf-netconf-server@2016-11-02
ietf-netconf-with-defaults@2011-06-01
ietf-ssh-server@2016-11-02
ietf-system@2014-08-06
ietf-tls-server@2016-11-02
ietf-x509-cert-to-name@2014-12-10
ietf-yang-library@2018-01-17
ietf-yang-metadata@2016-08-05
ietf-yang-types@2013-07-15
```

Figure 12-3 MG-SOFT NetConf Browser software interface



Connection type	SSH2 - ganymed
NETCONF version	Auto select
Host	2.0.1.1
Port	830
Username	admin

□ Public Key Authentication

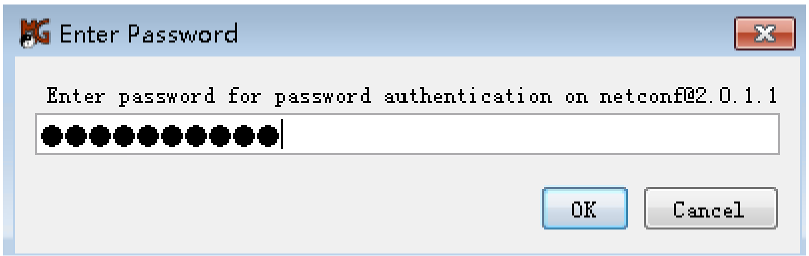
● Private key file

○ Private key from keystore

□ Send periodic queries (keep-alive)

□ Auto-reconnect on connection loss

Figure 12-4 NETCONF parameter configuration



Enter password for password authentication on netconf@2.0.1.1

●●●●●●●●●●●

Figure 12-5 Input the password

Step 7: Check the result.

#Query the connection between the MG-SOFT NetConf Browser client and the NETCONF server of the device.

```
Device1#show netconf session
 -------------------
 session id: 1
 transport: SSH
 user name: admin
 source host: 129.255.141.1
 login time: 2019-06-1T20:30:05Z
 in rpcs: 1
 in bad rpcs: 0
 out rpc errors: 0
out notifications: 0
```

13. EDP

13.1. Overview

In the solution of NGWAN, it is first necessary to configure the device to make the bearer network work normally, but the workload of device configuration is large. Manual configuration not only has huge manpower investment, but also is easy to make mistakes. Centralized configuration and distribution through SDN controller can greatly save manpower and time, and avoid some misoperations. Ethernet discovery protocol (EDP) is the basis of online solution for device 0-configuration. Ethernet network discovery protocol is mainly used for network topology discovery without device configuration, and provides support for subsequent network configuration and management.

EDP currently supports the Hub-spoke networking structure. The typical network topology is shown in Figure 13-1 ~ 13-5 below.

In the target network, the controller and the central node device (the core router in the networking diagram below) are generally located in the same LAN. The central node needs to be configured with a management interface to enable the L3 communication with the controller, and other service interfaces may not be configured. In this way, EDP only needs to be implemented on the device. On the one hand, it reduces the impact of broadcast packets on the LAN where the controller is located, on the other hand, it reduces the implementation cost. Otherwise, it needs to be implemented on both the controller and the device.

In the Hub-spoke network, topology discovery from the central node is more efficient and occupies less network bandwidth. Therefore, EDP supports two working modes: active mode and passive mode. The active mode initiates the query of topology discovery, while the passive mode can only work after receiving the query. After the upstream link ages, it will not send any packets.

By default, the device of supporting 0-configuration online enables the Ethernet discovery function and is in passive mode. The central node needs to be configured to work in active mode. After the topology collection is completed, the configuration distribution is completed, and the device is in normal working state, the controller can control to disable the topology discovery function of the central node, so as to suspend this function. You can also re-enable this function for the latest topology discovery when a new device gets online or line fault location is performed. Therefore, it is required that the device can work normally without configuration and with configuration. EDP supports a maximum network node size of 800, a maximum of 5 levels, and the convergence time of the whole topology is 10 minutes. Multiple central nodes can be configured in the whole topology, and each center finds its own centric topology.

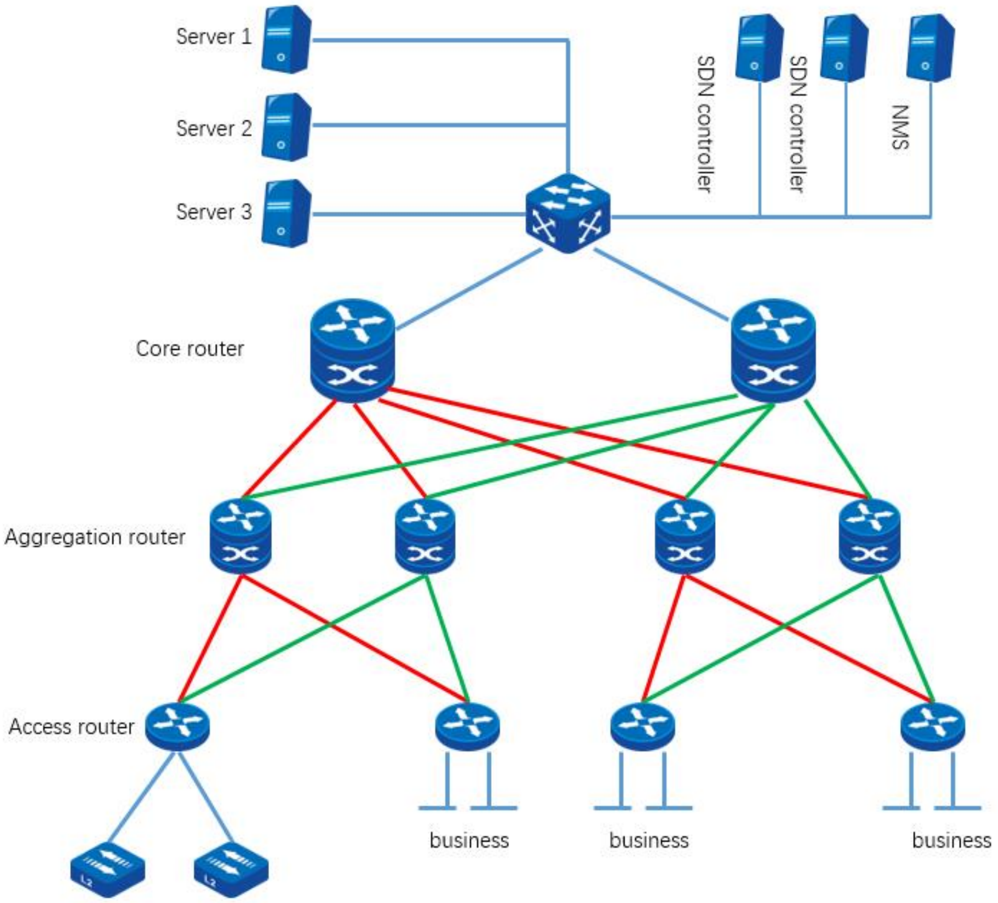


Figure 13-1 Typical network topology 1

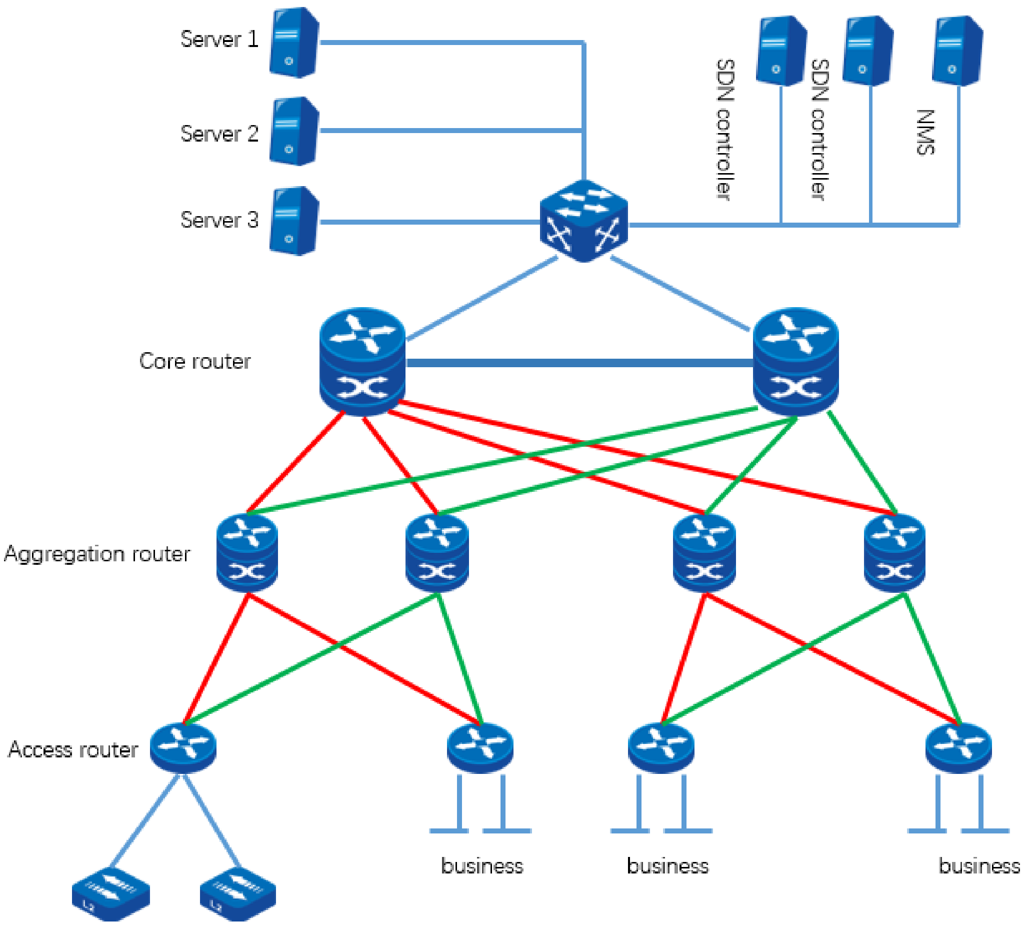


Figure 13-2 Typical network topology 2

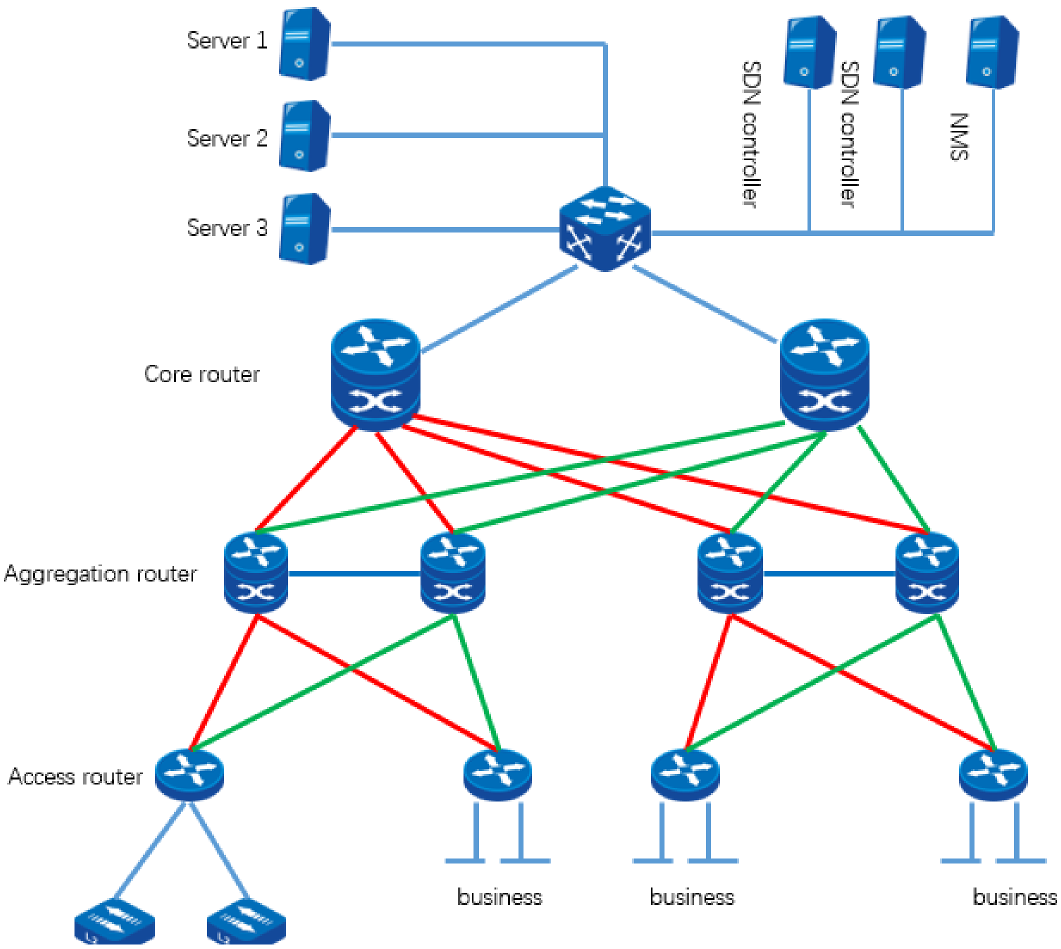


Figure 13-3 Typical network topology 3

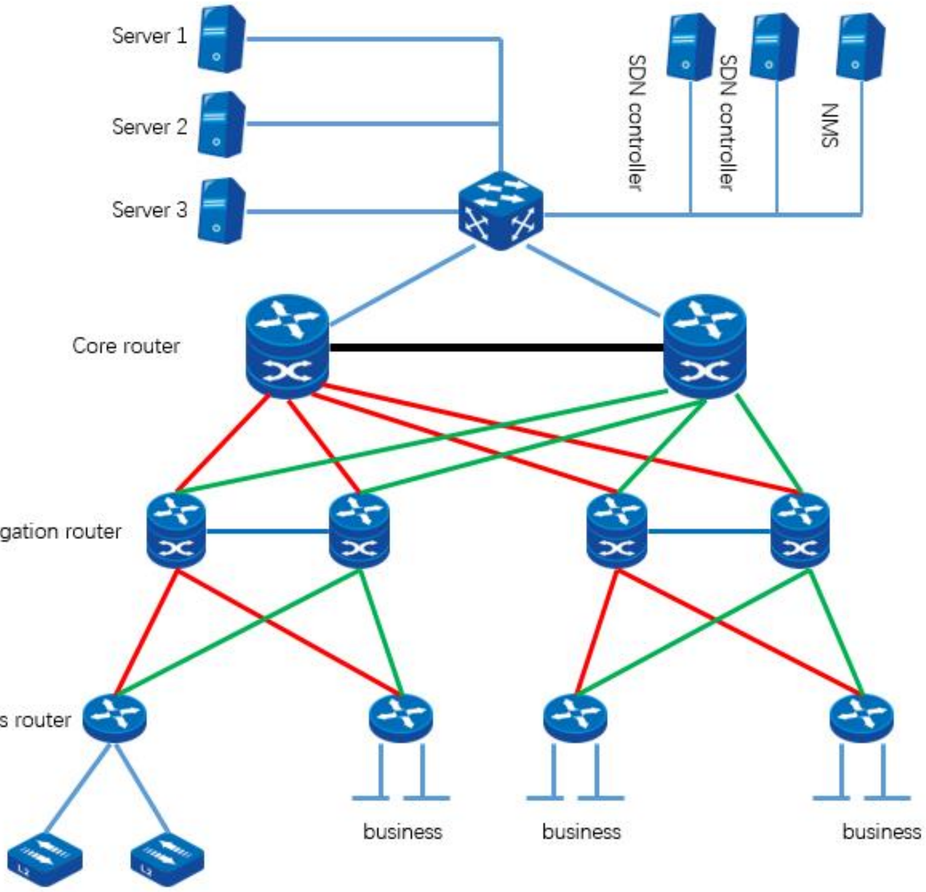


Figure 13-4 Typical network topology 4

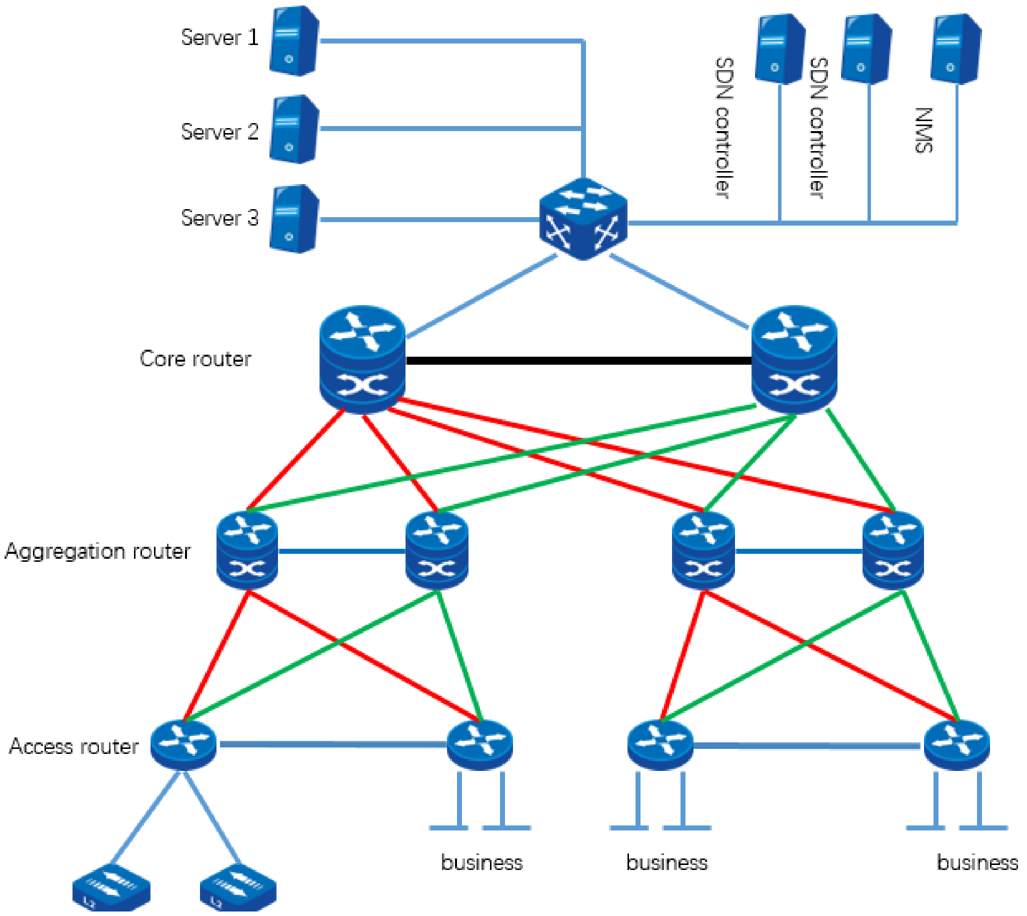


Figure 13-5 Typical network topology 5

13.2. EDP Function Configuration

Table 13-1 EDP function configuration list

Configuration Tasks	
Configure EDP basic functions	Enable EDP globally
	Enable EDP on the interface
	Configure EDP work mode
	Configure the EDP parameters
Configure other EDP functions	Configure EDP to collect the device information
	Configure EDP to create a sub interface
	Configure EDP weak check function

Configuration Tasks	
Configure the EDPS function	Configure EDPS to deliver files
	Configure EDPS to load files
	Configure EDPS to upload files

13.2.1. Configure EDP Basic Functions

Configuration Conditions

None

Enable EDP globally

By default, EDP is enabled under the interface, and global EDP is enabled by default. EDP topology discovery can only be triggered when global EDP and interface EDP are enabled at the same time.

Table 13-2 Enable global EDP

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable global EDP	**edp enable**	Mandatory By default, the global EDP is enabled.

Enable Interface EDP

Table 13-6 Enable interface EDP

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Enable the interface EDP	**edp enable**	Mandatory By default, the interface EDP is enabled.

Configure EDP Work Mode

EDP supports two working modes: active mode and passive mode. The active mode initiates the query of topology discovery, while the passive mode can only work after receiving the query. After the upstream link ages, it will not send any packets.

Table 13-3 Configure EDP work mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure EDP work mode	**edp mode** {**proactive** | **reactive** }	Mandatory By default, the EDP work mode is passive mode.

Configure EDP Parameters

Configure various EDP parameters to ensure that the EDP topology of the whole network is discovered smoothly.

Table 13-4 Configure EDP global parameters

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the unreachable hop value of the EDP packet of the whole network	**edp hop-limit** *hop-value*	Mandatory By default, the unreachable hops of the EDP packets of the whole network is 6.
Configure downstream link limits	**edp link-limit** *link-number*	Mandatory By default, the downstream link limit is 6.
Configure the query interval of the EDP entry	**edp query** *interval-second*	Mandatory By default, the query interval of the EDP entry is 5s.
Disable the function of sending the EDP HELLO packet	**edp hello disable**	Mandatory By default, the function of sending the EDP HELLO packets is enabled.

Table 13-5 Configure EDP interface parameters

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	After entering the interface configuration mode, subsequent configurations will only take effect on the current interface.
Configure the management cost of the interface	**edp hop-cost** *cos-value*	Mandatory By default, the management cost of the interface is 0.
Configure the Ethernet protocol type of the EDP packets	**edp proto-type** *type-value*	Mandatory By default, the Ethernet protocol type of the EDP packet is 1.

13.2.2. Configure Other EDP Functions

Configuration Conditions

None

Configure EDP to Collect Device Information

The function of collecting the device information can collect the information of the whole network and specified devices. The collected information includes device ID, serial number, device name, device type and other information.

Table 13-6 Configure EDP to collect the device information

Step	Command	Description
Configure EDP to collect the device information	**edp collect device** [*device-id*]	Mandatory By default, the device does not collect the device information actively.

Configure EDP to Create Sub Interface

In the point to multipoint networking topology of MSTP network, the upper device is connected to MSTP network through a physical line (typically Ethernet link). On the physical line, the operator divides logical channels by setting VLAN, and each logical channel corresponds to an access point at the lower end; Similarly, the underground access point is connected to the MSTP network through a physical link (also an Ethernet link), and is connected to the upper network through a logical channel on the upper device.

In order to discover the topology in the MSTP scenario, each device is required to trigger the establishment of sub interfaces after discovering VLAN channels. Otherwise, the links discovered through HELLO cannot transmit normal EDP sessions.

Table 13-7 Configure EDP to create sub interface

Step	**Command**	**Description**
Enter the global configuration mode	**configure terminal**	-
Configure EDP work mode	**edp create-subif disable**	Mandatory By default, the function of creating sub interface is disabled.

Configure EDP Weak Check Function

The weak check function is mainly to support the bypass function of the sub interface. The interface is connected to the switch. The IN TAG is different from the OUT TAG. The upstream and downstream are connected through one interface.

Table 13-8 Configure EDP weak check function

Step	**Command**	**Description**
Enter the global configuration mode	**configure terminal**	-
Configure EDP weak check function	**edp packet weak-limit**	Mandatory By default, the EDP weak check function is disabled.

13.2.3. Configure EDPS Function

Configuration Conditions

None

Configure EDPS to Distribute Files

It is initiated by the controller to notify the central node that the configuration file of the target device has been stored locally (downloaded to the specified directory of the central node through FTP) and needs to be distributed to the target device.

Table 13-9 Configure EDPS to distribute files

Step	Command	Description
Configure EDP to distribute files	**edps distribute-config** *center-id target-device-id file-name file-size*	Mandatory By default, the device does not distribute files.

Configure EDPS to Download Files

After the configuration file is successfully distributed, the controller can command the target device to load the configuration.

Table 13-10 Configure EDPS to load files

Step	Command	Description
Configure EDP to load files	**edps load-config** *center-id target-device-id* {**full** | **incremental**}	Mandatory By default, the device does not load files actively.

Configure EDPS to Upload Files

If required by the controller, the target node can be notified to upload the configuration file to the specified directory of the central node for the controller to obtain.

Table 13-11 Configure EDPS to upload files

Step	Command	Description
Configure EDP to upload files	**edps upload-config** *center-id target-device-id* { **init.data** | **running-config | startup | startup-snapshot**}	Mandatory By default, the device does not upload files.

13.2.4. EDP Monitoring and Maintaining

Table 13-12 EDP Monitoring and Maintaining

Command	Description
clear edp device	Clear all device information, taking effect only in the central node
clear edp forward	Clear the forwarding table information
clear edp statistics	Clear the EDP statistics information
clear edp subif	Clear the EDP sub interface information
clear edp topology	Clear the EDP topology information
clear edps statistics	Clear the EDPS statistics information
show edp center [*device-id*]	Display the center node information
show edp config	Display the configuration information of the device
show edp device [*device-id*]	Displays all the collected device information, which is only effective in the central node
show edp forward [*center-id*]	Display the forwarding information
show edp interface *interface-name*	Displays information about the specified interface
show edp statistics	Display the EDP statistics
show edp subif	Display the sub interface information
show edp topology [*center-id*]	Display the EDP topology information
show edps statistics	Display the EDPS statistics information

13.3. EDP Typical Configuration Example

13.3.1. Configure EDP Basic Functions

Network Requirements

- Configure the EDP function on Device1, Device2 and Device3 respectively to realize EDP TOPO discovery.

Network Topology

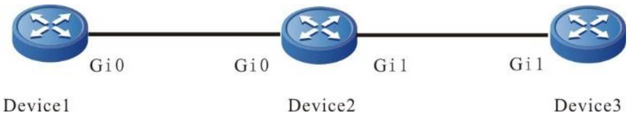


Figure 13-7 Networking of configuring the EDP basic functions

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Enable the EDP function on Device1, Device2 and Device3.

#On Device1, enable the EDP function.

```
Device1#configure terminal
Device1(config)#edp enable
```

#On Device2, enable the EDP function.

```
Device2#configure terminal
Device2(config)#edp enable
```

#On Device3, enable the EDP function.

```
Device3#configure terminal
Device3(config)#edp enable
```

Step 3: On Device1, enable the EDP active mode.

```
Device1#configure terminal
Device1(config)#edp  mode proactive
```

Step 4: Check the result.

#On Device1, view the link information of the whole network.

```
Device1#show edp topology
Flag: U-upstream link, D-downstream link, P-primary link, C-connected link, N-new
link
================================================================================
========================================
CenterId: 001f.ce75.0100(local)
DeviceId          Ifname                PeerDevId        PeerIfname           Hop
LifeTime          Flag
001f.ce75.0100          gigabitethernet0          001f.ce29.0200   gigabitethernet0
   1   2d:03:48:17                         -D-CN
```

```
001f.ce29.0200          gigabitethernet0      001f.ce75.0100  gigabitethernet0
   1    2d:03:48:18           U-P-N
001f.ce29.0200          gigabitethernet1          001f.ce29.0300    gigabitethernet1
   2    2d:03:48:17           -D--N
001f.ce29.0300          gigabitethernet1          001f.ce29.0200    gigabitethernet1
   2    2d:03:48:18                   U-P-N

Total links: 4

Total central devices: 1
```

14. BSM

14.1. Overview

BSM (Business Sensibility Measure) is used to measure the quality of IP network, including delay, jitter and packet loss.

Packet loss rate: the ratio of the number of lost packets to the number of sent packets within a period of time.

Network delay: it refers to the time spent on data packet transmission on the network.

Jitter: also known as delay change, it refers to the change degree of packet delay. It is mainly used to characterize the phenomenon that data packets sent at the same time interval arrive at the receiving end at irregular time intervals.

14.2. BSM Function Configuration

Table 14-1 BSM function configuration list

Configuration Tasks	
Configure BSM basic functions	Configure BSM ID
	Configure BSM sampling
	Configure BSM entity
Configure BSM deterioration	Configure deterioration threshold
	Configure the measurement level of the BSM entity

14.2.1. Configure BSM Basic Functions

Configuration Conditions

Before configuring BSM basic functions, first complete the following tasks:

- Configure the link-layer protocol, ensuring that the link layer communication is normal
- Configure the network-layer address of the interface, making the neighboring network node reachable at the network layer
- Configure NTP clock synchronization

Configure BSM ID

Table 14-2 Configure BSM ID

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure BSM ID	**bsm-id** *ip-address*	Mandatory By default, do not configure BSM id.

Configure BSM Sampling

Table 14-3 Configure BSM sampling

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure BSM only to sample the BFD packets	**bsm bfd-sampling**	Optional By default, BSM samples all packets.

Configure BSM Entity

Table 14-4 Configure BSM entity

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create BSM entity and enter the BSM configuration mode	**bsm** *entity-id*	Mandatory By default, do not create BSM entity.
Enable the management node function of the BSM entity and enter the BSM management node configuration mode	**mgt-node**	Mandatory By default, do not enable the management node function of the BSM entity.

Step	Command	Description
Configure the address of the statistics node	**stat-node** *ip-address*	Mandatory By default, do not configure the address of the statistics node.
Exit the BSM management node configuration mode	**exit**	
Enable the statistics node function of BSM entity and enter the BSM statistics node configuration mode	**stat-node**	Mandatory By default, do not enable the statistics node function of the BSM entity.
Configure the address of the management node	**mgt-node** *ip-address*	Mandatory By default, do not configure the address of the management node.
Configure the measuring period	**period-time** *period*	Optional By default, the measuring period is 10s.
Configure the measuring object	**measure-target ip source-address** *source-ip-address* **destination-address** *destination-ip-address* **protocol** *protocol* **source-port** *source-port* **destination-port** *destination-port* **dscp** *dscp*	Mandatory By default, do not configure the measuring object.
Configure the measuring interface	**measure-interface** *interface-name* {**send | receive**} **role** {**in | out**}	Mandatory By default, do not configure the measuring interface.

14.2.2. Configure BSM Deterioration

Configuration Conditions

Before configuring the BSM basic function, first complete the following task:

- Configure BSM basic functions

Configure Deterioration Threshold

Table 14-5 Configure the deterioration threshold

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the deterioration threshold	**bsm measure-level** {**high | medium | low**} **deteriorate-degree** {**normal | mild**} **threshold** {**delay** *delay-value* **/ jitter** *jitter-value* **/ lossrate** *lossrate-value*}	Optional

Configure Measuring Level of BSM Entity

Table 14-6 Configure measuring level of the BSM entity

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the BSM configuration mode	**bsm** *entity-id*	Mandatory
Enter the configuration mode of the BSM management node	**mgt-node**	Mandatory
Configure the measuring level of the BSM entity	**measure-level** { **high** | **low** | **medium** }	Mandatory By default, do not configure the measuring level of the BSM entity.

14.2.3. BSM Monitoring and Maintaining

Table 14-7 BSM Monitoring and Maintaining

Command	Description
show bsm entity [*entiry-id*]	Display the BSM entity information
show bsm measure [*entiry-id*]	Display the measuring result of the BSM entity
show bsm deteriorate-degree [*entiry-id*]	Display the deterioration of the BSM entity
show bsm deteriorate-degree threshold	Display the deterioration threshold

14.3. BSM Typical Configuration Example

14.3.1. Configure Basic Function of BSM Link Measuring

Network Requirements

- Device1 and Device2 are connected through Ethernet interface. PC1 can communicate with Device2 and PC2 through Device1. Check the line quality between Device1 and Device2.

Network Topology

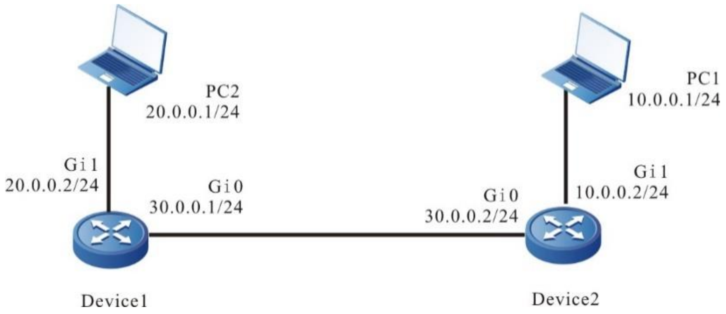


Figure 14-1 Networking of configuring BSM

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure BSM ID.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#bsm-id 30.0.0.1
```

#Configure Device2.

```
Device2#configure terminal
```

```
Device2(config)#bsm-id 30.0.0.2
```

Step 3: Configure the management node.

#Conigure Device2 as a management node, which contains statistical node addresses of 30.0.0.1 and 30.0.0.2, and the measurement level is high

```
Device2(config)#bsm 1
Device2(config-bsm)#mgt-node
Device2(config-bsm-mgt-node)#stat-node 30.0.0.1
Device2(config-bsm-mgt-node)#stat-node 30.0.0.2
Device2(config-bsm-mgt-node)#measure-level high
Device2(config-bsm-mgt-node)#exit
```

Step 4: Configure the statistics node.

#Configure Device1 as a statistics node, which contains a management node address of 30.0.0.2. The measurement cycle is 60s, the measurement interface is Gi0, and the packet source and destination addresses are 10.0.0.1 and 20.0.0.1 respectively.

```
Device1(config)#bsm 1
Device1(config-bsm)#stat-node
Device1(config-bsm-stat-node)#mgt-node 30.0.0.2
Device1(config-bsm-stat-node)#period-time 60
Device1(config-bsm-stat-node)#measure-target ip source-address 10.0.0.1 destination-address 20.0.0.1 protocol 0 source-port 0 destination-port 0 dscp 0
Device1(config-bsm-stat-node)#measure-interface gigabitethernet0 receive role out
Device1(config-bsm-stat-node)#exit
Device1(config-bsm)#exit
```

#Configure Device2 as a statistics node, which contains a management node address of 30.0.0.2. The measurement cycle is 60s, the measurement interface is Gi0, and the packet source and destination addresses are 10.0.0.1 and 20.0.0.1 respectively.

```
Device2(config)#bsm 1
Device2(config-bsm)#stat-node
Device2(config-bsm-stat-node)#mgt-node 30.0.0.2
Device2(config-bsm-stat-node)#period-time 60
Device2(config-bsm-stat-node)#measure-target ip source-address 10.0.0.1 destination-address 20.0.0.1 protocol 0 source-port 0 destination-port 0 dscp 0
Device2(config-bsm-stat-node)#measure-interface gigabitethernet0 send role in
Device2(config-bsm-stat-node)#exit
Device2(config-bsm)#exit
```

Step 5: PC1 and PC2 continuously ping the peer address, and check the result

```
Device2# show bsm measure 1
Entity   No.    Delay(ns)  Jitter(ns) LossRate(%)
1        1     1780500    11888     0
         2     1900600    10444      0
         3     1835050    12333      0
         4     2014150    13666     0
         5     1834500    12666      0
         6     1820500    12111     0
         7     1860300    12333      0
         8     1887700    12111     0
         9     1813100    12000      0
         10    1711900    11888     0
```

It can be seen that the line connected between Device1 and Device2 through Gi0 has started measuring.

Note:

- When configuring the measurement object of the instance statistics node, the source and destination addresses are the source and destination addresses in the packet header respectively.
- The measurement object, measurement period and management node address of the included statistical nodes of the same instance must be the same. The packet direction of the management node must be send and the role must be in. The packet direction of the pure statistics node must be receive and the role must be out.
- The statistics node clock must be consistent.

15. EASY 4G

15.1. Overview

Easy 4G is abbreviated as E4G, including E4G management platform and client. The E4G server is built based on the Linux operating system, and the E4G management platform runs on the E4G server. Through the E4G management platform, the wireless router of the node can be managed: opening service, updating configuration, device upgrading, forced offline, SMS activation, reading of basic information, traffic monitoring, alarm prompt and other functions.

The device can be registered to the E4G server in two ways: automatic registration and manual registration, also known as automatic online and manual online. Automatic online means that the management platform sends the service opening SMS to the device end, and the device will automatically carry out 4G related configuration, update the configuration file and register to the E4G server after receiving the SMS; Manual online refers to registering to E4G server through shell command after configuring E4G related information locally.

15.2. Easy 4G Function Configuration

Table 15-1Easy 4G function configuration

Configuration Task	
Configure E4G basic functions	Configure E4G basic parameters

15.2.1. Configure Easy 4G Basic Functions

Configuration Conditions

Before configuring the basic functions of Easy 4G, first complete the following task:

- Build the E4G server and SMS gateway

Configure Easy 4G Basic Parameters

If the device is registered to the E4G server by manual online mode, relevant parameters need to be configured, mainly including the IP address of the E4G server, the management IP address of the E4G device side and the SMS Gateway number.

Table 15-2 Configure Easy 4G basic parameters

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the IP address of the E4G server	**e4g server-ip** *ip-address*	Mandatory By default, do not configure the IP address of the E4G server.
Configure the management IP address of the E4G device	**e4g manage-ip** *ip-address*	Optional By default, do not configure the management IP address of the E4G device.
Configure the E4G SMS gateway number	**e4g sender-phone-number** *phone-number*	Mandatory By default, do not configure the E4G SMS gateway number.
Configure the source IP of the E4G register and protect packet	**e4g source-ip** *ip-address*	Optional By default, do not configure the source IP address of the E4G packet.

15.2.2. Easy 4G Monitoring and Maintaining

Table 15-3 Easy 4G Monitoring and Maintaining

Command	Description
show e4g platform	Display the relevant information registered to the E4G server on the device side, including the E4G server IP address, E4G device side management IP address, SMS gateway number, etc

15.3. Easy 4G Typical Configuration Example

15.3.1. Configure Easy 4G Typical Application

Network Requirements

- Upgrade and configure Device1 through Easy 4G server.

- The 4G interface fastcellular1/0 of Device1 uses LTE system.
- Device1 is the node device, the operator device is the LAC, and Device2 is the LNS. L2TP is established between LAC and Device2.
- In order to ensure the security of data communication between the networks where Device1 and Device2 are located, Device1 and Device2 establish an IPSec tunnel.
- The Easy 4G server sends and receives short messages through the SMS gateway, which is connected with the Easy 4G server.
- Device2 performs authentication and address allocation through AAA.

Network Topology

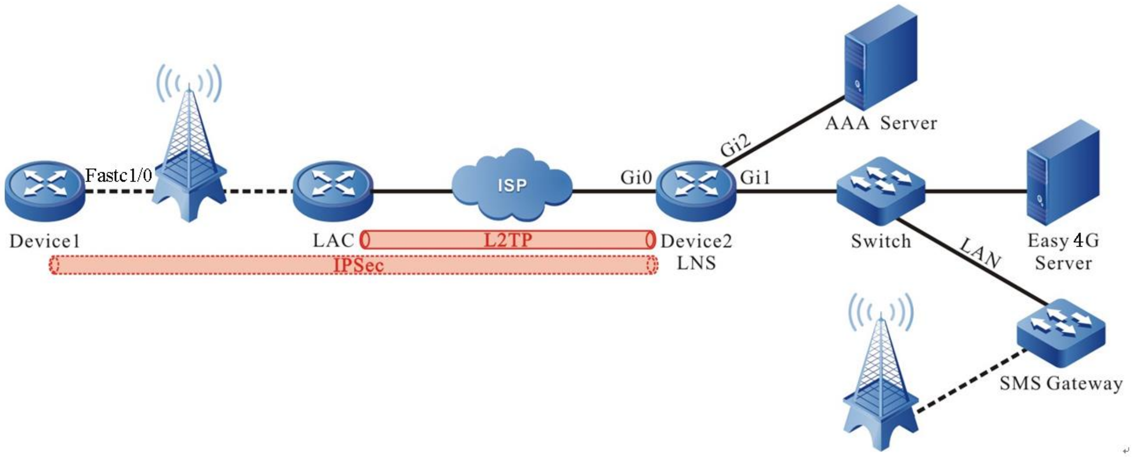


Figure 15-1 Networking of configuring E4G

Table 15-4 Networking of configuring Easy 4G typical application

Device	Interface	IP Address	Device	Interface	IP Address
Device1	Loopback0	192.168.100.1/24	Device2	Gi0	30.1.1.1/24
Easy 4G Server		192.168.201.3/24		Gi1	192.168.201.1/24
AAA		192.168.200.28/24		Gi2	192.168.200.1/24
				Loopback0	100.1.1.1/32

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the 4G private network dialing of Device1.

#Configure Device1, configure the 4G interface fastcellular1/0 as the automatic dialing mode, and automatically obtain the IP address through DHCP.

```
Device1#configure terminal
Device1(config)#interface  fastcellular1/0
Device1(config-if-fastcellular1/0)#dialer config apn cdmptx.sc
Device1(config-if-fastcellular1/0)#dialer config username test@cdmptx.sc
password 0 admin
Device1(config-if-fastcellular1/0)#dialer mode auto
Device1(config-if-fastcellular1/0)#ip address dhcp
Device1(config-if-fastcellular1/0)#exit
```

Step 3: Configure the loopback interface.

#Configure Device1, and create one loopback interface as the E4G management address.

```
Device1(config)#interface loopback0
Device1(config-if-loopback0)#ip address  192.168.100.1 255.255.255.0
Device1(config-if-loopback0)#exit
```

Step 4: Enable the FTP service.

```
Device1(config)# ftp enable
```

Step 5: Configure SNMP v2c proxy server.

Enable the SNMP proxy, and configure the node view name as public and the read-write community as public123

```
Device1(config)#snmp-server start
Device1(config)#snmp-server view public 1.3.6.1 include
Device1(config)#snmp-server community public123 view public rw
```

Note:

- The SNMP community name set on the device must be consistent with the SNMP community name of the E4G server system management office;

Step 6: Configure AAA.

#Configure Device2.

Radius is used for authentication. The authentication list and authorization list are named PPP. Configure the address, authentication port, statistics port and radius server password of radius server.

```
Device2(config)#aaa server group radius ppp
Device2(config-sg-radius-l2tp)# server 192.168.200.28 auth-port 1812 acct-port 1813
key ppp
Device2(config-sg-radius-l2tp)# exit
Device2(config)#domain ppp
Device2(config-isp-l2tpv2)# aaa authentication ppp radius-group ppp
```

```
Device2(config-isp-l2tpv2)# aaa authorization ppp radius-group ppp
Device2(config-isp-l2tpv2)# aaa accounting ppp start-stop radius-group ppp
Device2(config-isp-l2tpv2)# exit
```

Step 7: Configure the L2TP tunnel.

#Configure Device2.

Configure the virtual template virtual-template 1.

```
Device2(config)#interface virtual-template 1
Device2(config-if-virtual-template1)#encapsulation ppp
Device2(config-if-virtual-template1)#ppp mtu adaptive proxy
Device2(config-if-virtual-template1)#ppp authentication chap ppp
Device2(config-if-virtual-template1)#ppp authorization ppp
Device2(config-if-virtual-template1)#ip unnumber loopback0
Device2(config-if-virtual-template1)#exit
```

Enable the VPDN function and configure the VPDN group.

```
Device2(config)#vpdn enable
Device2(config)#vpdn-group 1
Device2(config-vpdn)#accept-dialin
Device2(config-vpdn-acc-in)#protocol l2tp
Device2(config-vpdn-acc-in)#virtual-template 1
Device2(config-vpdn-acc-in)#exit
```

Configure only to accept L2TP connection requests of LAC with hostname GGSNCD01 (optional).

```
Device2(config-vpdn)#terminate-from hostname GGSNCD01
```

Configure L2TP tunnel authentication password, which must be the same as the L2TP password provided by the operator.

```
Device2(config-vpdn)#l2tp tunnel password admin
```

Step 8: Configure IKE, IPSec proposal, pre-shared key and IPSec tunnel. (omitted)

Step 9: Configure IPsec security policy.

#Configure Device1, configure security policy policy1, protect IP communication from network 192.168.100.1/24 to network 192.168.201.3/24, and associate tunnel tun.

```
Device1(config)#crypto policy policy1
Device1(config-policy)#flow 192.168.100.0 255.255.255.0 192.168.201.0 255.255.255.0 ip ipv4-tunnel tun
Device1(config-policy)# set reverse-route
Device1(config-policy)#exit
```

#Configure Device2, configure security policy policy1, protect IP communication from network 192.168.201.3/24 to network 192.168.100.1/24, and associate tunnel tun.

```
Device2(config)#crypto policy policy1
Device2(config-policy)# flow 192.168.201.0 255.255.255.0 192.168.100.0 255.255.255.0 ip ipv4-tunnel tun
Device1(config-policy)# set reverse-route
Device2(config-policy)#exit
```

Step 10: On the Easy 4G server, configure the SIM card number of the online 4G device to bind with the corresponding IMSI number. (omitted)

Step 11: On Device1, configure manual online of Easy 4G.

#Configure Device1. Configure the IP address of the Easy 4G server.

```
Device1(config)#e4g server-ip 192.168.201.3
```

Configure the management address of the device.

```
Device1(config)#e4g manage-ip 192.168.100.1
```

Configure the mobile phone number of the SMS gateway.

```
Device1(config)#e4g sender-phone-number 18600000000
Device1(config)#exit
```

Configure the source IP of the E4G register and protect packet.

```
Device1(config)#e4g source-ip 192.168.100.1
```

#Send the register message command.

```
Device1#smpro register to e4g
```

Step 12: Check the result.

After manual registration is successful, “%SMPRO-4: Register in E4G success!” information will be printed on Device1. The information of the device can be obtained through the E4G server, and the device can be upgraded and configured.

Note:

- IPSec created in the private network environment is mainly used to protect service packets. In the public network environment, two private network addresses can communicate by establishing an IPSec tunnel between the node device and the central device.

- If you want to manage the device through Easy 4G, you should enable the SNMP function on the device. And ensure that the read-write authority is enabled.

16. ОБЩАЯ ИНФОРМАЦИЯ

16.1. Замечания и предложения

Мы всегда стремимся улучшить нашу документацию и помочь вам работать лучше, поэтому мы хотим услышать вас. Мы всегда рады обратной связи, в особенности:

- ошибки в содержании, непонятные или противоречащие места в тексте;
- идеи по улучшению документации, чтобы находить информацию быстрее;
- неработающие ссылки и замечания к навигации по документу.

Если вы хотите написать нам по поводу данного документа, то используйте, пожалуйста, форму обратной связи на qtech.ru.

16.2. Гарантия и сервис

Процедура и необходимые действия по вопросам гарантии описаны на сайте QTECH в разделе «Поддержка» −> «Гарантийное обслуживание».

Ознакомиться с информацией по вопросам тестирования оборудования можно на сайте QTECH в разделе «Поддержка» −> «Взять оборудование на тест».

Вы можете написать напрямую в службу сервиса по электронной почте sc@qtech.ru.

16.3. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться нашей автоматизированной системой запросов технического сервис-центра helpdesk.qtech.ru.

Телефон Технической поддержки +7 (495) 797-33-11 доб. 0