Security

QSR-1920, QSR-2920, QSR-3920

Оглавление

1. CPU PROTECTION

1.1. Overview

Network attack often results in lots of burst packets impacting the network devices. To prevent the control plane from being impacted and ensure the normal running of the upper application, it is necessary to provide one protection policy of the control plane. The CPU protection is the mechanism of providing the protection policy and its work principles mainly include controlling the submitted packets, identifying the type, priority scheduling and speed limiting.

CPP (CPU packet protection) provides a limit queue on the service card to process the packets to be handed over. If the speed limit function of the interface packet is enabled, the packet to be submitted will first be put into the limit queue for caching according to the submission type of the packet, and then dispatched out of the queue according to the task priority. After passing the speed limit of interface protocol, global protocol and limit queue, it will be submitted to the control surface. On the control plane, CPP delivers the packet to the upper application.

1.2. CPU Protection Configuration

Table 1-1 CPU protection configuration list

Configuration task	
Configure the CPP function	Configure the packet submitting
	Configure the packet speed limitation
	Configure the queue the packet enters
	Configure the queue depth and speed limit

1.2.1. Configure CPP Function

Configuration Condition

None

Configure Packet Submitting

Usually, the user does not need to configure the packet submitting, but in some special scenarios, the user can configure the submitting configuration status of various protocol packets, so as to control the packet submitting capability.

- The packet submitting capability should be controlled by the application status and configuration status together. The two kinds of status are also divided to global-class and interface-class. When the interface-class application status of the protocol and configuration status are enabled at the same time, enable the interface-class packet submitting capability of the protocol packet. When the global-class application status of the protocol and configuration status are enabled at the same time, enable the global-class packet submitting capability of the protocol packet, as shown in Figure 2-1.

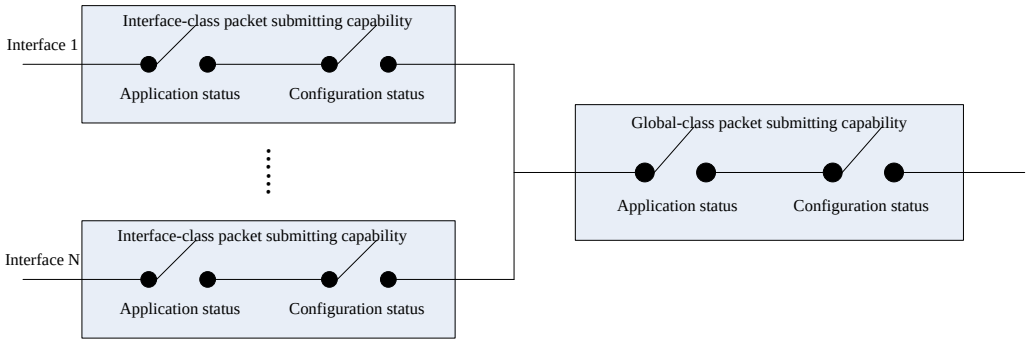


Figure 1-1 Packet submitting capability control

- The application status of the packet submitting capability is set automatically or set by default via the related application protocol, while the configuration status is set via the CPP configuration command.

Table 1-2 Configure the packet submitting

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Set the global configuration status of the submitting capability of the specified protocol packet to enable	**cpu-packet protocol** *type-string* **enable**	Optional
Enter the interface configuration mode	**interface** *interface-name*	-
Set the interface configuration status of the submitting capability of the specified protocol packet to enable	**cpu-packet protocol** { *type-number* | *type-string* } **enable**	Optional

By default, the submitting capability application status and configuration status of the protocol packet are as shown in the following table:

Table 1-3 Default values of the submitting capability application status and configuration status of the protocol packet

Protocol No.	Protocol Name	Global-class packet submitting capability		Interface-class packet submitting capability	
		Application status	Configuration status	Application status	Configuration status
0	misc	true	true	true	true
1	ipv6-misc	true	true	true	true
2	ip-alert	true	true	true	true
3	ucast-rt	true	true	true	true
4	ucast-nd	true	true	true	true
5	not-fastfwd	true	true	true	true
6	ipv4-host-group	true	true	true	true
7	ipv4-router-group	true	true	true	true
8	subnet-bcast	true	true	true	true
9	net-bcast	true	true	true	true
10	ipv6-mcast-resv	true	true	true	true

Protocol No.	Protocol Name	Global-class packet submitting capability		Interface-class packet submitting capability	
		Application status	Configuration status	Application status	Configuration status
11	ipv6-host-router-group	true	true	true	true
12	user-define	true	true	true	true
13	martian	false	true	false	true
14	mpls	false	true	false	true
15	tcap	true	true	true	true
16	ipv6-mcast-request	true	true	true	true
17	arp	true	true	true	true
18	dhcp	false	true	false	true
19	radius	false	true	false	true
20	mcast-data	false	true	false	true
21	mcast6-data	false	true	false	true
22	interface-packet	true	true	true	true
23	ipv6-interface-packet	true	true	true	true

Protocol No.	Protocol Name	Global-class packet submitting capability		Interface-class packet submitting capability	
		Application status	Configuration status	Application status	Configuration status
24	ipv6-nd-protocol	true	true	true	true
25	gre-packet	true	true	true	true
26	interface-icmp	true	true	true	true
27	pim	false	true	false	true
28	pim6	false	true	false	true
29	service-low	true	true	true	true
30	pv6-mcast-mld	true	true	true	true
31	ospf-v2	false	true	false	true
32	ospf-v3	false	true	false	true
33	rip-v1v2	false	true	false	true
34	rip-ng	false	true	false	true
35	irmp	false	true	false	true
36	bgp	false	true	false	true

Protocol No.	Protocol Name	Global-class packet submitting capability		Interface-class packet submitting capability	
		Application status	Configuration status	Application status	Configuration status
37	isis	false	true	false	true
38	ldp	false	true	false	true
39	rsvp	false	true	false	true
40	service-high	true	true	true	true
41	ipv4-ping	true	true	true	true
42	ipv6-ping	true	true	true	true
43	igmp-dvmrp	false	true	false	true
44	vrrp	false	true	false	true
45	vbrp	false	true	false	true
46	vrrpv3	false	true	false	true
47	telnet	true	true	true	true
48	l2tp	true	true	true	true
49	ike	true	true	true	true
50	link-ctrl	true	true	true	true

Protocol No.	Protocol Name	Global-class packet submitting capability		Interface-class packet submitting capability	
		Application status	Configuration status	Application status	Configuration status
51	mpls-oam	false	true	false	true
52	mvpn	false	true	false	true
53	netconf	true	true	true	true
54	manage	true	true	true	true
55	edp	true	true	true	true
56	dlsw	false	true	false	true
57	sdlc	false	true	false	true
58	bsm	false	true	false	true

Configure Packet Speed Limitation

Usually, the default limit speeds of the protocol packets meet the application demands, and do not need to be configured, but in some special scenarios, the user can configure the speed limit of the protocol packet via the command. The unit of the limited speed of the packet is pps.

CPP totally has three classes of speed limit processing:

- Interface protocol speed limit
- Global protocol speed limit
- Limit queue speed limit

Table 1-4 Configure the packet speed limit

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the limit speed of the limit queue	**cpu-packet queue** *limit-queue-id* **rx-limit** *limit-rate-value*	Optional
Configure the limit speed of the global protocol	**cpu-packet protocol** *type-string* **rx-limit** *limit-rate-value*	Optional
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the limit speed of the interface protocol	**cpu-packet protocol** { *type-number* | *type-string* } **rx-limit** *limit-rate-value*	Optional

By default, the interface limit speed and global limit speed of the protocol packet are as shown in the following table:

Table 1-5 Default values of the interface protocol limit speed and global protocol limit speed

Protocol No.	Protocol Name	Default Value of Interface Protocol Limit Speed	Default Value of Global Protocol Limit Speed
0	misc	210	300
1	ipv6-misc	210	300
2	ip-alert	1260	1800
3	ucast-rt	210	300
4	ucast-nd	210	300
5	not-fastfwd	210	300
6	ipv4-host-group	210	300
7	ipv4-router-group	210	300
8	subnet-bcast	210	300
9	net-bcast	210	300
10	ipv6-mcast-resv	210	300
11	ipv6-host-router-group	210	300
12	user-define	210	300
13	martian	1260	1800
14	mpls	1260	1800

Protocol No.	Protocol Name	Default Value of Interface Protocol Limit Speed	Default Value of Global Protocol Limit Speed
15	tcap	1260	1800
16	ipv6-mcast-request	420	600
17	arp	420	600
18	dhcp	280	400
19	radius	280	400
20	mcast-data	280	400
21	mcast6-data	280	400
22	interface-packet	1260	1800
23	ipv6-interface-packet	1260	1800
24	ipv6-nd-protocol	1400	2000
25	gre-packet	210	300
26	interface-icmp	1260	1800
27	pim	1050	1500
28	pim6	700	1000
29	service-low	350	500

Protocol No.	Protocol Name	Default Value of Interface Protocol Limit Speed	Default Value of Global Protocol Limit Speed
30	ipv6-mcast-mld	210	300
31	ospf-v2	1050	1500
32	ospf-v3	1050	1500
33	rip-v1v2	700	1000
34	rip-ng	700	1000
35	irmp	700	1000
36	bgp	700	1000
37	isis	700	1000
38	ldp	700	1000
39	rsvp	560	800
40	service-high	840	1200
41	ipv4-ping	1260	1800
42	ipv6-ping	1260	1800
43	igmp-dvmrp	1050	1500
44	vrrp	280	400

Protocol No.	Protocol Name	Default Value of Interface Protocol Limit Speed	Default Value of Global Protocol Limit Speed
45	vbrp	280	400
46	vrrpv3	280	400
47	telnet	280	400
48	l2tp	7000	10000
49	ike	7000	10000
50	link-ctrl	840	1200
51	mpls-oam	1260	1800
52	mvpn	700	1000
53	netconf	700	1000
54	manage	7000	10000
55	edp	2450	3500
56	dlsw	280	400
57	sdlc	490	700
58	bsm	4060	5800

By default, the limit speeds of the limit queues are shown in the following table:

Table 1-6 Default limit speed value of the limit queue

Limit queue No.	Default limit speed of limit queue
0	2000
1	300
2	2000
3	2000
4	2000
5	2000
6	1200
7	300
8	2000
9	2000
10	2000
11	5000

Note:

- When the limit speed is configured as 0, it has the same effect as disabling the packet submitting capability.
- “Global protocol speed limit” is for the whole device. For example, configure the global protocol limit speed as 100pps, that is, the total limit speed of all service cards is 100pps.

Configure the Queue the Packet Enters

Usually, the default entering queue of the packet can meet the application demand, and do not need to configure, but in some special scenarios, the user can configure the packet to enter the specified limit queue via the command.

Table 1-7 Configure the queue that the packet enters

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the specified protocol packet to enter the specified limit queue	**cpu-packet protocol** *type-string* **queue** *limit-queue-id*	Optional

By default, the entering limit queue of the protocol packet is shown in the following table:

Table 1-8 The default entering limit queue of the protocol packet

Protocol No.	Protocol Name	limit Queue No.
0	misc	0
1	ipv6-misc	0
2	ip-alert	0
3	ucast-rt	0
4	ucast-nd	0
5	not-fastfwd	0
6	ipv4-host-group	0
7	ipv4-router-group	0
8	subnet-bcast	0

Protocol No.	Protocol Name	limit Queue No.
9	net-bcast	0
10	ipv6-mcast-resv	0
11	ipv6-host-router-group	0
12	user-define	0
13	martian	0
14	mpls	0
15	tcap	0
16	ipv6-mcast-request	2
17	arp	2
18	dhcp	2
19	radius	2
20	mcast-data	2
21	mcast6-data	2
22	interface-packet	2
23	ipv6-interface-packet	2
24	ipv6-nd-protocol	2

Protocol No.	Protocol Name	limit Queue No.
25	gre-packet	3
26	interface-icmp	3
27	pim	3
28	pim6	3
29	service-low	3
30	pv6-mcast-mld	3
31	ospf-v2	4
32	ospf-v3	4
33	rip-v1v2	4
34	rip-ng	4
35	irmp	4
36	bgp	4
37	isis	4
38	ldp	4
39	rsvp	4
40	service-high	4

Protocol No.	Protocol Name	limit Queue No.
41	ipv4-ping	3
42	ipv6-ping	3
43	igmp-dvmrp	5
44	vrrp	5
45	vbrp	5
46	vrrpv3	5
47	telnet	5
48	l2tp	8
49	ike	9
50	link-ctrl	6
51	mpls-oam	3
52	mvpn	3
53	netconf	5
54	manage	8
55	edp	10
56	dlsw	7

Protocol No.	Protocol Name	limit Queue No.
57	sdlc	3
58	bsm	11

Configure Queue Length

The queue length is the maximum number of the packets permitted to enter the queue. Usually, the default length of the queue meets the application demand and do not need to be configured, but in some special scenarios, the user can configure the length of the limit queue via the command.

Table 1-9 Configure the queue length and scheduling weight

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the length of the specified limit queue	**cpu-packet queue** *limit-queue-id* **length** *length-value*	Optional

By default, the length and scheduling weight of the limit queue are shown in the following table:

Table 1-10 The default value of the limit queue length and scheduling weight

limit Queue No.	Length
0	500
1	500
2	700
3	2048

limit Queue No.	Length
4	2048
5	2048
6	500
7	500
8	2048
9	2048
10	2048
11	2048

1.2.2. CPU Protection Monitoring and Maintaining

Table 1-11 CPU protection monitoring and maintaining

Command	Description
show cpu-packet trap-class-description	Display the submit type description information
show cpu-packet protocol-description	Display the protocol description and application receiving register information
show cpu-packet config **interface** *interface-name* [**protocol** { *type-number* | *type-string* }]	Display the protocol parameter information of the specified interface

Command	Description
show cpu-packet config **limit-queue** [*limit-queue-id*]	Display the parameter information of the limit queue
show cpu-packet config **protocol** [*type-number* | *type-string*]	Display the global parameter information of the protocol
show cpu-packet statistics deliver [**protocol** *type-number*]	Display the protocol packet statistics information
show cpu-packet statistics limit [**protocol** *type-number*]	Display the queue statistics information of the protocol packet
show cpu-packet debug on-off	Display the CPP debugging status
show cpu-packet debug parameter	Display the CPP packet debugging parameters

2. PORT SECURITY

2.1. Overview

2.1.1. Overview of Port Security

Port security is the security mechanism of controlling the devices connected to the network. It is applied to the access layer and can limit the hosts of using the device port, permitting some specified hosts to access the network, while the other hosts cannot access the network.

The port security function can bind the user MAC address, IP address, IPv6 address, VLAN ID and port number, preventing the invalid user from accessing the network, so as to ensure the security of the network data and the valid user can get the enough bandwidth.

2.1.2. Port Security Rule

The port security rule is divided to four kinds:

MAC rule: Control whether the host can communicate according to the MAC address of the host. The binding mode of the MAC rule contains MAC binding, MAC+VLAN binding, MAC+IP binding, and MAC+IPv6 binding.

IP rule: Control whether the host can communicate according to the IP address of the host. The IP rule can be for the binding of a single IP address and also can be for the binding of the IP address segment.

IPv6 rules: It mainly controls whether the host can communicate according to the IPv6 address of the host. IPv6 rules can be bound for a single IPv6 address or for an IPv6 address segment;

MAX rule: Limit the number of the MAC addresses that can be learned by the port freely to control the host communication. The number of the MAC address entries does not contain the valid MAC address entries generated by the MAC rule, IP rule, and IPv6 rule.

STICKY rule: Control whether the host can communicate according to the MAC address of the host. The binding mode of the STICKY rule contains the MAC binding, MAC+VLAN binding, MAC+IP binding and MAC+IPv6 binding. The STICKY rule can automatically learn and also can configure manually, and is saved in the running configuration. If saving the running configuration before the device restarts, do not need to configure again after the device restarts and the STICKY rule automatically takes effect. When enabling the STICKY function in the port and the STICKY learn node is MAC mode, convert the dynamic MAC entry learned by the MAX rule to the STICKY rule and save in the running configuration.

2.1.3. Work Principle of Port Security

If only enabling the port security, the port security drops all packets received on the port. The rules of the port security rely on the ARP packets and IP packets of the device to trigger. When the device receives the ARP packet and IP packet, the port security extracts various packet information and matches with the configured rule. The matching order is first match the MAC rule, secondly match the STICKY rule, then match the IP rule and at last match the MAX rule, and control the L2 forwarding table of the port according to the matching result, so as to control the forwarding action of the port for the packet. The valid packet matching the MAX rule or STICKY rule is forwarded. For the packet matching the MAC rule or IP rule, if the action of the rule for the packet is permit, the packet belongs to the valid packet and is forwarded. Otherwise, the packet is invalid and dropped.

The action is the permitted MAC rule and IP rule. After taking effect, write the MAC address of the rule to the L2 forwarding table so that the L2 forwarding can be performed for the packets

matching the rule. If the action is the refused Mac rule and IP rule, the corresponding MAC is not written to the L2 forwarding table and the packet needs to be dropped via the port security.

After MAC rule and STICKY rule take effect, write to the MAC address entries to form the effective entries, making the packet perform the L2 forwarding. The processing flow of the IPv6 packet is the same as this.

2.2. Port Security Function Configuration

Table 2-1 Basic function configuration list of the port security

Configuration Task	
Configure the basic functions of the port security	Enable the port security function
Configure the port security rule	Configure the MAC rule
	Configure the IP rule
	Configure the IPv6 rule
	Configure the MAX rule
	Configure the STICKY rule
Configure the STICKY rule learn mode	Configure the STICKY rule learn mode
Configure the aging function of the static MAC address	Enable the aging function of the static MAC address
	Configure the age time of the static MAC address
Configure the processing mode when receiving the invalid packet	Configure the processing mode when receiving the invalid packet
Configure the interval of sending the log when receiving the invalid packet	Configure the interval of sending the log when receiving the invalid packet

2.2.1. Configure Basic Functions of Port Security

In the configuration tasks of the port security, you should first enable the port security so that the configuration of the other functions can take effect.

Configuration Condition

None

Enable Port Security Function

After enabling the port security and if not configuring any port security rule, the port cannot learn the MAC address.

Table 2-2 Configure the basic functions of the port security

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the port security function	**port-security enable**	Mandatory By default, the port security function is not enabled.

Note:

- The port security and 802.1x function cannot be used on one port at the same time.
- The port security and DAI (Dynamic ARP Inspection) cannot be used on one port at the same time.

2.2.2. Configure Port Security Rule

Configuration Condition

Before configuring the port security rule, first complete the following task:

- Enable the port security function

Configure MAC Rule

If hoping to control whether the terminal can communicate via the MAC address, the user can adopt the MAC rule. The permit packet can be forwarded and the refuse packet is dropped.

Table 2-3 Configure the MAC rule

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the MAC rule whose action is permit	**port-security permit mac-address** *mac-address-value* [**desc** *security-rule-description* **| ip-address** *ip-address-value* [**desc** *security-rule-description*] | **ipv6-address** *ipv6-address-value* [**desc** *security-rule-description*] **| vlan-id** *vlan-id* [**desc** *security-rule-description*]]	Either By default, the MAC rule is not configured in the port.

Step	Command	Description
Configure the action as the refused MAC rule	**port-security deny mac-address** *mac-address-value* [**ip-address** *ip-address-value*| **ipv6-address** *ipv6-address-value* **| vlan-id** *vlan-id*]	

Configure IP Rule

If hoping to control whether the terminal can communicate via the IP address, the user can use the IP rule and the packets whose matching action is the permit rule can be forwarded. The packets whose matching action is the refuse rule are dropped.

Table 2-4 Configure the IP rule

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Configure the IP rule whose action is permit	**port-security permit ip-address** *ip-address-value* [**to** *ip-address-value*]	Either By default, the IP rule is not configured in the port.
Configure the IP rule whose action is refuse	**port-security deny ip-address** *ip-address-value* [**to** *ip-address-value*]	

Note:

- The port security serves as the role of the security access on the data link layer. For the supported MAC+IP, IP and other rules related to the IP, once the corresponding effective entry is generated, the subsequent packet can be forwarded as long as matching the generated MAC+VLAN entry, and do not check the IP address.

Configure IPv6 Rule

If hoping to control whether the terminal can communicate via the IPv6 address, the user can use the IPv6 rule and the packets whose matching action is the permit rule can be forwarded. The packets whose matching action is the refuse rule are dropped.

Table 2-5 Configure the IPv6 rule

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Configure the IPv6 rule whose action is permit	**port-security permit ipv6-address** *ipv6-address-value* [**to** *ipv6-address-value*]	Either By default, the IPv6 rule is not configured in the port.
Configure the IPv6 rule whose action is refuse	**port-security deny ipv6-address** *ipv6-address-value* [**to** *ipv6-address-value*]	

Note:

- The port security serves as the role of the security access on the data link layer. For the supported MAC+IPv6, IPv6 and other rules related to the IPv6, once the corresponding effective entry is generated, the subsequent packet can be forwarded as long as matching the generated MAC+VLAN entry, and do not check the IPv6 address.

Configure MAX Rule

In the port enabled with the port security function, if hoping that the connected terminal not matching the MAC rule or IP rule also can communicate, the user can configure the MAX rule, the rule limits the number of the permitted access terminals.

Table 2-5 Configure the MAX rule

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Configure the MAX rule	**port-security maximum** *maximum-number*	Mandatory By default, the number of the MAC addresses permitted to be learned by the MAX rule is 0.

Note:

- The number of the dynamic addresses actually learned by the MAX rule is limited by the port, VLAN and the number of the system MAC addresses.

Configure STICKY Rule

If hoping that the MAC address and the VLAN information of the terminal permitted by the MAX rule can be saved in the configuration, the user can enable the STICKY function on the device so that the entries learned by the device via the MAX rule can be converted to the STICKY rule. After converting, the user can adjust the MAX rule quantity via the number of the current STICKY rules so that only the terminals matching the STICKY rule can communicate. In this way, the device can automatically learn the MAC address of the access terminal, convert to the STICKY rule, and save in the configuration, avoiding the operation of configuring the MAC rule manually.

Table 2-7 Configure the STICKY rule

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Configure the MAX rule	**port-security maximum** *maximum-number*	Mandatory By default, the number of the dynamic MAC addresses permitted to be learned by the MAX rule is 0. The STICKY rule can be configured only after configuring the number of the MAX rules.
Enable the STICKY function	**port-security permit mac-address sticky**	Mandatory By default, the STICKY function is disabled. The STICKY rule can be configured only after enabling the STICKY function.
Configure the STICKY rule	**port-security permit mac-address sticky** [*mac-address-value* [**desc** *security-rule-description* | **vlan-id** *vlan-id* [**desc** *security-rule-description*] **ip-address** *ip-address-value* [**desc** *security-rule-description*] | **ipv6-address** *ipv6-address-value* [**desc** *security-rule-description*]]]	Mandatory By default, the STICKY rule is not configured in the port.

Configure VOICE VLAN Rule

Under the port that enables the port security function, if the user wants to access the terminal that does not match the MAC rules and IP rules, VOICE-VLAN packets can also communicate, and does not want to be limited by the number of Max rule addresses, voice VLAN rules can be configured, which will allow all packets of OUI configured for VOICE-VLAN to pass through.

Table 2-6 Configure the VOICE VLAN rule

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

Step	Command	Description
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**interface link-aggregation** *link-aggregation-id*	
Configure the VOICE VLAN rule	**port-security permit voice vlan**	Mandatory By default, the VOICE VLAN rule is not configured in the port.

Note:

- The source MAC allowed by the voice VLAN rule is the OUI configured by the source VOICE-VLAN.
- After the max rule is enabled, the voice VLAN rule does not take effect.

2.2.3. Configure STICKY Rule Learning Mode

Configuration Condition

Before configuring the STICKY rule learning mode, first complete the following task:

- Enable the port security function

Configure STICKY Rule Learning Mode

If hoping to perform the STICKY learning by MAC or MAC+VLAN, the user can configure the STICKY rule learning mode to MAC mode. If hoping to perform the STOCKY rule learning by MAC+IP, the user can configure the STICKY rule learning mode to MAC+IP mode.

Table 2-7 Configure the STICKY rule learning mode

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**interface link-aggregation** *link-aggregation-id*	
Configure the STICKY rule learning mode	**port-security permit mac-address sticky mode** { **mac** | **mac-ip** }	Mandatory By default, the STICKY rule learning mode is MAC mode.

2.2.4. Configure Aging Function of Static MAC Address

Configuration Condition

Before configuring the aging function of the static MAC address, first complete the following task:

- Enable the port security function

Enable Aging Function of Static MAC Address

To detect whether the terminal of the effective entry of the MAC rule or IP rule is online, the user can enable the aging function of the static MAC address. After the aging function of the static MAC address and if it is detected that the terminal is offline, the effective entry of the terminal is deleted so that the chip resources can be released.

Table 2-8 Enable the aging function of the static MAC address

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**interface link-aggregation** *link-aggregation-id*	
Enable the aging function of the static MAC address	**port-security aging static**	Mandatory By default, the aging function of the static MAC address is disabled.

Configure Age Time of Static MAC Address

The user can configure the reasonable age time according to the actual network environment configuration. In the general application, just keep the default value.

Table 2-11 Configure the age time of the static MAC address

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**interface link-aggregation** *link-aggregation-id*	
Configure the age time of the static MAC address	**port-security aging time** *time-value*	Mandatory By default, the age time of the static MAC address is 1 minute.

2.2.5. Configure Processing Mode when Receiving Invalid Packet

Configuration Condition

Before configuring the processing mode when receiving the invalid packet, first complete the following task:

- Enable the port security function

Configure Processing Mode when Receiving Invalid Packet

The port security provides three kinds of processing modes for the invalid packet, that is, protect, restrict and shutdown. The user can select according to the security requirement. The specific functions of the three processing modes are as follows:

- **protect**: After receiving the invalid packet, drop the packet.
- **restrict**: After receiving the invalid packet, drop the packet and trap the information to the NMS.
- **shutdown**: After receiving the invalid packet, drop the packet, disable the port receiving the packet and trap the information to the NMS.

Table 2-9 Configure the processing mode when receiving the invalid packet

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**interface link-aggregation** *link-aggregation-id*	
Configure the processing mode of the invalid packet	**port-security violation** { **protect** | **restrict** | **shutdown** }	Mandatory By default, the processing mode when the port security receives the invalid packet is protect.

2.2.6. Configure the Interval of Sending the Log When Receiving Invalid Packet

Configuration Condition

Before configuring the interval of sending the log when receiving the invalid packet, first complete the following task:

- Enable the interface security function.

Configure the Interval of Sending the Log When Receiving Invalid Packet

The user can configure the interval of sending the log based on the actually received invalid packet. In the general application, just reserve the default value.

Table 2-10 Configure the interval of sending the log when receiving the invalid packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the interval of sending the log when receiving the invalid packet	**port-security violation log-interval** *log-interval-value*	Mandatory By default, the interval of sending the log when the interface receives the invalid packet securely is 5s.

2.2.7. Monitoring and Maintaining of Port Security

Table 2-14 Monitoring and maintaining of the port security

Command	Description
clear port-security statistics	Clear the statistics information of the sent and received packets
show port-security	Display the summary information of the port configured with the port security
show port-security ip-address	Display the configured IP rule
show port-security ipv6-address	Display the configured IPv6 rule
show port-security mac-address	Display the configured MAC rule and STICKY rule
show port-security active-address	Display the information of all effective entries
show port-security detect-mac	Display the current detected new MAC entry
show port-security violation log-interval	Display the period of printing the log when detecting the invalid MAC entry

Command	Description
show port-security violation-mac	Display the detected invalid MAC entry
show port-security statistics	Display the statistics information of the received and sent packets

2.3. Typical Configuration Example of Port Security

2.3.1. Configure MAC and IP Rule of Port Security

Network Requirements

- PC1, PC2 and the network printer are connected to the server via Device.
- Configure the port security function on Device, permitting PC1 to pass and refusing PC2 to pass; permit the network printer to execute the printing tasks delivered by the server and PC1 user.

Network Topology

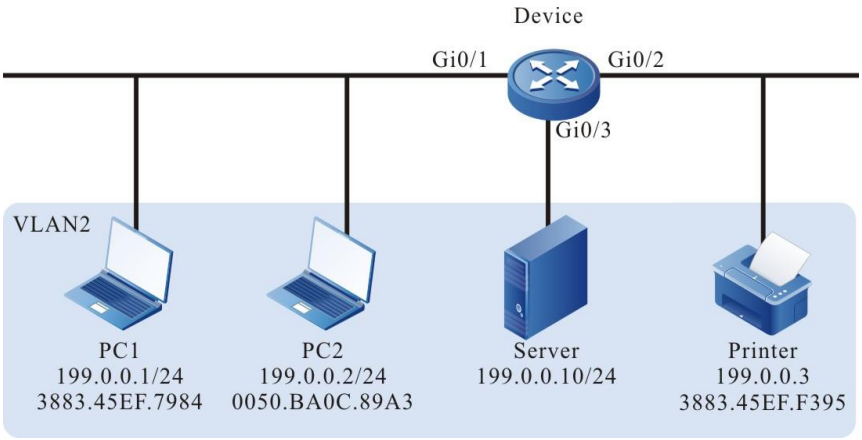


Figure 2–1 Networking of configuring port security MAC and IP rule

Configuration Steps

Step 1: Configure VLAN.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the port link type on gigabitethernet0/1-gigabitethernet0/3 of Device as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/3
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure the port security function.

#Configure the MAC+IP rule on gigabitethernet0/1 of Device, permitting PC1 to pass; configure the IP rule, refusing PC2 to pass.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#port-security enable
Device(config-if-gigabitethernet0/1)#port-security permit mac-address 3883.45ef.7984 ip-address 199.0.0.1
Device(config-if-gigabitethernet0/1)#port-security deny ip-address 199.0.0.2
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the MAC rule on gigabitethernet0/2 of Device, permitting the network printer to access the network.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#port-security enable
Device(config-if-gigabitethernet0/2)#port-security permit mac-address 3883.45ef.f395
Device(config-if-gigabitethernet0/2)#exit
```

Step 3: Check the result.

#View the effective entries of the port security on Device. The user can see that the MACs of PC1 and the network printer are written to the effective entries of the port security.

```
Device#show port-security active-address
-------------------------------------------------------------------------------
------------
Entry Interface        MAC address     VID  IP Addr      Derivation    Age(Sec)
-------------------------------------------------------------------------------
------------
1    gi0/1          38:83:45:EF:79:84 2    199.0.0.1     MAC+IP          0
2    gi0/2          38:83:45:EF:F3:95 2    199.0.0.3       MAC           0
```

#With the detection, we can see that PC1 can access the server and the network printer can execute the printing task delivered by PC1 and the server.

#With the detection, we can see that PC2 cannot ping the server or the network printer.

2.3.2. Configure MAC Rule of Port Security

Network Requirements

- PC1, PC2, and PC3 are connected to the server via Device; PC and the server are in the same LAN.
- Configure the port security rule on Device, permitting PC1 and PC2 to access the server and refusing PC3 to access the server.

Network Topology

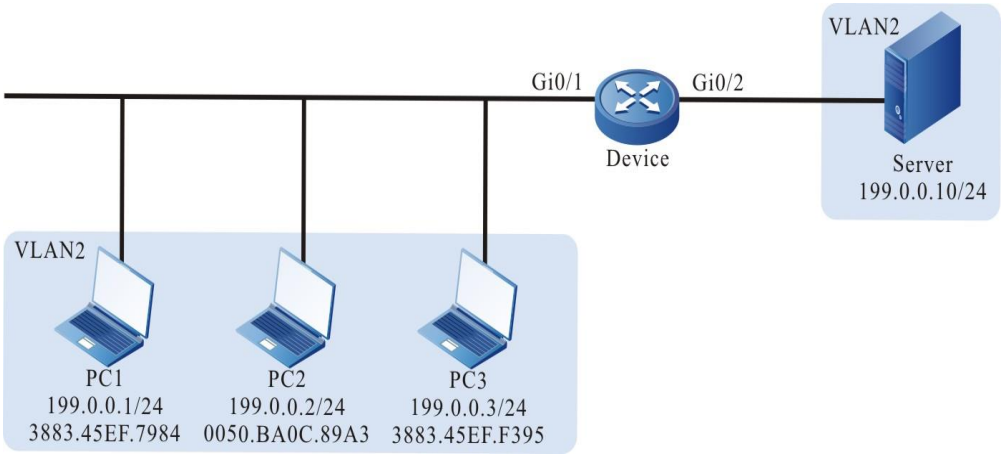


Figure 2–2 Networking of configuring the MAX rule of the port security

Configuration Steps

Step 1: Configure VLAN.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the port link type on gigabitethernet0/1-gigabitethernet0/2 of Device as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure the port security rule on Device.

#Configure the MAX rule on gigabitethernet0/1 of Device. The maximum number of the MAC rules is 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#port-security enable
Device(config-if-gigabitethernet0/1)#port-security maximum 2
Device(config-if-gigabitethernet0/1)exit
```

Step 3: Check the result.

PC1 and PC2 first communicate with the server, and both of them can access the serve normally. PC3 cannot access the server again. View the effective entries of the port security on

gigabitethernet0/1 of Device and you can see that the MAC addresses of PC1 and PC2 are written to the effective entries of the port security.

```
Device#show port-security active-address
-------------------------------------------------------------------------------
------------
Entry Interface        MAC address     VID  IP Addr       Derivation     Age(Sec)
-------------------------------------------------------------------------------
------------
1    gi0/1          00:50:ba:0c:89:a3 2    ---          FREE           0
2    gi0/1          38:83:45:EF:79:84 2    ---          FREE           0
Total Mac Addresses for this criterion: 2
```

2.3.3. Configure STICKY Rule of Port Security

Network Requirements

- PC1, PC2 and PC3 are connected to the server via Device; they are in the same LAN as the server.
- Configure the port security rule on Device, permitting two PCs to pass.
- After saving the configuration and restarting Device, the STICKY rule can take effect at once.

Network Topology

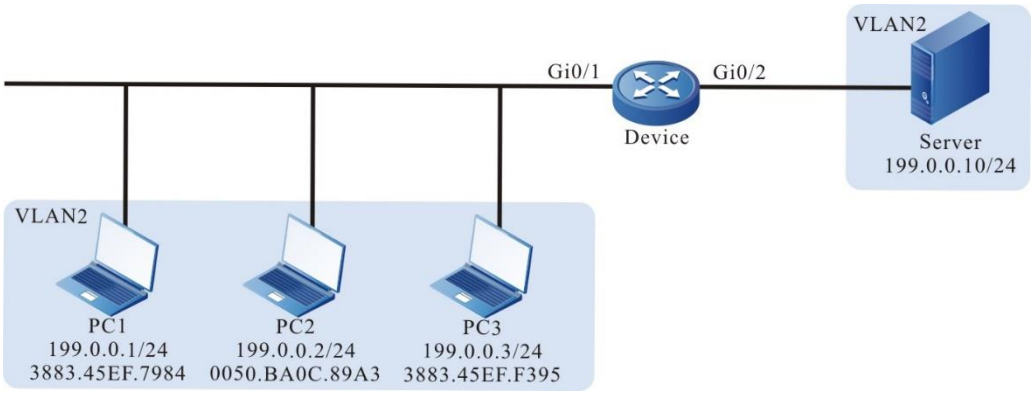


Figure 2–3 Networking of configuring the STICKY rule of the port security

Configuration Steps

Step 1: Configure VLAN.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the port link type on gigabitethernet0/1-gigabitethernet0/2 of Device as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
```

```
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure the MAX rule of the port security on Device.

#Configure the MAX rule on gigabitethernet0/1 of Device. The maximum number of the MAX rules is 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#port-security enable
Device(config-if-gigabitethernet0/1)#port-security maximum 2
Device(config-if-gigabitethernet0/1)exit
```

Step 3: Configure the STICKY rule of the port security on Device.

#Enable the STICKY function on gigabitethernet0/1 of Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#port-security permit mac-address sticky
Device(config-if-gigabitethernet0/1)#exit
```

Step 4: Check the result.

#PC1, PC2 and PC3 try to communicate with the server. View the effective entries of the port security on gigabitethernet0/1 of Device and you can see that the rule type on gigabitethernet0/1 is STICKY.

```
Device#show port-security active-address
------------------------------------------------------------------------
------------
Entry Interface        MAC address     VID  IP Addr       Derivation      Age(Sec)
------------------------------------------------------------------------
------------
1    gi0/1             38:83:45:EF:79:84 2    199.0.0.1       STICKY          0
2    gi0/1             38:83:45:EF:F3:95 2    199.0.0.3       STICKY          0
Total Mac Addresses for this criterion: 2
```

#After saving the configuration and restarting the device, the STICKY rule exists and takes effect.

```
Device#show port-security active-address
------------------------------------------------------------------------
------------
Entry Interface        MAC address     VID  IP Addr       Derivation      Age(Sec)
------------------------------------------------------------------------
------------
```

```
1    gi0/1          38:83:45:EF:79:84 2    199.0.0.1       STICKY          0
2    gi0/1          38:83:45:EF:F3:95 2    199.0.0.3       STICKY          0
Total Mac Addresses for this criterion: 2
```

3. IP SOURCE GUARD

3.1. Overview

The IP Source Guard function is one packet filter function and can filter and control the packets forwarded by the port, preventing the invalid packets from passing the port and improving the port security. The function can be divided to two kinds:

1. The port IP Source Guard function filters the IP packets received by the specified port. The filter mode includes IP+VLAN and IP+MAC+VLAN. The specific processing modes are as follows:

- IP+VLAN mode: If the source IP address and VLAN ID in the packet are the same as the IP address and VLAN ID recorded in the bound entries, the port forwards the packet. Otherwise, drop it.
- IP+MAC+VLAN mode: If the source IP address, source MAC address, and VLAN ID in the packet are the same as the IP address, MAC address and VLAN ID recorded in the bound entries, the port forwards the packet. Otherwise, drop the packet.
- The setting of filter type is only effective for dynamically bound table entries, and has no effect on statically bound table items.

The bound entries of the port IP Source Guard include two kinds:

- Static bound entries, manual configured port IP Source Guard static bound entries
- Dynamic bound entries, dynamically generated by the valid entries of the DHCP Snooping function.

2. Global IP Source Guard function filters the packets received by all ports, including ARP and IP packets. The specific filter modes are as follows:

- If the source IP address in the IP packet is the same as the IP address in the global IP Source Guard bound entries, but the source MAC address is different, drop the packet.
- If the sending IP address in the ARP packet is the same as the IP address in the bound entries, but the source MAC address is different, drop the packet.

3.2. IP Source Guard Function Configuration

Table 3-1 The configuration list of the IP Source Guard function

Configuration Task	
Configure the static bound entries of the port IP Source Guard	Configure the static bound entries of the port IP Source Guard
Configure the port IP Source Guard function	Configure the port IP Source Guard function
Configure the global IP Source Guard function	Configure the global IP Source Guard function

3.2.1. Configure Static Bound Entries of Port IP Source Guard

Configuration Condition

Before configuring the static bound entries of the port IP Source Guard, first complete the following task:

- Enable the port IP Source Guard function or enable the port Dynamic ARP Inspection function

Configure Static Bound Entries of Port IP Source Guard

The static bound entries of the port IP Source Guard are the basis of filtering the IP packets received by the specified port.

When the port Dynamic ARP Inspection function is enabled, the static bound entries of the port IP Source Guard are the basis of the validity detection for the ARP packets.

Table 3-2 Configure the static bound entries of the port IP Source Guard

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the static bound entries of the port IP Source Guard	**ip source binding** *mac-address* **vlan** *vlan-id ip-address*	Mandatory By default, there is no static bound entry of the port IP Source Guard.

Note:

- For the port Dynamic ARP Inspection function, refer to the Dynamic ARP Inspection chapter of the configuration manual.

3.2.2. Configure Port IP Source Guard Function

Configuration Condition

None

Configure Port IP Source Guard Function

After enabling the port IP Source Guard function, first write the port bound entry to the chip, including the static bound entry and dynamic bound entry. The static bound entry is first written. And then perform the security control for the IP packets received by the port according to the entries written to the chip, improving the security.

Table 3-3 Configure the port IP Source Guard function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the port IP Source Guard function	**ip verify source** [**ip-mac**]	Mandatory By default, the port IP Source Guard function is disabled. When the command does not carry the parameters, the filter mode for the IP packets is IP+VLAN; when the command carries the parameters, the filter mode for the IP packet is IP+MAC+VLAN.

Note:

- After enabling the port IP Source Guard function, the bound entries of the port IP Source Guard are written to the chip. The number of the entries written to the chip depends on the available chip entry resources. If the chip entry resources are used up and it is necessary to add bound entries or enable the port IP Source Guard function on the other port, we need to delete the related bound entries of some chip entry resources.
- If some port IP Source Guard bound entries cannot written to the chip because the chip entry resources are not enough, the system automatically try to write the bound entries to the chip again every 60s until all the bound entries are written to the chip or deleted.
- If the port IP Source Guard and global IP Source Guard functions are used at the same time, the IP packet received by the port needs to match the bound entries of the port IP Source Guard and global IP Source Guard so that it can be forwarded. Otherwise, it is dropped.
- Before enabling the port IP Source Guard function and if the terminal device connected to the port is non-DHCP client, or the terminal device is the DHCP client, but the local device does not enable the DHCP Snooping function, we need to configure the MAC address, IP address and the VLAN ID of the terminal device as the port IP Source Guard static bound entry, so as to ensure that after enabling the function, the terminal device communicates normally. For the DHCP Snooping function, refer to the DHCP Snooping chapter of the configuration manual.

3.2.3. Configure Global IP Source Guard Function

Configuration Condition

None

Configure Global IP Source Guard Function

To protect the security of the user IP address and prevent other user from using its own IP address, we can configure the global IP Source Guard function to bind the user IP address and MAC address. The global IP Source Guard bound entries of the configured user IP address and MAC address are directly written to the chip, so as to filter the invalid IP and ARP packets.

When enabling the global Dynamic ARP Inspection function, the configured global IP Source Guard bound entries serve as the basis of the validity detection of the global Dynamic ARP Inspection function for the ARP packets.

Table 3-4 Configure the global IP Source Guard function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the global IP Source Guard function	**source binding** *mac-address ip-address*	Mandatory By default, there is no global IP Source Guard bound entry and the function is disabled. The command enables the global IP Source Guard function. Meanwhile, one global IP Source Guard bound entry is configured.

Note:

- If Hybrid extended ACL is applied to the global (all ports) ingress, we need to cancel the application so that the global IP Source Guard function can be configured. Otherwise, the configuration fails. Refer to the ACL chapter of the configuration manual.
- The global IP Source Guard bound entries support 40 at most. After exceeding 40, the configuration fails.
- The configured global IP Source Guard bound entries are directly written to the chip. The number of the bound entries written to the chip depends on the available chip entry resources. If the chip entry resources are used up and it is necessary to add the global IP Source Guard bound entries, we need to delete the related bound entries of some chip entry resources.

If the port IP Source Guard and global IP Source Guard functions are used at the same time, the IP packet received by the port needs to match the bound entries of the port IP Source Guard and global IP Source Guard so that it can be forwarded. Otherwise, it is dropped.

Note:

- For the port Dynamic ARP Inspection function, refer to the Dynamic ARP Inspection chapter of the configuration manual.

3.2.4. IP Source Guard Monitoring and Maintaining

Table 3-5 IP Source Guard monitoring and maintaining

Command	Description
show ip binding table [**interface** *interface-name* | **link-aggregation** *link-aggregation-id* | **slot** | **summary**]	Display the statistics information of the port IP Source Guard bound entries and the bound entry quantity
show ip source guard [**interface** *interface-name* | **link-aggregation** *link-aggregation-id*]	Display the configuration information of the port IP Source Guard function
show source binding	Display the statics information of the global IP Source Guard bound entries and the entry quantity

3.3. Typical Configuration Example of IP Source Guard

3.3.1. Configure Port IP Source Guard Function Based on IP+VLAN

Network Requirements

1. PC1 and PC2 are connected to IP Network via Device.
2. Configure the port IP Source Guard function based on IP+VLAN, realizing that PC1 can access IP Network normally and PC2 cannot access IP Network.

Network Topology

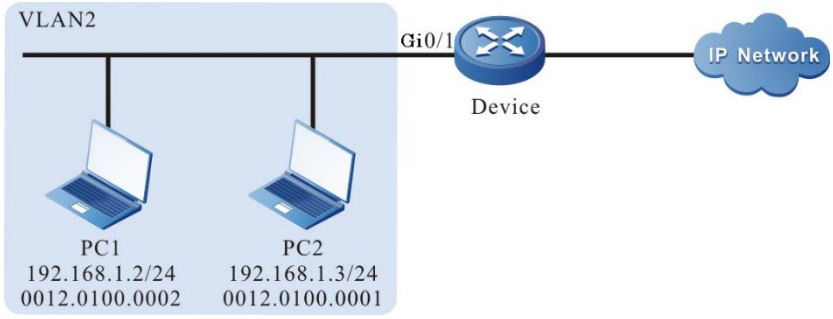


Figure 3–1 Networking of configuring port IP Source Guard function based on IP+VLAN

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the port IP Source Guard function on Device.

#Enable the port IP Source Guard function based on IP+VLAN on port gigabitethernet0/1, and configure the MAC address as 0012.0100.0001, IP address as 192.168.1.2, and the port IP Source Guard bound entry with VLAN 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip verify source
Device(config-if-gigabitethernet0/1)#ip source binding 0012.0100.0001 vlan 2 192.168.1.2
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

#View the configuration information of IP Source Guard.

```
Device#show ip source guard

-----------------------------------------
IP source guard interfaces on slot 0 :
  Total number of enabled interfaces : 1
-----------------------------------------------------
Interface Name      Status      Verify Type
-----------------------------------------------------
gi0/1           Enabled    IP        1
gi0/2           Disabled   Unknown   2
gi0/3           Disabled   Unknown   3
gi0/4           Disabled   Unknown   4
... ...
```

We can see that the IP Source Guard function based on IP+VLAN is enabled on port gigabitethernet0/1.

#View the port IP Source Guard bound entry.

```
Device#show ip binding table
-----------------------------------------
```

```
IP Source Guard binding table on slot 0
    Total binding entries    : 1
    Static binding entries   : 1
    Static not write entries : 0
    Dynamic binding entries  : 0
    Dynamic not write entries : 0
    PCE writing entries      : 1
-------------------------------------------------------------------------------
-----------------
Interface-Name   MAC-Address   IP-Address   VLAN-ID Type-Flag   Writing-
Flag   Entry-ID(H)
-------------------------------------------------------------------------------
-----------------
gi0/1          0012.0100.0001 192.168.1.2   2     Static       Wrote        65536
```

#PC1 can access IP Network normally and PC2 cannot access IP Network.

3.3.2. Configure Port IP Source Guard Function Based on IP+MAC+VLAN

Network Requirements

- PC1 and PC2 are connected to IP Network via Device.
- Configure the port IP Source Guard function based on IP+MAC+VLAN, realizing that PC1 can access IP Network normally and PC2 cannot access IP Network.

Network Topology

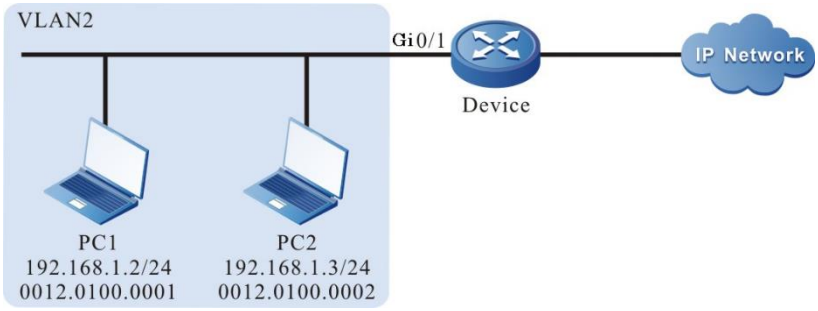


Figure 3–2 Networking of configuring port IP Source Guard function based on IP+MAC+VLAN

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the port IP Source Guard function on Device.

#Enable the port IP Source Guard function based on IP+MAC+VLAN on port gigabitethernet0/1, and configure the MAC address as 0012.0100.0001, IP address as 192.168.1.2, and the port IP Source Guard bound entry with VLAN 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip verify source ip-mac
Device(config-if-gigabitethernet0/1)#ip source binding 0012.0100.0001 vlan 2
192.168.1.2
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

#View the configuration information of IP Source Guard.

```
Device#show ip source guard

-----------------------------------------
IP source guard interfaces on slot 0 :
   Total number of enabled interfaces : 1
-----------------------------------------------------
Interface Name      Status      Verify Type  Interface ID
-----------------------------------------------------
gi0/1            Enabled     IP+MAC      1
gi0/2            Disabled    Unknown     2
gi0/3            Disabled    Unknown     3
gi0/4            Disabled    Unknown     4
… …
```

We can see that the IP Source Guard function based on IP+MAC+VLAN is enabled on port gigabitethernet0/1.

#View the port IP Source Guard bound entry.

```
Device#show ip binding table
-----------------------------------------
IP Source Guard binding table on slot 0
    Total binding entries    : 1
```

```
    Static binding entries    : 1
    Static not write entries  : 0
    Dynamic binding entries   : 0
    Dynamic not write entries : 0
    PCE writing entries       : 1
  ------------------------------------------------------------------------------
  ------------------
  Interface-Name    MAC-Address    IP-Address    VLAN-ID Type-Flag    Writing-
  Flag    Entry-ID(H)
  ------------------------------------------------------------------------------
  ------------------
  gi0/1             0012.0100.0001 192.168.1.2   2       Static       Wrote
  65536
```

#PC1 can access IP Network normally and PC2 cannot access IP Network.

4. DHCP SNOOPING

4.1. Overview

4.1.1. Overview of DHCP snooping Basic Functions

DHCP snooping is one security feature of DHCP (Dynamic Host Configuration Protocol) and has the following two functions:

1. Record the corresponding relation of the MAC address and IP address of the DHCP client:

Considering the security, the network administrator may need to record the IP address used when the user accesses the network, confirming the corresponding relation of the user host IP address and the IP address got from the DHCP server.

DHCP snooping listens to the DHCP request packet and the DHCP response packet received by the trust port and records the MAC address of the DHCP client and the obtained IP address. The administrator can view the IP address information got by the DHCP client via the bound entry recorded by DHCP snooping.

2. Ensure that the client gets the IP address from the valid server

If there is unauthorized DHCP server in the network, the DHCP client may get the wrong IP address, resulting in the communication abnormality or security risks. To ensure that the DHCP client can get the IP address from the valid DHCP server, the DHCP snooping function permits configuring the port as the trust port or un-trust port:

- Trust port is the port directly or indirectly connected to the valid DHCP server. The trust port forwards the received DHCP response packet normally, so as to ensure that the DHCP client can get the correct IP address.
- Un-trust port is the port not directly or indirectly connected to the valid DHCP server. If the un-trust port receives the DHCP response packet sent by the DHCP server, drop it, so as to prevent the DHCP client from getting the wrong IP address.

4.1.2. Brief Introduction of DHCP snooping Option82

DHCP snooping supports the adding, forwarding and managing for the Option82. Option82 is one DHCP packet option. The option is used to record the location information of the DHCP client and the administrator can locate the DHCP client according to the option, so as to perform some security control. For example, control the number of the IP addresses that can be distributed to one port or VLAN. The processing mode of Option82 varies with the DHCP packet type:

1. After the device receives the DHCP request packet, process the packet according to whether the packet contains the Option82, the processing policy configured by the user and the filling format, and then forward the processed packet to the DHCP server.

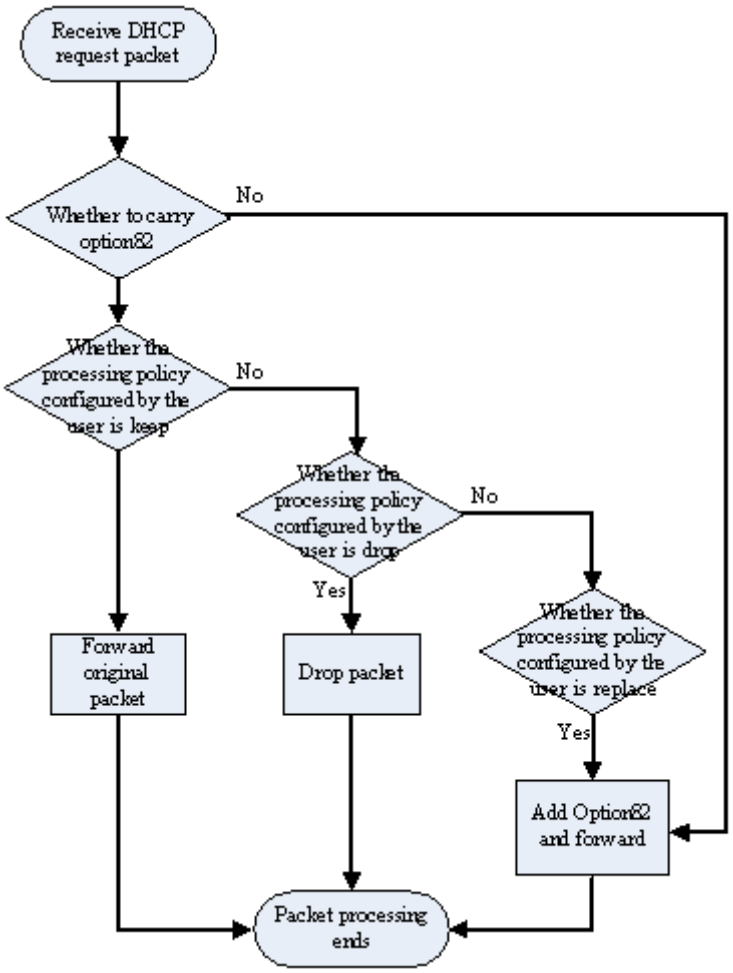


Figure 4-1 Processing flow of Option82

2. When the device receives the response packet of the DHCP server and if the packet contains the Option82, delete the Option82 and forward to the DHCP client; if the packet does not contain the Option82, directly forward to the DHCP client.

4.2. DHCP snooping Function Configuration

Table 4-1 DHCP snooping function configuration list

Configuration Task	
Configure the DHCP snooping basic functions	Configure the DHCP snooping function
	Configure the port trust status
	Configure the DHCP snooping rate limitation function

Configuration Task	
Configure DHCP snooping Option82	Configure the Remote ID content
	Configure the Circuit ID content
	Configure the filling format of the Option82
	Configure the processing policy of the Option82 packet
Configure the storing of the DHCP snooping bound entries	Configure the auto storing of the DHCP snooping bound entry
	Configure the manual storing of the DHCP snooping bound entry

4.2.1. Configure DHCP snooping Basic Functions

The DHCP snooping basic functions include enabling the DHCP snooping function, configuring the port trust status and limiting the rate of the DHCP packets.

Configuration Condition

None

Configure DHCP snooping Function

After enabling the DHCP snooping function, monitor the DHCP packets received by all the ports of the device:

1. For the received request packet, generate the corresponding bound entry according to the information in the packet
2. For the response packet received from the trust packet, update the status and lease time of the bound entry
3. For the response packet received from the un-trust port, directly drop it

Table 4-2 Configure the DHCP snooping function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable the DHCP snooping function	**dhcp-snooping**	Mandatory By default, DHCP snooping function is disabled.

Configure Port Trust Status

To prevent the DHCP client from getting the address from the invalid DHCP server, we can configure the port directly or in-directly connected to the valid server as the trust port.

After the port is configured as the trust port, permit the normal forwarding of the DHCP response packet. Otherwise, drop the DHCP response packet.

Table 4-3 Configure the port trust status

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the port trust status	**dhcp-snooping trust**	Mandatory By default, all ports are un-trust port.

Note:

- The port connected to the DHCP server needs to be configured as the trust port. Otherwise, the DHCP client cannot get the address.
- After the port is configured as the trust port, do not limit the rate of the DHCP packets passing the port.
- After changing the port status from the trust port to the un-trust port, the upper threshold of the port rate is the default 40.

Configure DHCP snooping Rate Limitation

Configuring the DHCP snooping rate limitation function can limit the number of the DHCP packets processed every second, avoiding that other protocol packets cannot be processed in time because the system processes the DHCP packets for a long time.

When the number of the DHCP packets received within one second exceeds the rate limitation, the subsequent DHCP packets are dropped. If the DHCP packets received by the port for successive 20s exceed the rate limitation, disable the port to isolate the packet impact source.

Table 4-4 Configure the DHCP snooping rate limitation function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the DHCP snooping rate limitation function	**dhcp-snooping rate-limit** *limit-value*	Mandatory By default, the upper rate threshold of the DHCP packets is 40pps.

Note:

- After configuring the rate threshold of the DHCP packets in the aggregation group configuration mode, the DHCP packet rate threshold of each member port of the aggregation group is the value.
- The DHCP packet rate limitation function just takes effect for the un-trust port and does not take effect for the trust port.
- After the port is disabled automatically, we can configure Error-Disable to enable the port automatically. By default, the auto disabling function of the port is enabled; if the DHCP packets received by the port for successive 20s exceed the rate limitation, but cannot disable the port automatically, we need to view the configuration of Error-Disable. For the Error-Disable function, refer to the Error-Disable chapter of the configuration manual.

4.2.2. Configure DHCP snooping Option82

The DHCP snooping function supports Option82. Option82 can contain 255 sub options at most. Maipu device supports two sub options, that is, Circuit ID and Remote ID.

Configuration Condition

Before configuring DHCP snooping Option82, first complete the following task:

- Enable the DHCP snooping function

Configure Remote ID

The content of Remote ID includes default content and non-default content. The filling format of the default content of Remote ID is as follows:

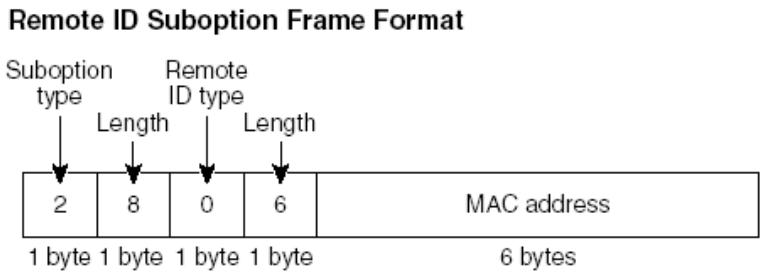


Figure 4-2 The filling format of the default content of Remote ID

The non-default content includes customized character string and device name, and needs to be configured to take effect in the user configuration format. The filling format of the non-default content of Remote ID is as follows:

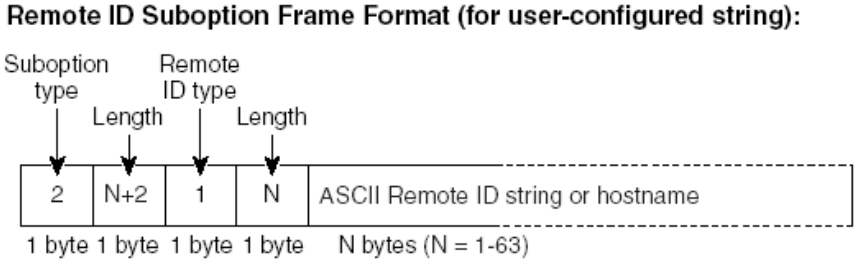


Figure 4-3 The filling format of the non-default content of Remote ID

Table 4-5 Configure the content of Remote ID

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the content of Remote ID	**dhcp-snooping information format remote-id** { *string* | **default** | **hostname** }	Mandatory By default, the content of Remote ID is the default content, that is, the MAC address of the device port.

Configure Circuit ID

The content of Circuit ID includes default content and non-default content. The filling format of the default content of Circuit ID is as follows:

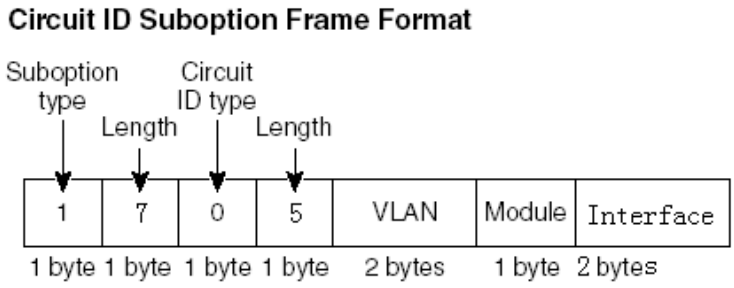


Figure 4-4 The filling format of the default content of Circuit ID

The non-default content needs to be configured to take effect in the user configuration format. The filling format of the non-default content of Circuit ID is as follows:

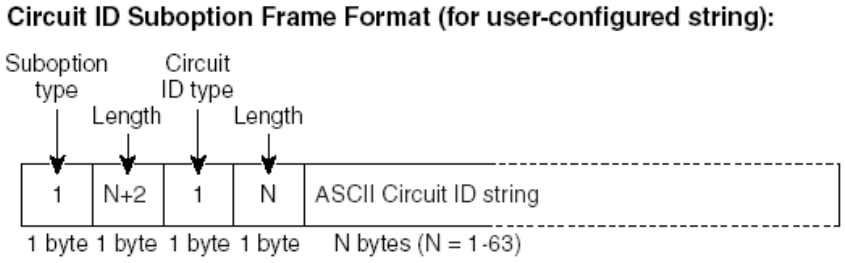


Figure 4-5 The filling format of the non-default content of Circuit ID

Table 4-6 Configure the content of Circuit ID

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the content of Circuit ID	**dhcp-snooping information format circuit-id** { *string* | **default** }	Mandatory By default, the content of Circuit ID is the default content.

Configure Filling Format of Option82

The filling format of Option82 includes default format and user configuration format.

When the filling format is the default format, the contents of Remote ID and Circuit ID are both default content; only after the filling format is configured as the user configuration format, the non-default contents of Remote ID and Circuit ID can take effect.

Table 4-7 Configure the filling format of Option82

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the filling format of Option82	**dhcp-snooping information format** { **default** | **user-config** }	Mandatory By default, the filling format is the default format.

Configure Packet Processing Policy of Option82

Configure the packet processing policy of Option82. We can adopt different forwarding policies for the DHCP request packet containing Option82.

Table 4-8 Configure the packet processing policy of Option82

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the packet processing policy of Option82	**dhcp-snooping information policy** { **drop** | **keep** | **replace** }	Mandatory By default, the processing policy is replace.

4.2.3. Configure Storing of DHCP snooping Bound Entries

The DHCP snooping function supports the auto or manual storing to the specified path of the bound entries. If the device restarts, the stored bound entries can be restored, avoiding affecting the communication because the bound entries are lost.

The specified path can be device FLASH, FTP server or TFTP server.

Configuration Condition

Before configuring the storing path of the bound entries as the FTP/TFTP server, first complete the following task:

1. FTP/TFTP server, enable the FTP/TFTP server function normally
2. The device can ping the IP address of the FTP/TFTP server.

Configure Auto Storing of DHCP snooping Bound Entries

DHCP snooping bound entries can be configured as the auto storing mode, that is, system automatically stores the bound entries regularly.

The system periodically refreshes the bound entries, detecting whether the bound entries are updated. If yes, we need to store the updated entries to the specified path after the storing delay arrives. The storing delay can prevent and control the frequent storing of the system because the entries are updated continuously.

Table 4-9 Configure the auto storing of DHCP snooping bound entries

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Step	**Command**	**Description**
Configure the auto storing of the DHCP snooping bound entries	**dhcp-snooping database savetype auto** { **flash** *file-name* | **ftp** *dest-ip-address ftp-username ftp-password file-name* | **tftp** *dest-ip-address file-name* }	Mandatory By default, the storing mode of the bound entries is auto mode, the storing path is flash, and the storing file name is dhcpsp_binding.db.
Configure the storing delay of the bound entries	**dhcp-snooping database savedelay** *seconds*	Optional By default, the storing delay of the bound entries is 1800s.
Configure the refresh interval of the bound entries	**dhcp-snooping database savepool** *seconds*	Optional By default, the refresh interval of the bound entries is 30s.

Configure Manual Storing of DHCP snooping Bound Entries

DHCP snooping bound entries can be configured as the manual storing mode, that is, execute the store command to complete the storing of the bound entries.

Table 4-10 Configure the manual storing of the DHCP snooping bound entries

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the manual storing of the DHCP snooping bound entries	**dhcp-snooping database savetype manual** { **flash** *file-name* | **ftp** *dest-ip-address ftp-username ftp-password file-name* | **tftp** *dest-ip-address file-name* }	Mandatory By default, the storing mode of the bound entries is auto mode, the storing path is flash and the storing file name is dhcpsp_binding.db.
Configure the storing bound file	**dhcp-snooping database save**	Mandatory Store the bound entries to the specified path. By default, the bound entries are not stored to the specified path.

4.2.4. Monitoring and Maintaining of DHCP snooping

Table 4-11 DHCP snooping monitoring and maintaining

Command	Description
clear dhcp-snooping database { **interface** *interface-list* | **link-aggregation** *link-aggregation-id* | *mac-address* | **all** }	Clear the bound entries
clear dhcp-snooping packet statistics [interface *interface-name* **| link-aggregation** *link-aggregation-id* **]**	Clear the statistics information of the received and sent DHCP packets

Command	Description
show dhcp-snooping [**interface** *interface-name* | **link-aggregation** *link-aggregation-id* | **save**]	Display the configuration information of DHCP snooping
show dhcp-snooping database [**|** { { **begin** | **exclude** | **include** } *expression* | **redirect** { **file** *file-name* | **ftp** [**vrf** *vrf-name*] { *hostname* | *dest-ip-address* } *ftp-username ftp-password file-name* } }] [**interface** *interface-name* | **link-aggregation** *link-aggregation-id* [**|** { { **begin** | **exclude** | **include** } *expression* | **redirect** { **file** *file-name* | **ftp** [**vrf** *vrf-name*] { *hostname* | *dest-ip-address* } *ftp-username ftp-password file-name* } }]]	Display the DHCP snooping bound entry information
show dhcp-snooping packet statistics [interface *interface-name* **| link-aggregation** *link-aggregation-id* **]**	Display the statistics information of the received and sent DHCP packets

4.3. Typical Configuration Example of DHCP snooping

4.3.1. Configure DHCP snooping Basic Functions

Network Requirements

- DHCP Server1 is the valid DHCP server; DHCP Server2 is the invalid DHCP server.
- After configuring the DHCP snooping function, PC1 and PC2 both can get address from DHCP Server1.

Network Topology

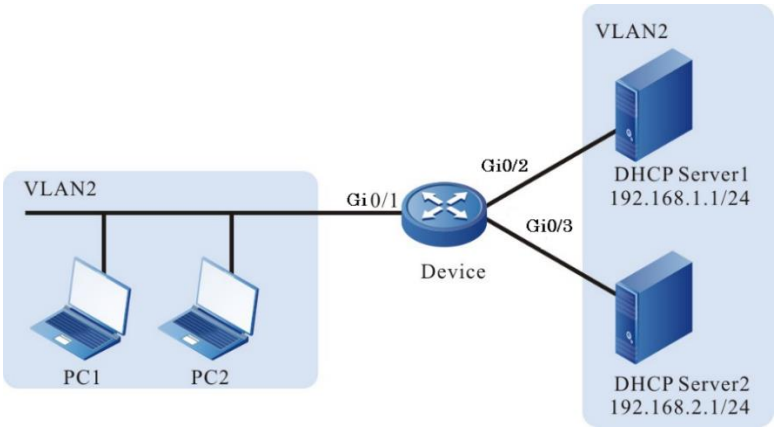


Figure 4-6 Networking of configuring DHCP snooping basic functions

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1-gigabitethernet0/3 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/3
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure the address pool of DHCP Server1 as 192.168.1.100-192.168.1.199 and the address pool of DHCP Server2 as 192.168.2.100-192.168.2.199. (Omitted)

Step 3: Configure the DHCP snooping function on Device.

#Enable the DHCP snooping function.

```
Device(config)#dhcp-snooping
```

#Configure the port gigabitethernet0/2 as trust port.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dhcp-snooping trust
Device(config-if-gigabitethernet0/2)#exit
```

Step 4: Check the result.

#After PC1 and PC2 get the address successfully, view the DHCP snooping entries on Device.

```
Device#show dhcp-snooping database
    dhcp-snooping database:
    database entries count:2
    database entries delete time :300
    --------------------------------
    macAddr       ipAddr        transtion-id   vlan  interface       leaseTime(s)
status
    0013.0100.0002  192.168.1.101  1          2     gi0/1           107990        active
```

```
------
0013.0100.0001  192.168.1.100  0          2     gi0/1          107989         active
------
Total valid DHCP Client binding table for this criterion: 2
```

PC1 and PC2 both can get address from DHCP Server1.

5. DYNAMIC ARP INSPECTION

5.1. Overview

Dynamic ARP Inspection is called DAI for short. Discover and prevent the ARP spoofing attack by checking the validity of the ARP packet, improving the network security. The DAI function is divided to two kinds:

1. Port DAI function: Check the validity of the ARP packet received by the specified port, so as to discover and prevent the ARP spoofing attack;

The basis of checking the validity of the ARP packet is the port IP Source Guard bound entry. The specific checking principle is as follows:

If the sending IP address, source MAC address and VLAN ID in the received ARP packet match with the port IP Source Guard bound entries, the ARP packet is valid packet and forward it. Otherwise, the ARP packet is invalid packet, drop it, and record the log information.

2. Global DAI function: Check the validity of the ARP packets received by all ports, preventing the counterfeiting users from sending the fake ARP packets and the device sets up the wrong ARP entry.

The basis of the ARP packet validity inspection is the global IP Source Guard bound entries. The specific detecting principle is as follows:

When the sending IP address in the received ARP packet is the same as the IP address in the global IP Source Guard bound entries, but the source MAC address is different, the ARP packet is fake packet, drop it and do not record the log information.

The port DAI and global DAI functions also check the effectiveness of the ARP packet. The specific checking principle is as follows:

When the source MAC address in the received ARP packet is different from the sending MAC address, the packet is ineffective packet, drop it and do not record the log information.

- Interface ARP Attack Detection: Do not perform validation detection for the ARP packet received on the specified interface. Only record the log information, which is used to detect the ARP attack.

5.2. Dynamic ARP Inspection Function Configuration

Table 5-1 The configuration list of Dynamic ARP Inspection function

Configuration Task	
Configure the port Dynamic ARP Inspection function	Configure the port Dynamic ARP Inspection function
Configure the global Dynamic ARP Inspection function	Configure the global Dynamic ARP Inspection function

5.2.1. Configure Port Dynamic ARP Inspection Function

Configuration Condition

Before configuring the port Dynamic ARP Inspection function, first complete the following task:

- Configure the port IP Source Guard bound entries

Configure Port Dynamic ARP Inspection

After enabling the port DAI function, the system checks the validity of the ARP packet received by the port according to the port IP Source Guard bound entries. The invalid packet is dropped and recorded in the logs.

The contents recorded in the logs include VLAN ID, receiving port, sending IP address, destination IP address, sending MAC address, destination MAC address and the number of the same invalid ARP packets. The user can analyze further according to the recorded log information, such as locate the host initiating the ARP packet.

By default, the log information is output periodically. We can control the recording, outputting and aging of the packet by configuring the output interval of the log. The log output interval serves as the basis of the following log parameters:

- Log refresh period: Used to judge whether the logs need to output and age. If the configured log output interval is smaller than 5s, the log refresh period is equal to 1s. Otherwise, the log refresh period is equal to 1/5 of the log output interval.
- Log age time: After the age time times out, the logs are deleted. The log age time is two multiples of the log output interval.
- Log token: In the log refresh period, the maximum number of the logs permitted to be recorded. The number of the log tokens is 15 multiples of the log refresh period.

After enabling the port DAI function, we can also configure the port ARP rate limitation function, that is, limit the number of the ARP packets that are processed every second, avoiding that the other protocol packets cannot be processed in time because the system processes lots of ARP packets for a long time.

Note:

- The port ARP rate limitation function is to limit the number of the ARP packets that are processed every second, avoiding that the other protocol packets cannot be processed in time because the system processes lots of ARP packets for a long time. After the number of the ARP packets received in one second exceeds the rate threshold, the subsequent received ARP packets are dropped. If the ARP packets received by the port in successive 15s exceed the rate, disable the port to isolate the packet impact source.

Table 5-2 Configure the port Dynamic ARP Inspection function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the port DAI function	**ip arp inspection**	Mandatory By default, the port DAI function is disabled.
Configure the upper threshold of the ARP packets processed by the port	**ip arp inspection rate-limit** *limit-value*	Optional By default, the upper threshold of the ARP packets processed by the port is 15pps.
Return to the global configuration mode	**exit**	-
Configure the number of the buffered logs	**ip arp inspection log-buffer** *buffer-size*	Optional By default, the system can buffer 32 logs. If it is configured as 0, it indicates that the logs are not buffered, that is, after detecting the invalid ARP packet, the logs are directly output to the terminal.

Step	Command	Description
Configure the log output interval	**ip arp inspection log-interval** *seconds*	Optional By default, the log output interval is 20s. If it is configured as 0, it indicates that the logs are not buffered, that is, after detecting the invalid ARP packet, the logs are directly output to the terminal.
Configure the log output level	**ip arp inspection log-level** *log-level*	Optional By default, the log output level is 6.

Note:

- After the port DAI function is enabled, all ARP packets received by the port (broadcast ARP and unicast ARP) are re-directed to the CPU for detecting, software forwarding, log recording and so on. When the number of the ARP packets is large, they seriously consume CPU resources, so when the device communicates normally, it is not suggested to enable the port DAI function. When it is doubted that there is ARP spoofing attack in the network, it is necessary to enable the port DAI function to detect and locate.
- In one port, the port DAI function cannot be used with the port security function at the same time.
- After configuring the rate threshold of the port processing the ARP packets in the aggregation group configuration mode, the ARP packet rate threshold of each member port of the aggregation group is the value.
- If the ARP packets received by the port in successive 20s exceed the upper threshold, but the port is not automatically disabled, it is necessary to refer to the Error-Disable chapter of the configuration manual.

5.2.2. Configure Global Dynamic ARP Inspection Function

Configuration Condition

Before configuring the global Dynamic ARP Inspection function, first complete the following task:

- Configure the global IP Source Guard bound entry

Configure Global Dynamic ARP Inspection Function

After enabling the global DAI function, the system checks the validity of the received ARP packet according to the global IP Source Guard bound entries. The invalid packet is dropped and not recorded in the logs.

Table 5-3 Configure the global Dynamic ARP Inspection function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable the global DAI function	**arp-security**	Mandatory By default, the global DAI function is disabled.

5.2.3. Configure Dynamic ARP Attack Inspection

Configuration Condition

None

Configure Dynamic ARP Attack Inspection

After the dynamic ARP attack detection is enabled, the system will not perform the validation inspection for the received ARP packet but only record the log.

Table 5-1 Configure the dynamic ARP attack inspection

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration can only take effect on the current interface. After entering the aggregation group configuration mode, the subsequent configuration can only take effect in the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the ARP attack detection on the interface	**ip arp inspection attack**	Mandatory By default, the ARP attack detection is not enabled on the interface.

5.2.4. Monitoring and Maintaining of Dynamic ARP Inspection

Table 5-5 Dynamic ARP Inspection monitoring and maintaining

Command	Description
clear ip arp inspection { log-information | log-statistics | pkt-statistics [interface *interface-name* | link-aggregation *link-aggregation-id*] }	Delete the statistics information recorded by the port DAI function
show arp-security	Display the status of the global DAI function
show ip arp inspection [**interface** *interface-name* | **link-aggregation** *link-aggregation-id*]	Display the configuration information of the port DAI function
show ip arp inspection log-information	Display the log information recorded by the port DAI function
show ip arp inspection log-statistics	Display the statistics information of the logs
show ip arp inspection pkt-statistics [**interface** *interface-name* | **link-aggregation** *link-aggregation-id*]	Display the statistics information of the ARP packet

5.3. Typical Configuration Example

5.3.1. Configure DAI Basic Functions

Network Requirements

- PC1 and PC2 are connected to IP Network via Device.
- Configure the port DAI function on Device, preventing the ARP attack and spoofing.

Network Topology

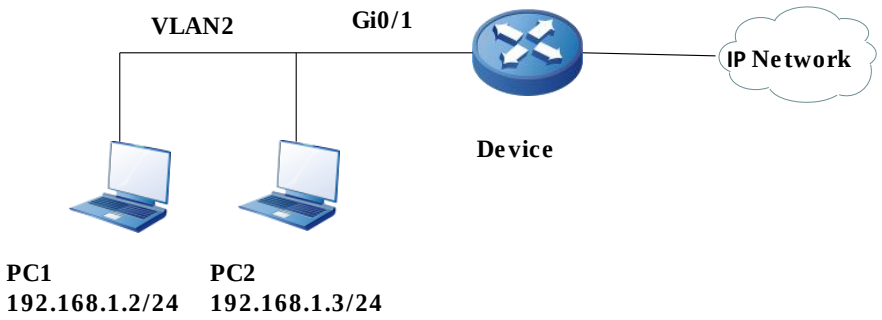


Figure 5–1 Networking of configuring the DAI basic functions

Configuration Steps

Step 1: Configure the link type of the VLAN and port on Device.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the port DAI function on Device.

#Enable the port DAI function on port gigabitethernet0/1 and configure the upper threshold of port gigabitethernet0/1 processing ARP packets as 30pps.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip arp inspection
Device(config-if-gigabitethernet0/1)#ip arp inspection rate-limit 30
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Configure the bound entries on Device.

#Configure the MAC address on port gigabitethernet0/1 as 0012.0100.0001, IP address as 192.168.1.2, and the port IP Source Guard bound entries with VLAN 2.

```
Device(config)#interface gigabitethernet 0/1
```

```
Device(config-if-gigabitethernet0/1)#ip source binding 0012.0100.0001 vlan 2
192.168.1.2
Device(config-if-gigabitethernet0/1)#exit
```

Step 4: Check the result.

#Configure the DAI configuration information.

```
Device#show ip arp inspection
    Dynamic ARP Inspection information:
    Dynamic ARP Inspection log buffer size: 30
    Dynamic ARP Inspection log Interval:   20
    Dynamic ARP Inspection log Level:     6
    Dynamic ARP Inspection interface information :
    ----------------------------------------
    interface        status    rate-limit(pps)
    gi0/1           enable    30
    gi0/2           disable   15
    ......
```

#When the rate of the port gigabitethernet0/1 receiving the ARP packets exceeds 30pps, Device drops the excessive packets and outputs the following prompt information.

```
Jan  1 02:21:06: The rate on interface gigabitethernet0/1 too fast ,the arp packet
drop!
```

#When the rate of the port gigabitethernet0/1 receiving the ARP packets exceeds 30pps for successive 20s, Device disables port gigabitethernet0/1 and outputs the following prompt information.

```
Jan   1  02:21:26:  %LINK-INTERFACE_DOWN-4:  interface  gigabitethernet0/1,
changed state to down
Jan  1 02:21:26: The rate of arp packet is too fast,dynamic arp inspection shut down
the gigabitethernet0/1 !
```

#When the ARP packets received by port gigabitethernet0/1 are inconsistent with the bound entries, Device records the following format of invalid information to the DAI logs and outputs regularly.

```
Jan  1 07:19:49:  SEC-7-DARPLOG: sender IP address: 192.168.1.3 sender MAC
address:0011.0100.0001  target  IP  address:  0.0.0.0  target  MAC
address:0000.0000.0000 vlan ID:2 interface ID:gigabitethernet0/1 record
packet :32 packet(s)
```

#View the DAI logs.

```
Device#show ip arp inspection log-information
LogCountInBuffer:1
```

SEC-7-DARPLOG: sender IP address: 192.168.1.3 sender MAC address:0011.0100.0001 target IP address: 0.0.0.0 target MAC address:0000.0000.0000 vlan ID:2 interface ID:gigabitethernet0/1 record packet :0 packet(s)

5.3.2. DAI Combining With DHCP Snooping

Network Requirements

- PC1 and PC2 are connected to IP Network via Device; PC2 is the DHCP client; Device2 is the DHCP relay.
- Device1 configures DHCP Snooping and port DAI function, realizing that PC2 can access IP Network normally and PC1 cannot access IP Network.

Network Topology

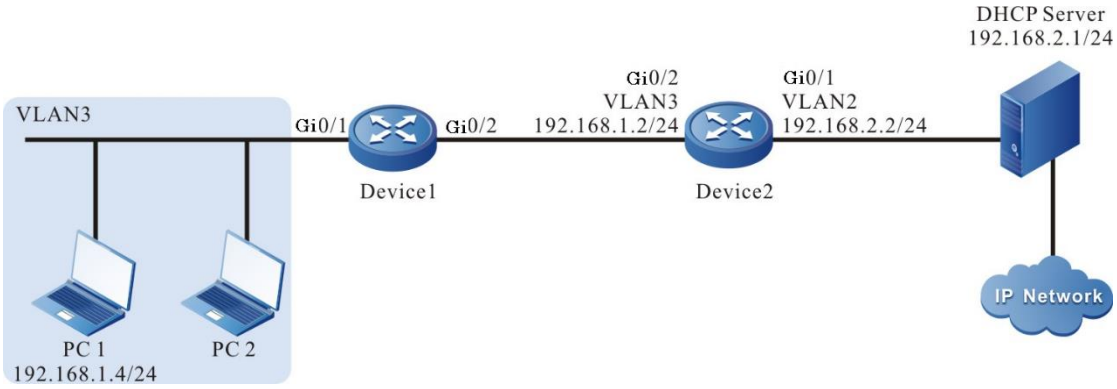


Figure 5–2 Networking of combing DAI with DHCP Snooping

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device1.

#Create VLAN3.

```
Device1#configure terminal
Device1(config)#vlan 3
Device1(config-vlan3)#exit
```

#Configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 as Access, permitting the services of VLAN3 to pass.

```
Device1(config)#interface gigabitethernet 0/1-0/2
Device1(config-if-range)#switchport access vlan 3
Device1(config-if-range)#exit
```

Step 2: Configure the link type of VLAN and port on Device2.

#Create VLAN2 and VLAN3.

```
Device2#configure terminal
Device2(config)#vlan 2-3
```

#Configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 as Access; port gigabitethernet0/1 permits the services of VLAN2 to pass; port gigabitethernet0/2 permits the services of VLAN3 to pass.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode access
Device2(config-if-gigabitethernet0/1)#switchport access vlan 2
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)#interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/2)#switchport mode access
Device2(config-if-gigabitethernet0/2)#switchport access vlan 3
Device2(config-if-gigabitethernet0/2)#exit
```

Step 3: Configure VLAN interface and IP address on Device1 and Device2. (Omitted)

Step 4: Configure the DHCP Snooping function on Device1.

#Enable the DHCP Snooping function and configure the port gigabitethernet0/2 as trust port.

```
Device1(config)#dhcp-snooping
Device1(config)#interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/2)#dhcp-snooping trust
Device1(config-if-gigabitethernet0/2)#exit
```

Step 5: Configure the port DAI function on Device1.

#Enable the port DAI function on port gigabitethernet0/1.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#ip arp inspection
Device1(config-if-gigabitethernet0/1)#exit
```

Step 6: Configure the IP address of the DHCP relay server on Device2.

#Configure the IP address of the DHCP relay server as 198.168.2.1.

```
Device2(config)#ip dhcp-server 192.168.2.1
```

Step 7: Check the result.

#After PC2 gets the address successfully; view the DHCP Snooping dynamic entries on Device1.

```
Device1#show dhcp-snooping database
    dhcp-snooping database:
```

```
        database entries count:1
        database entries delete time :300
        ---------------------------------
        macAddr        ipAddr        transtion-id    vlan  interface        leaseTime(s)
    status
        0013.0100.0001  192.168.1.100  2          2     gi0/1          107990         active
        ------
```

#PC2 can access IP Network normally and PC1 cannot access IP Network.

6. AAA

6.1. Overview

AAA refers to Authentication, Authorization, and Accounting. Since the network appeared, Authentication, Authorization, and Accounting mechanism has become the basis of the network operation. The using of the resources in the network needs to be managed by Authentication, Authorization, and Accounting. AAA adopts the client/server architecture. The client runs on NAS (Network Access Server) and the server manages the user information in a centralized manner. For the user, NAS is the server; for the server, NAS is the client.

Authentication means to authenticate the user when using the resources in the network system. During the process, get the ID information by interacting with the user and then submit to the authentication server; the latter checks and processes the ID information with the user information saved in the database, and then confirm whether the user ID is correct according to the processing result. Authorization means that the authorized user of the network system uses its resources by the specified mode. The process specifies the services and authorities that the authenticated user can use and own after being connected to the network, such as the authorized IP address. Accounting means that the network system collects and records the using of the user for the network resources, so as to charge the user for the network using fees, or used for auditing.

RADIUS is one protocol of the C/S architecture. Its client is the NAS server at first. RADIUS protocol authentication mechanism is flexible and can adopt PAP, CHAP or Unix login authentication mode. RADIUS is one expansible protocol and all its work is based on the vector of Attribute-Length-Value. The basic work principle of RADIUS is: The user is connected to NAS; NAS uses Access-Require packet to submit the user information to the RADIUS server, including user name, password, and so on. The user password is encrypted via MD5. The two parties use the share key, which is not spread via the network. RADIUS server checks the validity of the user name and password and provides one Challenge if necessary, requiring the further authentication for the user. We also can perform the similar authentication for NAS. If valid, return the Access-Accept packet to NAS, permitting the user to perform the next work. Otherwise, return the Access-Reject packet, refusing the user access. If permitting the access, NAS initiates the statistics request Account-Require to the RADIUS server. RADIUS server replies Account-Accept, beginning the statistics for the user. Meanwhile, the user can perform its own operations.

TACACS is one old authentication protocol for the Unix network. It permits the remote access server to transit the user login password to the authentication server. The authentication server decides whether the user can log in to the system. TACACS is one encryption protocol, but its security is poorer that TACACS+ and RADIUS. In fact, TACACS+ is one new protocol. TACACS+ and RADIUS replaces the earlier protocol in the present network. TACACS+ uses TCP, while RADIUS uses UDP. RADIUS combines the authentication and authorization from the user aspect, while TACACS+ separates the two operations.

6.2. AAA Function Configuration

Table 6-1 The configuration list of the AAA function

Configuration Task	
Configure the AAA domain	Configure ISP domain

Configuration Task	
Configure the authentication function in the AAA domain	Configure the default, login, ppp, and xauth authentication methods in the ISP domain
Configure the authorization function in the AAA domain	Configure the default, login, ppp, and xauth authorization methods in the ISP domain
Configure the accounting function in the AAA domain	Configure the default, login, ppp, and xauth accounting methods in the ISP domain
Configure the authentication method of the privileged mode	Configure the authentication method of the privileged mode
Configure enabling the CLI authorization	Configure enabling the CLI authorization
	Configure enabling the Console authorization
Configure the system statistics function	Configure the statistics method of the system event
Configure the statistics attributes	Configure disabling the empty user name statistics
	Configure sending the statistics update packet
	Configure sending the statistics failure processing mode
Configure the RADIUS scheme	Configure the RADIUS server
	Configure the RADIUS attributes
	Configure the source address of sending the RADIUS packet
Configure the TACACS scheme	Configure the TACACS server
	Configure the source address of sending the TACAS packet

6.2.1. Configure the AAA Domain

Domain: NAS user management is based on ISP (Internet Service Provider) domain, and each user belongs to an ISP domain. In general, the ISP domain to which the user belongs is determined by the user name provided when the user logs in. There is a system domain by default. Under the domain, you can configure the authentication, authorization, and accounting method of each access user.

The solution of the domain-based user and AAA management is described as follows:

The management of NAS devices for users is based on the ISP domain. Generally, the ISP domain to which the user belongs is determined by the user name provided when the user logs in.

"Input User Name "= "User Name Understood by Device"+ "Domain Name"

When authenticating users, devices determine their domains in the following order, and then execute AAA policies in the domains:

1. (Optional) Log into/access the module to configure the designated authentication domain;
2. ISP domain specified in user name;
3. The default ISP domain of the system

Configuration Condition

None

Configure the ISP Domain

Table 6-1 Configure the AAA domain

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the ISP domain view	**domain** *isp-name*	Optional By default, the system has one ISP domain named system.
Return to the global configuration mode	**exit**	-
Configure the default ISP domain	**domain default enable** *isp-name*	Optional By default, the default ISP domain of the system is the system domain.

6.2.2. Configure the Authentication Function in the AAA Domain

AAA provides a series of authentication methods to ensure the security of devices and network services. For example, authenticate user login to prevent illegal users from operating devices; authenticate users into privileged mode to restrict the using authorities of users for device; authenticate PPP session connections to restrict the setup of the illegal connections.

Configuration Condition

None

Configure the Authentication Method in the ISP Domain

AAA can authenticate a user when he tries to log into a specific ISP domain. Users who fail to authenticate cannot log into the specified ISP domain.

Table 6-2 Configure the authentication method list in the ISP domain

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the ISP domain view	**domain** *isp-name*	Mandatory By default, the system has one ISP domain named system.
Configure the default authentication method in the ISP domain	**aaa authentication default** { **none** / **local** / **radius-group** *group-name* / **tacacs-group** *group-name* }	Optional By default, the default authentication method in the ISP domain is local.
Configure the user login authentication method in the ISP domain	**aaa authentication login** { **none** / **enable** / **local** / **radius-group** *group-name* / **tacacs-group** *group-name* }	Optional By default, do not configure the login authentication method, but adopt the default authentication method in the domain.

Step	Command	Description
Configure the PPP authentication method in the ISP domain	**aaa authentication ppp { none / local / radius-group** group-name **/ tacacs-group** group-name **}**	Optional By default, do not configure the PPP authentication method, but adopt the default authentication method in the domain.
Configure the xauth authentication method in the ISP domain	**aaa authentication xauth** { **none** / **local** / **radius-group** *group-name* / **tacacs-group** *group-name* }	Optional By default, do not configure the xauth authentication method, but adopt the default authentication method in the domain.

6.2.3. Configure the Authorization Function in the AAA Domain

After successful authentication, the authorization function of AAA can control the rights of administrator users for device resources and access for network resources, restrict administrators to execute unauthorized commands, and restrict access users to access unauthorized network resources.

Configuration Condition

When configuring the command line authorization in the domain, first configure the authorization of enabling the command line so that the configured command line authorization in the domain can take effect.

Configure the Authorization Method in the ISP Domain

When a user executes an authorization item in a specific ISP domain, AAA can authorize the user, grant the user certain authorities, and prohibit the unauthorized user to execute the authorization item in the domain.

Table 6-3 Configure the authorization method list in the ISP domain

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the ISP domain view	**domain** *isp-name*	Mandatory By default, the system has one ISP domain named system.

Step	Command	Description
Configure the default authorization method in the ISP domain	**aaa authorization default** { **if-authenticated** / **local** / **none** / **radius-group** *group-name* / **tacacs-group** *group-name* }	Optional By default, the authorization method in the ISP domain is none.
Configure the commands authorization method in the ISP domain	**aaa authorization commands** *cmd-lvl* { **if-authenticated** / **none** / **radius-group** *group-name* / **tacacs-group** *group-name* }	Optional By default, do not configure the commands authorization method in the ISP domain, and the authorization method in the domain is none. The command authorization function must be enabled so that the configuration can take effect.
Configure the authorization method of the user logging into the device in the ISP domain	**aaa authorization login** { **if-authenticated** / **local** / **none** / **radius-group** *group-name* / **tacacs-group** *group-name* }	Optional By default, do not configure the login authorization method in the ISP domain, but adopt the default authorization method in the domain.
Configure the PPP authorization method in the ISP domain	**aaa authorization ppp** { **if-authenticated** / **local** / **none** / **radius-group** *group-name* / **tacacs-group** *group-name* }	Optional By default, do not configure the PPP authorization method in the ISP domain, but adopt the default authorization method in the ISP domain.

Step	Command	Description
Configure the xauth authorization method in the ISP domain	**aaa authorization xauth** { **if-authenticated** / **local** / **none** / **radius-group** *group-name* / **tacacs-group** *group-name* }	Optional By default, do not configure the xauth authorization method in the ISP domain, but adopt the default authorization method in the ISP domain.

Note:

- The AAA authorization commands and aaa authorization config-commands commands are configured in no sequence.

6.2.4. Configure the Accounting Function in the AAA Domain

The customized methods can be used to measure the command, login session, network service, and system events on the device. The statistical results can be used as the basis for charging users.

Configuration Condition

None

Configure the Accounting Method in the ISP Domain

When a user successfully logs into an ISP domain, AAA can count the user, including the start time of login, the end time of login, the commands entered, and so on.

Table 6-4 Configure the accounting method in the ISP domain

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the ISP domain view	**domain** *isp-name*	Mandatory By default, the system has one ISP domain named system.
Configure the command statistics method in the ISP domain	**aaa accounting commands** *cmd-lvl* { [**broadcast**] **tacacs-group** *group-name* }	Optional By default, do not configure the command statistics method, and do not perform the command statistics.
Configure the default statistics method in the ISP domain	**aaa accounting default** { **none** | { **start-stop** | **stop-only** | **wait-start** [**broadcast**] { **radius-group** *group-name* / **tacacs-group** *group-name* }}}	Optional By default, the statistics method in the ISP domain is none.
Configure the accounting method of the user logging into the device in the ISP domain	**aaa accounting login**{ **none** | { **start-stop** | **stop-only** | **wait-start** [**broadcast**] { **radius-group** *group-name* / **tacacs-group** *group-name* } } }	Optional By default, do not configure the accounting method of the user logging into the device in the ISP domain, but use the default accounting method in the ISP domain.

Step	Command	Description
Configure the ppp accounting method in the ISP domain	**aaa accounting ppp** { **none** | { **start-stop** | **stop-only** | **wait-start** [**broadcast**] { **radius-group** *group-name* / **tacacs-group** *group-name* } } }	Optional By default, do not configure the ppp accounting method in the ISP domain, but use the default accounting method in the ISP domain.
Configure the xauth accounting method in the ISP domain	**aaa accounting xauth** { **none** | { **start-stop** | **stop-only** | **wait-start** [**broadcast**] { **radius-group** *group-name* / **tacacs-group** *group-name* } } }	Optional By default, do not configure the xauth accounting method in the ISP domain, but adopt the default accounting method in the ISP domain.

6.2.5. Configure the Authentication Method of the Privileged Mode

After the user successfully logs into the device, AAA can authenticate the user entering the privileged mode by entering the enable command, and prohibit the user entering the privileged mode if the authentication fails.

Configuration Condition

None

Configure the Authentication Method of the Privileged Mode

Table 6-5 Configure the authentication method of the privileged mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the authentication method of the privileged mode	**aaa authentication enable-method** { **none** / **enable** / **radius-group** *group-name* / **tacacs-group** *group-name* }	Optional By default, the authentication method of the privileged mode is enable.

Note:

- When using RADIUS authentication method, the password of the user name in the format of $enabLEVEL $is used as the authentication password, where LEVEL represents the user level entered by the current user, and the range of values is 0-15, and the highest level is 15.

6.2.6. Enable Command Authorization

Configuration Condition

None

Enable Command Authorization

The device has commands of 0 to 15 levels. Command authorization is to determine the level of commands used by users by authorization method, and restrict users to use the commands higher than the current level.

Table 6-6 Enable the command authorization in the global mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the command authorization	**aaa authorization config-commands**	Mandatory By default, disable the command authorization function.

Enable Console Authorization

To perform the access restriction for the console port, you can enable Console port authorization, and need to enable the command authorization function. And then, the device will authorize the commands executed by console port.

Table 6-7 Enable the Console authorization

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the Console authorization	**aaa authorization console**	Mandatory By default, do not enable the Console authorization.

6.2.7. Configure the System Event Statistics Function

Users can send events, such as system boot and reboot, to the server for statistics by configuring the system event statistics method.

Configuration Condition

None

Configure the System Event Statistics Method

Table 6-8 Configure the system event statistics method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the system event statistics method	**aaa accounting system** { **none** / { **start-stop** [**broadcast**] { **tacacs-group** *group-name* } } }	Mandatory By default, do not account the system events.

Note:

- The system event statistics only supports the TACACS protocol, but does not support the RADIUS protocol.

6.2.8. Configure the Accounting Attributes

Configuration Condition

None

Disable Null-Username Accounting

The user can disable the AAA null-username accounting by configuring the command **aaa accounting suppress null-username**. By default, enable the AAA null-username accounting.

Table 6-9 Disable the null-username accounting

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Disable the null-username accounting	**aaa accounting suppress null-username**	Mandatory By default, enable the null-username accounting.

Send Accounting Update Packet

The user can configure the mode of sending the accounting update packet, mainly including send in real time and send periodically.

Table 6-10 Send the accounting update packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Send the accounting update packet	**aaa accounting update periodic** *interval*	Mandatory By default, do not send the accounting update packet.

Configure the Processing mode of Sending Accounting Failure

Table 6-11 Send the processing mode of sending accounting failure

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the processing mode of sending accounting failure	**aaa accounting start-fail {online | offline}**	Optional By default, if the accounting starting fails, the user cannot get online.

6.2.9. Configure the RADIUS Scheme

To configure the RADIUS scheme, you need to configure the key parameters of the server.

Configuration Condition

None

Configure the RADIUS Server

When AAA needs to use the RADIUS method for authentication, authorization and accounting, it is necessary to configure RADIUS server parameters, including server IP address, authentication/authorization port, accounting port and shared key information.

Before entering the RADIUS server, we need to configure the RADIUS server group. Reference the server group name when configuring the method list, and we can use the RADIUS server group to authenticate, authorize and count the users.

Table 6-12 Configure the RADIUS server

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the RADIUS server group name (the command also can enter the RADIUS server group configuration mode)	**aaa server group radius** *group-name*	Mandatory By default, do not configure the RADIUS server group name.

Step	Command	Description
Configure the RADIUS server	**server {***ip-address*|*ipv6 ip-address***} [acc-port** *acc-port-num* **] [auth-port** *auth-port-num* **] [priority** *priority* **] { key [0 | 7]** *key* **}**	Mandatory By default, do not configure the RADIUS server.
Configure the RADIUS dead time	**dead-time** *dead-time*	Optional By default, the dead time of the RADIUS server is 0, indicating not dead.
Configure the maximum re-transmit times of RADIUS	**retransmit** *retries*	Optional By default, the maximum re-transmit times of the RADIUS server is three times.
Configure the response timeout of the RADIUS server	**timeout** *timeout*	Optional By default, the timeout of waiting for the RADIUS server response is 5s.
Configure not checking TAG when resolving the tunnel attribute delivered by the RADIUS server	**tunnel without-tag**	Optional By default, need the TAG when resolving the tunnel attribute delivered by the RADIUS server.
Configure the VRF of the RADIUS server group	**ip vrf forwarding** *vrf-name*	Optional By default, the RADIUS server group belongs to the global VRF.

Note:

- Devices select the order in which RADIUS servers are used according to the configured priority value.

- Dead time means that the device marks the RADIUS servers that do not respond to authentication requests as unavailable and no requests are sent to these servers during dead-time.
- The configured share keys on the device and RADIUS server must be consistent.

Configure the RADIUS Attributes

Table 6-13 Configure the RADIUS attributes

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the attribute service-type value in the RADIUS packet of the login authentication	**radius login service-type** *attr-value*	Optional By default, the service-type value in the RADIUS packet is 7.
Configure the maximum concurrent packets of the NAS device and the RADIUS server	**radius control-speed** *pck-num*	Optional By default, the maximum concurrent packets of the NAS device and the RADIUS server is 100.
Configure the session ID field of the client and server	**radius session state**	Optional By default, the session ID field of the client and server is session-id.

Configure the Source Address of Sending the RADIUS Packet

Table 6-14 Configure the source address of sending the RADIUS packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the interface selected by the RADIUS source address	**ip radius source-interface** *interface-name* [**vrf** *vrf-name*]	Optional By default, the device automatically selects the source interface.

Configure the accounting-on Function of RADIUS

The account-on function is mainly used to designate all online users on the RADIUS server when the AAA process is pulled up for the first time. By default, the accounting-on function is disabled; when the account-on function is enabled, the default retransmit interval is 6 seconds, and the maximum retransmit times is 50 times; it is recommended that users set the retransmit times and the interval time not lower than the default values as far as possible.

Table 6-15 Configure the accounting-on function of RADIUS

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the RADIUS server group mode	**aaa server group radius** *group-name*	-
Configure the account on function of RADIUS	**accounting-on enable [interval** *seconds* **| send** *send-times***]**	Optional By default, the accounting-on function is disabled.

6.2.10. Configure the TACACS Scheme

To configure the TACACS scheme, it is necessary to configure the key parameters of the server.

Configuration Condition

None

Configure the TACACS Server

If AAA needs to use the TACACS method for authentication, authorization and accounting after configuring the TACACS server, it needs to configure the parameters of the TACACS server, including server IP address, shared key, server port number and other configuration information.

The TACACS server group can be used to authenticate, authorize and account users by referring to the server group name when configuring the method.

Table 6-16 Configure the TACACS server

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the TACACS server group name (the command also can enter the TACAS server group configuration mode)	**aaa server group tacacs** *group-name*	Mandatory By default, do not configure the TACAS server group name.
Configure the TACACS server	**server {***ip-address*|**ipv6** *ip-address*} [**port** *port-num*] [**priority** *priority*] { **key** [**0** | **7**] *key*}	Mandatory By default, do not configure the member server of the TACAS server group.
Configure the response timeout of the TACAS server	**timeout** *timeout*	Optional By default, the timeout of waiting for the TACAS server response is 5s.
Configure the VRF attribute of the TACAS server group	**ip vrf forwarding** *vrf-name*	Optional By default, the TACAS server group belongs to the global VRF.

Note:

- You can execute the command **server {***ip-address*|**ipv6** *ip-address*} [**port** *port-num*] [**priority** *priority*] { **key** [**0** | **7**] *key*} for many times to configure multiple TACAS servers in the Tacas server group. The device selects the server to authenticate according to the configuration order. When one server fails, the device automatically selects the next server.
- The configured share keys on the device and TACAS server must be consistent.

Configure the Source Address of Sending the TACAS Packet

Table 6-17 Configure the source address of sending the TACAS packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the interface selected by TACAS source address	**ip tacacs source-interface** *interface-name* [**vrf** *vrf-name*]	Optional By default, the device automatically selects the source interface.

6.2.11. AAA Monitoring and Maintaining

Table 6-18 AAA monitoring and maintaining

Command	Description
debug aaa { **authentication** | **authorization** | **accounting** | **event** | **error** | **all** }	Enable the AAA debug information
debug radius [details]	Enable the RADIUS debug information
debug tacacs [details]	Enable the TACAS debug information
show aaa configuration	Display the AAA configuration information
show aaa module [*module-name***]**	Display the AAA function modules, and the result about the module operating AAA for the last time
show aaa server [**radius** | **tacacs**]	Display the RADIUS/TACACS server configuration and status of AAA

Command	Description
show aaa session [*module-name***]**	Display the AAA statistics session
show aaa source-address	Display the source address used by AAA

6.3. AAA Typical Configuration Example

6.3.1. Configure Telnet User Login to Use Local Authentication

Network Requirement

Configure Device to use local authentication for Telnet user login

Network Topology

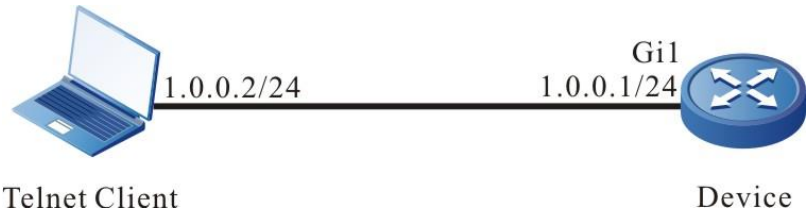


Figure 6-1 Networking of configuring Telnet user login to use local authentication

Configuration Steps

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

Step 2: Configure Device.

#Configure the user name as admin1 and password as admin2.

```
Device#configure terminal
Device(config)#local-user admin1 class manager
Device(config-user-manager-admin1)#service-type telnet
Device(config-user-manager-admin1)#password 0 admin2
Device(config-user-manager-admin1)#exit
```

#Configure the Telnet session and enable the AAA local authentication.

```
Device(config)#line vty 0 15
Device(config-line)#login aaa default
Device(config-line)#exit
```

Step 3: Check the result.

#On Device, query the AAA configuration information.

```
Device#show aaa configuration
```

```
domain system
```

You can see that there is the default system domain on Device.

When Telnet client logs in to Device, input the user name admin1 and password admin2 according to the prompt, and then log in to the Shell user interface of Device successfully.

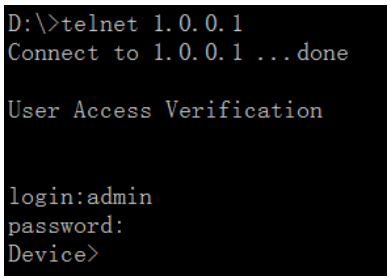


Figure 6-2 Use the local authentication login

Note:

- The default domain of the device is the system domain. And the default authentication method of the system domain is local method.

6.3.2. Configure Telnet User Login to Use RADIUS Authentication/Authorization and Statistics

Network Requirements

1. Device is connected to the Telnet and RADIUS server and the IP route is available.
2. The IP address of the RADIUS server is 2.0.0.2/24, the authentication/authorization port is 1812, the statistics port is 1813, and the share key is admin.
3. When Telnet user logs into Device, it is required to authenticate/authorize and measure via the RADIUS server.
4. When the RADIUS server fails, use the local authentication and authorization.

Network Topology

Figure 6-3 Networking of configuring Telnet user login to use RADIUS authentication/authorization and accounting

Configuration Steps

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

Step 2: Configure Device.

#Configure the RADIUS server, the authentication port is 1812, the statistics port is 1813, and the share key is admin.

```
Device#configure terminal
Device(config)#aaa server group radius rg1
Device(config-sg-radius-rg1)#server 2.0.0.2 auth-port 1812 acct-port 1813 key admin
```

```
Device(config-sg-radius-rg1)#exit
```

#Configure AAA and use the RADIUS authentication/authorization and statistics.

Note:

- Authentication and authorization first use the first method in the method list; when the server fails, use the second method to authenticate and authorize.

```
Device(config)#domain test
Device(config-isp-test)#aaa authentication login radius-group rg1 local
Device(config-isp-test)#aaa authorization login radius-group rg1 local
Device(config-isp-test)#aaa accounting login start-stop radius-group rg1
Device(config-isp-test)#exit
```

#Configure the Telnet session and enable the RADIUS authentication/authorization and statistics.

```
Device(config)#line vty 0 15
Device(config-line)#login aaa test
Device(config-line)#exit
```

Step 3: Configure the RADIUS server.

For the interface setting of the RADIUS server, refer to the help document of the server. The following lists the main steps.

#Add the user admin on the RADIUS server, set the password as admin and configure the user label as 15.

#Set the IP address of the server as 2.0.0.2, share key as admin, authentication port as 1812 and statistics port as 1813.

#Set the IP address of the client as 2.0.0.1 and the share key as admin.

Step 4: Check the result, and verify the authentication/authorization and statistics.

#After Telnet user logs in to Device, authorize successfully, and use the **show privilege** command to view the user priority 15.

```
D:\>telnet 1.0.0.1
Connect to 1.0.0.1 ...done

User Access Verification


login:admin
password:
Device#show privilege
Current privilege level is 15
Device#
```

Figure 6-4Authorize the user priority as 15

#We can view the login and disconnection statistics information on the RADIUS server.

6.3.3. Configure Telnet User to Carry Different Domain Names to Log in and Use Different Authentication/Authorization/Accounting Methods

Network Requirements

1. Device is connected to the Telnet client and RADIUS server, and the IP route is reachable.
2. The IP address of the RADIUS server is 2.0.0.2/24, authentication/authorization port is 1812, accounting port is 1813, and the share key is admin.
3. The Telnet user logs into Device by carrying the domain name test1, requiring authentication/authorization and accounting by the RADIUS server.
4. The Telnet user logs into Device by carrying the domain name test2, requiring local authentication/authorization and accounting by the RADIUS server.

Network Topology

Figure 6-5 Networking of configuring Telnet user to carry different domain names to log in and use different authentication/authorization and accounting methods

Configuration Steps

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

Step 2: Configure Device.

#Configure the user name as admin1, password as admin2, and authorization level as 1.

```
Device#configure terminal
Device(config)#local-user admin1 class manager
Device(config-user-manager-admin1)#service-type telnet
Device(config-user-manager-admin1)#privilege 1
Device(config-user-manager-admin1)#password 0 admin2
Device(config-user-manager-admin1)#exit
```

#Configure the RADIUS server: the authentication port is 1812, statistics port is 1813, and the share key is admin.

```
Device#configure terminal
Device(config)#aaa server group radius rg1
Device(config-sg-radius-rg1)#server 2.0.0.2 auth-port 1812 acct-port 1813 key 0 admin
Device(config-sg-radius-rg1)#exit
```

#Configure the test1 domain, and use the RADIUS authentication/authorization and accounting.

```
Device(config)#domain test1
```

```
Device(config-isp-test1)#aaa authentication login radius-group rg1
Device(config-isp-test1)#aaa authorization login radius-group rg1
Device(config-isp-test1)#aaa accounting login start-stop radius-group rg1
Device(config-isp-test1)#exit
```

#Configure test2 domain, use the local authentication/authorization, and use the RADIUS accounting.

```
Device(config)#domain test2
Device(config-isp-test2)#aaa authentication login local
Device(config-isp-test2)#aaa authorization login local
Device(config-isp-test2)#aaa accounting login start-stop radius-group rg1
Device(config-isp-test2)#exit
```

#Configure the Telnet session, and enable multi-domain AAA scheme.

```
Device(config)#line vty 0 15
Device(config-line)#login aaa
Device(config-line)#exit
```

Note:

- In Line vty, configure login aaa, enable multi-domain AAA scheme; in Line vty, configure login aaa [default | domain-name], and enable the AAA scheme of the specified domain name.

Step 3: Configure the RADIUS server.

For the setting of the RADIUS server interface, refer to the help document of the server. The following lists the steps.

#On the RADIUS server, add user admin1, set the password as admin2, and configure the user level as 15.

#Set the IP address of the server as 2.0.0.2, the share key as admin, authentication port as 1812, and accounting port as 1813.

#Set the IP address of the client as 2.0.0.1, and share key as admin.

Step 4: Check the result, and verify the authentication/authorization and accounting.

#The Telnet user carries the domain name test1, that is, input the user name admin1@test1 and password admin2. After logging into Device and authorizing successfully, use the command **show privilege** to view the user priority 15.

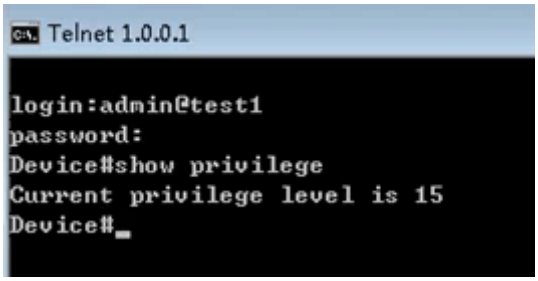


Figure 6-6 Authorize the user priority as 15

#You can query the login and disconnection accounting information on the RADIUS server.

#The Telnet user carries the domain name test2, that is, input the user name admin1@test2 and password admin2. After logging into Device and authorizing successfully, use the command **show privilege** to view the user priority 1.

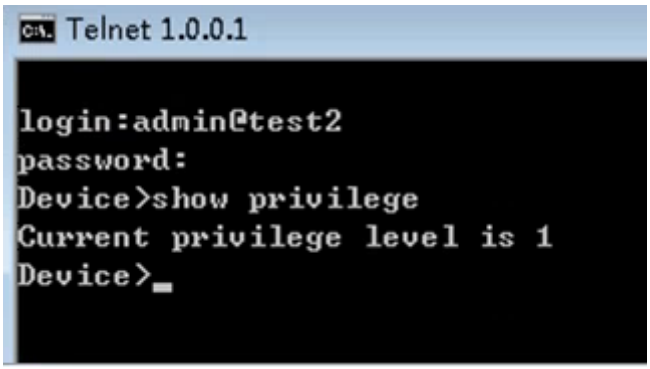


Figure 6-7 Authorize the user priority as 1

#You can query the login and disconnection accounting information on the RADIUS server.

6.3.4. Configure Telnet User Level Switching to Use RADIUS Authentication

Network Requirements

1. Device is connected to the Telnet and RADIUS server and the IP route is available.
2. The IP address of the RADIUS server is 2.0.0.2/24, the authentication/authorization port is 1812, and the share key is admin.
3. When the user level switches from 1 to 3 after Telnet user logs in to Device, it is required to authenticate via RADIUS server.

Network Topology

Figure 3-5 Networking of configuring Telnet user level switching to use RADIUS authentication

Configuration Steps

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

Step 2: Configure Device.

#Configure the RADIUS server, authentication port as 1812 and share key as admin.

```
Device(config)#aaa server group radius rg1
Device(config-sg-radius-rg1)#server 2.0.0.2 auth-port 1812 acct-port 1813 key 0 admin
Device(config-sg-radius-rg1)#exit
#Configure the user level switching to use the RADIUS authentication.
Device#configure terminal
Device(config)#aaa authentication enable-method radius-group rg1
```

Step 3: Configure the RADIUS server.

For the interface setting of the RADIUS server, refer to the help document of the server. The following lists the main steps.

#Add the user name $enab3$ with user level 3 and set the password as admin.

Note:

- User level switching is fixed to use the user name in the format of $enabLEVEL$ for authentication. LEVEL is the level that the user wants to switch to.
- When the user level is reduced, do not need authentication.

Step 4: Check the result.

After Telnet user inputs the user name and password to log in according to the prompt, the user level is 1 by default. After executing the command enable 3, input the password admin. After being authenticated by RADIUS server successfully, the user level is switched to 3.

```
Device>show privilege
Current privilege level is 1
Device>enable 3
password:
Device#show privilege
Current privilege level is 3
Device#
```

Figure 6–8 Switch Telnet user level from 1 to 3

6.3.5. Configure PPP User to Use RADIUS Authentication/Authorization/Accounting

Network Requirements

- Device2 is connected with the RADIUS server and connected to Device1 via the SDH network, and the IP route is reachable;
- The IP address of the RADIUS server is 2.0.0.2/24; the authentication/authorization port is 1812; the statistics port is 1813; the share key is admin;
- Device1 serves as the PPP client and authenticates, authorizes and gets the IP address via the RADIUS server when setting the PPP session connection with Device2;
- It is required that the setup and disconnection of the PPP session can be measured on the RADIUS server.

Network Topology

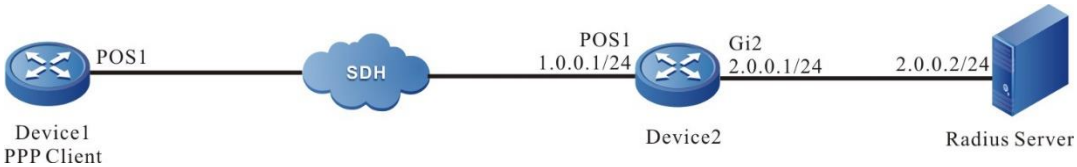


Figure 6-9 Networking of configuring the PPP user to use the RADIUS authentication/authorization and accounting

Configuration Steps

Step 1: Configure Device1.

#Configure the interface IP address as auto negotiation.

```
Device1#configure terminal
Device1(config)#interface pos1
Device1(config-if-pos1)#ip address negotiated
Device1(config-if-pos1)#exit
```

#Configure the interface encapsulation protocol as PPP, the authentication user name as admin, and password as admin.

```
Device1(config-if-pos1)#encapsulation ppp
Device1(config-if-pos1)#ppp chap hostname admin
Device1(config-if-pos1)#ppp chap password admin
Device1(config-if-pos1)#exit
```

Step 2: Configure Device2.

#Configure the RADIUS server: the authentication/authorization port is 1812; the accounting port is 1813 and the share key is admin.

```
Device2(config)#aaa server group radius rg
Device2(config-sg-radius-rg)#server 2.0.0.2 auth-port 1812 acct-port 1813 key admin
```

#Configure the PPP user to use the RADIUS authentication/authorization and accounting.

```
Device2(config)#domain test
Device2(config-isp-test)#aaa authentication ppp radius-group rg
Device2(config-isp-test)#aaa authorization ppp radius-group rg
Device2(config-isp-test)#aaa accounting ppp start-stop radius-group rg
Device2(config-isp-test)#exit
```

#Configure the interface IP address. (Omitted)

#Configure the encapsulation protocol of interface pos1 as PPP and provide the clock for the peer.

```
Device2(config)#interface pos1
Device2(config-if-pos1)#encapsulation ppp
Device2(config-if-pos1)#clock source internal
Device2(config-if-pos1)#exit
```

#Configure the interface pos1 to enable the RADIUS authentication/authorization and accounting.

```
Device2(config-if-pos1)#ppp authentication chap test
Device2(config-if-pos1)#exit
```

Step 3: Configure the RADIUS server.

For the interface setting of the RADIUS server, refer to the help document of the server. The following lists the main steps.

#Add the user name admin and the password is admin.

#Configure the IP address pool ppp-pool; the start and end IP addresses of the address pool are 1.0.0.2.

#Bind the IP address pool ppp-pool for the PPP user admin or the belonging user group.

Step 4: Check the result.

#View the protocol status as UP on Device1 and get the IP address 1.0.0.2/32.

```
Device1#show interface pos1
pos1:
    line protocol is up
    Flags: (0x80080f1) POINT-TO-POINT MULTICAST RUNNING
    Type: PPP
    Internet address: 1.0.0.2/32
    Destination Internet address: 1.0.0.1
    Metric: 0, MTU: 1500, BW: 155000 Kbps, DLY: 20000 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
    Last clearing of "show interface" counters never
    input peak rate 575 bits/sec,  1 hour 21 minutes 47 seconds ago
    output peak rate 188 bits/sec,  0 hour 3 minutes 26 seconds ago
    5 minutes input rate 22 bits/sec, 0 packet/sec
    5 minutes output rate 15 bits/sec, 0 packet/sec
    5116 packets received; 1892 packets sent
    0 multicast packets received
    0 multicast packets sent
    0 input errors; 0 output errors
    0 collisions; 0 dropped
     LCP:OPENED
     IPCP:OPENED   NDSPCP:OPENED
     encap-type: simply PPP
     rxFrames: 533634, rxChars 22001403
     txFrames: 530195, txChars 21737969
     rxNoOctet 0, rxAbtErrs 0, rxCrcErrs 0
     rxOverrun 0, rxLenErrs 0, txUnderrun 0
     DCD: UP
```

#On the RADIUS server, we can see the statistics information after the PPP session is set up and disconnected.

6.3.6. Configure TACACS Authorization and Statistics of Shell Command

Network Requirements

1. Device is connected to the Telnet and RADIUS server and the IP route is available.
2. The IP address of the RADIUS server is 2.0.0.2/24, the service port is 49, and the share key is admin.
3. After Telnet client logs in to Device, the operated shell command with user level 15 is required to be authorized via TACACS server and record the shell command to the TACACS server.

Network Topology

Figure 6–10 Networking of configuring the TACACS authorization and accounting of the Shell command

Configuration Steps

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

Step 2: Configure Device.

#Configure the TACACS server, the service port is 49, and the share key is admin.

```
Device(config)#aaa server group tacacs-group tg1
Device(config-sg-tacacs-tg1)#server 2.0.0.2 port 49 key 0 admin
Device(config-sg-tacacs-tg1)#exit
```

#Configure the TACACS command authorization and accounting.

```
Device#configure terminal
Device(config)#aaa authorization config-commands
Device(config)#domain test
Device(config-isp-test)#aaa authentication login tacacs-group tg1
Device(config-isp-test)#aaa authorization commands 15 tacacs-group tg1
Device(config-isp-test)#aaa accounting commands 15 tacacs-group tg1
Device(config-isp-test)#exit
```

#Configure the Telnet session and enable the TACACS authorization and accounting.

```
Device(config)#line vty 0 15
Device(config-line)#login aaa test
Device(config-line)#exit
```

Note:

- Before authorization and accounting, the authentication should be successful.

Step 3: Configure the TACACS server.

For the interface setting of the TACACS server, refer to the help document of the server. The following lists the main steps.

#Add the client 2.0.0.1 on the server, the share key is admin, and select “TACACS+(Cisco IOS)” authentication.

#Set the Shell command authorization for Telnet user admin. Permit the commands **configure terminal**, **router ospf** and **router rip**, and refuse the other commands.

Step 4: Check the result.

#After Telnet user logs in to Device, execute the Shell command. The authorized command can be executed successfully and the un-authorized command authorization failed.

```
Device#configure terminal
% Enter configuration commands, one per line.  End with CNTL+Z.
Device(config)#router ospf 100
Device(config-ospf)#exit
Device(config)#router rip
Device(config-rip)#exit
Device(config)#interface fastethernet 1
Command authorization failed
Device(config)#router bgp 100
Command authorization failed
```

#View the Shell command statistics information.

On the TACACS server, we can see the statistics information of the Shell command.

6.3.7. Configure RADIUS Server Group Service

Network Requirements

- Device is connected to the Telnet and RADIUS server and the IP route is available.
- The IP address of RADIUS 1 server is 2.0.0.2/24, the IP address of RADIUS 2 server is 2.0.0.3/24, the authentication/authorization port is 1812; the accounting port is 1813 and the share key is admin.
- The PPP user is connected to Device2 via the SDH network. When setting up the PPP connection, it is required to perform the authentication/authorization and accounting via the RADIUS 1 server; when the Telnet user logs into Device2, it is required to perform the authentication/authorization and accounting via the RADIUS 2 server.

Network Topology

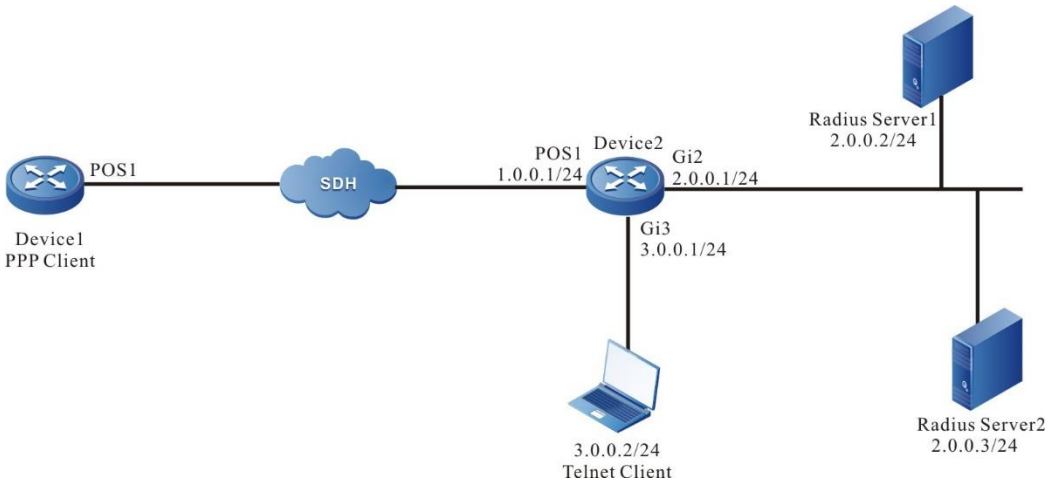


Figure 6-11 Networking of configuring the RADIUS server group service

Configuration Steps

Step 1: Configure the IP address of the device interface and the related parameters.

#Configure the IP address of Device1 interface pos1 as auto negotiation.

```
Device1#configure terminal
Device1(config)#interface pos1
Device1(config-if-pos1)#ip address negotiated
Device1(config-if-pos1)#exit
```

#Configure the encapsulation protocol and chap authentication of Device1 interface pos1.

```
Device1(config-if-pos1)#encapsulation ppp
Device1(config-if-pos1)#ppp chap hostname admin
Device1(config-if-pos1)#ppp chap password admin
Device1(config-if-pos10)#exit
```

#Configure the interface IP address of Device2 (omitted).

#Configure the encapsulation protocol of Device 2 interface pos1 as ppp.

```
Device2#configure terminal
Device2(config)#interface pos1
Device2(config-if-pos1)#encapsulation ppp
Device2(config-if-pos1)#clock source internal
Device2(config-if-pos1)#exit
```

Step 2: Configure the RADIUS commands on Device2.

#Configure the RADIUS server RADIUS 1 and RADIUS 2; the authentication port is 1812; the accounting port is 1813; the share key is admin. RADIUS 1 belongs to the “aaa-ppp” server group and RADIUS 2 belongs to “aaa-telnet” server group.

```
Device2(config)#aaa server group radius aaa-ppp
```

```
Device2(config-sg-radius-rg)#server 2.0.0.2 auth-port 1812 acct-port 1813 key 0
admin
Device2(config-sg-radius-rg)#exit
Device2(config)#aaa server group radius aaa-telnet
Device2(config-sg-radius-rg)#server 2.0.0.3 auth-port 1812 acct-port 1813 key 0
admin
Device2(config-sg-radius-rg)#exit
```

#Configure the method of the PPP authentication/authorization and accounting.

```
Device2(config)#domain ppp
Device2(config-isp-test)#aaa authentication ppp radius-group aaa-ppp
Device2(config-isp-test)#aaa authorization ppp radius-group aaa-ppp
Device2(config-isp-test)#aaa accounting ppp start-stop radius-group aaa-ppp
Device2(config-isp-test)#exit
```

#Configure the method of the Telnet authentication/authorization and accounting.

```
Device2(config)#domain telnet
Device2(config-isp-system)#aaa authentication login radius-group aaa-telnet
Device2(config-isp-system)#aaa authorization login radius-group aaa-telnet
Device2(config-isp-system)#aaa accounting login start-stop radius-group aaa-
telnet
Device2(config-isp-system)#exit
```

Step 3: Configure the PPP session and Telnet login to enable the RADIUS authentication/authorization, accounting.

#Configure the PPP session to use the “aaa-ppp” server group for authentication/authorization/accounting.

```
Device2(config)#interface 10
Device2(config-if-pos1)#ppp authentication chap ppp
Device2(config-if-pos1)#exit
```

#Configure Telnet login to use the “aaa-telnet” server group for authentication/authorization/accounting.

```
Device2(config)#line vty 0 15
Device2(config-line)#login
Device2(config-line)#exit
```

Step 4: Check the result.

#When the PPP user initiates the PPP connection to Device2, perform the authentication/authorization and accounting via the server RADIUS 1. We can view the accounting information on RADIUS1.

#When the Telnet user initiates the PPP connection to Device2, perform the authentication/authorization and accounting via the server RADIUS 2. We can view the accounting information on RADIUS2.

7. 802.1X

7.1. Overview

7.1.1. 802.1X

802.1X is a broadband access authentication solution put forward by IEEE in June, 2001. It defines the Port-Based Network Access Control. By utilizing LAN's physical access features of IEEE 802 LAN, 802.1X provides a set of methods for authenticating and authorizing devices access connected to LAN ports via point-to-point.

The 802.1X system is the typical client/server structure, as shown in the following figure, including three entities: Supplicant system (client), Authentication system (authentication device), and Authentication server system (authentication server).

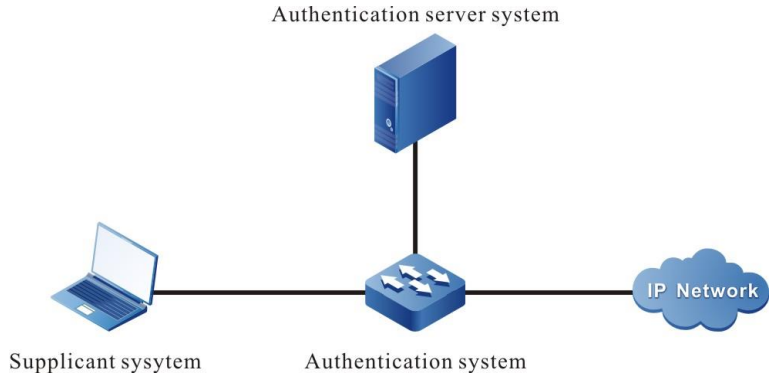


Figure 7-1 802.1X system architecture

- The client installation supports the client software of the 802.1X authentication, sending the authentication request to the authentication device. If authenticating successfully, connect to the network normally.
- The authentication device is between the client and the authentication server, controlling the network access of the client by interacting with the server.
- Usually, the authentication server is the RADIUS (Remote Authentication Dial-In User Service) server, used to verify the validity of the client and inform the authentication result to the authentication device. The authentication device controls the network access of the client according to the authentication result.

EAP (Extensible Authentication Protocol) used by the 802.1X authentication is one general protocol of the PPP authentication, used to interact the authentication information among the client, authentication device and authentication server. The 802.1X protocol uses EAPOL (EAP Over LAN) frame encapsulation format to encapsulate the EAP packet, realizing the interacting between the client and the authentication device. According to the different application scenarios, the 802.1X protocol encapsulates the EAP packet in the different frame formats, realizing the interacting between the authentication device and the authentication server. In the relay authentication mode, the EAP packet is encapsulated in the EAPOR (EAP Over RADIUS) frame format; in the terminating authentication mode, the EAP packet is encapsulated in the standard RADIUS frame format.

The 802.1X authentication mode includes relay authentication mode and terminating authentication mode.

The relay authentication flow is as follows:

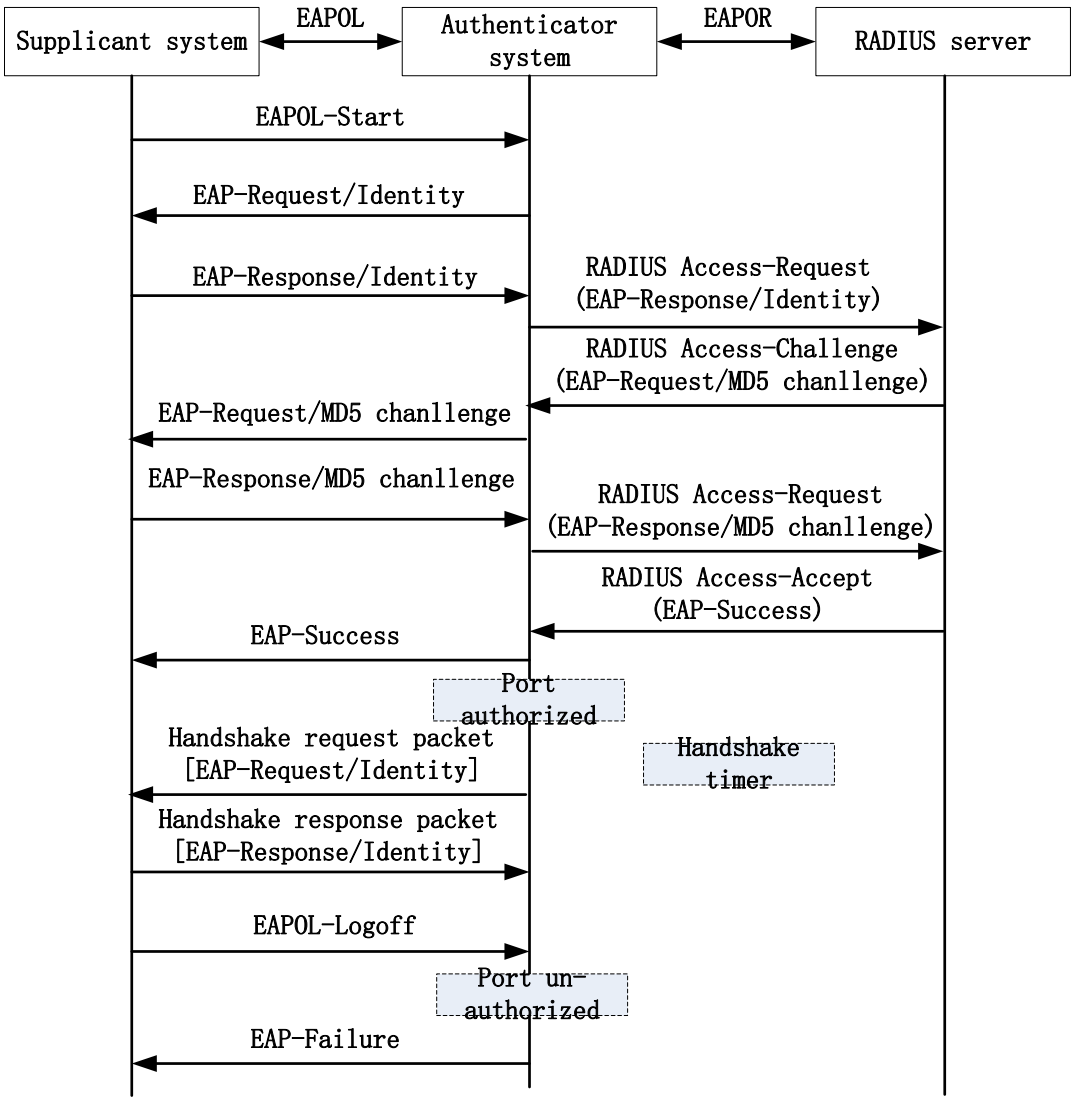


Figure 7–2 802.1X relay authentication flow

The relay authentication flow is as follows:

- When the user has the network access requirement, enable the 802.1X client program, input the valid user name and password registered on the authentication server, and initiate the authentication request (EAPOL-Start packet). Here, the client program sends the request authentication packet to the authentication device and starts one authentication process.
- After the authentication device receives the data frame of requesting authentication, send one request frame (EAP-Request/Identity packet) to request the user client program to send the input user name.
- The client program answers the request sent by the authentication device, sending the user name information to the authentication device via the data frame (EAP-Response/Identity packet). The authentication device encapsulates the data frame sent by the client in the packet (RADIUS Access-Request packet) and sends to the authentication server for processing.

- After the RADIUS server receives the user name information forwarded by the authentication device, compare the information with the user name table in the database, find the corresponding information of the user name, and use one randomly-generated encrypting word to encrypt it. Meanwhile, send the encrypted word to the authentication device via the RADIUS Access-Challenge packet; the authentication device forwards it to the client program.
- After the client program receives the encrypted word forwarded by the authentication device (EAP-Request/MD5 Challenge packet), use the encrypted word to encrypt the password (the encryption algorithm is irreversible, generating the EAP-Response/MD5 Challenge packet), and forward to the authentication server via the authentication device.
- RADIUS authentication server compares the received encrypted password information (RADIUS Access-Request packet) with the local encrypted password information. If they are the same, regard the user as valid user and feed back the message of passing the authentication (RADIUS Access-Accept packet and EAP-Success packet);
- After the authentication device receives the message of passing the authentication, change the port to the authorized state, permitting the user to access the network via the port.
- The client also can send the EAPOL-Logoff packet to the authentication device, actively requesting offline. The authentication device changes the port status from authorized to un-authorized, and sends the EAP-Failure packet to the client.

The authentication needs the authentication device and authentication server to support the EAP protocol.

The terminating authentication flow is as follows:

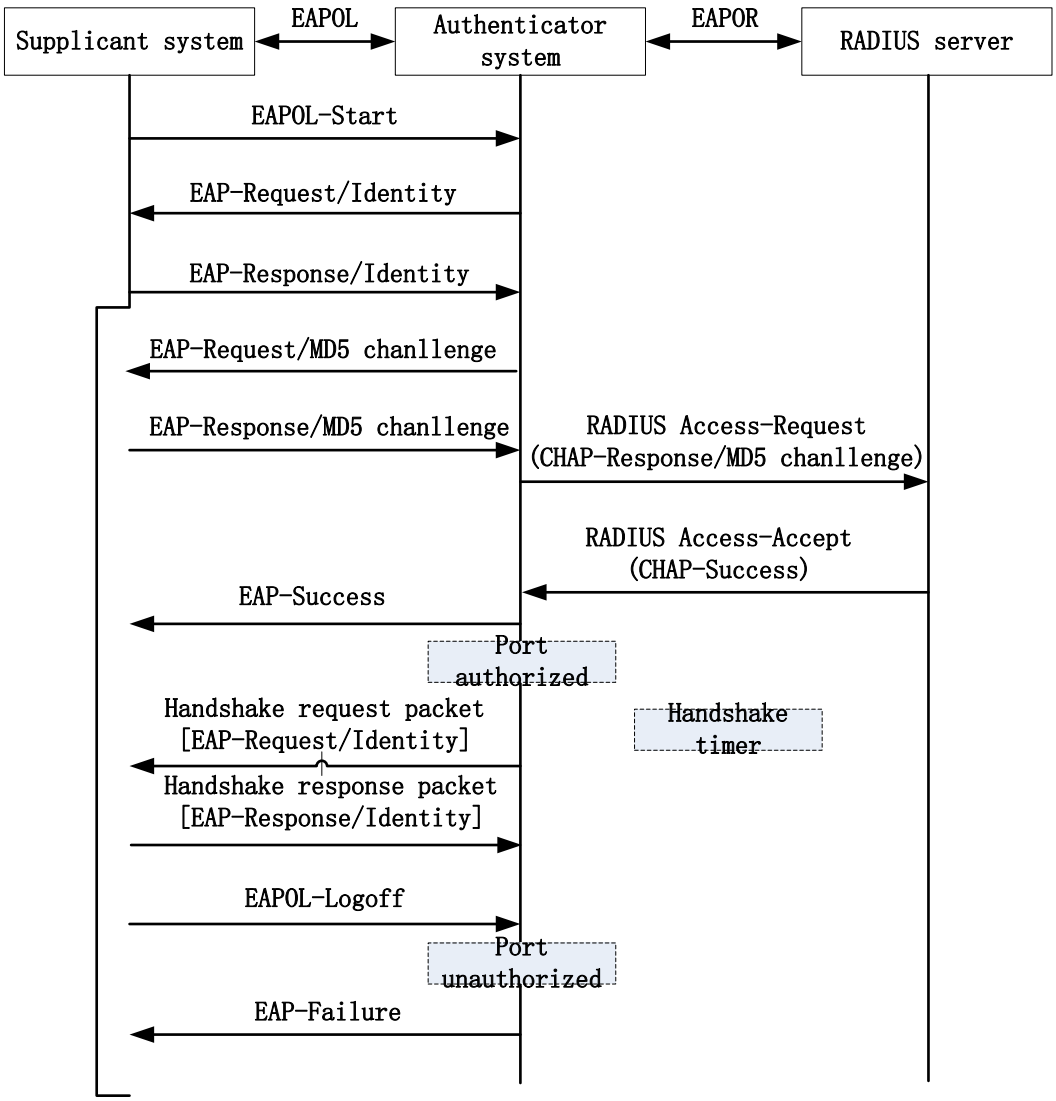


Figure 7-3 802.1X terminating authentication flow

- The difference between the terminating authentication mode and relay authentication mode is: The random encrypting word used to encrypt the user password information is generated by the authentication device. And the authentication device sends the user name, random-encrypting word and password information encrypted by the client to the RADIUS server for authentication.

The terminating authentication mode is used by the authentication server that is deployed earlier and does not support the EAP protocol.

The authentication device supports two access control modes:

- Port-based access control mode (Portbased): After the first user in the port is authenticated successfully, the other access users can access the network without authentication, but after the first user gets offline, the other users also are refused to access the network.

- User-based access control mode (Macbased): All access users in the port need to be authenticated separately. After one user gets offline, only the user cannot access the network and the other users still can access the network.

Auto VLAN is also called Assigned VLAN. When the client passes the server authentication, the server delivers the authorized VLAN information to the authentication device. If the delivered VLAN exists on the authentication device and is valid, the authentication port is added to the delivered VLAN. After the client gets offline, the port restores to the un-authorized state. The port is deleted from the Auto VLAN and the default VLAN of the port restores to the previous configured VLAN.

After enabling Guest VLAN, the user also can and only can access the resources in the VLAN without authentication. After the user is authenticated successfully, the port leaves Guest VLAN and the user can access other network resources. Usually, the user can get the 802.1X client software in Guest VLAN to upgrade the client, or execute other application program (such as anti-virus software, operation system patch) upgrade. After enabling the 802.1X authentication and configuring Guest VLAN correctly, the port is added to Guest VLAN in Untagged mode. Here, the user in the port of Guest VLAN initiates authentication. If the authentication fails, the port is still in Guest VLAN; if the authentication succeeded, there are two cases:

- If the authentication server delivers one VLAN, the port leaves Guest VLAN and is added to the delivered VLAN. After the user gets offline, the port returns to Guest VLAN.
- If the authentication server does not deliver VLAN, the port leaves Guest VLAN and is added to the configured Config VLAN in the authentication device. After the user gets offline, the port returns to Guest VLAN.

7.1.2. Secure Channel Authentication

Based on the 802.1X authentication function, the secure channel authentication function can achieve both the 802.1X authentication and pioneer a secure channel for the specified end users. Thus, the end user can visit the resources in the specified network in the unauthentication mode or specify an end user to visit the network resources without authentication.

7.1.3. MAC Address Authentication

In the actual network, besides lots of terminal users, there may be some network terminals (such as network printer). The terminals do not carry or cannot install the 802.1X authentication client software and can use the free-client authentication mode to access the network. The authentication method does not need the user to install any 802.1X authentication client software. After the authentication device detects the MAC address of the user for the first time, the authentication device uses the configured user name and password or the user MAC address as the user name and password to send to the authentication server for authentication.

The user name and password format used by the MAC address authentication has two cases:

The MAC address serves as user name and password: Use the MAC address of the authenticated user as the user name and password;

Fixed user name and password: Use the configured user name and password on the authentication device.

7.2. 802.1X Function Configuration

Table 7–1 802.1X function configuration list

Configuration Task	
Configure the 802.1X authentication	Enable the 802.1X authentication
Configure the secure channel authentication	Enable the secure channel authentication function
	Configure and apply the secure channel
Configure the 802.1X authentication and secure channel authentication	Configure the port authentication mode
	Configure the multicast triggering function
	Configure the re-authentication function
	Configure the maximum authentication failure times of the port
	Configure the function of omitting the IP field function in the user name
	Configure the packet transparent-transmission function
	Configure the keepalive function
	Configure the EAPOU function
	Configure the function of not waiting for the server response
	Configure the domain name delimiter
	Configure the format of the authentication user name

Configuration Task	
Configure the MAC address authentication	Enable the MAC address authentication function
	Configure the MAC address authentication user name format
Configure the public attributes	Configure the controlled direction
	Configure the authenticatable host list
	Configure the IP authorization function
	Configure the maximum sending times of the authentication request packet
	Configure the maximum sending times of the authentication packet
	Configure the authentication failure recording log function
	Configure the ARP keepalive function
	Configure the maximum users of the port
	Configure the IP ACL prefix name
	Configure the default valid VLAN
	Configure the unauthenticated user to communicate in the VLAN which the PVID locates in
	Configure the port access control mode
	Configure Guest VLAN
	Configure Guest ACL
	Configure Critical VLAN
	Configure the timer parameters
	Restore the default configuration of the port
	Configure the MAB function

7.2.1. Configure 802.1X Authentication Function

The 802.1X authentication and the MAC address authentication are allowed to be configured simultaneously on the same interface.

- If the authentication is successful when the end user first performs the MAC address authentication, the 802.1X authentication initiated by the end user will not be processed. Otherwise, the 802.1X authentication initiated by the end user will be processed normally.
- When the end user first initiates the 802.1X authentication, do not perform the MAC address authentication any more.

Configuration Condition

None

Enable 802.1X Authentication

To enable the 802.1X authentication function, the terminal user needs to install the client software with the 802.1X authentication function.

When configuring the 802.1X authentication parameters in the authentication device port and if the port does not enable the 802.1X authentication function, the configured function cannot take effect.

Table 7–2 Enable 802.1X

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable the global 802.1X authentication	**dot1x { enable | disable }**	Optional By default, the global 802.1X authentication function is enabled.
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Enable the 802.1X authentication	**dot1x port-control** { **enable** | **disable** }	Mandatory By default, the 802.1X authentication function in the port is disabled.

Note:

- Do not enable the 802.1X authentication function and secure cahnnel authentication function simultaneously on one interface.
- The 802.1X authentication function and port security function can be enabled on one port at the same time, but it has the following restriction: The port cannot be configured with the IP rule and MAX rule of the port security.

7.2.2. Configure Secure Channel Authentication

Configuration Condition

None

Enable Secure Channel Authentication

Based on the 802.1X authentication function, the secure channel authentication function can achieve both the 802.1X authentication and pioneer a secure channel for the specified end users. Thus, the end user can visit the resources in the specified network in the unauthentication mode or specify an end user to visit the network resources without authentication.

Table 7–3 Enable the secure channel authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration can only take effect on the current interface. After entering the aggregation group configuration mode, the subsequent configuration can only take effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Enable the secure channel authentication	**dot1x free-ip**	Mandatory By default, the secure channel authentication function under the interface is disabled.

Note:

- Do not enable the secure channel authentication function and port security function simultaneously on one interface.
- Do not enable the 802.1X authentication function and secure channel authentication function simultaneously on one interface.
- Do not enable the MAC address authentication function and the secure channel authentication function simultaneously on one interface.
- When the secure channel authentication function is enabled under the interface but the secure channel rule is not applied or the secure channle rule is not configured, the secure channel authentication function adn the 802.1X authentication function is identical.

During the secure channel authentication, when the user authentication succeeds, it will occupy the chip resources. If the chip resources are insufficient, it will cause user authentication failure.

Configure and Apply Secure Channel

After the secure channel authentication is enabled under the interface, it is hoped that the end user can visit the resources in the specified network when the end user is not authenticated or specify an end user to visit the network resources without authentication. In this case, configure and apply the secure channel.

Rules for configuring the secure channel can be classified into the following types:

- Configure to allow the end user to visit the specified network resources.
- Configure the specified end user to visit the network resources.

Table 7-4 Apply secure channel

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the secure channel	**hybrid access-list advanced** { *access-list-number* | *access-list-name* }	Mandatory By default, the secure channel is not configured on the device.

Step	Command	Description
Configure the secure channel rule	[*sequence*] **permit** *protocol* { **any** | *source-ip-addr source-wildcard* | **host** *source-ip-addr* } { **any** | *source-mac-addr source-wildcard* | **host** *source-mac-addr* } { **any** | *destination-ip-addr destination-wildcard* | **host** *destination-ip-addr* } { **any** | *destination-mac-addr destination-wildcard* | **host** *destination-mac-addr* }	Mandatory By default, the secure channel rule is not configured in the secure channel.
Apply the secure channel	**global security access-group** { *access-group-number* | *access-group-name* }	Mandatory By default, no any secure channel is applied in the system.

Note:

- The device can be configured with multiple secure channels. A secure channel can be configured with multiple secure channel rules.
- The secure channel type can only be the hybrid advanced ACL. Only one secure channel is allowed to be applied to the device.

7.2.3. Configure 802.1X Authentication and Secure Channel Authentication Property

If the 802.1X authentication function or the secure channel authentication function is not enabled on the interface, then the conifgured related property does not take effect.

Configuration Condition

None

Configure Port Authentication Mode

802.1X authentication mode includes relay authentication mode and terminating authentication mode.

802.1X authentication system comprises client, authentication device and authentication server. The standard 802.1X protocol defines that the client and authentication server interact via the EAP packet. The authentication device plays as the “relay” role during the interacting. The authentication device encapsulates the EAP data sent by the client in the other protocol, such as the RADIUS protocol, and send to the authentication server. Similarly, the authentication device encapsulates the EAP data sent by the authentication server in the EAPOL packet and forwards to the client. The interacting mode is called relay authentication mode. The relay authentication mode requires that the authentication server supports the EAP protocol. Configuring the

authentication mechanism supported by the EAP relay authentication mode depends on the client and authentication server.

The earlier deployed authentication server may not support the EAP protocol and needs to be configured as the terminating authentication mode. The EAP packet of the client is not directly sent to the authentication server, but the authentication device completes the EAP packet interacting with the client. After getting the enough user authentication information, the authentication device sends the authentication information to the authentication server for authentication.

EAP terminating authentication mode supports PAP (Password Authentication Protocol) authentication and CHAP (Challenge Handshake Authentication Protocol) authentication.

Table 7-5 Configure the port authentication mode

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the port authentication mode	**dot1x eap-relay** { **enable** | **disable** }	Mandatory By default, the authentication mode in the port is the terminating authentication mode.

Note:

- Configuring terminating authentication mode only supports the MD5-based (Message Digest Algorithm) EAP authentication. The 802.1x authentication function and secure channel authentication function support the relay and terminating authentication mode.
- When the client adopts the certificate authentication, the authentication port needs to be configured as the relay authentication mode.
- The MAC address authentication can only support the terminating authentication mode.

Configure Multicast Triggering Function

Some terminal is installed with the 802.1X authentication client, but the client does not actively initiates the authentication. The authentication process can only depend on the authentication device to trigger. The authentication device periodically sends the multicast packet requesting the user name to the port configured with the multicast triggering. After receiving the packet, the client answers the authentication request of the authentication device and starts the 802.1X authentication.

Table 7–6 Configure the multicast triggering function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the 802.1X multicast trigger	**dot1x multicast-trigger**	Mandatory By default, the multicast trigger function in the port is disabled.
Configure the multicast triggering period	**dot1x multicast-period** *multicast-period-value*	Optional By default, the multicast trigger time in the port is 15s.

Note:

- If the client does not support the multicast trigger function, the adapter display of the client may be abnormal. Meanwhile, it may cause the re-authentication failure.

Configure Re-authentication Function

To check whether the client is online, avoid the abnormal crashing of the client affecting the correctness of the user accounting, and prevent the client from being used by others, the

authentication device periodically initiates the re-authentication request to the client. During the process, the user does not need to input the user name or password again.

Table 7-7 Configure the re-authentication function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the 802.1X re-authentication	**dot1x reauthentication**	Mandatory By default, the re-authentication function is enabled in the port.

Configure Maximum Authentication Failure Times of the Port

After the client authentication failure times reaches the threshold, the client enters the dead state. During the dead time, the authentication device does not answer the authentication request initiated by the client any more.

Table 7–8 Configure the maximum authentication failure times

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation link-aggregation-id**	
Configure the maximum port authentication failure times	**dot1x max-authfail** *max-authfail-value*	Mandatory By default, the maximum authentication failure times of the port is 1.

Configure to Omit IP Field in User Name

Some 802.1X authentication clients can configure to upload the IP address property and load the IP address before the user name and then send them to the server for authentication. When the IP address of the end user contains 0, for example, the user IP address 192.168.0.1, it may cause authentication failure. In this case, you can configure to omit the IP field in the user name to avoid such problem. After this function is configured, when the user name in the authentication packet carries the IP address which contains 0, the device will omit the IP address contained in the user name of the packet to ensure normal authentication.

Table 7-9 Configure to omit the IP filed in the user name

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure to omit the IP field in the user name	**dot1x ignore user-name-ip**	Mandatory By default, the function of omitting the IP field in the user name is disabled.

Configure Packet Transparent Transmission Function

In the actual application environment, the authentication terminal and authentication device may cross the intermediate device. If the intermediate device cannot transmit the EAPOL packet transparently, the authentication cannot be performed normally. To make the authentication be done normally, we need to enable the function of transmitting the EAPOL packet transparently on the port of the intermediate device receiving the EAPOL packet and configure one uplink port for the port. If the port enabled with the function of transmitting the EAPOL packet transparently receives the EAPOL packet, send the packet from the configured uplink port. If the device directly connected to the uplink port is authentication device, the authentication device processes after receiving the EAPOL packet.

Table 7–10 Configure the packet transparent transmission function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Configure the packet transparent transmission function	**dot1x eapol-relay** { **enable** | **disble** }	Mandatory By default, the function of transmitting the packet transparently in the port is disabled.

Note:

- The uplink port does not support forwarding the received multicast packet to the other ports, so the multicast packet entering from the uplink port does not trigger the 802.1X client software on other ports, but can only initiate the authentication request via the client software to start the 802.1X authentication.

Configure Keepalive Function

To detect whether the client is online, the authentication device periodically sends the EAP-Request/Identity packet to the client. If receiving the EAP-Response/Identity packet from the client, send the EAP-Request/MD5 Challenge packet to the client. If the authentication system receives the EAP-Response/MD5 Challenge packet, confirm that the client is online normally and send the EAP-Success packet to inform the client of keepalive success.

Table 7–11 Configure the keepalive function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Configure the keepalive function	**dot1x keepalive** { **enable** | **disable** }	Mandatory By default, the keepalive function in the port is disabled.
Configure the keepalive time	**dot1x keepalive period** *period-value*	Optional By default, the keepalive period in the port is 60s.
Configure the times of re-transmitting the keepalive packet	**dot1x keepalive retries** *retries-value*	Optional By default, the maximum keepalive times in the port is 3.

Note:

- The keepalive function needs to be supported by the 802.1X authentication client software (such as Maipu TC client). If the client does not support, it may result in the keepalive failure and the user gets offline.

Configure EAPOU Function

EAPOU is the EAP Over UDP protocol. In the standard 802.1X function, the client and authentication device interact with each other via the EAPOL (EAP Over LAN) packet. In the actual application environment, because of the network complexity, the terminal to be authenticated (client) and the authentication device may cross the intermediate device. If the intermediate device does not transmit the EAPOL packet transparently, the authentication cannot be performed normally. Enabling the EAPOU function can make the authentication packet (EAP packet) cross the intermediate device, the EAPOU packet is not limited by the intermediate device, and the intermediate device forwards the packet as the general packet, realizing the across-device authentication.

To enable the EAPOU function, we need to configure one interface address on the authentication device, used to receive the EAPOU packet sent by the client. Before sending the EAPOU packet, the client needs to specify the interface address of the authentication device so that the EAPOU packet can be forwarded to the authentication device correctly; after the authentication device receives the EAPOU packet, extract the EAP content from the packet, and then encapsulate as the EAPOR packet and send to the authentication server for authentication. The subsequent process is consistent with the EAPOL authentication mode.

Table 7-12 Configure the EAPOU function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the EAPOU function	**dot1x eapou layer2**	Mandatory By default, the EAPOU function in the port is disabled.
Configure the UDP port used by the EAPOU function	**dot1x eapou udp-port** *udp-port-value*	Optional By default, the UDP protocol port number used by the EAPOU function is 5651.

Note:

- To configure the EAPOU function, both the client and authentication device need to support the EAPOU protocol.

Configure Not Waiting for Server Response

In the relay authentication mode, the client may send some packets that the server does not answer. The packets make the session channel between the authentication device and the authentication server be occupied and as a result, the subsequent client authentication fails. We can enable the function of not waiting for the server response in the port to avoid the problem.

Table 7-13 Configure the function of not waiting for the server response

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the function of not waiting for the server response	**dot1x nowait-result**	Mandatory By default, the function of not waiting for the server response is disabled.

Configure Domain Name Delimiter

The authentication device can manage the user based on the domain. If the authentication user name carries the domain name, the device uses the server in the AAA server group to authenticate, authorize and account the user. If the authentication user name does not carry the domain name, use the default configured authentication server in the system to authenticate. Therefore, the authentication device needs to parse the user name and domain name correctly, playing the decisive function for the user to provide the authentication service. Different clients support different user name and domain name delimiters. To manage and control the user access of different user name formats better, it is necessary to specify the supported domain name delimiter on the authentication device.

Currently, the supported domain name delimiters include @, /, and \.

When the domain name delimiter is @, the authenticated user name format is username@domain.

When the domain name delimiter is /, the authenticated user name format is username/domain.

When the domain name delimiter is \, the authenticated user name format is domain\username.

Here, username is the pure user name, and domain is the domain name. If the user name contains multiple domain name delimiters, the authentication device only identifies the first domain name delimiter as the actual used domain name delimiter and the other characters as one part of the domain name.

Table 7-14 Configure the domain name delimiter

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the domain name delimiter	**dot1x domain-delimiter** *domain-delimiter-type*	Mandatory By default, the domain name delimiter in the port is @.

Note:

- When using the user name with the domain name to authenticate, it is necessary to configure the corresponding authentication server group on the authentication device.

Configure Authentication User Name Format

The authentication user is named by the format of username@domain. The domain name is behind the domain name delimiter @. The authentication device decides which authentication server group authenticates the user by parsing the domain name. The early server cannot accept the user name with the domain name, so the authentication device needs to delete the domain name carried in the user name and just send the authentication user name to the server. You can select whether the authentication user name sent to the authentication device carries the domain name by configuring the format of the authentication user name.

Currently, the supported domain name delimiter includes @, \, /.

Table 7-15 Configure the authentication user name format

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the format of the authentication user name	**dot1x user-name-format** { with-domain | without-domain }	Mandatory By default, send the authentication user name with the domain name to the authentication server.

Note:

- Configure the port of sending the authentication user name without domain name to the authentication server not to support the certificate authentication.

Configure MAC Address Authentication

The 802.1X authentication and MAC address authentication are allowed to be configured simultaneously on the same interface.

- If the authentication is successful when the end user first performs the MAC address authentication, the 802.1X authentication initiated by the end user will not be processed. Otherwise, the 802.1X authentication initiated by the end user will be processed normally.
- When the end user first initiates the 802.1X authentication, then do not perform the MAC address authentication any more.

Configuration Condition

None

Enable MAC Address Authentication Function

The MAC address authentication is also called free-client authentication. The authentication mode is applicable to the terminal that cannot install the client software for authentication, and

also applicable to the terminal user that does not install client software, but can authenticate without inputting the user name and password.

When configuring the parameters of the MAC address authentication in the authentication device port and if the port does not enable the MAC address authentication function, the configured function does not take effect.

Table 7-16 Enable the MAC address authentication function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the MAC address authentication function	**dot1x mac-authentication** { **enable** | **disable** }	Mandatory By default, the MAC address authentication function in the port is disabled.

Note:

- The MAC address authentication function and port security function can be enabled on one port at the same time, but it has the following restriction: The port cannot be configured with the IP rule and MAX rule of the port security.
- Do not enable the MAC address authentication function and secure cahnnel authentication function simultaneously on one interface.

Configure MAC Address Authentication User Name Format

The user name and password format used by the MAC address authentication includes two cases: fixed user name and password format and MAC address user name and password format.

Fixed user name and password format: When receiving the packets of the terminal user, the authentication device sends the configured user name and password to the authentication server for authentication.

MAC address user name and password format: The authentication device takes the MAC address of the terminal user as the user name and password. The MAC address format as the user name and password includes two cases: One is with the hyphen, such as 00-01-7a-00-00-01; the other is not with hyphen, such as 00017a000001.

Table 7–17 Configure the MAC address authentication user name format

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the MAC address authentication user name format	**dot1x mac-authentication user-name-format** { **fixed account** *account-value* **password** *password-value* | **mac-address** [**with-hyphen** | **without-hyphen**] }	Mandatory By default, the MAC address authentication adopts the MAC address with hyphen as the user name and password.

7.2.4. Configure Public Attributes

When configuring the public attribute parameters and if the 802.1X authentication function, secure channel authentication, or MAC address authentication function is not enabled in the port, the configured function does not take effect.

Configuration Condition

When configuring the IP authorization function in the port, it is necessary to configure the ARP keepalive function at the same time.

Configure Control Direction

The control direction of the port includes the bi-directional control and uni-directional control.

- Bi-directional control indicates that the port cannot receive or send the packet.

- Uni-directional control indicates that the port cannot receive the packet of the client, but can forward the packet to the client.

The function can be used with the WOL (Wake On Lan) function. Some terminal is in the dormant state, but its network card still can process some special packets, such as WOL packet. After the network card receives the WOL packet, enable the terminal device and enter the working state.

When the access port of the dormant terminal enables the authentication function, you can configure the port as the uni-directional control, ensuring that it can normally send the WOL packet to the terminal. After the terminal starts, initiate the authentication, and after passing the authentication, it can access the network resources normally.

When sending the WOL packet across the segment, it is necessary to configure the ARP forwarding entry on the authentication device.

Table 7–18 Configure the control direction

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Configure the control direction	**dot1x control-direction** { **both** | **in** }	Mandatory By default, the port is controlled bi-directionally.

Configure Authenticatable Host List

After enabling the authenticatable host list function, only permit the user whose MAC address is in the authenticatable host list to authenticate and the authentication initiated by other user is refused.

Table 7–19 Configure the authenticatable host list

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the authenticatable host list	**dot1x auth-address** { **enable | disable |** *mac-address* }	Mandatory By default, the authenticatable host list in the port is disabled.

Configure IP Authorization Function

In the port, enable the IP authorization function. If it is detected that the IP address of the authenticated user changes, force the user to get offline. It can be divided to the following several modes:

Disable: In the mode, do not detect the IP address of the user.

dhcp-server: When configuring the mode, it is necessary to configure the DHCP Snooping function on the device. After the authenticated user gets the IP address from the DHCP server, record the binding relation of the authenticated user and IP address on the device. If it is detected that the user IP address changes, force the user offline.

radius-server: The RADIUS Server encapsulates in the RADIUS packet, encapsulating the IP address used by the authenticated user in the Frame-IP-Address field and recording the binding relation of the user and IP address on the authenticated user. If it is detected that the user IP address changes, force the user offline.

Supplicant: After the user passes the authentication for the first time, record the binding relation of the authenticated user and IP address on the device. If it is detected that the user IP address changes, force the user offline.

Table 7–20 Configure IP authorization function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure IP authorization function	**dot1x authorization ip-auth-mode { disable | dhcp-server | radius-server | supplicant }**	Mandatory By default, the IP authorization function in the port is disabled.

Configure Max. Sending Times of Authentication Request Packet

After the authenticated device receives the EAPOL-Start packet, send the authentication request EAP-Request/Identity packet to the client. If the authentication device does not receive the response packet, re-transmit the packet. The function is used to configure the maximum sending times of the EAP-Request/Identity packet. If the sending times exceeds the configured maximum threshold, the authentication device judges that the client is disconnected and ends the authentication.

The process of re-transmitting the EAP-Request/Identity packet is shown in the following figure:

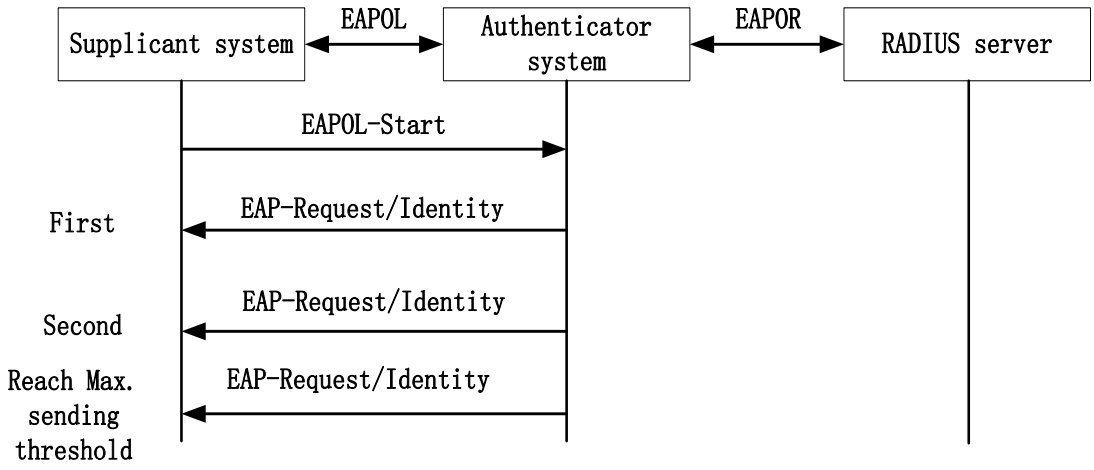


Figure 7–4 The process of re-transmitting the EAP-Request/identity packet

Table 7–21 Configure the maximum sending times of the authentication request packet

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the maximum sending times of the authentication request packet	**dot1x max-reauth** *count*	Mandatory By default, the maximum sending times of the authentication request packet is 3.

Configure Max. Sending Times of Authentication Packet

During authentication, the authentication device will send the other EAP-Request packet (except for EAP-Request/Identity) to the client, such as EAP-Request/MD5 challenge packet. If the authentication device does not receive the response packet, re-transmit the packet. The function is used to configure the maximum sending times of this kind of packet. If the sending times exceeds the configured maximum threshold, the authentication device judges that the client failed to authenticate.

The process of re-transmitting the EAP-Request packet is shown in the following figure:

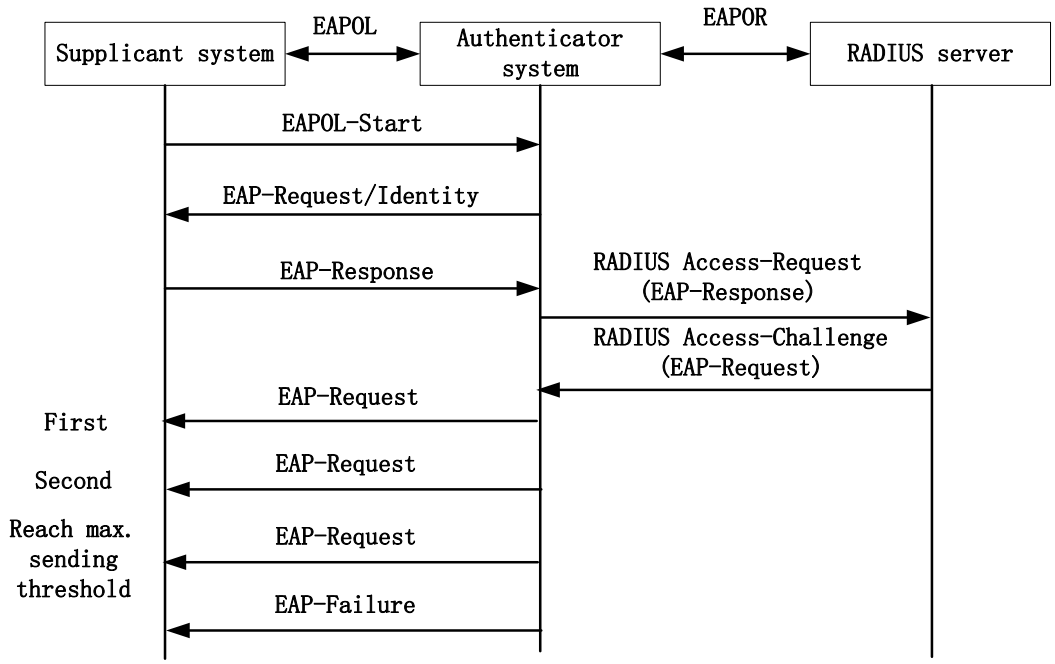


Figure 7–5 The process of re-transmitting the EAP-Request packet

Table 7–22 Configure the maximum sending times of the authentication packet

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the maximum sending times of the authentication packet	**dot1x max-req** *count*	Mandatory By default, the maximum sending times of the authentication packet in the port is 2.

Configure Authentication Failure Record Log Function

After enabling the authentication failure record log function, the authentication device will record the information about the authentication failure, so as to detect the fault reason.

Table 7-23 Configure the authentication failure record log function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current interface. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the log function of recording the authentication failure	**dot1x logging security-data {abnormal-logoff | failed-login | normal-logoff | successful-login }***	Mandatory By default, the port does not enable any data log.

Configure ARP Keepalive Function

To detect whether the user is online after the terminal user passes the authentication, the authentication device sends the ARP request packet to the authenticated user. The authentication device determines whether the user is online by whether the ARP response packet of the user is received.

Table 7-24 Configure the ARP keepalive function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current interface. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the ARP keepalive function	**dot1x client-probe** { **enable** | **disable** }	Mandatory By default, the ARP keepalive function in the port is disabled.

Note:

- The authentication device can trigger the ARP keepalive function normally after getting the IP address of the authenticated user. If not receiving the ARP response packet of the authentication device during the protection period, force the user offline.

Configure Maximum Users of a Port

After the number of the authenticated users in the port reaches the configured threshold, the authentication system does not answer the new authentication request initiated by the user.

Table 7–25 Configure the maximum users of the port

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the maximum users of the port	**dot1x port-control max-user-num** *max-uer-num-value*	Mandatory By default, the maximum number of the users permitted to be connected in the port is 256.

Note:

- The port needs to be configured as the user-based access control mode (Macbased). Otherwise, the configured access users cannot take effect.

Configure IP ACL Prefix Name

After the end user authentication is successful, when the server sends the IP ACL with the number greater than 2000, it is required to configure the IP ACL with the name as "IP ACL prefix name+ACL number" on the device. For example, the server sends the ACL with the number as 2001 and then configure the IP ACL with the name as "assignacl-2001" on the device.

Table 7-26 Configure the IP ACL prefix name

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the IP ACL prefix name	**dot1x number-acl-prefix** *number-acl-prefix-name*	Mandatory By default, the IP ACL prefix name is "assignacl-".

Note:

- When the access control mode is configured to portbased multi-hosts, the function of delivering ACL does not take effect.

Configure Default Valid VLAN

When the interface control mode is the user-based access control mode and the server does not send the VLAN (Auto VLAN), this configuration can be used to specify the VLAN if the authenticated users are expected to communicated in the specified VLAN.

Table 7-27 Configure the default valid VLAN

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the default valid VLAN	**dot1x default-active-vlan** *default-active-vlan-id*	Mandatory By default, the default valid VLAN is not configured.

Note:

- When the user-based access control mode (Macbased) is configured on the interface,the priority of the binding relationship after the user authentication is in the following order: server sending the VLAN, default valid VLAN, VLAN which the PVID of the interface locates in.

Configure to Allow Unauthenticated User to Communicate in VLAN which PVID Locates in

When multiple interfaces access to the interface, each terminal needs to perform the access control. Some terminals that cannot initiate the 802.1X authentication also hopes to visit the network resources and you can enable the command. After the function is enabled, the unauthenticated end user can normally communicate in the VLAN which the PVID locates in.

This function must meet the following functions to ensure normal running.

- Enable the 802.1X authentication or MAC address authentication on the interface.
- The access control mode of the interface is the user-based access control mode (Macbased).

- The VLAN mode of the interface is the Hybrid mode.
- The function of only receiving the Untag packet needs to be enabled on the interface.

Table 7-28 Configure to allow the unauthenticated user to communicate in the VLAN which the PVID locates in

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure to allow the unauthenticated user to communicate in the VLAN which the PVID locates in	**dot1x native-vlan-free**	Mandatory By default, the function of allowing the unauthenticated user to communicate in the VLAN which the PVID locates in is disabled,

Note:

- After the function is enabled on the interface, the function of only receicing the untage packet needs to be enabled on the interface by configuring the **switchport accept frame-type untag** command on the interface to ensure that the packet sent by the unauthenticated user can only be forwarded in the VLAN which the PVID locates in.
- It is recommended that this function be used together with the VLAN sent by the server or the default valid VLAN.
- The function does not support the secure channel authentication.

Configure Port Access Control Mode

There are two kinds of port access control modes: port-based access control mode and user-based access control authentication mode.

Port-based access control mode (Portbased): In the port, only permit one user authentication to pass;

User-based access control mode (Macbased): In the port, permit multi-user authentication to pass. The users in the port need to pass the authentication respectively so that they can access the network.

Port-based access control mode includes two kinds: multi-host mode and single-host mode.

Multi-host mode (Multi-hosts): After one user in the port passes the authentication, the other users in the port can access the network without authentication.

Single-host mode (Single-host): In the port, only permit one user to pass the authentication and access the network; the other users cannot access the network and also cannot pass the authentication.

Table 7-29 Configure the port access control mode

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the access control mode	**dot1x port-method** { **macbased** | **portbased** }	Mandatory By default, enable the user authentication mode in the port.
Configure the port-based access control mode	**dot1x port-method portbased host-mode** { **multi-hosts** | **single-host** }	Optional By default, enable the multi-host authentication mode in the port.

Note:

- When configuring the host mode of the port-based access control mode, we need to ensure that the access control mode is configured as the port-based access control mode (Portbased).

Configure Guest VLAN

The user can get the 802.1X client software in Guest VLAN to upgrade the client, or execute other application program (such as anti-virus software and operation system patch) upgrade.

Table 7-30 Configure Guest VLAN

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure Guest VLAN	**dot1x guest-vlan** *guest-vlan-id*	Mandatory By default, Guest VLAN is not configured in the port; the value range is 1-4094.

Note:

- Guest VLAN of the port cannot be applied to the dynamic VLAN. If VLAN ID specified by Guest VLAN is the VLAN automatically created by GVRP, Guest VLAN can be configured successfully, but cannot take effect.
- To ensure that the functions can be used normally, please distribute different VLAN IDs for Voice VLAN, Private VLAN, and Guest VLAN.

Configure Guest ACL

If the user is not authenticated or does not pass the authentication, we can configure Guest ACL in the port to limit the resources accessed by the user in Guest VLAN.

Table 7-31 Configure Guest ACL

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure Guest ACL	**dot1x guest-acl** *guest-acl-name*	Mandatory By default, Guest ACL is not configured in the port.

Note:

- If Guest VLAN is not configured in the port, the configured Guest ACL does not take effect.
- Guest ACL can take effect only in the macbased mode.
- The ACL rule is configured in the authentication device.

Configure Critical VLAN

When the user adopts the RADIUS authentication, the authentication server is unavailable and as a result, the authentication fails and the user is permitted to access the resources in the specified VLAN. The VLAN is called Critical VLAN.

When the port is configured to the port-based access control mode and the port has the user to authenticate, but all authentication servers are unavailable, the port will be added to Critical VLAN and all users in the port can access the resources in the Critical VLAN.

When the port is configured to user-based access control mode and the port has the user to authenticate, but all authentication servers are unavailable, the user is only permitted to the resources in the Critical VLAN.

To be configured to the user-based access control mode, the port needs to meet the following conditions so that it can run normally:

- The port VLAN mode is Hybrid.

The port enables the MAC VLAN function. The user in the Critical VLAN initiates the authentication. If the authentication server is still unavailable, the user is still in the Critical VLAN. If the

authentication server is available, the user exits Critical VLAN with the authentication result.

Table 7-32 Configure Critical VLAN

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure Critical VLAN	**dot1x critical-vlan** *critical-vlan-id*	Mandatory By default, do not configure Critical VLAN in the port and the value range is 1-4094.

Note:

- The function only supports the RADIUS authentication.
- If the radius and escape function are configured on the device, that is, **aaa authentication connection default radius none** and **critical vlan** are configured, and when the user authenticates and the authentication server is available, the user enters the Critical VLAN. If only the escape function is configured, that is, **aaa authentication connection default none** and **critical vlan** are configured, and when the user authenticates, the authentication server is unavailable, the escape function takes effect.
- When only Guest VLAN function is configured in the port, the authentication failed users are all in Guest VLAN. When both Guest VLAN and Critical VLAN are configured in the port at the same time, the authentication server is unavailable and as a result, the user fails to authenticate and will enter Critical VLAN. If the user fails to authenticate because of other reasons, it will enter Guest VLAN.

Configure User Authentication Migration Function

The user authentication migration function is applicable to the scenario that one user (distinguish based on the terminal MAC address) migrates from one authentication port to another authentication port of one device. When disabling the user authentication migration function, the user cannot initiate the authentication on another authentication port of the device after being authenticated on one port of the device; when enabling the user authentication migration function

and after being authenticated on one port and detecting that the user migrates to another authentication port, the device first deletes the authentication information on the previous port, and then permits the user to initiate the authentication on the new authentication port.

No matter whether to enable the user authentication migration function, the device will record the log after detecting that the user is migrated between the authentication ports.

Table 4-33 Configure the user authentication migration function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the user authentication migration function	**dot1x station-move { enable | disable }**	Mandatory By default, the user authentication migration function is disabled.

Configure Timer Parameters

The timer parameters in the port contain: re-authentication timer, quiet timer, server timeout timer, client timeout timer, MAC authentication user offline check timer.

Re-authentication timer (re-authperiod): After configuring the re-authentication function in the port, the authentication device regularly initiates the re-authentication request to the client, applicable to the 802.1X authentication.

Quiet timer (quiet-period): When the client reaches the maximum authentication failure times, the authentication device can answer the client authentication request again after the quiet time times out, applicable to the 802.1X authentication and MAC address authentication.

Server timeout timer (server-timeout): If the authentication device does not receive the response packet of the server within the specified time, it is regarded to be disconnected with the server, applicable to the 802.1X authentication and MAC address authentication.

Client timeout timer (supp-timeout): If the authentication device does not receive the response packet of the 802.1X client within the specified time, it is regarded to be disconnected with the user, applicable to the 802.1X authentication.

MAC address authentication user offline check timer (offline-detect): After enabling the MAC address authentication, the port periodically detects whether the user is online, applicable to the MAC address authentication.

Table 7-33 Configure the timer parameters

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the timer parameters	**dot1x timeout** { **re-authperiod** *re-authperiod-value* | **quiet-period** *quiet-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **offline-detect** *offline-detect-value* }	Mandatory By default, the re-authentication time in the port is 3600s; the value range is 5-65535; The quiet time is 60s; the value range is 1-65535; The timeout of the server is 30s; the value range is 5-3600; The timeout of the client is 30s; the value range is 5-3600; The offline check time of the client is 30s; the value range is 5-3600;

Restore Port Default Configuration

Restore the default configuration of the 802.1X authentication and MAC address authentication in the port.

Table 7–34 Restore the default configuration of the port

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Restore the default configuration of the port	**dot1x default**	Mandatory In the port, disable the 802.1X authentication and MAC address authentication function; the related configuration parameters are restored to the default values and the default configuration parameters do not take effect.

Note:

- The command show dot1x is used to view the detailed authentication default configuration parameters.

Configure the MAB Function

When the terminal passes the MAC address authentication and needs to use higher access rights through client authentication, this function can be enabled.

Table 7–35 Enable the MAB function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**interface link-aggregation** *link-aggregation-id*	
Enable the 802.1X authentication	**dot1x port-control** { **enable** | **disable** }	Mandatory By default, the 802.1X authentication function of the port is disabled.
Enable the MAC address authentication function	**dot1x mac-authentication** { **enable** | **disable** }	Mandatory By default, the MAC address authentication function of the port is disabled.
Enable the MAB function	**dot1x after-mac-auth** { **enable** | **disable** }	Mandatory By default, the MAB function of the port is disabled.

7.2.5. 802.1X Monitoring and Maintaining

Table 7-36 802.1X monitoring and maintaining

Command	Description
clear dot1x statistic [**interface** *interface-name* | **link-aggregation** *link-aggregation-id* | **mac** { *mac-address* | **all** }]	Clear the authentication statistics information
clear dot1x auth-fail-user history [**mac** *mac-address*]	Clear the authentication failure record information
show dot1x	Display the default configuration information of the authentication
show dot1x auth-fail-user history [**recent** | **mac** *mac-address*]	Display the authentication failure information
show dot1x auth-address [*mac-address* | **interface** *interface-name* | **link-aggregation** *link-aggregation-id*]	Configure the authenticatable host list information
show dot1x config [**interface** *interface-name* | **link-aggregation** *link-aggregation-id*]	Display the configuration information of the authentication
show dot1x free-ip	Display secure channel configuration information
show dot1x global config	Display the global configuration information
show dot1x statistic [**interface** *interface-name* | **link-aggregation** *link-aggregation-id* | **mac {** *mac-address* | **all** }]	Display the authentication statistics information
show dot1x user [**interface** *interface-name* | **link-aggregation** *link-aggregation-id* | **summary**]	Display the user information

7.3. 802.1X Typical Configuration Example

7.3.1. Configure 802.1X Portbased Authentication

Network Requirements

1. The user PC1 and PC2 on one VLAN are connected to IP Network via Device. On Device, enable the 802.1X access control;
2. The authentication mode adopts the RADIUS authentication;
3. When the user does not pass the authentication, only permit accessing Update Server; after the user passes the authentication, permit accessing IP Network;
4. After one user on LAN passes authentication, the other users on the VLAN can access IP Network without authentication.

Network Topology

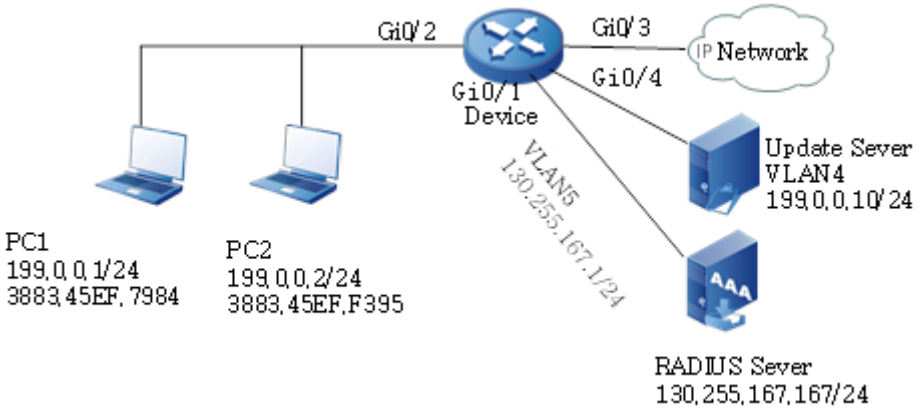


Figure 7–6 Networking of configuring 802.1X Portbased authentication

Configuration Steps

Step 1: Configure VLAN.

#Create VLAN2 on Device, configure the port link type on gigabitethernet0/2 as Access, and permit the services of VLAN2 to pass.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the port link type on gigabitethernet0/3~gigabitethernet0/4 of Device as Access, permitting the services of VLAN3-VLAN4 to pass respectively. (Omitted)

Step 2: Configure the interface IP address of Device.

#Create VLAN5 and add gigabitethernet0/1 to the corresponding VLAN.

```
Device(config)#vlan 5
```

```
Device(config-vlan5)#exit
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 5
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the IP address of VLAN5 as 130.255.167.1/24.

```
Device(config)#interface vlan 5
Device(config-if-vlan5)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan5)#exit
```

Step 3: Configure the AAA authentication.

#On Device, configure the RADIUS server group and the group name is test. The server key is admin, the priority is 1, and the RADIUS server address is 130.255.167.167/24. And then, configure the test server group for dot1x authentication in the default domain system.

```
Device(config)# aaa server group radius test
Device(config-sg-radius-test)# server 130.255.167.167 priority 1 key admin
Device(config)#exit
Device(config)# domain system
Device (config-isp-system)#aaa authentication dot1x radius-group test
Device(config)#exit
```

Step 4: Configure the AAA server.

#Configure the user name, password and key as admin on the AAA server. (Omitted)

#On the AAA server, configure RADIUS to deliver the three attributes of Auto VLAN: 64 is VLAN, 65 is 802, and 81 is VLAN3. (Omitted)

Step 5: Configure the port 802.1X authentication.

#Enable the 802.1X authentication on the port and the authentication mode is Portbased.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#dot1x port-method portbased
Device(config-if-gigabitethernet0/2)#exit
```

#Configure Guest VLAN of the port as VLAN4.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x guest-vlan 4
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Check the result.

#Before passing the authentication, gigabitethernet0/2 is added to Guest VLAN. Here, PC1 and PC2 users are in VLAN4 and permit accessing Update Server.

```
Device#show vlan 4
---- ---- ------------------------------ ------- --------- ----------------
------------
NO.  VID  VLAN-Name                      Owner   Mode      Interface
---- ---- ------------------------------ ------- --------- ----------------
------------
1    4    VLAN0004                       static  Untagged  gi0/2 gi0/4
```

#Verify that PC1 can pass the authentication; the authentication server delivers VLAN3. Here, PC1 and PC2 users are in VLAN3 and can access IP Network.

```
Device#show dot1x user
--------------------
NO 1  : MAC_ADDRESS= 3883.45ef.7984  STATUS=    Authorized    USER_NAME=
admin
     VLAN=      3          IP_ADDRESS= Unknown      INTERFACE=  gi0/2
     AUTH_STATE= AUTHENTICATED  BACK_STATE= IDLE          USER_TYPE=
DOT1X
     Online time: 0 week 0 day 0 hours 0 minute 51 seconds


 Total: 1   Authorized: 1   Unauthorized/guest/critical: 0/0/0   Unknown: 0
```

7.3.2. Configure 802.1X Transparent Transmission Mode

Network Requirements

1. PC is connected to Device2 enabled with the 802.1X access control via Device1 and connected to IP Network.
2. Device1 enables the transparent transmission function; Device2 uses the RADIUS authentication mode.
3. After passing authentication, PC can access IP Network.

Network Topology

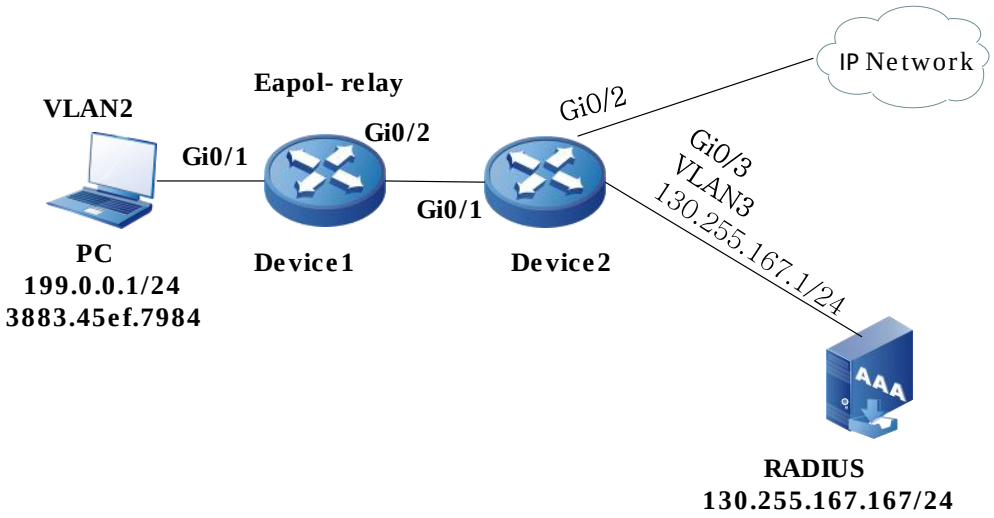


Figure 7-7 Networking of configuring the 802.1X transparent transmission mode

Configuration Steps

Step 1: Configure port VLAN of Device2.

#Create VLAN2 on Device2, configure the port link type on gigabitethernet0/1 as Access, and permit the services of VLAN2 to pass.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode access
Device2(config-if-gigabitethernet0/1)#switchport access vlan 2
Device2(config-if-gigabitethernet0/1)#exit
```

#Configure the port link type on gigabitethernet0/2 of Device2 as Access, permitting the services of VLAN2 to pass. (Omitted)

Step 2: Configure the interface IP address of Device2.

#Create VLAN3 and add gigabitethernet0/3 to the corresponding VLAN.

```
Device2(config)#interface gigabitethernet 0/3
Device2(config-if-gigabitethernet0/3)#switchport mode access
Device2(config-if-gigabitethernet0/3)#switchport access vlan 3
Device2(config-if-gigabitethernet0/3)#exit
```

#Configure the IP address of VLAN5 as 130.255.167.1/24.

```
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ip address 130.255.167.1 255.255.255.0
```

```
Device2(config-if-vlan3)#exit
```

Step 3: Configure the AAA authentication.

#On Device, configure the RADIUS server group and the group name is test. The server key is admin, the priority is 1, and the RADIUS server address is 130.255.167.167/24. And then, configure the test server group for dot1x authentication in the default domain system.

```
Device(config)# aaa server group radius test
Device(config-sg-radius-test)# server 130.255.167.167 priority 1 key admin
Device(config)#exit
Device(config)# domain system
Device (config-isp-system)#aaa authentication dot1x radius-group test
Device(config)#exit
```

Step 4: Configure the AAA server.

#Configure the user name, password, and key as admin on the AAA server. (Omitted)

Step 5: Configure the port VLAN of Device1.

#Configure the port link type on gigabitethernet0/1-gigabitethernet0/2 of Device1 as Access, permitting the services of VLAN2 to pass. (Omitted)

Step 6: Enable the 802.1X transparent transmission function on Device1.

#Configure the 802.1X transparent transmission mode on gigabitethernet0/1 of Device1 and the uplink port is gigabitethernet0/2.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#dot1x eapol-relay enable
Device1(config-if-gigabitethernet0/1)#dot1x eapol-relay uplink interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)#exit
```

Step 7: Configure the 802.1X authentication mode on Device2.

#Enable the 802.1X authentication of gigabitethernet0/1 and the port authentication mode is Portbased.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#dot1x port-control enable
Device2(config-if-gigabitethernet0/1)#dot1x port-method portbased
Device2(config-if-gigabitethernet0/1)#exit
```

Step 8: Check the result.

#PC user can be authenticated successfully and can access IP Network.

```
Device2#show dot1x user
--------------------
NO 1  : MAC_ADDRESS= 3883.45ef.7984  STATUS=  Authorized  USER_NAME=
admin
    VLAN=  2  IP_ADDRESS=  Unknown  INTERFACE=  gi0/2
    AUTH_STATE=  AUTHENTICATED  BACK_STATE=  IDLE  USER_TYPE=
DOT1X
    Online time: 0 week 0 day 0 hours 0 minute 51 seconds

Total: 1  Authorized: 1  Unauthorized/guest/critical: 0/0/0  Unknown: 0
```

7.3.3. Configure 802.1X Free-Client Authentication

Network Requirements

1. The network printer is connected to IP Network via Device; Device adopts the 802.1X access control;
2. Device regularly performs the offline detection for the network printer.
3. Use the RADIUS authentication mode.
4. After passing the authentication, the network printer can execute the printing task from IP Network.

Network Topology

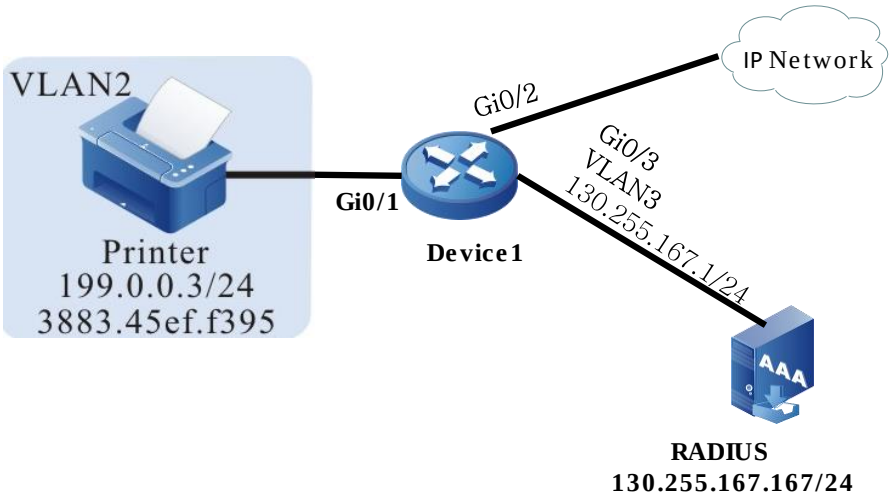


Figure 7-8 Networking of configuring the 802.1X free-client authentication

Configuration Steps

Step 1: Configure the port VLAN.

#Create VLAN2 on Device2, configure the port link type on gigabitethernet0/1 as Access, and permit the services of VLAN2 to pass.

```
Device#configure terminal
```

```
Device(config)#vlan 2
Device(config-vlan2)#exit
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the port link type on gigabitethernet0/2 of Device as Access, permitting the services of VLAN2 to pass. (Omitted)

Step 2: Configure the interface IP address of Device.

#Configure VLAN3 and add gigabitethernet0/3 to the corresponding VLAN.

```
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode access
Device(config-if-gigabitethernet0/3)#switchport access vlan 3
Device(config-if-gigabitethernet0/3)#exit
```

#Configure the IP address of VLAN3 as 130.255.167.1/24.

```
Device(config)#interface vlan 3
Device(config-if-vlan3)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan3)#exit
```

Step 3: Configure the AAA authentication.

#On Device, configure the RADIUS server group and the group name is test. The server key is admin, the priority is 1, and the RADIUS server address is 130.255.167.167/24. And then, configure the test server group for dot1x authentication in the default domain system.

```
Device(config)# aaa server group radius test
Device(config-sg-radius-test)# server 130.255.167.167 priority 1 key admin
Device(config)#exit
Device(config)# domain system
Device (config-isp-system)#aaa authentication dot1x radius-group test
Device(config)#exit
```

Step 4: Configure the AAA server.

#Configure the user name, password, and key as admin on the AAA server. (Omitted)

Step 5: Configure the 802.1X authentication.

#Configure the 802.1X free-client authentication mode, and use the MAC address of the network printer as user name and password.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#dot1x mac-authentication enable
Device(config-if-gigabitethernet0/1)#exit
```

#Configure Device to perform the offline detection for the printer every 120s.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#dot1x timeout offline-detect 120
Device(config-if-gigabitethernet0/1)#exit
```

Step 6: Check the result.

#The network printer can pass the authentication and can execute the printing task from IP Network.

```
Device#show dot1x user
--------------------
NO 1  : MAC_ADDRESS= 3883.45ef.f395  STATUS=  Authorized  USER_NAME=
38-83-45-ef-f3-95
    VLAN=  2  IP_ADDRESS= 199.0.0.3  INTERFACE= gi0/1
    AUTH_STATE= AUTHENTICATED  BACK_STATE= IDLE  USER_TYPE= MAC
    Online time: 0 week 0 day 0  hours 1  minutes 6 seconds

Total: 1  Authorized: 1  Unauthorized/guest/critical: 0/0/0  Unknown: 0
```

7.3.4. Configure Secure Channel

Network Requirements

- User PC1 and PC2 on the same VLAN access the IP network through Device. Enable the secure channel access control on Device.
- Authentication adopts the RADIUS authentication.
- PC1 is allowed to visit Update Server before authentication success and is allowed to visit Update Server and IP Network after authentication success.
- PC2 is allowed to visit Update Server and IP Network without authentication.

Network Topology

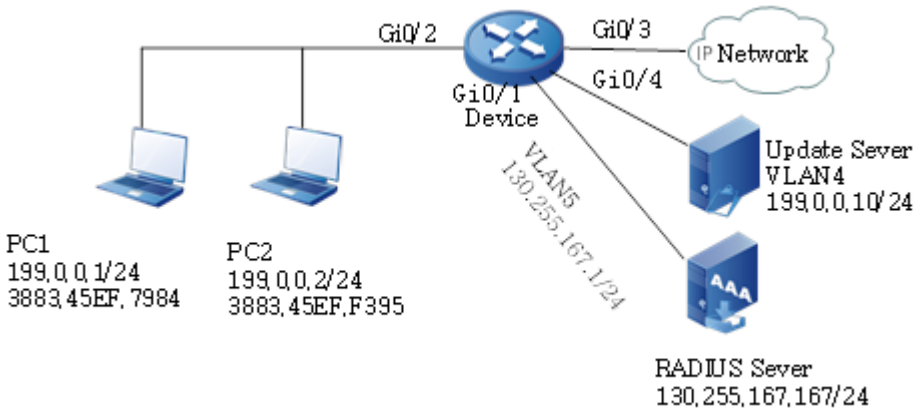


Figure 7-9 Networking of configuring secure channel

Configuration Steps

Step 1: Configure the link type of the VLAN and interface on the interface.

#Create VLAN2 and VLAN5 on Device.

```
Device#configure terminal
Device(config)#vlan 2,5
Device(config)#exit
```

#Configure the link type of interface gigabitethernet0/2 as Access, permitting services of VLAN2 to pass.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)# switchport mode access
Device(config-if-gigabitethernet0/2)# switchport access vlan 2
Device(config-if-gigabitethernet0/2)#end
```

#Configure link type of interface gigabitethernet 0/3–gigabitethernet 0/4 as Access on Device, permitting services of VLAN2 to pass. Configure the link type of interface gigabitethernet 0/1 as Access, permitting services of VLAN5 to pass. (Omitted)

Step 2: Configure the interface IP address of Device.

#Configure the IP address of VLAN5 as 130.255.167.1/24.

```
Device#configure terminal
Device(config)#interface vlan 5
Device(config-if-vlan5)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan5)#exit
```

Step 3: Configure AAA authentication.

#On Device, configure the RADIUS server group and the group name is test. The server key is admin, the priority is 1, and the RADIUS server address is 130.255.167.167/24. And then, configure the test server group for dot1x authentication in the default domain system.

```
Device(config)# aaa server group radius test
Device(config-sg-radius-test)# server 130.255.167.167 priority 1 key admin
Device(config)#exit
Device(config)# domain system
Device (config-isp-system)#aaa authentication dot1x radius-group test
Device(config)#exit
```

Step 4: Configure AAA server.

#Configure the user name, password, and key value on the AAA server as admin. (Omitted)

Step 5: Configure secure channel.

#Enable the secure channel.

```
Device#configure terminal
Device(config)#dot1x free-ip 199.0.0.10 24
```

Step 6: Check the result.

#PC1 can viist the Update Server and cannot visit other network resources before the authentication success.

#View the user authentication information after user PC1 initiates the authentication and authentication succeeds.

```
Device#show dot1x user
--------------------
NO 1  : MAC_ADDRESS= 3883.45ef.7984  STATUS=  Authorized  USER_NAME= admin
    VLAN=  2  IP_ADDRESS= 199.0.0.1  INTERFACE=  gi0/2
    AUTH_STATE= AUTHENTICATED  BACK_STATE= IDLE  USER_TYPE= DOT1X
    Online time: 0 week 0 day 0 hours 0 minute 51 seconds

Total: 1  Authorized: 1  Unauthorized/guest: 0/0  Unknown: 0
```

It can be viewed that user PC1 has passed the authentication and then PC1 can visit Update Server and IP Network.

#PC2 can visit Update Server and IP Network without authentication.

7.3.5. Configure IP Authorizing DHCP Server Mode

Network Requirements

- PC is connected IP Network via Device; Device enables the 802.1X access control.
- Authentication adopts the RADIUS authentication.
- PC1 can access IP Network after getting the IP address via the specified DHCP Server.
- PC2 cannot access IP Network after being configured to carry the static IP address authentication.

Network Topology

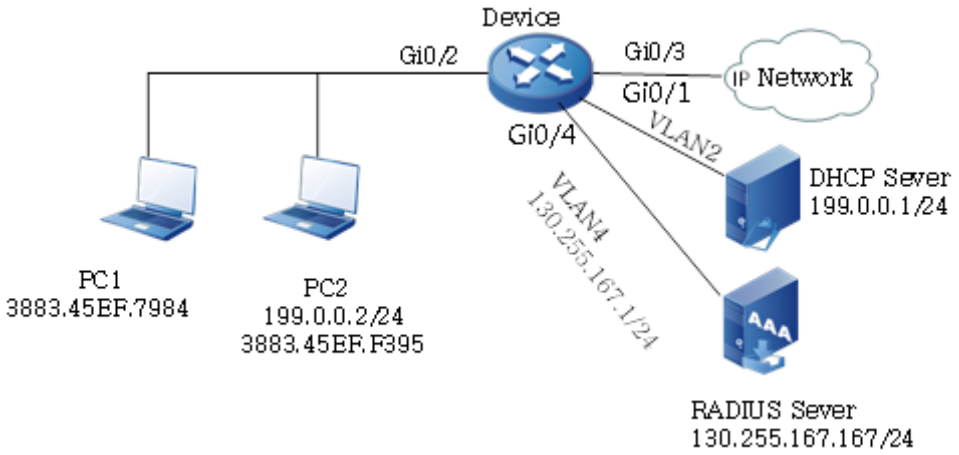


Figure 7-10 Networking of configuring 802.1X IP authorizing DHCP Server mode

Configuration Steps

Step 1: Configure the link type of the VLAN and port on the Device.

#Create VLAN 2 and VLAN4 on Device, configure the port link type on gigabitethernet0/2 as Hybrid, permitting the services of VLAN2 to pass, and configure the PVID as 2.

```
Device#configure terminal
Device(config)#vlan 2,4
Device(config)#intergice gigabitethernet 0/2
Device(config-if- gigabitethernet0/2)#switchport mode hybrid
Device(config-if- gigabitethernet0/2)#switchport hybrid untagged vlan 2
Device(config-if- gigabitethernet0/2)#switchport hybrid pvid vlan 2
Device(config-if- gigabitethernet0/2)#exit
```

#On gigabitethernet0/1 of Device, configure the port link type as Access and permit the services of VLAN2 to pass (omitted).

#On gigabitethernet0/4 of Device, configure the port link type as Access and permit the services of VLAN4 to pass (omitted).

Step 2: Configure the interface IP address of Device.

Configure the IP address of VLAN4 as 130.255.167.1/24.

```
Device(config)#intergice vlan 4
Device(config-if-vlan4)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan4)#exit
```

Step 3: Configure AAA authentication.

#On Device, configure the RADIUS server group and the group name is test. The server key is admin, the priority is 1, and the RADIUS server address is 130.255.167.167/24. And then, configure the test server group for dot1x authentication in the default domain system.

```
Device(config)# aaa server group radius test
Device(config-sg-radius-test)# server 130.255.167.167 priority 1 key admin
Device(config)#exit
Device(config)# domain system
Device (config-isp-system)#aaa authentication dot1x radius-group test
Device(config)#exit
```

Step 4: Configure AAA server.

#Configure the user name, password, and key value on the AAA server as admin. (Omitted)

Step 5: Configure the DHCP server.

#On the DHCP server, configure distributing the IP address segment 199.0.0.2-199.0.0.10 and subnet mask 255.255.255.0 (omitted).

Step 6: On Device, enable the DHCP Snooping function and configure port gigabitethernet0/1 of Device to trust port.

```
Device(config)#dhcp-snooping
Device(config)#intergice gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#dhcp-snooping trust
Device(config-if-gigabitethernet0/1)#exit
```

Step 7: On Device, configure 802.1X authentication.

#Enable the 802.1X authentication of gigabitethernet0/2.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if- gigabitethernet0/2)#dot1x port-control enable
Device(config-if- gigabitethernet0/2)#exit
```

Confgure the IP authorization of gigabitethernet0/2 as DHCP Server mode.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if- gigabitethernet0/2)#dot1x authorization ip-auth-mode dhcp-server
```

```
Device(config-if- gigabitethernet0/2)#exit
```

Enable the ARP keepalive of gigabitethernet0/2.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if- gigabitethernet0/2)#dot1x client-probe enable
Device(config-if- gigabitethernet0/2)#exit
```

Step 8: Check the result.

PC1 user can be authenticated successfully and can get IP address from the DHCP server and access IP Network.

```
Device#show dot1x user
--------------------
NO 1  : MAC_ADDRESS= 3883.45ef.7984  STATUS=    Authorized      USER_NAME=
admin
     VLAN=      2          IP_ADDRESS=  199.0.0.3      INTERGICE=   gi0/2
     AUTH_STATE=  AUTHENTICATED   BACK_STATE=  IDLE          USER_TYPE=
DOT1X
     Online time: 0 week 0 day 0 hours 0 minutes 36 seconds

Total: 1   Authorized: 1   Unauthorized/guest/critical: 0/0/0 Unknown: 0
```

#After being authenticated, PC2 user is in the GET-IP state and cannot get the IP address.

```
NO 1  : MAC_ADDRESS= 3883.45ef.f381  STATUS=    Authorized      USER_NAME=
admin
     VLAN=      2          IP_ADDRESS=  Unknown        INTERGICE=   gi0/2
     AUTH_STATE=  GET_IP       BACK_STATE=  IDLE          USER_TYPE=   DOT1X
     Online time: 0 week 0 day 0 hour 0 minute 34 seconds

Total: 1   Authorized: 1   Unauthorized/guest/critical: 0/0/0 Unknown: 0
```

#After checking, PC2 cannot access IP Network.

7.3.6. Configure 802.1x and Port Security Share

Network Requirements

- PC accesses IP Network via Device; Device enables the 802.1X access control and port security.
- Authentication adopts the RADIUS authentication.
- Configure the port security rule of not matching the MAC address of PC1, and PC1 can access IP Network via authentication.
- Configure the port security deny rule of matching the MAC address of PC2, and PC2 cannot be authenticated.

Network Topology

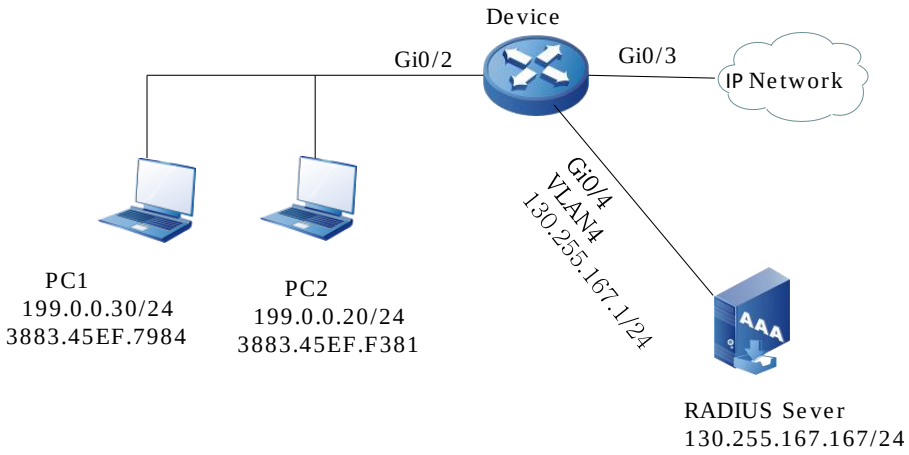


Figure 7-11 Networking of configuring 802.1X and port security share

Configuration Steps

Step 1: Configure the link type of the VLAN and port on the Device.

#Create VLAN 2 and VLAN4 on Device, configure the port link type on gigabitethernet0/2 as Hybrid, permitting the services of VLAN2 to pass, and configure the PVID as 2.

```
Device#configure terminal
Device(config)#vlan 2,4
Device(config)#intergice gigabitethernet0/2
Device(config-if- gigabitethernet0/2)#switchport mode hybrid
Device(config-if- gigabitethernet0/2)#switchport hybrid untagged vlan 2
Device(config-if- gigabitethernet0/2)#switchport hybrid pvid vlan 2
Device(config-if- gigabitethernet0/2)#exit
```

#On gigabitethernet0/4 of Device, configure the port link type as Access and permit the services of VLAN4 to pass (omitted).

Step 2: Configure the interface IP address of Device.

Configure the IP address of VLAN4 as 130.255.167.1/24.

```
Device(config)#intergice vlan 4
Device(config-if-vlan4)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan4)#exit
```

Step 3: Configure AAA authentication.

#On Device, configure the RADIUS server group and the group name is test. The server key is admin, the priority is 1, and the RADIUS server address is 130.255.167.167/24. And then, configure the test server group for dot1x authentication in the default domain system.

```
Device(config)# aaa server group radius test
```

```
Device(config-sg-radius-test)# server 130.255.167.167 priority 1 key admin
Device(config)#exit
Device(config)# domain system
Device (config-isp-system)#aaa authentication dot1x radius-group test
Device(config)#exit
```

Step 4: Configure AAA server.

#Configure the user name, password, and key value on the AAA server as admin. (Omitted)

Step 5: Configure the 802.1X authentication on Device.

#Enable the 802.1X authentication of gigabitethernet0/2.

```
Device(config)#intergice gigabitethernet0/2
Device(config-if- gigabitethernet0/2)#dot1x port-control enable
Device(config-if- gigabitethernet0/2)#exit
```

Step 6: Configure the port security on Device.

#Enable the port security on port gigabitethernet0/2.

```
Device(config)#intergice gigabitethernet0/2
Device(config-if- gigabitethernet0/2)#port-security enable
Device(config-if- gigabitethernet0/2)exit
```

#Configure the port security rule on port gigabitethernet0/2.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#port-security deny mac-address 3883.45EF.7984
Device(config-if-gigabitethernet0/2)exit
```

Step 7: Check the result.

#PC1 user can be authenticated successfully and then can access IP Network.

```
Device#show dot1x user
_____________________

NO 1 : MAC_ADDRESS= 3883.45EF.7984 STATUS= Authorized USER_NAME= admin
    VLAN= 2 IP_ADDRESS= Unknown INTERGICE= gi0/2
    AUTH_STATE= AUTHENTICATED BACK_STATE= IDLE USER_TYPE= DOT1X
    Online time: 0 week 0 day 0 hour 0 minute 1 second

Total: 1 Authorized: 1 Unauthorized/guest/critical: 0/0/0 Unknown: 0
```

#PC2 user cannot be authenticated successfully and cannot access the network.

8. PKI

8.1. Overview

PKI (Public Key Infrastructure) is one key management platform of complying with the established standard and one system of comprising hardware, software, policy and people. It is the security infrastructure of using the public key concept and technology to carry out and provide the security services, such as reality, confidentiality, integrity, and accountability. KPI overcomes the problems of the using the traditional symmetric cryptography, such as complicated key management, low security and hard to expand the network capacity.

PKI components mainly include CA (Certification Authorities), RA (Registration Authorities), Endpoint Entities and so on. The PKI of this configuration manual refers to the related functions of the terminal entity and can be used with Maipu CMS (Certificate Manage Server), Windows Server 2000 CA, Windows Server 2003 CA, Windows Server 2008 CA, Cisco CA and China Telecom CA, realizing the high-strength authentication for the terminal entity via the digital certificate. PKI can provide the certificate management mechanism for IPSec (IP Security), SSL (Secure Sockets Layer), security HTTP (Hypertext Transport (or Transfer) Protocol) and so on.

PKI is mainly to check the validity of the certificate applied by the terminal entity from CA. The typical work process of PKI: The terminal entity sends the DN (Distinguished Name) and public key to CA in the digital signature mode; CA audits the terminal entity ID, checks the digital signature, agrees the application of the terminal entity, and issues the certificate; the terminal entity gets the certificate and makes use of the certificate to use the encryption and digital signature to perform the security communication with other terminals; when the terminal entity hopes to cancel its own certificate, submit the application to CA and the CA agrees the terminal entity to cancel the certificate and updates the CRL (Certificate Revocation List). Canceling the certificate also can be initiated by CA actively.

8.2. PKI Function Configuration

Table 8-1 PKI function configuration list

Configuration Task	
Configure trust domain	Configure the trust domain
	Configure the CA address
	Configure the CA update
	Configure the CA type
	Configure the terminal entity DN
	Configure the HTTP user name and password
	Configure the hash algorithm
	Configure the source interface or source IP address

Configuration Task	
Configure certificate authentication	Configure getting and authenticating CA certificate
	Configure getting and authenticating CRL list
	Configure the policy of checking certificate canceling
	Configure the policy of checking the valid period of the certificate
	Configure forcing to set the certificate trust status
Configure certificate application and getting	Configure the certificate application
	Configure getting successful-issued certificate
	Configure certificate importing
Configure LDAP to get certificate	Configure LDAP to get certificate
Configure deleting certificate	Configure deleting certificate

8.2.1. Configure Trust Domain

Before applying for the digital certificate, the terminal entity needs to configure some registration information to help complete the application. The set of the information is the trust domain of one terminal entity. One trust domain corresponds o one certificate trust chain. The trust chain can comprise multi-level CAs and also can have only one root CA. The configuration parameters of one trust domain include the address of accessing CA, the policy of checking the certificate in the domain and so on. The device supports creating 64*1024 trust domains at the same time.

The trust domain is one local concept. Creating the trust domain is to facilitate the certificate management and let other applications, such as IKE (Internet Key Exchange) and SSL, use the certificate safely. The trust domain configured on one device is invisible for the CA and other devices. Each trust domain has the separate domain parameter configuration.

Configuration Condition

None

Configure Trust Domain

The trust domain name can be configured by the user according to the readability and other requirements. If CA has the special requirement for the trust domain name, we should configure according to the requirement of the CA.

Table 8-2 Configure trust domain

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one trust domain and enter the trust domain configuration mode	**crypto ca identity** *ca-name*	Mandatory By default, do not configure trust domain.

Note:

- The device permits creating 64*1024 trust domains at most.
- Some CA servers limit that the trust domain name is consistent with the CN (Common Name) in the CA self-signature certificate DN. Otherwise, it cannot get the CA certificate. For example, if the CN of Kaiyuan EJBCA (Enterprise Java Bean CA, the CA server developed by the commercial application component technology in JAVA) is AdminCA1, the trust domain name should be configured as crypto ca identify AdminCA1. The CA server of Cisco and Microsoft does not have the limitation. Before configuration, we should get to know whether the CA server have the related limitation.

Configure CA Address

If adopting the function of applying for and getting the certificate online, we need to use the command to configure the IP address or domain name of the CA. If adopting the mode of applying for the certificate offline, do not need to configure the item.

Table 8-3 Configure the CA address

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the trust domain configuration mode	**crypto ca identity** *ca-name*	-
Configure the URL of the CA server	**enrollment** { **url** *url-string* [**vrf** *vrf-name*] | **renewable** | **auto-enroll** *percent*}	Either By default, do not configure the address of the CA server.

Note:

- The address format of each CA server is different and we need to get the correct address from the maintaining staff of the CA server and then configure. For example, the address format of Kaiyuan EJBCA is enrollment url 192.168.1.1:8080/ejbca/publicweb/apply/scep/pkiclient.exe, while the CA servers of Cisco and Microsoft just need to specify the IP address, such as enrollment url 192.168.1.1.

Configure CA Update

If online certificate application, acquisition and other functions are adopted, you can use this command to configure CA auto update. If the offline certificate application method is adopted, this configuration is not required.

Table 8-4 Configure the CA update

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the trust domain configuration mode	**crypto ca identity** *ca-name*	-
Configure the URL of the CA server	**enrollment** { **url** *url-string* [**vrf** *vrf-name*] | **renewable** | **auto-enroll** *percent*}	Mandatory By default, do not configure the CA server address.
Configure the auto update when the CA server certificate is expired	**enrollment renewable**	-
Automatically update the CA server certificate when a certain percentage of its validity period is configured	**enrollment auto-enroll** *percent*	The default value is 60%. If the automatic update fails, try 3 times at most. Perform the next update according to the percentage of the remaining time of the certificate; The range of configuration is 50% - 99%.

Note:

- The auto update function of the CA server certificate expiration only supports the CA using the SCEP protocol (Simple Certificate Enrollment Protocol). In the configuration parameters of CA, the type should be configured as SCEP.

Configure CA Type

If using the function of applying for and getting the certificate online, the device needs to adopt different protocol standard to communicate according to different CA type, so it is necessary to configure the CA type; if adopting the mode of applying for the certificate offline, we also need to configure the item and the device needs to generate different contents of PKCS #10 according to different CA types (Public-Key Cryptography Standards, Certification Request Syntax Standard) certificate requests.

Currently, the device supports the following CA types that can be applied for online:

- ctca (China Telecom Certificate Authority): Adopt China Telecom private protocol to apply for the certificate online or offline, support China Telecom CA;
- other: Other types of CA; currently, the configuration can only be used for the offline certificate application. The generated PKCS #10 content of the device in the configuration is the same as the generated PKCS #10 content when the CA type is scep;
- scep (Simple Certificate Enrollment Protocol): Adopt Cisco certificate registration protocol to apply for the certificate online or offline; support using the CA of the SCEP protocol;
- windows: Adopt Microsoft private protocol to apply for the certificate online or offline; support Windows Server 2000 CA, Windows Server 2003 CA, Windows Server 2008 CA.

Table 8-5 Configure the CA type

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the trust domain configuration mode	**crypto ca identity** *ca-name*	-
Configure the CA type	**ca type** { **other** | **scep** | **ctca** | **windows** [**renewal** *renewal-number*] }	Optional By default, the CA type is scep.

Note:

- After renewing the CA certificate on windows CA server, the new, old CA certificates and CRL list all exist, and the CA certificate and CRL list serial numbers increase by degrees from 0. Therefore, when the CA type is windows, we can configure the renewal parameter to get the CA certificate and CRL list of the specified renewal-number.

Configure Terminal Entity DN

One digital certificate is the binding of one public key and one identity, while the identity should be associated with one specified terminal entity. DN (Distinguished Name) is the identity

information of the terminal entity. CA uniquely identifies the certificate applicant according to the identity information provided by the terminal entity.

The common parameters of the terminal entity DN include:

- Locality name: L for short, indicating the name of the located geographical area;
- Country name: C for short, indicating the code of the belonging country, expressed by the standard two-character code. For example, “CN” is the valid country code of China;
- State or province name: ST for short, indicating the name of the located state or province;
- Organization name: O for short, indicating the name of the located organization;
- Organizational Unit Name: OU for short, indicating the name of the located department;
- Email address: E for short, indicating the email address;
- Common name: CN for short, indicating the name;

During the configuration, use the abbreviation. For example, one DN indicating Zhangsan is C=CN, ST= Sichuan, O=China Telecom, OU=Technical office, OU=operation, maintenance and management, CN=Zhangsan, E=zs@ctca.com.cn.

Table 8-6 Configure the terminal entity DN

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the trust domain configuration mode	**crypto ca identity** *ca-name*	-
Create the DN and enter the DN configuration mode	**subject-name** *subject-name*	Mandatory By default, do not configure the topic name.

Step	Command	Description
Configure the key type and length	**key-type** { **rsa** { **key-size** {**1024** | **2048** | **512** } } | **sm2** }	Optional By default, the key type is RSA and the key length is 512 bits.
Configure the password	**password** *password*	Optional By default, DN is not configured with password; when configuring the CA type as scep, we need to configure the password.
Configure the auto registration	**auto-enroll**	Optional By default, do not apply for the terminal entity certificate automatically. After configuring auto application, the device will apply for the certificate automatically; if application fails, the device will re-try until the certificate is applied successfully; if applying for the certificate manually and automatically is configured at the same time and when the applying for the certificate manually fails, the device will re-try until the certificate is applied successfully.

Note:

- Multiple different terminal entity subject names cannot be configured in the same trust domain, that is, only one subject name can be configured under the trust domain, and the subject name must be configured to apply for a certificate.
- The format content of the DN takes the requirements of the CA server as reference. For example, some CA server requires that there should be CN; the CA server of Microsoft has the limitation for the DN length;

- The content of DN is specified by the user or pre-distributed by the CA server. For example, some CA server binds the distributed DN with the password. When the terminal entity applies for the certificate, it should configure the specified DN and carry the matching password. Otherwise, the certificate cannot be applied successfully.

Configure HTTP User Name and Password

The packets of applying for and getting the online certificate need the security guarantee. This can ensure the security and reliability of the certificate better. There can be various modes, such as adopting the SSL protocol protection, or enabling the HTTP authentication mode to protect.

When configuring the CA type as windows and Microsoft CA server enables the HTTP integrating Windows ID authentication and adopts NTLM (WindowsNT LAN Manager Challenge/Response) mode and basic ID authentication (sending password by the plaintext mode), the user needs to provide the authentication user name and password for the authentication and interaction of the HTTP protocol packets, completing the application and getting of the online certificate.

Table 8-7 Configure the HTTP user name and password

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the trust domain configuration mode	**crypto ca identity** *ca-name*	-
Configure the HTTP user name and password	**ca username** *username* **password** *password*	Mandatory By default, do not configure the authentication user name or password; do not encapsulate the authentication information for the HTTP request packet. The specific user name and password are got from the system administrator of the CA server.

Configure Hash Algorithm

When the terminal entity applies for the certificate, it is necessary to adopt the specified hash algorithm for the signature of the self-signature certificate. Currently, the device mainly supports configuring sha1 (Secure Hash Algorithm) and country commercial password hash algorithm sm3.

Table 8-8 Configure the hash algorithm

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the trust domain configuration mode	**crypto ca identity** *ca-name*	-
Configure the hash algorithm	**hash** { **sha1 | sm3** }	Optional By default, the self-signature certificate of the device uses the secure hash algorithm sha1.

Configure Source Interface or Source IP Address

In the specified environment, if the source addresses for the online certificate application packets are limited, we can configure the source interface or source IP address of the packet sent by the device, avoiding the failure of the certificate application. Please configure the item according to the actual environment requirement.

Table 8-9 Configure the source interface or source IP address

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the trust domain configuration mode	**crypto ca identity** *ca-name*	-
Configure the source interface or source IP address	**local** { **address** *ip-address* | **interface** *interface-name* }	Mandatory By default, the source IP address of the online certificate application packet is the IP address of the egress interface of the route to the CA server.

8.2.2. Configure Certificate Authentication

The validity of the digital certificate mainly includes three parts: the correctness of the CA digital signature (that is, the authenticity of the digital certificate), whether the digital certificate is canceled, and whether the digital certificate is in the validity. The premise of using the digital

certificate is that it is valid. Therefore, we should check the validity of the used digital certificate first.

- The core of the digital certificate authentication is to check the signature of the CA on the digital certificate. Therefore, before authenticating the digital certificate, first get the CA certificate;
- When configuring the certificate authentication, we can set whether to check the CRL canceling list;
- When configuring the certificate authentication, we can set whether to check the validity. If setting to check, ensure that the system clock of the device is synchronized with the system clock of the CA server. The validity check contains the valid start date of the digital certificate and the valid end date of the digital certificate;
- The user can force to set the certificate trust status as trust (forced to be valid), un-trust (forced to be invalid) or auto trust (that is, check the validity by the above certificate authentication modes).

Configuration Condition

When configuring the certificate authentication, first complete the following task:

- Configure one trust domain
- To get the CA certificate or CRL list online, we need to ensure that the network between the device and CA is reachable.

Configure Getting and Authenticating CA Certificate

The CA certificate is the certificate identifying the CA itself. If there are multiple CAs in the PKI system, form one CA hierarchy. The top CA is the root CA and it has one CA “self-signature” certificate. The root CA is the starting point of the trust and its lower layer may be the sub CA, or RA, or the root CA directly faces the terminal entity.

CA is the core of PKI and the importance of its certificate goes without saying. The concern of the terminal entity is how to get the CA certificate and validate its validity, so as to prepare for the trust chain for authenticating the CRL list and terminal entity certificate later (certificate chain).

Besides the above mentioned, the validity authentication of the CA certificate also needs to appraise that the CA certificate is really from the specified CA, because maybe the CA certificate is replaced by one hacker. If we do not appraise the CA certificate, the later security actions are wasted, because the starting point of the trust has problems. One common appraising mode is to check the fingerprint of the CA certificate. It needs one secure mode to get the fingerprint of its certificate from the CA and calculates the fingerprint after the device gets the CA certificate. Compare the two. If consistent, it indicates that the source of the CA certificate is reliable. The fingerprint can be got offline or online based on the security, such as SSL.

Table 8-10 Configure getting and authenticating CA certificate

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the trust domain configuration mode	**crypto ca identity** *ca-name*	-
Configure getting and authenticating the CA certificate automatically	**auto-authenticate** [**fingerprint** *fingerprint-string*]	Optional By default, do not get the CA certificate automatically. After automatically applying for and authenticating the certificate, the device will automatically apply for the certificate. If applying fails, the device will re-try until the certificate is applied successfully; if applying for the certificate manually and automatically is configured at the same time and when the applying for the certificate manually fails, the device will re-try until the certificate is applied successfully.
Return to the global configuration mode	**exit**	-

Step	Command	Description
Configure getting and authenticating the CA certificate manually	**crypto ca authenticate** *ca-name* [**no-confirm**]	Optional By default, do not get the CA certificate manually. If not configuring no-confirm and not configuring getting and authenticating the CA certificate automatically, display the fingerprint of the CA certificate and prompt the user to confirm whether to accept the got CA certificate.
Configure offline importing and authenticating the CA certificate	**crypto ca import certificate** [*file-name* [**to** *ca-name*] | **to** *ca-name*]	Optional By default, the device does not import the CA certificate manually. The importing format supports DER (Distinguished Encoding Rules), Base64 (a commonly-used encoding standard of converting hexadecimal data into visible character) and PKCS # 7 (Cryptographic Message Syntax Standard).

Note:

- If there is the root CA certificate in the specified trust domain, do not permit to re-execute the operation of getting the root CA certificate. To re-get, first delete the root CA certificate and then re-execute the operation of getting the root CA certificate.
- To ensure that the existing certificate on the device (including CA certificate, terminal entity certificate, CRL list) is available, please ensure that the current system time of the device is in the validity of the certificate and had better be synchronous with the system time of the CA server.
- When importing a certificate, if the **subject-name** command is configured under the trust domain, the subject name, secret key length and type of the imported certificate are consistent with the subject name, secret key length and type of the certificate configured by **subject-name**. Otherwise, failed to import the certificate; If the **subject-name** command is not configured under the trust domain, the device creates a subject-name object under the trust domain according to the imported certificate.

Configure Getting and Authenticating CRL List

The structure of the CRL list is similar to the digital certificate. After one digital certificate is canceled, CA will add the certificate to the cancel list and then issues the digital signature to the list, so as to create one valid X.509 v2 CRL list. CA publishes the CRL list to one public repository and the terminal entity can search the repository. When the terminal entity receives one digital certificate, first search CRL according to the policy and judge whether the certificate is canceled. The largest trouble of using the CRL list is to shorten the interval between cancelling the certificate and the terminal entity knowing the message.

The device supports updating the CRL list automatically and the auto update frequency depends on two factors, that is, the CRL next releasing time set by CA policy and the updating period configured by the device.

Table 8-11 Configure getting and authenticating CRL list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the trust domain configuration mode	**crypto ca identity** *ca-name*	-
Configure updating and getting the CRL list automatically	**crl autorenew period** *period-value*	Optional By default, do not update the CRL list automatically.
Return to the global configuration mode	**exit**	-
Configure getting the CRL list manually	**crypto ca crl request** *ca-name*	Optional By default, the device does not get the CRL list manually.
Configure importing the CRL list offline	**crypto ca import CRL** [*file-name* [**to** *ca-name*] | **to** *ca-name*]	Optional By default, the device does not import the CRL list manually. The importing format supports DER and Base64.

Note:

- CRL auto update period refers to the interval of the device downloading the CRL list from the CRL storing server. Compare the manual configured CRL update period plus the current system clock with the update time specified in the CRL list and take the smaller one as the time of updating and getting the CRL list next time.
- If the LDAP server is configured under the trust domain, the CRL is obtained through the LDAP protocol. If the LDAP server is not configured, the CRL is obtained through the enrollment URL.
- CRL auto update function needs to ensure that the system clock of the device is correct and keep synchronous with the system clock of the CA server. We can consider using the NTP (network time protocol) to synchronize the clock. If the system is not correct, or modifying the system clock manually, it may result in the abnormality of CRL updating action.

Configure Policy of Checking Certificate Canceling

The configuration decides whether to check whether the certificate is canceled strictly when authenticating the certificate.

If the configuration is enabled, strictly check the certificate canceling. If we cannot get the valid CRL list, it is regarded that the certificate authentication fails. Ensure the maximum security, but it will reduce the availability.

Usually, the probability of canceling the certificate caused by the leakage of the certificate private key is low and we can control the access for the certificate user, so it is not suggested to enable the option, but ensure the maximum service availability. (By default, check the certificate canceling when the system has the CRL list. Otherwise, omit)

Table 8-12 Configure the policy of checking certificate canceling

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the trust domain configuration mode	**crypto ca identity** *ca-name*	-
Configure the policy of checking certificate canceling	**revoke check** { **off** | **on** }	Optional By default, the function of checking whether the certificate is canceled strictly via the CRL list is disabled.

Configure Policy of Checking Valid Period of Certificate

The configuration decides whether to check the valid period of the certificate strictly when authenticating the certificate validity.

Different system times may cause the mistake of checking the valid period of the certificate and result in the authentication failure, so usually we can omit the check item. The certificate security

is high and according to the present technology, it is nearly impossible to decode the private key of the certificate with a long time, so omitting the check item will not affect the certificate security greatly.

Table 8-13 Configure the policy of checking the valid period of the certificate

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the trust domain configuration mode	**crypto ca identity** *ca-name*	-
Configure the policy of checking certificate validity	**time check** { **off** | **on** }	Optional By default, the function of checking the valid period of the certificate is disabled.

Note:

- If selecting to check the valid period of the certificate, we should configure and synchronize the system time of the device and the CA server correctly. Otherwise, it may result in the failure of checking the valid period of the certificate.

Configure Forcing to Set Certificate Trust Status

Forcing to set the certificate trust status means to set the certificate status as auto check or always trust or never trust. For example, after some certificate passes the validity check and when being used to perform the invalid access, the administrator can contact the system CA administrator and set the trust status of the certificate as never trust.

Table 8-14 Configure forcing to set the certificate trust status

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure forcing to set the certificate trust status	**crypto ca certificate** { **trust** | **autotrust** | **untrust** } *ca-name* { **name** *subject-name* | **sn** *sn-string* }	Optional By default, judge the certificate validity automatically according to the policy of checking the certificate.

8.2.3. Configure Certificate Application and Getting

Certificate application means the terminal entity introduces the process of binding with DN to CA. The terminal entity provides the ID information (DN) for CA and the corresponding public key. The information becomes the important part of the certificate issued to the terminal entity.

Configuration Condition

Before configuring the certificate application and getting, first complete the following task:

- Configure one trust domain and configure the environment for checking the certificate;
- To apply for and get the terminal entity certificate online, ensure the network between the device and CA is reachable.

Configure Certificate Application

The terminal entity puts forward the certificate application to CA and gets the issued certificate. There are two modes, online and offline. In the offline application mode, CA permits the applicant to provide the application information for CA via the out-band mode (such as telephone, disk and email) and get the issued certificate; in the online application mode, the terminal entity interacts with CA via the online protocol to complete the certificate application and getting according to the CA type.

Table 8-15 Configure the certificate application

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the online certificate application	**crypto ca enroll** *ca-name*	Optional By default, the device does not apply for the certificate online manually. When using this command, the trust domain must configure the subject-name command to use the specified key type, key length and subject name, so as to apply for a certificate. subject-name is the configured terminal entity subject name in the trust domain configuration. If **auto-enroll** is configured in subject name the device re-tries automatically when executing the command fails. If not specifying subject-name or subject-name does not configure the password and when the CA type is scep, the user needs to input the password after configuring the command.

Step	Command	Description
Configure the offline certificate application	**crypto ca pkcs10-enroll** *ca-name*	Optional By default, the device will not apply for the certificate offline. When using this command, the trust domain must configure the subject-name command to use the specified key type, key length and subject name, so as to apply for a certificate. Offline certificate application uses the PKCS #10 format and can support any third-party CA.

Note:

- Auto certificate application is configured when configuring the terminal entity subject name.
- The local user certificates of two single certificates are not allowed in the same trust domain. Only the local user certificate of one single certificate is allowed. Two local user certificates with the same subject name are allowed only when there are dual certificates.
- If checking the valid period of the certificate is configured, ensure that the system clock of the device is synchronous with the system time of CA. Otherwise, the valid period of the applied certificate will become abnormal.

Configure Getting Successful-Issued Certificate

There are two modes for CA to audit the issued certificate. One is to audit and issue the terminal entity certificate automatically according to the policy; the other is that the CA system administrator audits and manually issues the terminal entity certificate. The former is convenient when the terminal entity certificate is updated automatically, but the security and controllability are poor; the latter first needs to confirm whether the certificate is issued after the terminal entity issues the certificate application. If the certificate is issued, get the certificate to the local. The mode is not flexible enough, but the security is relatively strong.

Table 8-16 Configure getting successful-issued certificate

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure getting successful-issued certificate	**crypto ca retrieve** *ca-name* {**local** | **peer** *subject-name*}	Optional By default, the device does not get the certificate issued by CA manually. When configuring the command **auto-enroll** of the terminal entity subject name, the device automatically queries the current certificate status and gets back the issued certificate.

Note:

- If checking the valid period of the certificate is configured, ensure that the system time of the device is synchronous with the CA clock. Otherwise, the valid period of the got certificate will become abnormal.

Configure Certificate Importing

There are several kinds of certificates imported via configuration: One is the certificate issued successfully after PKCS #10 request; the second is the certificate of other terminal entity; the third is the terminal entity certificate imported via PKCS #12 (Personal Information Exchange Syntax Standard) format.

Table 8-17 Configure the certificate importing

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure importing the certificate without private key	**crypto ca import certificate** [*file-name* [**to** *ca-name*] | **to** *ca-name*]	Optional By default, the device does not import the certificate manually. The importing format supports DER, Base64, and PKCS #7.

Step	Command	Description
Configure importing the certificate with private key	**crypto ca import pkcs12** { *file-name* [*pkcs12-password* [**to** *ca-name*] | **to** *ca-name*] | **ftp** *ip-address username ftp-password file-name* [*pkcs12-password* [**to** *ca-name*] | **to** *ca-name*] | **inputs** [*pkcs12-password* [**to** *ca-name*] | **to** *ca-name*] | **tftp** *ip-address file-name* [*pkcs12-password* [**to** *ca-name*] | **to** *ca-name*] }	Optional By default, the device does not import the pkcs12 certificate manually. The importing format supports PKCS #12.

Note:

- If checking the valid period of the certificate is configured, ensure that the system clock of the device is synchronous with the CA clock. Otherwise, the valid period of the imported certificate will become abnormal.

8.2.4. Configure LDAP to Get Certificate

The local certificate and peer certificate can be got via the LDAP server.

Configuration Conditions

Before configuring the certificate, first complete the following tasks:

- Configure a trust domain and configure the certificate acquisition environment;
- Online application for terminal entity certificate needs to ensure that the network between the device and the CA is reachable.
- Configure the LDAP server.

Configure the LDAP Server

Create a trust domain and configure the LDAP server.

Table 8-18 Configure the LDAP server

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the trust domain configuration mode	**crypto ca identity** *ca-name*	Mandatory Create a trust domain.
Configure the LDAP server	**ldap-server host** *host-name* **[port** *port-num***] [vrf** *vrf-name***]**	Optional By default, the device does not configure the LDAP server.

Configure LDAP to Get Certificate

Table 8-19 Configure LDAP to get the certificate

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure LDAP to get the local or peer certificate	**crypto ca retrieve** *ca-name* {local | peer *subject-name*}	Optional By default, the device will not manually obtain the local and peer certificates through LDAP online. When obtaining the local or peer user certificates through LDAP, you need to configure the LDAP server address to ensure that the LDAP server address is reachable and the network is connected, and the certificates to be obtained also need to ensure that they have been successfully published on the LDAP server. Otherwise ,obtaining the certificates through LDAP will fail. When obtaining the local user certificate, subject-name must be configured under the trust domain, and the private key corresponding to the certificate exists locally. Otherwise, the obtained certificate will be regarded as the peer certificate; When obtaining the peer user certificate, you only need to ensure that the certificate has been successfully published on the LDAP server.

8.2.5. Configure Deleting Certificate

Unless the certificate has expired, or has been archived, or do not recommend the user to delete the local saved certificate, especially the certificate of the local device. Once being deleted, we can only re-apply for the new certificate from CA.

Configuration Condition

None

Configure Deleting Certificate

Table 8-20 Configure deleting certificate

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure deleting certificate	**no crypto ca certificate** *ca-name* { **name** *subject-name* | **sn** *sn-string* | **type** { **all** | **crl** | **my** | **remote** | **requesting** | **root** } }	Mandatory By default, do not delete the certificate. The types of the certificates that can be deleted include CA certificate, terminal entity certificate, CRL list, self-signature certificate in the request state.

8.2.6. PKI Monitoring and Maintaining

Table 8-21 PKI monitoring and maintaining

Command	Description
show crypto ca identity	Display the trust domain information
show crypto ca remotepubkey der [**name** *subject-name*]	Display the local saved remote public key information
show crypto ca mypubkey der [**name** *subject-name*]	Display the public key information saved at the local
show crypto ca certificates der [*ca-name* [**name** *subject-name* | **sn** *sn-string*] | **name** *subject-name* | **sn** *sn-string*]	Display the certificate information in the hex DER code format according to the certificate domain, certificate domain plus certificate topic or certificate serial number, or directly display the certificate information according to the certificate topic or certificate serial number

Command	Description
show crypto ca certificates general [*ca-name* [**name** *subject-name* | **sn** *sn-string*] | **name** *subject-name* | **sn** *sn-string*]	Display the certificate information in the general format according to the certificate domain, certificate domain plus certificate topic or certificate serial number, or directly display the certificate information according to the certificate topic or certificate serial number
show crypto ca certificates list	Display all certificate information on the device in the general format
show crypto ca certificates pem [*ca-name* [**name** *subject-name* | **sn** *sn-string*] | **name** *subject-name* | **sn** *sn-string*]	Display the certificate information in the PEM format according to the certificate domain, certificate domain plus certificate topic or certificate serial number, or directly display the certificate information according to the certificate topic or certificate serial number
show crypto ca ca-certificates [**der** | **general** | **pem**]	Display the CA certificate information
show crypto ca event	Display the information of the event to be processed
show crypto ca eventstatis [*ca-name*]	Display the data of executing the PKI statistics event
show crypto ca my-certificates [**der** | **general** | **pem**]	Display the local certificate information
show crypto ca remote-certificates [**der** | **general** | **pem**]	Display the remote certificate information
show crypto ca **crls** [**der** | **general** | **pem**]	Display the certificate canceling list information
show crypto ca pkcs10 [*ca-name* [*subject-name*]]	Display the PKCS10 offline certificate application information

Command	Description
show crypto ca state	Display the information of the nodes in the PKI status list
clear crypto ca eventstatis	Clear the statistics data of the PKI event

8.3. PKI Typical Configuration Example

8.3.1. Configure Online Applying for Certificate

Network Requirements

- Device1 and Devices set up the IPsec tunnel by the pre-share key mode; Device applies for the certificate online from the CMS server via the IPsec tunnel; Device2 applies for the certificate online from CMS;
- After Device1 and Device2 apply for the certificate, set up the IPsec tunnel by the digital signature authentication mode, protecting the data communication of the network where PC1 and PC2 are located;
- IPsec proposal security protocol adopts ESP, IKE proposal and IPsec proposal encryption algorithm adopts 3DES and the authentication algorithm adopts MD5.

Network Topology

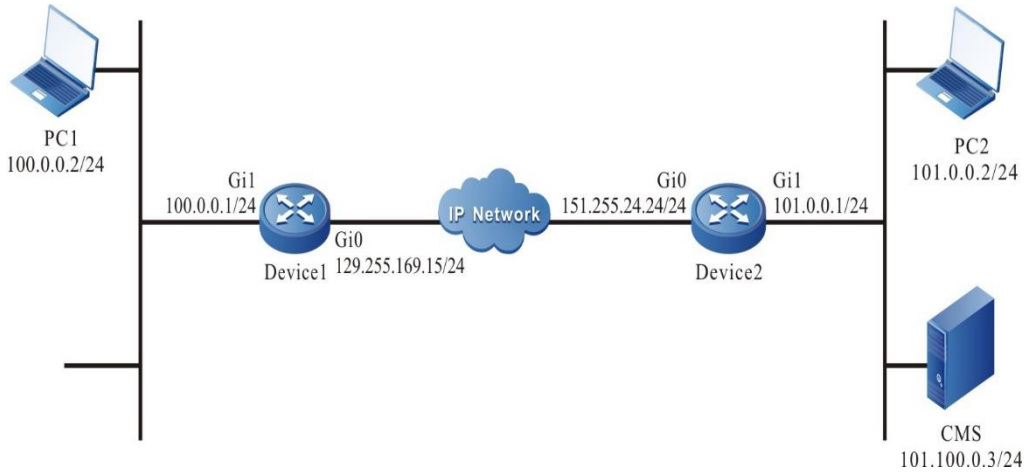


Figure 8-1Networking of configuring the online applying for certificate

Configuration Steps

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

Step 2: Configure the CMS server.

#For the configuration of the CMS server, refer to the CMS chapter of the configuration manual.

#On CMS server, register two users; the user DNs are CN=Device1, C=CN and CN=Device2, C=CN respectively; the user passwords are both set as admin.

Step 3: Configure trust domain.

#On Device1, configure trust domain myca, configure the address of the CA server as 101.0.0.3, and the source address of the applied certificate is 100.0.0.1.

```
Device1#configure terminal
Device1(config)#crypto ca identity myca
Device1(ca-identity)#enrollment url 101.0.0.3
Device1(ca-identity)#local address 100.0.0.1
Device1(ca-identity)#subject-name CN=Device1,C=CN
Device1(config-subject-name)#key-type rsa key-size 1024
Device1(config-subject-name)#exit
Device1(ca-identity)#exit
```

#On Device2, configure trust domain myca and configure the address of the CA server as 101.0.0.3.

```
Device2#configure terminal
Device2(config)#crypto ca identity myca
Device2(ca-identity)#enrollment url 101.0.0.3
Device2(ca-identity)#subject-name CN=Device2,C=CN
Device2(config-subject-name)#key-type rsa key-size 1024
Device2(config-subject-name)#exit
Device2(ca-identity)#exit
```

Note:

- Subject-name must be configured in the trust domain to apply for user certificate. Each trust domain can only be configured with one subject-name.

Step 4: Configure the IKE and IPSec proposal.

#On Device1, configure the IKE proposal ikepro, use the encryption algorithm 3DES, authentication algorithm MD5; configure IPsec proposal ippro, use the ESP security protocol, use the encryption algorithm 3DES, and authentication algorithm MD5.

```
Device1(config)#crypto ike proposal ikepro
Device1(config-ike-prop)#encryption 3des
Device1(config-ike-prop)#integrity md5
Device1(config-ike-prop)#exit
Device1(config)#crypto ipsec proposal ippro
Device1(config-ipsec-prop)#esp 3des md5
Device1(config-ipsec-prop)#exit
```

#On Device2, configure the IKE proposal ikepro, use the encryption algorithm 3DES, authentication algorithm MD5; configure IPsec proposal ippro, use the ESP security protocol, use the encryption algorithm 3DES, and authentication algorithm MD5.

```
Device2(config)#crypto ike proposal ikepro
Device2(config-ike-prop)#encryption 3des
Device2(config-ike-prop)#integrity md5
```

```
Device2(config-ike-prop)#exit
Device2(config)#crypto ipsec proposal ippro
Device2(config-ipsec-prop)#esp 3des md5
Device2(config-ipsec-prop)#exit
```

Step 5: Configure the pre-share key.

#On Device1, configure the pre-share key, key is admin and permit all peers to use the key.

```
Device1(config)#crypto ike key admin any
```

#On Device2, configure the pre-share key, key is admin and permit all peers to use the key.

```
Device2(config)#crypto ike key admin any
```

Step 6: Configure the IPSec tunnel.

#On Device1, configure the tunnel tun, use gigabitethernet0 interface as the local interface of the tunnel, configure the peer address of the tunnel as 151.255.24.24, the IKE proposal uses ikepro, IPsec proposal uses ippro, and enable the auto initiating negotiation.

```
Device1(config)#crypto tunnel tun
Device1(config-tunnel)#local interface gigabitethernet0
Device1(config-tunnel)#peer address 151.255.24.24
Device1(config-tunnel)#set ike proposal ikepro
Device1(config-tunnel)#set ipsec proposal ippro
Device1(config-tunnel)#set auto-up
Device1(config-tunnel)#exit
```

#On Device2, configure the tunnel tun, use gigabitethernet0 interface as the local interface of the tunnel, configure the peer of the tunnel as any, the IKE proposal uses ikepro, and IPsec proposal uses ippro.

```
Device2(config)#crypto tunnel tun
Device2(config-tunnel)#local interface gigabitethernet0
Device2(config-tunnel)#peer any
Device2(config-tunnel)#set ike proposal ikepro
Device2(config-tunnel)#set ipsec proposal ippro
Device2(config-tunnel)#exit
```

Note:

- When not specifying the authentication mode, first use the digital signature authentication; if no certificate, adopt the pre-share key authentication.

Step 7: Configure the IPSec security policy.

#On Device1, configure the security policy policy1, protect the IP communication from network 100.0.0.0/24 to network 101.0.0.0/24, and associate the tunnel tun.

```
Device1(config)#crypto policy policy1
Device1(config-policy)#flow 100.0.0.0 255.255.255.0 101.0.0.0 255.255.255.0 ip ipv4-tunnel tun
Device1(config-policy)#exit
```

#Configure security policy policy1 on Device2 to protect IP communication from 101.0.0.0/24 to network 100.0.0.0/24 and associate the tunnel tun.

```
Device2(config)#crypto policy policy1
Device2(config-policy)#flow 101.0.0.0 255.255.255.0 100.0.0.0 255.255.255.0 ip ipv4-tunnel tun
Device2(config-policy)#exit
```

Step 8: Configure getting the CA certificate and CRL online and applying for and getting the user certificate online.

#On Device1, get the CA certificate and CRL tunnel online, and apply for and get the user certificate via the IPsec online; the user certificate DN is CN=Device1, C=CN, and the password is admin.

```
Device1(config)#crypto ca authenticate myca


% The Root CA Certificate has the following attributes:
  Serial Number: 179dd41c4574f7e15351
  Subject: CN=root, C=CN
  Issuer : CN=root, C=CN
  Validity
    Start date: 2013-03-28 06:23:51
    End   date: 2028-03-27 06:23:51
  Usage: Sign

  Fingerprint(sha1):7e4b7407cc705a8a66642d00cea139edfd273400

% Do you accept this certificate?[yes]/[no]:

% PKI: Get CA certificate success.

Device1(config)#crypto ca crl request myca

% PKI: Get CRL success.
```

```
Device1(config)#crypto ca enroll myca

% Please input request password:*****
% The Certificate DN will be: CN=Device1,C=CN
% Waiting,Generate 1024 bit RSA keys!
% Generating .
% PKI: Certificate enroll success.
```

#On Device2, get the CA certificate and CRL tunnel online, and apply for and get the user certificate online; the user certificate DN is CN=Device2, C=CN, and the password is admin.

```
Device2(config)#crypto ca authenticate myca


% The Root CA Certificate has the following attributes:
  Serial Number: 179dd41c4574f7e15351
  Subject: CN=root, C=CN
  Issuer : CN=root, C=CN
  Validity
    Start date: 2013-03-28 06:23:51
    End   date: 2028-03-27 06:23:51
  Usage: Sign

  Fingerprint(sha1):7e4b7407cc705a8a66642d00cea139edfd273400

% Do you accept this certificate?[yes]/[no]:

% PKI: Get CA certificate success.

Device2(config)#crypto ca crl request myca

% PKI: Get CRL success.

Device2(config)#crypto ca enroll myca

% Please input request password:*****
% The Certificate DN will be: CN=Device2,C=CN
% Waiting,Generate 1024 bit RSA keys!
```

```
% Generating
% PKI: Certificate enroll success.
```

Step 9: Check the result.

#On Device1, view the tunnel information.

```
Device1#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 34      STATE_QUICK_I2      129.255.24.25   151.255.24.24   151.255.24.24
 33      STATE_MAIN_I4       129.255.24.25   151.255.24.24   151.255.24.24
Device1#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  100.0.0.0/24  101.0.0.0/24  ip  any  any
 local tunnel endpoint : 129.255.24.25 remote tunnel endpoint : 151.255.24.24 , fabric
lpu-node : 0
 the pairs of ESP ipsec sa : id : 34, algorithm : 3DES HMAC-MD5-96
  inbound esp ipsec sa :  spi : 0x6dc22061(1841438817)
     current input 33 packets, 7 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28036/4294967287
     uptime is 0 hour 12 minute 44 second
  outbound esp ipsec sa :  spi : 0x4fc11055(1338052693)
     current output 29 packets, 5 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28036/4294967289
     uptime is 0 hour 12 minute 44 second

total sa and sa group is 1
```

We can see that Device1 and Device2 set up the IPsec tunnel successfully; the source and destination of the applied certificate are the network protected by the IPsec tunnel.

#On Device1, view the online got CA certificate, user certificate, and CRL information.

```
Device1#show crypto ca certificates
Root CA Certificate:
  Status: Valid
  Serial Number: 179dd41c4574f7e15351
  Subject: CN=root, C=CN
```

```
  Issuer : CN=root, C=CN
  Validity
    Start date: 2013-03-28 06:23:51
    End   date: 2028-03-27 06:23:51
  Key Type: RSA(1024 bit)
  Usage: Sign
  Fingerprint(sha1):7e4b7407cc705a8a66642d00cea139edfd273400
  Associated Identity: myca
      index: 10


My Certificate:
  Status: Valid
  Serial Number: ccca972bfc9a4c755551
  Subject: CN=Device1, C=CN
  Issuer : CN=root, C=CN
  Validity
    Start date: 2013-03-29 11:04:44
    End   date: 2014-03-28 11:04:44
  Key Type: RSA(1024 bit)
  Usage: Sign
  Fingerprint(sha1):7808a39ddb643361a625a07bbc6f86ae35c5f628
  Associated Identity: myca
      index: 11

Device1#show crypto ca crls
Certificate Revocation List (CRL):
  Issuer : CN=root, C=CN
  This Update: 2013-03-29 11:01:46
  Next Update: 2013-04-01 11:01:46
  Revoted Certificate count: 9
  Associated Identity: myca
```

We can see that getting CA certificate, user certificate, and CRL online succeeds on Device1.

#On Device2, view the online got CA certificate, user certificate, and CRL information.

```
Device2#show crypto ca certificates
Root CA Certificate:
  Status: Valid
```

```
    Serial Number: 179dd41c4574f7e15351
    Subject: CN=root, C=CN
    Issuer : CN=root, C=CN
    Validity
      Start date: 2013-03-28 06:23:51
      End   date: 2028-03-27 06:23:51
    Key Type: RSA(1024 bit)
    Usage: Sign
    Fingerprint(sha1):7e4b7407cc705a8a66642d00cea139edfd273400
    Associated Identity: myca
        index: 4


  My Certificate:
    Status: Valid
    Serial Number: 441f99bf2a71b2615551
    Subject: CN=Device2, C=CN
    Issuer : CN=root, C=CN
    Validity
      Start date: 2013-03-29 09:41:06
      End   date: 2016-03-28 09:41:06
    Key Type: RSA(1023 bit)
    Usage: Sign
    Fingerprint(sha1):5d4e2f0128fccc8f970cb9038d7abaaa8ed70b9e
    Associated Identity: myca
        index: 5

  Device2#show crypto ca crls
  Certificate Revocation List (CRL):
    Issuer : CN=root, C=CN
    This Update: 2013-03-29 09:35:22
    Next Update: 2013-04-01 09:35:22
    Revoted Certificate count: 8
    Associated Identity: myca
```

We can see that getting CA certificate, user certificate, and CRL online succeeds on Device2.

#On Device1, use the command **clear crypto sa** to clear the tunnel, re-negotiate the tunnel by the digital signature mode, and view the tunnel information.

```
Device1#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 36      STATE_QUICK_I2      129.255.24.25    151.255.24.24    CN=Device2, C=CN
 35      STATE_MAIN_I4       129.255.24.25    151.255.24.24    CN=Device2, C=CN

Device1#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  100.0.0.0/24  101.0.0.0/24  ip  any  any
 local tunnel endpoint : 129.255.24.25 remote tunnel endpoint : 151.255.24.24 , fabric
lpu-node : 0
 the pairs of ESP ipsec sa : id : 36, algorithm : 3DES HMAC-MD5-96
  inbound esp ipsec sa :  spi : 0x78412062(2017534050)
     current input 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28618/4294967295
     uptime is 0 hour 3 minute 2 second
  outbound esp ipsec sa :  spi : 0x14ff1056(352260182)
     current output 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28618/4294967295
     uptime is 0 hour 3 minute 2 second

total sa and sa group is 1
```

We can see that Device1 sets up the IPsec tunnel with Device2 successfully by the digital signature mode.

#On Device1, view the remote got certificate information.

```
Device1# show crypto ca remote-certificates
Remote Certificate:
  Status: Valid
  Serial Number: 441f99bf2a71b2615551
  Subject: CN=Device2, C=CN
  Issuer : CN=root, C=CN
  Validity
    Start date: 2013-03-29 09:41:06
    End   date: 2016-03-28 09:41:06
  Key Type: RSA(1023 bit)
```

```
Usage: Sign
Fingerprint(sha1):5d4e2f0128fccc8f970cb9038d7abaaa8ed70b9e
Associated Identity: myca
    index: 12
```

We can see that Device1 gets the certificate of Device2 CN=Device2, C=CN successfully.

#On Device2, view the tunnel information.

```
Device2#show crypto ike sa
sa-id   negotiation-state     localaddr       peeraddr        peer-identity
 30      STATE_QUICK_R2       151.255.24.24    129.255.24.25    CN=Device1, C=CN
 29      STATE_MAIN_R3        151.255.24.24    129.255.24.25    CN=Device1, C=CN


Device2#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  101.0.0.0/24  100.0.0.0/24  ip  any  any
policy name : subflow-1610612749, the parent policy name : policy1
 f (src, dst, protocol, src port, dst port) :  101.0.0.0/24  100.0.0.0/24  ip  any  any
 local tunnel endpoint : 151.255.24.24 remote tunnel endpoint : 129.255.24.25 , fabric
lpu-node : 0
 the pairs of ESP ipsec sa : id : 30, algorithm : 3DES HMAC-MD5-96
  inbound esp ipsec sa :  spi : 0x14ff1056(352260182)
     current input 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28492/4294967295
     uptime is 0 hour 5 minute 8 second
  outbound esp ipsec sa :  spi : 0x78412062(2017534050)
     current output 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28492/4294967295
     uptime is 0 hour 5 minute 8 second


total sa and sa group is 1
```

We can see that Device2 sets up the IPsec tunnel with Device1successfully by the digital signature mode.

#On Device2, view the remote got certificate information.

```
Device2#show crypto ca remote-certificates
Remote Certificate:
```

Status: Valid

Serial Number: ccca972bfc9a4c755551

Subject: CN=Device1, C=CN

Issuer : CN=root, C=CN

Validity

Start date: 2013-03-29 11:04:44

End date: 2014-03-28 11:04:44

Key Type: RSA(1024 bit)

Usage: Sign

Fingerprint(sha1):7808a39ddb643361a625a07bbc6f86ae35c5f628

Associated Identity: myca

index: 7

We can see that Device2 gets the certificate of Device1 CN=Device1, C=CN successfully.

PC1 can ping PC2 via the IPsec tunnel between Device1 and Device2; the packet is protected by the IPsec tunnel.

8.3.2. Configure Offline Getting Certificate

Network Requirements

- Import the CA certificate, user certificate, and CRL to Device1 and Device2 via the offline mode.
- After Device1 and Device2 get the certificate, set up the IPsec tunnel by the digital signature mode, protecting the data communication of the network where PC1 and PC2 are located;
- IPsec proposal security protocol adopts ESP, encryption algorithm adopts 3DES, authentication algorithm adopts SHA1, IKE proposal encryption algorithm adopts AES128 and the authentication algorithm adopts SHA1.

Network Topology

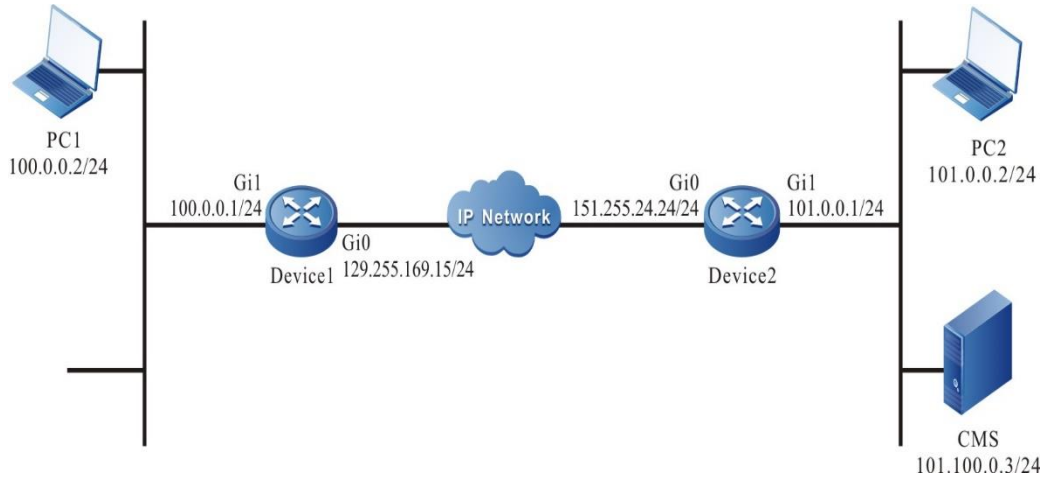


Figure 8-2 Networking of configuring offline getting the certificate

Configuration Steps

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

Step 2: Configure the CMS server and download the certificate.

#For the initializing of the CMS server and the generating of the root certificate and administrator, refer to the CMS chapter of the configuration manual.

#Download the CA certificate and CRL from the CMS server.

#On the CMS server, register two users; the user DNs are CN=Device1, C=CN and CN=Device2, C=CN, and then apply for the certificate and save as the certificate file in the PKCS#12 code format; the exporting password of the certificate is admin. Refer to the CMS chapter of the configuration manual.

Register two users on the CMS server,

Step 3: Configure trust domain.

#On Device1, configure trust domain myca.

```
Device1#configure terminal
Device1(config)#crypto ca identity myca
Device1(ca-identity)#exit
```

#On Device2, configure trust domain myca.

```
Device2#configure terminal
Device2(config)#crypto ca identity myca
Device2(ca-identity)#exit
```

Step 4: Configure importing the CA certificate, user certificate and CRL offline.

#On Device1, import the CA certificate offline. First open the certificate by the notepad, and then copy the content; on Shell, input the **crypto ca import certificate to myca** command and operate according to the prompt and import the CA certificate to the trust domain myca.

```
Device1(config)#crypto ca import certificate to myca
% Input the certificate data, press <Enter> twice to finish:
MIICSQYJKoZIhvcNAQcCoIICOjCCAjYCAQExADALBgkqhkiG9w0BBwGgggleMIICG
jCCAYOgAwIBAgIKF53UHEV09+FTUTANBgkqhkiG9w0BAQUFADAcMQ0wCwYDVQQ
DEw
Ryb290MQswCQYDVQQGEwJDTjAeFw0xMzAzMjgwNjIzNTFaFw0yODAzMjcwNjIzNT
F
aMBwxDTALBgNVBAMTBHJvb3QxCzAJBgNVBAYTAkNOMIGfMA0GCSqGSIb3DQEBA
QUA
A4GNADCBiQKBgQCG31rAAqsZL2kjK+8dttVUyhUwx4BATMIGjD++KIwok6ZD1XP3z
KItRIdk3EFgBD61AuGcTOjexLyWXtWrjEElpVdowerW3ZIeQ02fp7biLtDA6bdioz
Xp0JIHdlZpUmBo6ISLFcqtTGppx28iHxfPLZevE68veBpqVEQOOPkTvwIDAQABo2M
```

wYTAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQU
CVug

KxLpA7IZi26xYqMZNGhZwrcwHwYDVR0jBBgwFoAUCVugKxLpA7IZi26xYqMZNGhZw

rcwDQYJKoZIhvcNAQEFBQADgYEASXjJ0CtwnY6K8g8nxnhUOX9oo9LNnH3eWdFxTh

cVy12HEUAUOc7Bfd+ybmkpyO14TQPoQMFS7Y5ZZ/vJMkiVIoEGQTKPbTWpzh6pp4a

hZJEEzjVm7N2RvB2GPNylV67lmdUPNdyXRvPJCxGYqTMrQlE9zzHqmcGMW+HNK/X
N

4tQxAH==

% The Root CA Certificate has the following attributes:

Serial Number: 179dd41c4574f7e15351

Subject: CN=root, C=CN

Issuer : CN=root, C=CN

Validity

Start date: 2013-03-28 06:23:51

End date: 2028-03-27 06:23:51

Usage: Sign

Fingerprint(sha1):7e4b7407cc705a8a66642d00cea139edfd273400

% Do you accept this root ca-certificate[yes]/[no]:

% PKI: Import Certificate success.

Note:

- The format of the CA certificate is BASE64 code.

#On Device1, import the user certificate offline, select the PKCS12 mode to download the certificate from PC1 via FTP; import the certificate to the trust domain myca and the password is admin; import CRL offline and download CRL to FLASH from PC1 via FTP, and then import CRL in FLASH to the trust domain myca.

Device1(config)#crypto ca import pkcs12 ftp 100.0.0.2 admin admin cn=Device1,c=CN.p12 admin to myca

Downloading###OK!

Import cert from pkcs12 success.

Device1(config-fs)#ftpcopy 100.0.0.2 admin admin CmsCrl0.crl /flash/CmsCrl0.crl

Downloading##OK!

Device1(config)#crypto ca import CRL CmsCrl0.crl to myca

% PKI: Import Certificate success.

#On Device2, import the CA certificate offline. First open the certificate by the notepad, and then copy the content; on Shell, input the **crypto ca import certificate to myca** command and operate according to the prompt and import the CA certificate to the trust domain myca.

Device2(config)#crypto ca import certificate to myca

% Input the certificate data, press <Enter> twice to finish:

MIICSQYJKoZIhvcNAQcCoIICOjCCAjYCAQExADALBgkqhkiG9w0BBwGgggIeMIICG

jCCAYOgAwIBAgIKF53UHEV09+FTUTANBgkqhkiG9w0BAQUFADAcMQ0wCwYDVQQDEw

Ryb290MQswCQYDVQQGEwJDTjAeFw0xMzAzMjgwNjIzNTFaFw0yODAzMjcwNjIzNTF

aMBwxDTALBgNVBAMTBHJvb3QxCzAJBgNVBAYTAkNOMIGfMA0GCSqGSIb3DQEBAQUA

A4GNADCBiQKBgQCG31rAAqsZL2kjK+8dttVUyhUwx4BATMIGjD++KIwok6ZD1XP3z

KItRldk3EFgBD61AuGcTOjexLyWXtWrjEElpVdowerW3ZIeQ02fp7biLtDA6bdioz

Xp0JIHdlZpUmBo6ISLFcqtTGppx28iHxfPLZevE68veBpqVEQOOPkTvwIDAQABo2M

wYTAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUCVug

KxLpA7IZi26xYqMZNGhZwrcwHwYDVR0jBBgwFoAUCVugKxLpA7IZi26xYqMZNGhZw

rcwDQYJKoZIhvcNAQEFBQADgYEASXjJ0CtwnY6K8g8nxnhUOX9oo9LNnH3eWdFxTh

cVy12HEUAUOc7Bfd+ybmkpyO14TQPoQMFS7Y5ZZ/vJMkiVIoEGQTKPbTWpzh6pp4a

hZJEEzjVm7N2RvB2GPNylV67lmdUPNdyXRvPJCxGYqTMrQlE9zzHqmcGMW+HNK/XN

4tQxAH==

% The Root CA Certificate has the following attributes:

Serial Number: 179dd41c4574f7e15351

Subject: CN=root, C=CN

Issuer : CN=root, C=CN

Validity

```
  Start date: 2013-03-28 06:23:51
  End   date: 2028-03-27 06:23:51
 Usage: Sign

  Fingerprint(sha1):7e4b7407cc705a8a66642d00cea139edfd273400

 % Do you accept this root ca-certificate[yes]/[no]:

 % PKI: Import Certificate success.
```

#On Device2, import the user certificate offline, select the PKCS12 mode to download the certificate from PC2 via FTP; import the certificate to the trust domain myca and the password is admin; import CRL offline and download CRL to FLASH from PC2 via FTP, and then import CRL in FLASH to the trust domain myca.

```
Device2(config)#crypto ca import pkcs12 ftp 101.0.0.2 admin admin cn=Device2,c=CN.p12 admin to myca

Downloading###OK!
 Import cert from pkcs12 success.

Device2(config-fs)#ftpcopy 101.0.0.2 admin admin CmsCrl0.crl /flash/CmsCrl0.crl

Downloading##OK!

Device2(config)#crypto ca import CRL CmsCrl0.crl to myca
% PKI: Import Certificate success.
```

#On Device1, view the CA certificate, user certificate, and CRL.

```
Device1#show crypto ca certificates
Root CA Certificate:
  Status: Valid
  Serial Number: 179dd41c4574f7e15351
  Subject: CN=root, C=CN
  Issuer : CN=root, C=CN
  Validity
    Start date: 2013-03-28 06:23:51
    End   date: 2028-03-27 06:23:51
  Key Type: RSA(1024 bit)
  Usage: Sign
  Fingerprint(sha1):7e4b7407cc705a8a66642d00cea139edfd273400
```

Associated Identity: myca

index: 1

My Certificate:

Status: Valid

Serial Number: 34a9765647f716e65351

Subject: CN=Device1, C=CN

Issuer : CN=root, C=CN

Validity

Start date: 2013-03-28 06:41:26

End date: 2016-03-27 06:41:26

Key Type: RSA(511 bit)

Usage: Sign

Fingerprint(sha1):357462d37b911cba1ecddaa2e7a72019e0ca7014

Associated Identity: myca

index: 2

Device1#show crypto ca crls

Certificate Revocation List (CRL):

Issuer : CN=root, C=CN

This Update: 2013-03-28 06:44:55

Next Update: 2013-03-31 06:44:55

Revoted Certificate count: 1

Associated Identity: myca

We can see that getting the CA certificate, user certificate and CRL succeeds offline on Device1.

#On Device1, view the CA certificate, user certificate and CRL.

Device2#show crypto ca certificates

Root CA Certificate:

Status: Valid

Serial Number: 179dd41c4574f7e15351

Subject: CN=root, C=CN

Issuer : CN=root, C=CN

Validity

Start date: 2013-03-28 06:23:51

End date: 2028-03-27 06:23:51

Key Type: RSA(1024 bit)

Usage: Sign

```
    Fingerprint(sha1):7e4b7407cc705a8a66642d00cea139edfd273400
    Associated Identity: myca
        index: 1


  My Certificate:
    Status: Valid
    Serial Number: 34a9765647f785e65351
    Subject: CN=Device2, C=CN
    Issuer : CN=root, C=CN
    Validity
      Start date: 2013-03-28 06:43:17
      End   date: 2016-03-27 06:43:17
    Key Type: RSA(511 bit)
    Usage: Sign
    Fingerprint(sha1):fc3606db8fe2fbd376ec94e7cccaa090ec128587
    Associated Identity: myca
        index: 2
  Device2#show crypto ca crls
  Certificate Revocation List (CRL):
    Issuer : CN=root, C=CN
    This Update: 2013-03-28 06:44:55
    Next Update: 2013-03-31 06:44:55
    Revoted Certificate count: 1
    Associated Identity: myca
```

We can see that getting the CA certificate, user certificate and CRL succeeds offline on Device2.

Step 5: Configure the IKE and IPSec proposal.

#On Device1, configure the IKE proposal ikepro, use the encryption algorithm AES128, authentication algorithm SHA1; configure IPsec proposal ippro, use the ESP security protocol, use the encryption algorithm 3DES, and authentication algorithm SHA1.

```
Device1(config)#crypto ike proposal ikepro
Device1(config-ike-prop)#encryption aes128
Device1(config-ike-prop)#integrity sha1
Device1(config-ike-prop)#exit
Device1(config)#crypto ipsec proposal ippro
Device1(config-ipsec-prop)#esp 3des sha1
Device1(config-ipsec-prop)#exit
```

#On Device2, configure the IKE proposal ikepro, use the encryption algorithm AES128, authentication algorithm SHA1; configure IPsec proposal ippro, use the ESP security protocol, use the encryption algorithm 3DES, and authentication algorithm SHA1.

```
Device2(config)#crypto ike proposal ikepro
Device2(config-ike-prop)#encryption aes128
Device2(config-ike-prop)#integrity sha1
Device2(config-ike-prop)#exit
Device2(config)#crypto ipsec proposal ippro
Device2(config-ipsec-prop)#esp 3des sha1
Device2(config-ipsec-prop)#exit
```

Step 6: Configure the IPSec tunnel.

#On Device1, configure the tunnel tun, use gigabitethernet0 address as the local address of the tunnel, configure the peer address of the tunnel as 151.255.24.24, the IKE proposal uses ikepro, IPsec proposal uses ippro, and enable the auto initiating negotiation.

```
Device1(config)#crypto tunnel tun
Device1(config-tunnel)#local address 129.255.169.15
Device1(config-tunnel)#peer address 151.255.24.24
Device1(config-tunnel)#set ike proposal ikepro
Device1(config-tunnel)#set ipsec proposal ippro
Device1(config-tunnel)#set auto-up
Device1(config-tunnel)#exit
```

#On Device2, configure the tunnel tun, use gigabitethernet0 address as the local address of the tunnel, configure the peer of the tunnel as any, the IKE proposal uses ikepro, and IPsec proposal uses ippro.

```
Device2(config)#crypto tunnel tun
Device2(config-tunnel)#local address 151.255.24.24
Device2(config-tunnel)#peer any
Device2(config-tunnel)#set ike proposal ikepro
Device2(config-tunnel)#set ipsec proposal ippro
Device2(config-tunnel)#exit
```

Step 7: Configure the IPSec security policy.

#On Device1, configure the security policy policy1, protect the IP communication from network 100.0.0.0/24 to network 101.0.0.0/24, and associate the tunnel tun.

```
Device1(config)#crypto policy policy1
Device1(config-policy)#flow 100.0.0.0 255.255.255.0 101.0.0.0 255.255.255.0 ip ipv4-tunnel tun
```

```
Device1(config-policy)#exit
```

#On Device2, configure the security policy policy1, protect the IP communication from network 101.0.0.0/24 to network 100.0.0.0/24, and associate the tunnel tun.

```
Device2(config)#crypto policy policy1
Device2(config-policy)#flow 101.0.0.0 255.255.255.0 100.0.0.0 255.255.255.0 ip ipv4-tunnel tun
Device2(config-policy)#exit
```

Step 8: Check the result.

#On Devie1, view the tunnel setup information.

```
Device1#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 6       STATE_QUICK_I2      129.255.169.15  151.255.24.24    CN=Device2, C=CN
 5       STATE_MAIN_I4       129.255.169.15  151.255.24.24    CN=Device2, C=CN

Device1#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  100.0.0.0/24  101.0.0.0/24  ip  any  any
 local tunnel endpoint : 129.255.169.15 remote tunnel endpoint : 151.255.24.24 , fabric lpu-node : 0
 the pairs of ESP ipsec sa : id : 6, algorithm : 3DES HMAC-SHA1-96
  inbound esp ipsec sa :  spi : 0xb788104b(3079147595)
     current input 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28178/4294967295
     uptime is 0 hour 10 minute 22 second
  outbound esp ipsec sa :  spi : 0x9e00104b(2650804299)
     current output 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28178/4294967295
     uptime is 0 hour 10 minute 22 second

total sa and sa group is 1
```

We can see that Device1 sets up the tunnel with Device2 successfully by the digital signature mode.

#View the tunnel setup information on Device2.

```
Device2#show crypto ike sa
sa-id   negotiation-state     localaddr       peeraddr        peer-identity
 22      STATE_QUICK_R2       151.255.24.24   129.255.169.15  CN=Device1, C=CN
 21      STATE_MAIN_R3        151.255.24.24   129.255.169.15  CN=Device1, C=CN

Device2#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  101.0.0.0/24  100.0.0.0/24  ip  any  any
policy name : subflow-1610612738, the parent policy name : policy1
 f (src, dst, protocol, src port, dst port) :  101.0.0.0/24  100.0.0.0/24  ip  any  any
 local tunnel endpoint : 151.255.24.24 remote tunnel endpoint : 129.255.169.15 , fabric
lpu-node : 0
 the pairs of ESP ipsec sa : id : 22, algorithm : 3DES HMAC-SHA1-96
  inbound esp ipsec sa :  spi : 0x9e00104b(2650804299)
     current input 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28068/4294967295
     uptime is 0 hour 12 minute 12 second
  outbound esp ipsec sa :  spi : 0xb788104b(3079147595)
     current output 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28068/4294967295
     uptime is 0 hour 12 minute 12 second

total sa and sa group is 1
```

We can see that Device2 sets up the tunnel with Device1 successfully by the digital signature mode.

PC1 can ping PC2 via the IPsec tunnel between Device1 and Device2; the packet is protected by the IPsec tunnel.

8.3.3. Configure LDAP to Download User Certificate

Network Requirements

- After Device1 and Device2 apply for SM2 certificate from JIT server offline and online respectively, Device1 downloads local user certificate and peer user certificate from CMS server via LDAP through IPSec tunnel.
- After obtaining the certificate, Device1 and Device2 establish an IPSec tunnel in the form of digital envelope authentication to protect the data communication of the network where PC1 and PC2 are located.

- IPSec proposes ESP as the security protocol, 3DES as the encryption algorithm, SHA1 as the authentication algorithm, and IKE proposes 3DES as the encryption algorithm and SHA1 as the authentication algorithm.

Network Topology

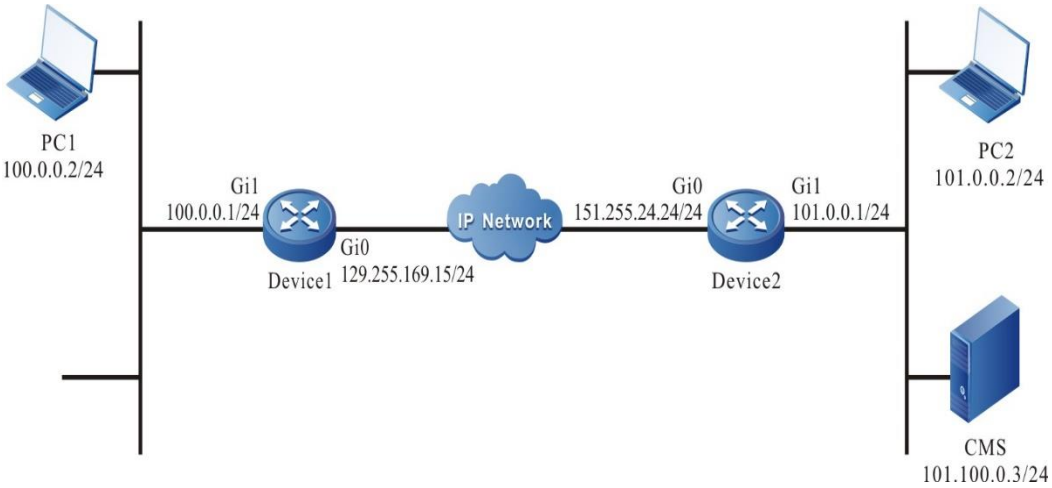


Figure 8-3 Networking of configuring LDAP to download the user certificate

Configuration Steps

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

Step 2: Configure the CMS server.

#Refer to the certificate server installation and deployment manual for CMS server initialization installation.

#Log into CMS server http://101.0.0.3:8443, enter the CA signing certificate information page in the system settings directory and download the CA certificate rootcert.cer.

#Log into CMS server http://101.0.0.3:9443, enter the template management page in the system management directory, select the general certificate template, and then check Yes when publishing the certificate to the directory server.

#Log into CMS server http://101.0.0.3:8443, enter the SCEP configuration page in the system setting directory, and select the general certificate template for the certificate template.

Note:

- The certificate in the certificate template is published to the directory server. If yes is checked, the offline user certificate applied through the template can be published and downloaded using LDAP.

Step 3: Configure the trust domain.

#Configure the trust domain myca on Device1, configure the LDAP server address as 101.0.0.3, the download certificate source address as 100.0.0.1, and the user certificate name as C=CN, O=MPTEST, CN=Device1.

```
Device1#configure terminal
Device1(config)#crypto ca identity myca
Device1(ca-identity)#hash sm3
Device1(ca-identity)#ldap-server host 101.0.0.3
```

```
Device1(ca-identity)#local address 100.0.0.1
Device1(ca-identity)#subject-name C=CN, O=MPTEST, CN=Device1
Device1(config-subject-name)#key-type sm2
Device1(config-subject-name)#exit
Device1(ca-identity)#exit
```

#Configure the trust domain myca on Device2, configure the CA server address as 101.0.0.3, and the user certificate name as C=CN, O=MPTEST, CN=Device2.

```
Device2#configure terminal
Device2(config)#crypto ca identity myca
Device2(ca-identity)#enrollment url 101.0.0.3:30445/pkiclient.exe
Device2(ca-identity)#hash sm3
Device2(ca-identity)#subject-name C=CN, O=MPTEST, CN=Device2
Device2(config-subject-name)#key-type sm2
Device2(config-subject-name)#exit
Device2(ca-identity)#exit
```

Caution:

- For the user certificate published to the directory server through the certificate, the fields except for CN must be the same as the root certificate fields of the certificate server before it can be published and downloaded through LDAP. The certificate name of the current root certificate is C=CN, O=MPTEST, CN=MAIPU CA, and the certificate name of Device1 is the same as the root certificate except for the CN field

Step 4: Configure the IKE and IPsec proposal.

#On Device1, configure IKE proposal ikepro, use encryption algorithm 3DES and authentication algorithm MD5; Configure IPSec proposal ippro, use ESP security protocol, use encryption algorithm 3DES and authentication algorithm MD5.

```
Device1(config)#crypto ike proposal ikepro
Device1(config-ike-prop)#encryption 3des
Device1(config-ike-prop)#integrity md5
Device1(config-ike-prop)#exit
Device1(config)#crypto ipsec proposal ippro
Device1(config-ipsec-prop)#esp 3des md5
Device1(config-ipsec-prop)#exit
```

#On Device2, configure IKE proposal ikepro, use encryption algorithm 3DES and authentication algorithm MD5; Configure IPSec proposal ippro, use ESP security protocol, use encryption algorithm 3DES and authentication algorithm MD5.

```
Device2(config)#crypto ike proposal ikepro
Device2(config-ike-prop)#encryption 3des
Device2(config-ike-prop)#integrity md5
Device2(config-ike-prop)#exit
```

```
Device2(config)#crypto ipsec proposal ippro
Device2(config-ipsec-prop)#esp 3des md5
Device2(config-ipsec-prop)#exit
```

Step 5: Configure the pre-share key.

#On Device1, configure the pre-share key, and the key is admin, permitting all peers to use the key.

```
Device1(config)#crypto ike key admin any
```

#On Device2, configure the pre-share key, and the key is admin, permitting all peers to use the key.

```
Device2(config)#crypto ike key admin any
```

Step 6: Configure the IPsec tunnel.

#On Device1, configure the tunnel Tun, use the address of gigabitethernet0 as the local address of the tunnel, configure the peer address of the tunnel as 151.255.24.24, IKE proposal uses ikepro, IPSec proposal uses ippro, and configure the authentication mode as pre-sharing and digital envelope.

```
Device1(config)#crypto tunnel tun
Device1(config-tunnel)#local address 129.255.169.15
Device1(config-tunnel)#peer address 151.255.24.24
Device1(config-tunnel)#set ike proposal ikepro
Device1(config-tunnel)#set ipsec proposal ippro
Device1(config-tunnel)#set authentication preshared sm2-de
Device1(config-tunnel)#set auto-up
Device1(config-tunnel)#exit
```

#On Device2, configure tunnel Tun, use the address of gigabitethernet0 as the local address of the tunnel, configure the peer end of the tunnel as any, IKE proposal uses ikepro, and IPSec proposal uses ippro.

```
Device2(config)#crypto tunnel tun
Device2(config-tunnel)#local address 151.255.24.24
Device2(config-tunnel)#peer any
Device2(config-tunnel)#set ike proposal ikepro
Device2(config-tunnel)#set ipsec proposal ippro
Device2(config-tunnel)#exit
```

Note:

- Preshared and sm2-de authentication methods are configured. If there is no certificate, the tunnel is established by pre-shared key authentication. When the certificate is applied, the tunnel is renegotiated and the tunnel is established by digital envelope authentication.

Step 7*:* Configure the IPsec security policy.

#On Device1, configure the security policy policy1, protect the IP communication between network 100.0.0.0/24 to network 101.0.0.0/24, and associate the tunnel tun.

```
Device1(config)#crypto policy policy1
Device1(config-policy)#flow 100.0.0.0 255.255.255.0 101.0.0.0 255.255.255.0 ip ipv4-tunnel tun
Device1(config-policy)#exit
```

#On Device2, configure the security policy policy1, protect the IP communication between network 100.0.0.0/24 to network 101.0.0.0/24, and associate the tunnel tun.

```
Device2(config)#crypto policy policy1
Device2(config-policy)#flow 101.0.0.0 255.255.255.0 100.0.0.0 255.255.255.0 ip ipv4-tunnel tun
Device2(config-policy)#exit
```

Step 8: Configure import CA certificate offline, and download local user certificate and peer user certificate through LDAP.

#On Device1, import the CA certificate offline. First copy the CA certificate to PC1, download it to flash through FTP on Device1, and then import the CA certificate in flash into the trust domain myca.

```
Device1(config-fs)#copy 100.0.0.2 admin admin rootcert.cer file-system /flash/rootcert.cer


Downloading##OK!


Device1(config)#crypto ca import certificate rootcert.cer to myca


% The Root CA Certificate has the following attributes:
  Serial Number: 3af9ec4c00eef786
  Subject: C=CN, O=MPTEST, CN=MAIPU CA
  Issuer : C=CN, O=MPTEST, CN=MAIPU CA
  Validity
    Start date: 2019-08-30 06:26:02
    End   date: 2049-08-22 06:26:02
  Usage: Sign

Fingerprint(sm3) :78b0072ca26e6b7d01fb57021747e95242e0f81f31c7cea6acf83dfd55e96e60
  Fingerprint(sha1):bc31c9e3fcb8f53854e0181e07f658ad60078c4a


% Do you accept this root ca-certificate[yes]/[no]:yes
% PKI: Import Certificate success.
```

#On Device1, apply for the local user certificate offline.

```
Device1(config)#crypto ca pkcs10-enroll myca


% The Certificate DN will be: C=CN, O=MPTEST, CN=Device1
% Waiting, Generate 256 bit SM2 keys!
% Generating
Generate PKCS10 request success, send it to ca.
After CA issue the certificate, import it by commond 'crypto ca import certificate'.
PKCS10 request is:

-----BEGIN CERTIFICATE REQUEST-----
MIIBCzCBsAIBADAwMQswCQYDVQQGEwJDTjEPMA0GA1UEChMGTVBURVNUMRAwDgYD
VQQDEwdEZXZpY2UxMFkwEwYHKoZIzj0CAQYIKoEcz1UBgi0DQgAEuvOZFCYiVmsV
Us8w+Dva6hVhvAA7LAUVCElRlEHBGoXazkVilHo/DovWMnINqP8ueZWhFpbjBVMo
e6801/l3g6AeMBwGCSqGSIb3DQEJDjEPMA0wCwYDVR0PBAQDAgSwMAwGCCqBHM9V
AYN1BQADSAAwRQIhANvPWS8z232OPqxhZ6weGWx6O8/ufkAFLe/tF+A+vFleAiBO
JI98VdUuh+SqBrsEU0JAjLaPcri1mcFykdAUkPicZq==
-----END CERTIFICATE REQUEST-----
```

#On the CMS server, publish the user certificate of Device1. Device1 generates the public key, private key and other information of the certificate through PKCS10, and then logs in to the CMS server http://101.0.0.3:9443 , enter the page of applying for the device certificate in the certificate management directory, and select the general certificate template, copy the content between BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST generated on the device to the custom P10 application on the certificate server, and then submit the application; log into CMS server http://101.0.0.3:8443 after successful application, enter the publishing management page in the system maintenance directory, check the user certificate, and click Publish.

#On Device1, download the local user certificate via LDAP.

```
Device1(config)#crypto ca retrieve myca local


%PKI: Retrieve cert success.
```

#On Device2, apply for the CA certificate online.

```
Device2(config)#crypto ca authenticate myca



% The Root CA Certificate has the following attributes:
  Serial Number: 3af9ec4c00eef786
  Subject: C=CN, O=MPTEST, CN=MAIPU CA
  Issuer : C=CN, O=MPTEST, CN=MAIPU CA
  Validity
```

```
  Start date: 2019-08-30 06:26:02
  End   date: 2049-08-22 06:26:02
 Usage: Sign

Fingerprint(sm3) :78b0072ca26e6b7d01fb57021747e95242e0f81f31c7cea6acf83dfd5
5e96e60
 Fingerprint(sha1):bc31c9e3fcb8f53854e0181e07f658ad60078c4a

% Do you accept this certificate?[yes]/[no]:yes
% PKI: Get CA certificate success.
```

#On Device2, apply for the user certificate online.

```
Device2(config)#crypto ca enroll myca

% Please input request password:
% The Certificate DN will be: C=CN, O=MPTEST, CN=Device2
% Waiting, Generate 256 bit SM2 keys!
% Generating
% PKI: Certificate enroll success.
```

#On Device1, download the peer user certificate via LDAP.

```
Device1(config)#crypto ca retrieve myca peer CN=Device2

%PKI: Retrieve cert success.
```

Step 9: Check the result.

#On Device1, view the setup information of the tunnel.

```
Device1#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 18154      STATE_QUICK_I2      129.255.24.25    151.255.24.24    CN=Device2
 18166      STATE_MAIN_I4       129.255.24.25    151.255.24.24    CN=Device2
Device1#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  100.0.0.0/24  101.0.0.0/24  ip  any  any
 local tunnel endpoint : 129.255.24.25 remote tunnel endpoint : 151.255.24.24 , fabric
lpu-node : 0
 the pairs of ESP ipsec sa : id : 18166, algorithm : 3DES HMAC-MD5-96
  inbound esp ipsec sa :  spi : 0x6dc22061(1841438817)
     current input 33 packets, 7 kbytes
     encapsulation mode : Tunnel
```

```
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28036/4294967287
    uptime is 0 hour 12 minute 44 second
  outbound esp ipsec sa :  spi : 0x4fc11055(1338052693)
    current output 29 packets, 5 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28036/4294967289
    uptime is 0 hour 12 minute 44 second


total sa and sa group is 1
```

It can be seen that Device1 and Device2 successfully established IPSec tunnel in pre-share mode, and the source and destination addresses of the certificate downloaded by LDAP are the network protected by IPSec tunnel.

#View CA certificate, local user certificate and peer user certificate on Device1.

```
Device1#show cry ca certificates
Root CA Certificate:
  Status: Valid
  Serial Number: 3af9ec4c00eef786
  Subject: C=CN, O=MPTEST, CN=MAIPU CA
  Issuer : C=CN, O=MPTEST, CN=MAIPU CA
  Validity
    Start date: 2019-08-30 06:26:02
    End   date: 2049-08-22 06:26:02
  Key Type: SM2(256 bit)
  Usage: Sign

Fingerprint(sm3):78b0072ca26e6b7d01fb57021747e95242e0f81f31c7cea6acf83dfd5
5e96e60
  Fingerprint(sha1):bc31c9e3fcb8f53854e0181e07f658ad60078c4a
  Associated Identity: myca
    index: 3014


My Certificate:
  Status: Valid
  Serial Number: 12458bb6df5a445d
  Subject: C=CN, O=MPTEST, CN=Device1
```

Issuer : C=CN, O=MPTEST, CN=MAIPU CA

Validity

Start date: 2019-09-23 02:43:18

End date: 2020-09-22 02:43:18

Key Type: SM2(256 bit)

Usage: General

Fingerprint(sm3):81f060b72a396a29d9f25a5f4d867fb6de6c02ec838fdffad1ef8bab4e590d5f

Fingerprint(sha1):f525ef7a8e0cac4bd0c818f0b23839ed76abe365

Associated Identity: myca

index: 3016

Remote Certificate:

Status: Valid

Serial Number: 573dcc67a1e5d444

Subject: C=CN, O=MPTEST, CN=Device2

Issuer : C=CN, O=MPTEST, CN=MAIPU CA

Validity

Start date: 2019-09-23 03:14:22

End date: 2020-09-22 03:14:22

Key Type: SM2(256 bit)

Usage: General

Fingerprint(sm3):da1999c7872856c6ac496018418948b7914c87020556fa9ba56ef76c82dcd2da

Fingerprint(sha1):6bf0a46040cd9990bca78268c110ee93a3215a49

Associated Identity: myca

index: 3018

It can be seen that the local user certificate and the peer user certificate are successfully downloaded through LDAP on Device1.

#View the CA certificate and local user certificate on Device2.

Device2#show crypto ca certificates g myca

Root CA Certificate:

Status: Valid

Serial Number: 3af9ec4c00eef786

Subject: C=CN, O=MPTEST, CN=MAIPU CA

Issuer : C=CN, O=MPTEST, CN=MAIPU CA

Validity

Start date: 2019-08-30 06:26:02

End date: 2049-08-22 06:26:02

Key Type: SM2(256 bit)

Usage: Sign

Fingerprint(sm3):78b0072ca26e6b7d01fb57021747e95242e0f81f31c7cea6acf83dfd55e96e60

Fingerprint(sha1):bc31c9e3fcb8f53854e0181e07f658ad60078c4a

Associated Identity: myca

index: 23

My Certificate:

Status: Valid

Serial Number: 573dcc67a1e5d444

Subject: C=CN, O=MPTEST, CN=Device2

Issuer : C=CN, O=MPTEST, CN=MAIPU CA

Validity

Start date: 2019-09-23 03:14:22

End date: 2020-09-22 03:14:22

Key Type: SM2(256 bit)

Usage: General

Fingerprint(sm3):da1999c7872856c6ac496018418948b7914c87020556fa9ba56ef76c82dcd2da

Fingerprint(sha1):6bf0a46040cd9990bca78268c110ee93a3215a49

Associated Identity: myca

index: 24

It can be seen that the CA certificate and local user certificate are successfully obtained online on Device2.

#Use the command **clear crypto sa** on Device1 to clear the tunnel, renegotiate the tunnel in the form of digital envelope, and view the tunnel information.

Device1#show crypto ike sa

sa-id	negotiation-state	localaddr	peeraddr	peer-identity
18155	STATE_MAIN_I4	129.255.169.15	151.255.24.24	C=CN,O=MPTEST,CN=Device2

```
 18167          STATE_QUICK_I2                129.255.169.15          151.255.24.24
C=CN,O=MPTEST,CN=Device2


Device1#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  100.0.0.0/24  101.0.0.0/24  ip  any  any
      local tunnel endpoint : 129.255.169.15 remote tunnel endpoint : 151.255.24.24,
fabric lpu-node : 9
      the pairs of ESP ipsec sa : id : 18167, algorithm : 3DES HMAC-SHA1-96
   inbound esp ipsec sa :  spi : 0xf38287cc(4085417932)
      current input 0 packets, 0 kbytes
      encapsulation mode : Tunnel
      replay protection : ON
      remaining lifetime (seconds/kbytes) : 28545/4294967295
      uptime is 0 hour 4 minute 15 second
   outbound esp ipsec sa :  spi : 0xe9d75db5(3923205557)
      current output 0 packets, 0 kbytes
      encapsulation mode : Tunnel
      replay protection : ON
      remaining lifetime (seconds/kbytes) : 28545/4294967295
      uptime is 0 hour 4 minute 15 second


total sa and sa group is 1
```

It can be seen that Device1 and Device2 successfully established the tunnel in the form of digital envelope.

#View the setup information of the tunnel on Device2.

```
Device2#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 12005          STATE_MAIN_R3                 151.255.24.24           129.255.169.15
C=CN,O=MPTEST,CN=Device1
 12106          STATE_QUICK_R2                151.255.24.24           129.255.169.15
C=CN,O=MPTEST,CN=Device1


Device2#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  101.0.0.0/24  100.0.0.0/8  ip  any  any
policy name : subflow-52785194271315, the parent policy name : policy1
 f (src, dst, protocol, src port, dst port) :  101.0.0.0/24  100.0.0.0/24  ip  any  any
```

```
        local tunnel endpoint : 151.255.24.24 remote tunnel endpoint : 129.255.169.15,
fabric lpu-node : 3
        the pairs of ESP ipsec sa : id : 12106, algorithm : 3DES HMAC-SHA1-96
    inbound esp ipsec sa :  spi : 0xe9d75db5(3923205557)
        current input 0 packets, 0 kbytes
        encapsulation mode : Tunnel
        replay protection : ON
        remaining lifetime (seconds/kbytes) : 28343/4294967295
        uptime is 0 hour 7 minute 37 second
    outbound esp ipsec sa :  spi : 0xf38287cc(4085417932)
        current output 0 packets, 0 kbytes
        encapsulation mode : Tunnel
        replay protection : ON
        remaining lifetime (seconds/kbytes) : 28343/4294967295
        uptime is 0 hour 7 minute 37 second


    total sa and sa group is 1
```

It can be seen that Device2 and Device1 successfully established the tunnel in the form of digital envelope.

#PC1 can ping PC2 through the IPSec tunnel between Device1 and Device2, and the packet is protected by the IPSec tunnel.

9. IPSEC

9.1. Overview

IPsec (IP Security) protocol standards provide the security of the IP layer in the TCP/IP network. It provides the high-quality, inter-operable and cryptography-based security guarantee for the data transmitted on Internet. It is one traditional security technology of realizing the L3 VPN (Virtual Private Network). The security services provided by IPsec include data confidentiality, data integrality, data source authentication, and anti-replay attack.

IPsec includes AH (Authentication Header) and ESP (Encapsulating Security Payload) protocol standards to protect the communication of the IP layer. The operation modes include transmission mode and tunnel mode. The data protected by the transmission mode is IP payload and the data protected by the tunnel mode is the whole IP packet. The function features of the two protocols are as follows:

1. The main functions provided by AH include data source authentication, data integrity checking, and anti-replay attack, while AH does not encrypt the protected packets;
2. Besides all functions of the AH protocol (the data integrity checking does not include IP header), ESP also provides the encryption function for the IP packet. Therefore, we usually use the ESP protocol.

IPsec VPN is mainly to construct the secure information transmission channel on the public network for the two parties of the communication, so as to provide the functions similar to the private network. The two parties of the IPsec communication perform the ID authentication via the key management protocol and sets up the SA for information encryption or integrity protect negotiation, ensuring the security of the information transmitted on the un-reliable public network.

9.2. IPsec Function Configuration

Table 9-1 IPsec function configuration list

Configuration Task	
Configure IPsec tunnel	Configure auto negotiated tunnel
	Configure the manual tunnel
Configure profile	Configure profile
Configure the desired materials of the authentication	Configure the pre-share key
	Configure the RSA/SM2 key pair
	Configure the RSA/SM2 certificate

Configuration Task	
Configure security proposal	Configure the IKE proposal
	Configure the IPsec proposal
	Configure the security level
Configure IPSec policy	Configure IPSec policy
Configure extended authentication	Configure extended authentication mode
Configure initializing the tunnel	Configure initializing the tunnel
Configure authorizing VRC client to access	Configure the authorization function

9.2.1. Configure IPsec Tunnel

IPsec provides the security communication of the IP layer. The two parties of the communication negotiate together to set up IPsec SA, that is, IPsec tunnel. There are two modes of setting up the IPsec tunnel: auto negotiation and manual configuration. The auto negotiation mode automatically creates and maintains IPsec SA via IKE (Internet Key Exchange) and can provide the flexible and convenient configuration and higher security. For example, perform the ID authentication based on the pre-share key or digital certificate. The mode of configuring the tunnel manually is complicated and all information needed by creating the IPsec SA needs to be specified manually and cannot support some advanced features. For example, do not support IPsec SA lifetime limitation and it cannot perform the valid management for the IPsec session key. The manual configuration is feasible for the small static network, but in the actual environment, the distribution, management, and maintenance of the key are hard, so it is not suggested to use the mode of configuring the tunnel manually.

Configuration Condition

Before configuring IPsec tunnel, first complete the following task:

1. Configure the security proposal referenced by tunnel
2. To specify the peer ID in the auto negotiation tunnel, we need to configure the peer ID alias or alias group of the tunnel
3. Before configuring the auto negotiated tunnel, we need to configure the authentication material of the authentication mode.

Configure Auto Negotiated Tunnel

To configure auto negotiated tunnel, we need to configure the local address or interface. When the tunnel peer is clear, we also need to set the peer address or name, so as to decide with

which to set up IPsec. When the peer address or name cannot be confirmed in advance, it is not necessary to configure the peer address or name. It indicates that the local end does not initiate the IKE negotiation actively, but just accept the peer negotiation request. For the other configuration items, the system usually has the default values and we can decide whether to enable or modify according to the actuality.

Table 9-2 Configure auto negotiated the tunnel

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create IPv4/IPv6 auto negotiated tunnel and enter the auto negotiated tunnel configuration mode	**crypto tunnel/ipv6-tunnel** *tunnel-name*	Mandatory By default, do not configure the auto negotiated tunnel. The auto negotiated tunnel and the manual tunnel cannot have the same name.
Configure the peer address	**peer** { **address** { *ip-address* | *ipv6-address* } | **hostname** *host-name* | **any** }	Optional By default, respond to the negotiation request of any peer.
Configure the local address	**local** { **address** { *ip-address* | *ipv6-address* } | **interface** *interface-name* | **vrf** *vrf-name* **address** { *ip-address* | *ipv6-address* }}	Mandatory By default, do not configure the local address.
Configure the peer ID	**set peer-id** { *peer-id* | **alias** *alias-name* | **group** *group-name* }	Optional By default, the peer ID is the peer address.
Configure the local ID	**set local-id** *local-id*	Optional By default, for the pre-share key authentication mode, adopt the local IP address as the local ID; for the certificate authentication mode, select the first valid local certificate automatically and take the certificate subject name as the local ID.

Step	Command	Description
Configure the IKE authentication mode	**set authentication** { **preshared** | **rsa-sig** | **rsa-encr** | **rsa-encr-cisco** | **rsa-de** | **rsa-de-sc** | **rsa-de-gongan** | **sm2-de** | **sm2-de-sc** | **sm2-de-nc** }	Optional By default, the usable authentication modes include **rsa-sig rsa-encr rsa-de sm2-de preshared.** We can specify multiple authentication modes at the same time.
Configure the IKE phase-1 negotiation mode	**set mode** { **aggressive** | **main** }	Optional By default, the IKE negotiation mode is **main**.
Configure DPD (Dead Peer Detection)	**set dpd** { **on-demand** [*delay_time* | *retry_time* | *retry_count*] | **periodical** [*delay_time* | *retry_time* | *retry_count*] }	Optional By default, send the DPD packet every 30s, and re-transmit after 20s if the peer does not respond.
Specify the security level	**set sec-level** { **basic** | **medium** | **high** }	Optional By default, the tunnel uses the basic security level. The security level adopts the IKE proposal and pre-set proposal IPsec proposal.
Specify the IKE proposal	**set ike proposal** *proposal-name* [*proposal-name*] [*proposal-name*] [*proposal-name*] [*proposal-name*]	Optional By default, use the corresponding IKE proposal of the security level.

Step	Command	Description
Specify the IPsec proposal	**set ipsec proposal** *proposal-name* [*proposal-name*] [*proposal-name*] [*proposal-name*]	Optional By default, use the corresponding IPsec proposal of the security level.
Configure auto initiating tunnel negotiation	**set auto-up**	Optional By default, do not enable the function of initiating the tunnel negotiation automatically. If the corresponding interface of the tunnel is unavailable, even the function is enabled, it cannot initiate the tunnel negotiation.

Note:

- When adopting the certificate authentication, use the first valid certificate subject name as the local ID by default, so usually do not need to configure the local ID. Only when there are multiple valid local certificates and need to use different local certificates in different tunnels, we can configure the local ID according to the used certificate name, used to select the certificate used by the tunnel.
- When configuring multiple authentication modes at the same time, the selection of the authentication mode is not related with the configuration order. As the initiator, select by the order of rsa-sig, rsa-encr (or rsa-encr-cisco), rsa-de (or rsa-de-gongan or rsa-de-sc), sm2-de (or sm2-de-nc or sm2-de-sc), preshare from the configured authentication modes. As the responder, select the authentication mode the same as the initiator. rsa-encr and rsa-encr-cisco cannot exist at the same time. You can select only one of rsa-de, rsa-de-sc and rsa-de-gongan; you can select only one of sm2-de, sm2-de-sc and sm2-de-nc. rsa-de, rsa-de-sc, rsa-de-gongan, sm2-de, sm2-de-sc, sm2-de-nc all belong to the digital envelop authentication mode and when using the three authentication modes, the first phase of the IKE negotiation can only use the main mode, but cannot use the aggressive mode.
- When tunnel auto negotiation (**set auto-up**) is configured, the idle time limitation of the tunnel is invalid (**set idletime**). The idle time limitation will delete the tunnel when the time arrives. But if the tunnel auto negotiation is configured, re-negotiate the tunnel at once after the tunnel is deleted. In this way, the period from deleting the tunnel to re-negotiating the tunnel may result in the packet loss and occupies the system resources.
- The tunnel will initiate negotiation only when the interface is up and the IP address is configured; If **set auto up** is configured after interface is up and IP address is configured, tunnel negotiation needs to be triggered manually through the **clear** command.

Configure Manual Tunnel

To configure the manual tunnel, the two parties of the communication first need to get the information needed for setting up IPsec SA and then use the information to complete the tunnel configuration at the local. The setup of IPsec SA is not completed by the IKE negotiation.

Table 9-3 Configure the manual tunnel

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the IPv4/IPv6 manual tunnel and enter the manual tunnel configuration	**crypto tunnel/ipv6-tunnel** *tunnel-name* **manual**	Mandatory By default, do not configure the manual tunnel.
Configure the peer IPv4/IPv6 address	**peer** { **address** { *ip-address* | *ipv6-address* }}	Mandatory By default, do not specify the peer address.
Configure the local IPv4/IPv6 address	**local** { **address** { *ip-address* | *ipv6-address* } | **interface** *interface-name*}	Mandatory By default, do not configure the local address.
Specify the IPsec proposal	**set ipsec proposal** *proposal-name*	Mandatory By default, do not specify the IPsec proposal.
Configure the ingress IPsec SA attribute	**set inbound** { **esp** *spi-value* [**encryption** *key-value* | **authentication** *key-value*] | **ah** *spi-value key-value* | **compression** *cpi-value* }	Mandatory By default, do not configure the ingress IPsec SA attribute.
Configure the egress IPsec SA attribute	**set outbound** { **esp** *spi-value* [**encryption** *key-value* | **authentication** *key-value*] | **ah** *spi-value key-value* | **compression** *cpi-value* }	Mandatory By default, do not configure the egress IPsec SA attribute.

9.2.2. Configure Profile

Profile is a template used to create IPSec tunnel. At present, it is mainly used to create dynamic tunnel protection mgre packet.

Configuration Conditions

Before configuring profile, first complete the following tasks:

- Configure the security proposal that tunnel needs to reference;
- Before configuring the auto negotiation tunnel, the authentication materials corresponding to the authentication method shall be configured.

Configure profile

To configure profile, do not need to specify the local address/interface, as well as the peer device address.

Table 9-4 Configure profile

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create profile and enter the profile configuration mode	**crypto profile** *tunnel-name*	Mandatory By default, do not configure profile.
Configure the peer ID	**set peer-id** { *peer-id* | **alias** *alias-name* | **group** *group-name* }	Optional By default, the peer ID is the peer address.
Configure the local ID	**set local-id** *local-id*	Optional By default, for the pre shared key authentication method, the local IP address is used as the local identity; For the certificate authentication method, the first valid local certificate is automatically selected, and the certificate subject name is used as the local identity

Step	Command	Description
Configure the IKE authentication mode	**set authentication** { **preshared** | **rsa-sig** | **rsa-encr** | **rsa-encr-cisco** | **rsa-de** | **rsa-de-sc** | **rsa-de-gongan** | **sm2-de** | **sm2-de-sc** | **sm2-de-nc** }	Optional By default, the available authentication methods are rsa-sig rsa-encr rsa-de sm2-de preshared. You can specify multiple authentication methods at the same time.
Configure IKE phase-1 negotiation mode	**set mode** { **aggressive** | **main** }	Optional By default, IKE negotiation mode is the main mode (main).
Configure DPD (dead peer detection)	**set dpd** { **on-demand** [*delay_time* | *retry_time* | *retry_count*] | **periodical** [*delay_time* | *retry_time* | *retry_count*] }	Optional By default, the DPD packet is sent every 30 seconds. If the peer does not respond, it will be retransmitted after 20 seconds.
Specify the security level	**set sec-level** { **basic** | **medium** | **high** }	Optional By default, the tunnel uses the basic security level Each security level adopts the preset proposal in IKE proposal and IPSec proposal.
Specify the IKE proposal	**set ike proposal** *proposal-name* [*proposal-name*] [*proposal-name*] [*proposal-name*] [*proposal-name*]	Optional By default, the IKE proposal corresponding to the security level is used.
Specify the IPsec proposal	**set ipsec proposal** *proposal-name* [*proposal-name*] [*proposal-name*] [*proposal-name*] [*proposal-name*]	Optional By default, the IPSec proposal corresponding to the security level is used.

9.2.3. Configure Desired Materials of Authentication

The common authentication modes include pre-share key authentication, RSA public key encryption authentication, RSA digital signature authentication and RSA/SM2 digital envelop authentication. The chapter mainly describes how to configure the desired authentication materials for the four authentication modes.

Configuration Condition

None

Configure Pre-share Key

When the IKE phase-1 negotiation adopts the pre-share key authentication mode, we need to configure the pre-share key at the two sides of the tunnel.

Table 9-5 Configure the pre-share key

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the pre-share key of the tunnel	**crypto ike key** *key-string* { **address** { *ip-address* | *ipv6-address* } [**seed**] [**temp** { **start** *start-time* **end** *end-time* | **end** *end-time* **start** *start-time* }] | **identity** *identity-string* [**seed**] [**temp** { **start** *start-time* **end** *end-time* | **end** *end-time* **start** *start-time* }] | **any** [**seed**] }	Mandatory By default, do not configure the pre-share key of the tunnel.
Configure generating the pre-share key	**crypto ike generate-key identity** *remote-id* [**any** | *group-id*]	Optional By default, do not configure generating the pre-share key. According to the seed key *remote-id*, each ID in the specified group generates one pre-share key. The seed key is specified in the tunnel pre-share key.

Configure RSA/SM2 Key Pair

Configure the RSA/SM2 key pair at the two parties of the IPsec communication in advance. When the IKE phase-1 negotiation adopts the RAS public key encryption authentication, it is necessary to use the key pair; when the IKE phase-1 negotiation adopts the RSA digital

signature authentication or RSA/SM2 digital envelop authentication, maybe use the key pair, too.

Table 9-6 Configure the RSA/SM2 key pair

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the RSA/SM2 key pair	**crypto key generate** { **rsa** | **sm2** } [**usage-keys**]	Mandatory By default, do not configure the RSA or SM2 key pair
Enter the RSA/SM2 public key chain configuration mode	**crypto key pubkey-chain** { **rsa** | **sm2** }	Mandatory
Configure the named key	**addressed-key** { *ip-address* | *ipv6-address* } [**encryption** | **signature**]	Either By default, do not configure any named key. When the peer IKE ID is the IP address or FQDN, we need to configure the named key and public key.
	named-key *key-id* [**encryption** | **signature**]	
Specify the peer IP address	**address** { *ip-address* | *ipv6-address* }	Optional By default, do not specify the peer IP address. It is used only when the peer IKE ID is FQDN.
Configure the key	**key-string** [**help**]	Mandatory By default, do not configure the key.

Configure RSA/SM2 Certificate

When the IKE phase-1 negotiation authentication needs certificate, there should be valid certificate in the system. For the application and configuration of the certificate, refer to the PKI chapter of the configuration manual.

Note:

- RSA public key encryption authentication uses the RSA/SM2 key pair. RSA digital signature authentication and RSA/SM2 digital envelop authentication can use RSA/SM2 key or RSA/SM2 certificate. When the certificate and key pair exist at the same time, first select the certificate.

9.2.4. Configure Security Proposal

The security proposal is one component of the IPSec policy and tunnel. It is used to customize the specified security protocol, encryption/authentication algorithm and encapsulating mode used by IPsec and provides various security parameters for the IPsec negotiation SA. The reference of the proposal can use the pre-set proposal of the system or use the customized proposal, also can use the security level directly. In the security level, the corresponding proposal is defined.

Configuration Condition

None

Configure IKE Proposal

Configuring the IKE proposal is mainly to configure the encryption algorithm, hash algorithm, Diffie-Hellman group ID used by the IKE negotiation, and SA life time of the IKE negotiation. The system pre-sets eight IKE proposals. When configuring the tunnel or security level, the user can use the customized proposal and also can directly select using some IKE proposal provided by the system. Their naming rule adopts the mode of group ID-encryption algorithm name-hash algorithm name, as shown in the following table:

Table 9-7 The pre-set IKE proposal of the system

Name	Encryption Algorithm	Authentication Algorithm	Diffie-Hellman Group	Lifetime (s)
g1-des-sha1	DES	SHA1	1 (768 -bit modulus)	86400
g1-des-md5	DES	MD5	1 (768 -bit modulus)	86400
g2-3des-sha1	3DES	SHA1	2 (1024-bit modulus)	86400
g2-3des-md5	3DES	MD5	2 (1024-bit modulus)	86400
g2-aes128-sha1	AES128	SHA1	2 (1024-bit modulus)	86400

Name	Encryption Algorithm	Authentication Algorithm	Diffie-Hellman Group	Lifetime (s)
g2-sm1-sha1	SM1	SHA1	2 (1024-bit modulus)	86400
g5-3des-sha256	3DES	SHA2-256	5 (1536-bit modulus)	86400
g5-aes256-sha256	AES256	SHA2-256	5 (1536-bit modulus)	86400

Table 9-8 Configure the IKE proposal

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create the IKE proposal and enter the IKE proposal configuration mode	**crypto ike proposal** *proposal-name*	Mandatory By default, do not configure the IKE proposal.
Configure the encryption algorithm used by IKE	**encryption** { **3des** | **des** | **aes128** | **aes192** | **aes256** | **blowfish** | **cast** | **sm1** | **sm4** | **sm4-old** }	Optional By default, use the DES encryption algorithm.
Configure the hash algorithm used by IKE	**integrity** { **md5** | **sha1** | **sha2-256** | **sha2-512** | **sm3** }	Optional By default, use the SHA1 hash algorithm.
Configure the modulus group used by the IKE Diffie-Hellman algorithm	**group** { **group1** | **group2** | **group5** | **group14** | **group15** | **group16** | **group17** | **group18** }	Optional By default, use **group1** modulus group, that is, 768-bit modulus
Configure the lifetime set up by IKE	**lifetime** *lifetime-value*	Optional By default, the SA life time set up by IKE is 86400s.

Configure IPsec Proposal

IPsec proposal is the combination of the security protocol (AH or ESP) and algorithm accepted by the local end and the main referred security parameters include the authentication algorithm of the AH protocol, encryption algorithm and authentication algorithm of the ESP protocol, the compression algorithm and encapsulating mode of the IPComp (IP Compress) protocol. The system pre-sets eight proposals and the user can directly use during the tunnel configuration or security level configuration, also can use the customized IPsec proposal. The eight pre-set IPsec proposals are as shown in the following table. All pre-set proposals adopt the ESP protocol and tunnel mode to encapsulate, and the naming rule of “security protocol name- PFS (Perfect Forward Secrecy) group ID-encryption algorithm-authentication algorithm”.

Table 9-9The pre-set IPsec proposal of the system

Name	PFS	Encryption Algorithm (ESP)	Authentication Algorithm (ESP)
esp-nopfs-des-sha1	-	DES	SHA1
esp-nopfs-des-md5	-	DES	MD5
esp-g2-3des-sha1	group2	3DES	SHA1
esp-g2-3des-md5	group2	3DES	MD5
esp-g2-aes128-sha1	group2	AES128	SHA1
esp-g2-sm1-sha1	group2	SM1	SHA1
esp-g5-3des-sha256	group5	3DES	SHA2-256
esp-g5-aes256-sha256	group5	AES256	SHA2-256

Table 9-10 Configure the IPsec protocol

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create the IPsec proposal and enter the IPsec proposal configuration mode	**crypto ipsec proposal** *proposal-name*	Mandatory By default, do not configure the IPsec proposal.

Step	Command	Description
Configure the encryption and authentication algorithm used by ESP	**esp** { **3des** | **des** | **aes128** | **aes192** | **aes256** | **blowfish** | **cast** | **serpent** | **twofish** | **sm1** | **sm4** | **sm4-old** | **null** } [**md5** | **sha1** | **sha2-256** | **sha2-512** | **rmd160** | **aes-mac** | **sm3**]	Optional By default, the encryption algorithm used by the ESP protocol is DES and the authentication algorithm is MD5. The ESP authentication algorithm cannot be used separately, but should be used with the ESP encryption algorithm.
Configure the authentication algorithm used by AH	**ah** { **md5** | **sha1** | **sha2-256** | **sha2-512** | **sm3** }	Optional By default, do not use the AH protocol.
Configure the compression algorithm used by IPComp	**compression** { **lzs** }	Optional By default, do not use the IPComp protocol.
Configure the encapsulation mode	**mode** { **transport** | **tunnel** }	Optional By default, use the tunnel mode.
Configure PFS	**pfs** { **group1** | **group2** | **group5** | **group14** | **group15** | **group16** | **group17** | **group18** }	Optional By default, do not configure PFS.
Configure the lifetime of IPsec SA	**lifetime** { **seconds** *second-number* **| kbytes** *kbytes-number* }	Optional By default, the lifetime is 28800s.

Note:

- In the IPsec traversing NAT environment, do not use the AH protocol. The AH protocol checks the IP header of the packet, but NAT will change the IP header of the packet. The packet IP header after traversing NAT is not consistent with the IP header check of the original packet.
- When using the RSA/SM2 digital envelop authentication, do not support the Diffie-Hellman algorithm, so do not need to configure group or pfs.

Configure Security Level

The security level contains the IKE proposal and IPsec proposal. The user selects the corresponding security level according to the security requirement of the actual communication and does not need to configure the IKE proposal or IPsec proposal again.

Table 9-11 Configure the security level

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the security level and enter the security level configuration mode	**crypto sec-level custom** { **basic** | **medium** | **high** }	Mandatory By default, the corresponding proposal of the security level keeps unchanged.
Configure the IKE proposal in the security level	**ike proposal** *proposal-name* [*proposal-name*] [*proposal-name*] [*proposal-name*]	Optional By default, the IKE proposal of the basic security level is g1-des-sha1 and g1-des-md5; the IKE proposal of the medium security level is g2-3des-sha1, g2-3des-md5, g2-aes128-sha1, g2-sm1-sha1; the IKE proposal of the high security level is g5-3des-sha256, g5-aes256-sha256.
Configure the IPsec proposal in the security level	**ipsec proposal** *proposal-name* [*proposal-name*] [*proposal-name*] [*proposal-name*]	Optional By default, the IPsec proposal of the basic security level is esp-nopfs-des-sha1, esp-nopfs-des-md5; the IPsec proposal of the medium security is esp-g2-3des-sha1, esp-g2-3des-md5, esp-g2-aes128-sha1, esp-g2-sm1-sha1; the IPsec proposal of the high security level is esp-g5-3des-sha256, esp-g5-aes256-sha256.

Note:

- In the IPSec policy, tunnel, and security level, we can specify the proposal. When the proposal is specified in the IPSec policy, the IPSec policy does not use the proposal specified in the tunnel or security level. Similarly, when the proposal is specified in the tunnel, the tunnel does not use the proposal specified in the security level.

9.2.5. Configure IPSec Policy

The IPSec policy is to specify the specified data flow to apply one specified action. The actions include permit, deny and apply IPsec (tunnel). Here, permit means to directly forward, but not use the IPsec when forwarding the matched data flow; deny means to directly drop the matched data flow, but do not forward; apply means to perform the specified IPsec tunnel processing when forwarding the matched data flow.

Configuration Condition

Before configuring the IPSec policy, first complete the following task:

- Configure the tunnel used by the IPSec policy.

Configure IPSec Policy

Table 9-12 Configure IPSec policy

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create the IPv4/IPv6 IPSec policy and enter the IPSec policy configuration mode	**crypto policy/ipv6-popicy** *policy-name*	Mandatory By default, do not configure IPv4/IPv6 IPSec policy.
Configure the corresponding data flow of the IPSec policy	**flow** [**vrf** *vrf-name*] { *source-ip-address mask* | *source- ipv6-prefix/length* **| any** | **host** { *source-ip-address* | *source-ipv6-address* }} { *destination-ip-address mask* | *destination-ipv6-prefix/length* | **any** | **host** { *destination-ip-address* | *destination-ipv6-address* }} *protocol-name* [*source -port destination-port*] { **permit** | **deny** | **tunnel** *tunnel-name* [*tunnel-name*] [*tunnel-name*] [*tunnel-name*] [**bypass**] }	Mandatory By default, do not configure the corresponding data flow information of the IPSec policy.

Step	Command	Description
Configure the IPSec proposal for the IPSec policy	**set ipsec proposal** *proposal-name*	Optional By default, use the proposal specified in the tunnel.
Configure the route added to the peer protect network automatically	**set reverse-route**	Optional By default, do not configure the route added to the peer protect network automatically.
Exit the IPSec policy configuration mode	**exit**	
Change the order of the IPSec policies	**crypto policy insert** *policy-name* { **before** | **after** | **head** | **tail** } [policy-*name*]	Optional By default, the IPSec policies are arranged by the order of creating the IPSec policies. The IPSec policies are in order. When searching for the IPSec policy for the packet, match the policy according to the order of the IPSec policies.

Note:

- One policy can associate with 1-4 tunnels. When associating multiple tunnels, the subsequent tunnel serves as the tunnel backup or load balance. One tunnel cannot be bound to multiple policies with different VRF attributes at the same time.

Caution:

- The security policy with the source address or destination address of a network segment in FLOW must be configured before the security policy with the source address and destination address of any, such as **flow any IP tunnel test bypass**. The security policy must be the last security policy in the configuration. When the traffic forwarding matches the security policy, it is matched from front to back according to the sequence of the configured security policies, When the previously configured network segment security policy is not matched, the security policy with the last configured source address and destination address of any will be matched.
- In FLOW, only one security policy with the source address and destination address of any can be configured, and the policy can be bound with up to four different tunnels.

- When a security policy with source address and destination address of any is configured and a security policy with source address or destination address of a network segment is added, after policy configuration, use the **crypto policy insert** command to modify the security policy order, Insert the security policy whose source address or destination address is a network segment before the security policy whose source address and destination address are any. The configuration order related to the security policy in the modified configuration file changes according to the modified order.
- The tunnel at the central end supports multiple authentication methods by default, such as pre sharing, digital signature, and digital envelope. If local-id, local sig-cert, and local enc-cert do not need to be specified in the central end tunnel, and there is only one tunnel address, multiple node devices adopt multiple authentication methods. The central end tunnel does not need to specify authentication methods, and only one tunnel needs to be configured; If local-id or local sig-cert and local enc-cert need to be specified for some tunnels at the central end, different tunnels need to be configured at the central end according to different local-id and local sig-cert and local enc-cert. For example, some node devices adopt digital envelope dual-certificate authentication, and some nodes adopt pre shared authentication, so multiple tunnels need to be configured at the central end.

9.2.6. Configure Extended Authentication

Extended authentication is to perform the user ID authentication via AAA (Authentication Authorization Accounting) based on the basic IKE tunnel negotiation. If passing the authentication, continue to perform the IKE negotiation; if not passing the authentication, the IKE negotiation fails.

Configuration Condition

Before configuring the extended authentication, first complete the following tasks:

- Configure the desired extended authentication and authorization method list in AAA
- Configure the related parameters of the AAA server

Configure Extended Authentication Mode

To configure the extended authentication, it is necessary to define the IKE ID alias and specify the extended authentication mode based on the alias.

Table 9-13 Configure the authentication, authorization, and accounting mode of the extended authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create the alias of the specified IKE ID and enter the alias configuration mode	**crypto ike id alias** *alias-name*	Mandatory By default, do not configure the IKE ID alias.
Configure the corresponding IKE ID of the alias	**id** *ike-id*	Mandatory By default, match any ID.
Configure the AAA-based extended authentication	**xauth authentication [domain** *domain-name*] [**optional** | **user** *user-name* [**optional**] | **user-group** *group-name* [**optional**]] [**authen_imsi** [**authen_systemid**]| **authen_systemid** [**authen_imsi**]] [**optional**]	Mandatory By default, do not configure extended authentication.

Note:

- The authorization attributes in the IKE ID alias takes effect only after passing the AAA authentication.

9.2.7. Configure Initializing Tunnel

When the device is powered on, it is necessary to download the device configuration from the network management server. The tunnel initializing sets up the IPsec tunnel between the device and the network management server, so as to ensure the transmission security of the configuration information.

Configuration Condition

Before configuring initializing tunnel, first complete the following tasks:

- Configure the static route or IGP protocol, ensuring the intercommunication between the device and the network management server at the network layer.
- Distribute the user name and password of logging in to the network management server for the device.

Configure Initializing Tunnel

Table 9-14 Configure initializing the tunnel

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the initial configuration mode	**crypto init-config**	Mandatory
Configure the server address	**server** { **address** { *ip-address* | *ipv6-address* } | **hostname** *host-name* }	Mandatory By default, do not specify the server address.
Configure the local egress	**local** { **address** { *ip-address* | *ipv6-address* } | **interface** *interface-name* }	Optional By default, select the local interface according to the server address automatically.
Configure the user name	**user-name** *user-name*	Mandatory By default, do not configure the user name.
Configure the user password	**password** *user-password*	Mandatory By default, do not configure the user password.
Configure setting up the initialized tunnel automatically	**auto-start**	Optional By default, do not set up the initialized tunnel when the device is started.
Return to the privileged mode	**end**	-

Step	Command	Description
Enable initializing the tunnel setup	**start crypto init-config**	Optional By default, do not trigger setting up the initialized tunnel manually.

Note:

- When the device needs to download the configuration again, first delete the two files in the file system, that is, initConf and startup, and restart the device. And then perform the configuration of the initialized tunnel and start downloading.
- If configuration downloading fails, it is necessary to re-download after removing the fault. We can first execute the **clear crypto sa unrebuild** operation and then execute the **start crypto init-confit** operation. This can enable the configuration downloading more quickly.
- The **auto-start** command and the **start crypto init-config** command cannot be used at the same time.

9.2.8. Configure Authorizing VRC Client to Access

The VRC client and the device build IPSec tunnels, and the number of the accessed VRC clients can be controlled by configuring the authorization function. The license file needs to be imported on the device, and the authorization information is generated through the license file information, so as to control the access of VRC clients.

Configuration Conditions

Before configuring the authorization function, first complete the following task:

- Apply for the corresponding license authorization file of the device

Configure Authorization Function

Table 9-15 Configure the authorization function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Install the license file	**license install** { **ftp** *dest-ip-address ftp-username ftp-password* | **file-system** } *filename*	Mandatory

Note:

- The SN information of the device in the license file must be consistent with the shelf SN information of the device. Otherwise, the installation will fail.
- After installing the license file, the device does not need to be restarted and it takes effect immediately.

- The license file does not support uninstallation.

9.2.9. IPsec Monitoring and Maintaining

Table 9-16 IPsec monitoring and maintaining command list

Command	Description
clear crypto sa { **policy/ipv6-policy** *policy-name* | **tunnel/ipv6-tunnel** *tunnel-name* } [**unrebuild**]	Clear and re-build IPsec SA
clear crypto ipv4 { **ahstat** | **espstat** | **compstat** | **fabricstat** | **ipsecstat** | **ipipstat** }	Clear the protocol statistics information
clear crypto ipv6 { **ahstat** | **espstat** | **compstat** | **fabricstat** | **ipsecstat** | **ip6ip6stat** }	Clear the protocol statistics information
show crypto ike version	Display the IKE version information
show crypto key mypubkey rsa	Display the public key information of the local RSA key pair
show crypto key mypubkey sm2	Display the public key information of the peer SM2 key pair
show crypto key pubkey-chain rsa [**named-key** *name* | **addressed-key** { *ip-address* | *ipv6-address* }]	Display the public key information of the peer RSA key pair
show crypto key pubkey-chain sm2 [**named-key** *name* | **addressed-key** { *ip-address* | *ipv6-address* }]	Display the public key information of the local SM2 key pair
show crypto ike sa [*id-number* [**detail**] | **tunnel/ipv6-tunnel** *tunnel-name* [**detail**] | **policy/ipv6-policy** *policy-name* [**detail**] | **detail** | **statistics**]	Display the IKE SA status information

Command	Description
show crypto ipsec sa [**policy/ipv6-policy** *policy-name* | **tunnel/ipv6-tunnel** *tunnel-name*]	Display the IPsec SA information
show crypto ike proposal [*proposal-name*]	Display the specified or all IKE proposal
show crypto ipsec proposal [*proposal-name*]	Display the specified or all IPsec proposal
show crypto sec-level	Display the current security level configuration
show crypto db-context *tunnel-name* [**ike proposal** | **ipsec proposal**]	Display the parameter information of the IPsec tunnel proposal
show crypto tunnel/ipv6-tunnel [*tunnel-name*]	Display the specified or all IPsec tunnel configuration information
show crypto policy/ipv6-policy [*policy-name*]	Display the specified or all IPSec policy configuration information
show crypto bitmap	Display the IPsec SA utilization
show crypto ike id alias [*alias-name*]	Display the IKE alias information
show crypto ike id group [*group-name*]	Display the IKE alias group information
show crypto ike-comb statistics	Display the IKE external event merging statistics information
show crypto ike-limit statistics	Display IKE packet statistics with restrictions
show crypto rt { **ahstate | espstate | ipsecstate** }	Display the security packet statistics of IPv6 Routing

Command	Description
show crypto ipv4 ahstat	Display the AH protocol packet statistics information
show crypto ipv4 espstat	Display the ESP protocol packet statistics information
show crypto ipv4 compstat	Display the IP compression protocol packet statistics information
show crypto ipv4 ipsecstat	Display the IPsec packet statistics information
show crypto ipv4 fabricstat	Display the IPsec across-card forwarding statistics information
show crypto ipv4 ipipstat	Display the IPinIP packet statistics information
show crypto ipv6 ahstat	Display the AH protocol packet statistics information
show crypto ipv6 espstat	Display the ESP protocol packet statistics information
show crypto ipv6 compstat	Display the IP compression protocol packet statistics information
show crypto ipv6 ipsecstat	Display the IPsec packet statistics information
show crypto ipv6 fabricstat	Display the IPsec across-card forwarding statistics information
show crypto ipv6 ip6ip6stat	Display the IPinIP packet statistics information
show crypto ipsec fabric-info	Display the IPsec across-card distribution information

Command	Description
show crypto ipsec fabric-stat	Display the IPsec across-card distribution statistics information
show crypto ipsec-al ddb errorstat	Displays the error statistics of IPSec adaptation layer calling DDB
show crypto ipsec-al ddbOperateTime statistics	Display the maximum time difference statistics of IPSec adaptation layer calling DDB task
show crypto ipsec-al error	Display IPSec adaptation layer error information
show crypto ipsec-al memorystat	Display IPSec adaptation layer memory usage information
show crypto ipsec-al statistics [**detail**]	Display IPSec adaptation layer task statistics information
show crypto ike dpd	Display the statistics of DPD packets sent and received by the IKE tunnel
show crypto ike downloaded-script	Display the configuration information downloaded via the IKE tunnel
show crypto license	Display the VRC license information
show crypto software-vrc statistics	Display the VRC connection status statistics information
show crypto vpn-client statistics	Displays the maximum number of VRC clients allowed to access and the number of VRC clients currently accessed in the device
show license information	Display the effective license information

Command	Description
show license installed	Display the effective license file name

9.3. IPsec Typical Configuration Example

9.3.1. Configure IPsec tunnel Mode

Network Requirements

1. Adopt the tunnel mode to set up the IPsec tunnel between Device1 and Device2, protecting the data communication of the network where PC1 and PC2 are located;
2. IPsec proposal security protocol adopts ESP; IKE proposal and IPsec proposal encryption adopts 3DES; the authentication algorithm adopts SHA1.

Network Topology

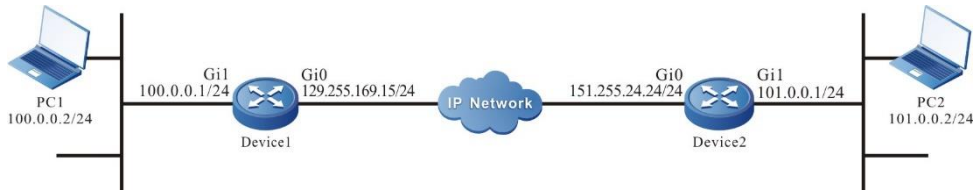


Figure 9-1 Networking of configuring IPsec tunnel mode

Configuration Steps

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

Step 2: Configure the IKE and IPSec proposal.

#On Device1, configure the IKE proposal ikepro, use the encryption algorithm 3DES, authentication algorithm SHA1; configure IPsec proposal ippro, use the ESP security protocol, use the encryption algorithm 3DES, and authentication algorithm SHA1.

```
Device1#configure terminal
Device1(config)#crypto ike proposal ikepro
Device1(config-ike-prop)#encryption 3des
Device1(config-ike-prop)#integrity sha1
Device1(config-ike-prop)#exit
Device1(config)#crypto ipsec proposal ippro
Device1(config-ipsec-prop)#esp 3des sha1
Device1(config-ipsec-prop)#exit
```

#On Device2, configure the IKE proposal ikepro, use the encryption algorithm 3DES, authentication algorithm SHA1; configure IPsec proposal ippro, use the ESP security protocol, use the encryption algorithm 3DES, and authentication algorithm SHA1.

```
Device2#configure terminal
Device2(config)#crypto ike proposal ikepro
Device2(config-ike-prop)#encryption 3des
```

```
Device2(config-ike-prop)#integrity sha1
Device2(config-ike-prop)#exit
Device2(config)#crypto ipsec proposal ippro
Device2(config-ipsec-prop)#esp 3des sha1
Device2(config-ipsec-prop)#exit
```

Step 3: Configure the pre-share key.

#On Device1, configure the pre-share key, key is admin and permit all peers to use the key.

```
Device1(config)#crypto ike key admin any
```

#On Device2, configure the pre-share key, key is admin and permit all peers to use the key.

```
Device2(config)#crypto ike key admin any
```

Note:

- The peer of using the pre-share key also can be the specific IP address or identity.

Step 4: Configure the IPSec tunnel.

#On Device1, configure the tunnel tun, use gigabitethernet0 address as the local address of the tunnel, configure the peer address of the tunnel as 151.255.24.24, configure the authentication mode as the pre-share key authentication, the IKE proposal uses ikepro, IPsec proposal uses ippro, and enable the auto initiating negotiation.

```
Device1(config)#crypto tunnel tun
Device1(config-tunnel)#local address 129.255.169.15
Device1(config-tunnel)#peer address 151.255.24.24
Device1(config-tunnel)#set authentication preshared
Device1(config-tunnel)#set ike proposal ikepro
Device1(config-tunnel)#set ipsec proposal ippro
Device1(config-tunnel)#set auto-up
Device1(config-tunnel)#exit
```

#On Device2, configure the tunnel tun, use gigabitethernet0 address as the local address of the tunnel, configure the peer of the tunnel as any, the IKE proposal uses ikepro, and IPsec proposal uses ippro.

```
Device2(config)#crypto tunnel tun
Device2(config-tunnel)#local address 151.255.24.24
Device2(config-tunnel)#peer any
Device2(config-tunnel)#set ike proposal ikepro
Device2(config-tunnel)#set ipsec proposal ippro
Device2(config-tunnel)#exit
```

Note:

- If the address of the local interface of the tunnel is not fixed, we can adopt **local interface** to configure.

- IKE proposal and IPsec proposal are the optional configuration. If the proposal is not configured in the tunnel, IKE negotiation encryption algorithm uses des by default, authentication algorithm uses sha1 by default, IPsec tunnel security protocol uses esp by default, encryption algorithm uses des by default, and authentication algorithm uses md5 by default.

Step 5: Configure the IPSec policy.

#On Device1, configure the IPSec policy policy1, protect the IP communication from network 100.0.0.0/24 to network 101.0.0.0/24, and associate the tunnel tun.

```
Device1(config)#crypto policy policy1
Device1(config-policy)# flow 100.0.0.0 255.255.255.0 101.0.0.0 255.255.255.0 ip ipv4-tunnel tun
Device1(config-policy)#exit
```

#On Device2, configure the IPSec policy policy1, protect the IP communication from network 101.0.0.0/24 to network 100.0.0.0/24, associate the tunnel tun, and add the route to the peer protect network automatically.

```
Device2(config)#crypto policy policy1
Device2(config-policy)#flow 101.0.0.0 255.255.255.0 100.0.0.0 255.255.255.0 ip tunnel tun
Device2(config-policy)#set reverse-route
Device2(config-policy)#exit
```

Caution:

- The security policy with the source address or destination address of a network segment in FLOW must be configured before the security policy with the source address and destination address of any, such as **flow any IP tunnel test bypass**. The security policy must be the last security policy in the configuration. When the traffic forwarding matches the security policy, it is matched from front to back according to the sequence of the configured security policies, When the previously configured network segment security policy is not matched, the security policy with the last configured source address and destination address of any will be matched.
- In FLOW, only one security policy with the source address and destination address of any can be configured, and the policy can be bound with up to four different tunnels.
- When a security policy with source address and destination address of any is configured and a security policy with source address or destination address of a network segment is added, after policy configuration, use the **crypto policy insert** command to modify the security policy order, Insert the security policy whose source address or destination address is a network segment before the security policy whose source address and destination address are any. The configuration order related to the security policy in the modified configuration file changes according to the modified order.
- The tunnel at the central end supports multiple authentication methods by default, such as pre sharing, digital signature, and digital envelope. If local-id, local sig-cert, and local enc-cert do not need to be specified in the central end tunnel, and there is only one tunnel address, multiple node devices adopt multiple authentication methods. The central end tunnel does not need to specify authentication methods, and only one tunnel needs to be configured; If local-id or local sig-cert and local enc-cert need to be specified for some tunnels at the central end, different tunnels need to be configured at the central end according to different local-id and local sig-cert and local enc-cert. For example, some

node devices adopt digital envelope dual-certificate authentication, and some nodes adopt pre shared authentication, so multiple tunnels need to be configured at the central end.

Step 6: Check the result.

#On Devie1, view the tunnel setup information.

```
Device1#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 60      STATE_QUICK_I2      129.255.169.15  151.255.24.24   151.255.24.24
 1       STATE_MAIN_I4       129.255.169.15  151.255.24.24   151.255.24.24
Device1#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  100.0.0.0/24  101.0.0.0/24  ip  any  any
 local tunnel endpoint : 129.255.169.15 remote tunnel endpoint : 151.255.24.24 , fabric lpu-node : 0
 the pairs of ESP ipsec sa : id : 60, algorithm : 3DES HMAC-SHA1-96
  inbound esp ipsec sa :  spi : 0xa1ce1081(2714636417)
    current input 0 packets, 0 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28496/4294967295
    uptime is 0 hour 5 minute 4 second
  outbound esp ipsec sa :  spi : 0xb42f1047(3022983239)
    current output 0 packets, 0 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28496/4294967295
    uptime is 0 hour 5 minute 4 second

total sa and sa group is 1
```

We can see that Device1 sets up the tunnel with Device2 successfully.

#View the tunnel setup information on Device2.

```
Device2#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 2       STATE_QUICK_R2      151.255.24.24   129.255.169.15  129.255.169.15
 1       STATE_MAIN_R3       151.255.24.24   129.255.169.15  129.255.169.15
Device2#show crypto ipsec sa
policy name : policy1
```

```
 f (src, dst, protocol, src port, dst port) :  101.0.0.0/24  100.0.0.0/24  ip  any  any
policy name : subflow-1610612736, the parent policy name : policy1
 f (src, dst, protocol, src port, dst port) :  101.0.0.0/24  100.0.0.0/24  ip  any  any
 local tunnel endpoint : 151.255.24.24 remote tunnel endpoint : 129.255.169.15 , fabric
lpu-node : 0
 the pairs of ESP ipsec sa : id : 2, algorithm : 3DES HMAC-SHA1-96
  inbound esp ipsec sa :  spi : 0xb42f1047(3022983239)
     current input 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28454/4294967295
     uptime is 0 hour 5 minute 46 second
  outbound esp ipsec sa :  spi : 0xa1ce1081(2714636417)
     current output 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28454/4294967295
     uptime is 0 hour 5 minute 46 second


total sa and sa group is 1
```

We can see that Device2 sets up the tunnel with Device1 successfully.

#On Device2, view the information of the route automatically added to the peer protect network.

```
Device2#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 151.255.24.38 to network 0.0.0.0


S   0.0.0.0/0 [1/10] via 151.255.24.38, 00:00:21, gigabitethernet0
S   100.0.0.0/24 [1/10] via 129.255.169.15, 00:00:08, gigabitethernet0
C   101.0.0.0/24 is directly connected, 01:15:08, gigabitethernet1
C   127.0.0.0/8 is directly connected, 53:03:26, lo0
C   130.255.0.0/16 is directly connected, 53:02:26, gigabitethernet2
C  151.255.24.0/24 is directly connected, 01:15:21, gigabitethernet0
```

We can see that 100.0.0.0/24 is the static route automatically added for IPsec on Devcie2.

PC1 can ping PC2 via the IPsec tunnel between Device1 and Device2; the packet is protected by the IPsec tunnel.

9.3.2. Configure Ipsec Transmission Mode

Network Requirements

1. Adopt the tunnel mode to set up the IPsec tunnel between Device1 and Device2, protecting the end-to-end data communication between Device1 and Device2.
2. IPsec proposal adopts the security protocol AH and ESP; the AH protocol authentication algorithm adopts MD5; ESP encryption algorithm adopts SM1; authentication algorithm adopts MD5; IKE proposal encryption algorithm adopts SM1; authentication algorithm adopts MD5.

Network Topology

Figure 9-2 Networking of configuring the IPsec transmission mode

Configuration Steps

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

Step 2: Configure the IKE and IPSec proposal.

#On Device1, configure the IKE proposal ikepro, use the encryption algorithm SM1, authentication algorithm MD5; configure IPsec proposal ippro, use the ESP security protocol, use the encryption algorithm SM1, and authentication algorithm MD5. Use the AH security protocol and authentication algorithm MD5; use the transmission mode.

```
Device1#configure terminal
Device1(config)#crypto ike proposal ikepro
Device1(config-ike-prop)#encryption sm1
Device1(config-ike-prop)#integrity md5
Device1(config-ike-prop)#exit
Device1(config)#crypto ipsec proposal ippro
Device1(config-ipsec-prop)#esp sm1 md5
Device1(config-ipsec-prop)#ah md5
Device1(config-ipsec-prop)#mode transport
Device1(config-ipsec-prop)#exit
```

#On Device2, configure the IKE proposal ikepro, use the encryption algorithm SM1, authentication algorithm MD5; configure IPsec proposal ippro, use the ESP security protocol, use the encryption algorithm SM1, and authentication algorithm MD5. Use the AH security protocol and authentication algorithm MD5; use the transmission mode.

```
Device2#configure terminal
Device2(config)#crypto ike proposal ikepro
Device2(config-ike-prop)#encryption sm1
Device2(config-ike-prop)#integrity md5
```

```
Device2(config-ike-prop)#exit
Device2(config)#crypto ipsec proposal ippro
Device2(config-ipsec-prop)#esp sm1 md5
Device2(config-ipsec-prop)#ah md5
Device2(config-ipsec-prop)#mode transport
Device2(config-ipsec-prop)#exit
```

Caution:

- AH security protocol does not support the NAT traversing. If there is NAT traversing, it may result in the failure of the IKE negotiation.
- The AH security protocol can be used with ESP; we also can disable ESP (it is enabled by default) and just use AH.

Step 3: Configure the pre-share key.

#On Device1, configure the pre-share key, key is admin and permit all peers to use the key.

```
Device1(config)#crypto ike key admin any
```

#On Device2, configure the pre-share key, key is admin and permit all peers to use the key.

```
Device2(config)#crypto ike key admin any
```

Step 4: Configure the IPSec tunnel.

#On Device1, configure the tunnel tun, use gigabitethernet0 as the local interface of the tunnel, configure the peer address of the tunnel as 151.255.24.24, configure the authentication mode as the pre-share key authentication, the IKE proposal uses ikepro, IPsec proposal uses ippro, and enable the auto initiating negotiation.

```
Device1(config)#crypto tunnel tun
Device1(config-tunnel)#local interface gigabitethernet 0
Device1(config-tunnel)#peer address 151.255.24.24
Device1(config-tunnel)#set authentication preshared
Device1(config-tunnel)#set ike proposal ikepro
Device1(config-tunnel)#set ipsec proposal ippro
Device1(config-tunnel)#set auto-up
Device1(config-tunnel)#exit
```

#On Device2, configure the tunnel tun, use gigabitethernet0 as the local interface of the tunnel, configure the peer of the tunnel as any, the IKE proposal uses ikepro, IPsec proposal uses ippro.

```
Device2(config)#crypto tunnel tun
Device2(config-tunnel)#local interface gigabitethernet 0
Device2(config-tunnel)#peer any
Device2(config-tunnel)#set ike proposal ikepro
Device2(config-tunnel)#set ipsec proposal ippro
```

```
Device2(config-tunnel)#exit
```

Step 5: Configure the IPSec policy.

#On Device1, configure the IPSec policy policy1, protect the IP communication from host 129.255.169.15/32 to host 151.255.24.24/32, and associate the tunnel tun.

```
Device1(config)#crypto policy policy1
Device1(config-policy)#flow host 129.255.169.15 host 151.255.24.24 ip tunnel tun
Device1(config-policy)#exit
```

#On Device2, configure the IPSec policy policy1, protect the IP communication from host 151.255.24.24/32 to host 129.255.169.15/32, and associate the tunnel tun.

```
Device2(config)#crypto policy policy1
Device2(config-policy)#flow host 151.255.24.24 host 129.255.169.15 ip tunnel tun
Device2(config-policy)#exit
```

Step 6: Check the result.

#On Devie1, view the tunnel setup information.

```
Device1#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 2       STATE_QUICK_I2      129.255.169.15  151.255.24.24   151.255.24.24
 1       STATE_MAIN_I4       129.255.169.15  151.255.24.24   151.255.24.24
Device1#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  129.255.169.15/32  151.255.24.24/32  ip  any any
 local tunnel endpoint : 129.255.169.15 remote tunnel endpoint : 151.255.24.24 , fabric lpu-node : 0
 the pairs of AH ipsec sa : id : 2, algorithm : HMAC-MD5-96
  inbound ah ipsec sa :  spi : 0xe9c21048(3921809480)
    current input 0 packets, 0 kbytes
    encapsulation mode : Transport
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28724/4294967295
    uptime is 0 hour 1 minute 16 second
  outbound ah ipsec sa :  spi : 0x490b1047(1225461831)
    current output 0 packets, 0 kbytes
    encapsulation mode : Transport
    replay protection : ON
```

```
    remaining lifetime (seconds/kbytes) : 28724/4294967295
    uptime is 0 hour 1 minute 16 second
  local tunnel endpoint : 129.255.169.15 remote tunnel endpoint : 151.255.24.24 , fabric
lpu-node : 0
  the pairs of ESP ipsec sa : id : 2, algorithm : SM1 HMAC-MD5-96
   inbound esp ipsec sa :  spi : 0xb92f1047(3106869319)
    current input 0 packets, 0 kbytes
    encapsulation mode : Transport
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28724/4294967295
    uptime is 0 hour 1 minute 16 second
   outbound esp ipsec sa :  spi : 0xa2d61048(2731937864)
    current output 0 packets, 0 kbytes
    encapsulation mode : Transport
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28724/4294967295
    uptime is 0 hour 1 minute 16 second


total sa and sa group is 1
```

We can see that Device1 sets up the tunnel with Device2 successfully.

#View the tunnel setup information on Device2.

```
Device2#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 18      STATE_QUICK_R2      151.255.24.24   129.255.169.15  129.255.169.15
 17      STATE_MAIN_R3       151.255.24.24   129.255.169.15  129.255.169.15
Device2#show crypto ipsec sa
policy name : policy1
  f (src, dst, protocol, src port, dst port) :  151.255.24.24/32  129.255.169.15/32  ip  any
any
policy name : subflow-1610612736, the parent policy name : policy1
  f (src, dst, protocol, src port, dst port) :  151.255.24.24/32  129.255.169.15/32  ip  any
any
  local tunnel endpoint : 151.255.24.24 remote tunnel endpoint : 129.255.169.15 , fabric
lpu-node : 0
  the pairs of AH ipsec sa : id : 18, algorithm : HMAC-MD5-96
   inbound ah ipsec sa :  spi : 0x490b1047(1225461831)
    current input 0 packets, 0 kbytes
    encapsulation mode : Transport
```

```
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28695/4294967295
    uptime is 0 hour 1 minute 45 second
  outbound ah ipsec sa :  spi : 0xe9c21048(3921809480)
    current output 0 packets, 0 kbytes
    encapsulation mode : Transport
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28695/4294967295
    uptime is 0 hour 1 minute 45 second
 local tunnel endpoint : 151.255.24.24 remote tunnel endpoint : 129.255.169.15 , fabric
lpu-node : 0
 the pairs of ESP ipsec sa : id : 18, algorithm : SM1 HMAC-MD5-96
  inbound esp ipsec sa :  spi : 0xa2d61048(2731937864)
    current input 0 packets, 0 kbytes
    encapsulation mode : Transport
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28695/4294967295
    uptime is 0 hour 1 minute 45 second
  outbound esp ipsec sa :  spi : 0xb92f1047(3106869319)
    current output 0 packets, 0 kbytes
    encapsulation mode : Transport
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28695/4294967295
    uptime is 0 hour 1 minute 45 second

total sa and sa group is 1
```

We can see that Device2 sets up the tunnel with Device1 successfully.

PC1 can ping PC2 via the IPsec tunnel between Device1 and Device2; the packet is protected by the IPsec tunnel.

```
Device1#ping 151.255.24.24

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 151.255.24.24 , timeout is 2 seconds:
!!!!!
```

Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.

9.3.3. Configure Ipsec Load Balance

Network Requirements

1. Set up two IPsec tunnels between Device1 and Device2 and configure as the load balance; PC1 accesses PC2 and PC3 by the load balance mode via the IPsec tunnel of IP Network1 and IP Network2.
2. IPsec protocol security protocol adopts ESP; IKE proposal and IPsec proposal encryption algorithm adopts SM1; authentication algorithm adopts SHA1.

Network Topology

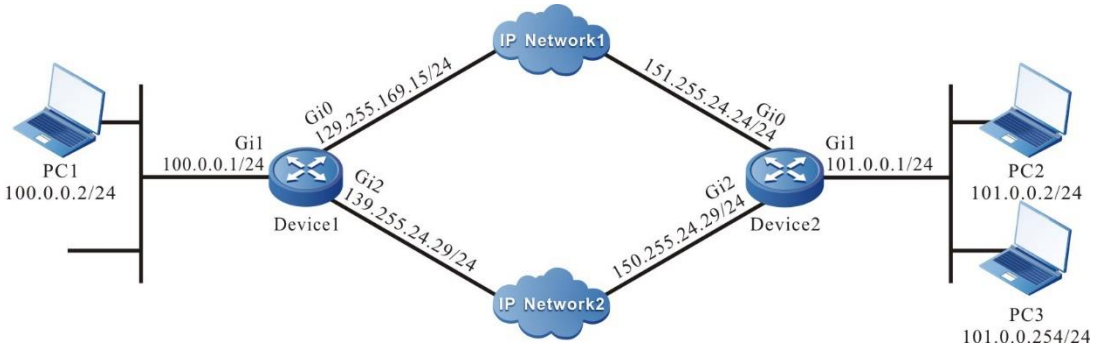


Figure 9-3 Networking of configuring the IPsec load balance

Configuration Steps

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

Step 2: Configure the IKE and IPSec proposal.

#On Device1, configure the IKE proposal ikepro, use the encryption algorithm SM1, authentication algorithm SHA1; configure IPsec proposal ippro, use the ESP security protocol, use the encryption algorithm SM1, and authentication algorithm SHA1.

```
Device1#configure terminal
Device1(config)#crypto ike proposal ikepro
Device1(config-ike-prop)#encryption sm1
Device1(config-ike-prop)#integrity sha1
Device1(config-ike-prop)#exit
Device1(config)#crypto ipsec proposal ippro
Device1(config-ipsec-prop)#esp sm1 sha1
Device1(config-ipsec-prop)#exit
```

#On Device2, configure the IKE proposal ikepro, use the encryption algorithm SM1, authentication algorithm SHA1; configure IPsec proposal ippro, use the ESP security protocol, use the encryption algorithm SM1, and authentication algorithm SHA1.

```
Device2#configure terminal
Device2(config)#crypto ike proposal ikepro
Device2(config-ike-prop)#encryption sm1
Device2(config-ike-prop)#integrity sha1
Device2(config-ike-prop)#exit
```

```
Device2(config)#crypto ipsec proposal ippro
Device2(config-ipsec-prop)#esp sm1 sha1
Device2(config-ipsec-prop)#exit
```

Step 3: Configure the pre-share key.

#On Device1, configure the pre-share key, key is admin and permit all peers to use the key.

```
Device1(config)#crypto ike key admin any
```

#On Device2, configure the pre-share key, key is admin and permit all peers to use the key.

```
Device2(config)#crypto ike key admin any
```

Step 4: Configure the IPSec tunnel.

#On Device1, configure the two tunnels tun1and tun2, use gigabitethernet0 and gigabitethernet2 as the local interfaces of the tunnels, configure the peer address of the tunnel as 151.255.24.24 and 150.255.24.29 respectively, configure the authentication mode as the pre-share key authentication, the IKE proposal uses ikepro, IPsec proposal uses ippro, and enable the auto initiating negotiation.

```
Device1(config)#crypto tunnel tun1
Device1(config-tunnel)#local interface gigabitethernet 0
Device1(config-tunnel)#peer address 151.255.24.24
Device1(config-tunnel)#set authentication preshared
Device1(config-tunnel)#set ike proposal ikepro
Device1(config-tunnel)#set ipsec proposal ippro
Device1(config-tunnel)#set auto-up
Device1(config-tunnel)#exit
Device1(config)#crypto tunnel tun2
Device1(config-tunnel)#local interface gigabitethernet 2
Device1(config-tunnel)#peer address 150.255.24.29
Device1(config-tunnel)#set authentication preshared
Device1(config-tunnel)#set ike proposal ikepro
Device1(config-tunnel)#set ipsec proposal ippro
Device1(config-tunnel)#set auto-up
Device1(config-tunnel)#exit
```

#On Device2, configure the two tunnels tun1and tun2, use gigabitethernet0 and gigabitethernet2 as the local interfaces of the tunnels, configure the peer of the tunnel as any, the IKE proposal uses ikepro, IPsec proposal uses ippro.

```
Device2(config)#crypto tunnel tun1
Device2(config-tunnel)#local interface gigabitethernet 0
```

```
Device2(config-tunnel)#peer any
Device2(config-tunnel)#set ike proposal ikepro
Device2(config-tunnel)#set ipsec proposal ippro
Device2(config-tunnel)#exit
Device2(config)#crypto tunnel tun2
Device2(config-tunnel)#local interface gigabitethernet 2
Device2(config-tunnel)#peer any
Device2(config-tunnel)#set ike proposal ikepro
Device2(config-tunnel)#set ipsec proposal ippro
Device2(config-tunnel)#exit
```

Step 5: Configure the IPSec policy.

#On Device1, configure IPSec policy policy1, protecting the IP communication from network 100.0.0.0/24 to network 101.0.0.0/24; associate the tunnel tun1 and tun2; configure the load balance and the route automatically added to the peer protect network.

```
Device1(config)#crypto policy policy1
Device1(config-policy)#flow 100.0.0.0 255.255.255.0 101.0.0.0 255.255.255.0 ip tunnel tun1 tun2
Device1(config-policy)#set payload-balance
Device1(config-policy)#set reverse-route
Device1(config-policy)#exit
```

#On Device2, configure IPSec policy policy1, protecting the IP communication from network 101.0.0.0/2 to network 100.0.0.0/24; associate the tunnel tun1 and tun2; configure the load balance and the route automatically added to the peer protect network.

```
Device2(config)#crypto policy policy1
Device2(config-policy)#flow 101.0.0.0 255.255.255.0 100.0.0.0 255.255.255.0 ip tunnel tun1 tun2
Device2(config-policy)#set payload-balance
Device2(config-policy)#set reverse-route
Device2(config-policy)#exit
```

Note:

- If IPsec is not configured with the load balance, it is backup by default, that is, the data communication is performed just via tun1; after tun1 is disconnected, communicate via tun2.

Step 6: Check the result.

#On Devie1, view the tunnel setup information.

```
Device1#show crypto ike sa
sa-id  negotiation-state  localaddr  peeraddr  peer-identity
```

```
 63      STATE_QUICK_I2      139.255.24.29    150.255.24.29    150.255.24.29
 62      STATE_MAIN_I4       139.255.24.29    150.255.24.29    150.255.24.29
 61      STATE_QUICK_I2      129.255.169.15   151.255.24.24    151.255.24.24
 60      STATE_MAIN_I4       129.255.169.15   151.255.24.24    151.255.24.24
Device1#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  100.0.0.0/24  101.0.0.0/24  ip  any  any
 local tunnel endpoint : 129.255.169.15 remote tunnel endpoint : 151.255.24.24 , fabric
lpu-node : 0
 the pairs of ESP ipsec sa : id : 61, algorithm : SM1 HMAC-SHA1-96
  inbound esp ipsec sa :  spi : 0x6c911061(1821446241)
     current input 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28700/4294967295
     uptime is 0 hour 1 minute 40 second
  outbound esp ipsec sa :  spi : 0xb404106a(3020165226)
     current output 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28700/4294967295
     uptime is 0 hour 1 minute 40 second
 local tunnel endpoint : 139.255.24.29 remote tunnel endpoint : 150.255.24.29 , fabric
lpu-node : 0
 the pairs of ESP ipsec sa : id : 63, algorithm : SM1 HMAC-SHA1-96
  inbound esp ipsec sa :  spi : 0x903e1062(2419986530)
     current input 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28710/4294967295
     uptime is 0 hour 1 minute 30 second
  outbound esp ipsec sa :  spi : 0x8672106b(2255622251)
     current output 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28710/4294967295
     uptime is 0 hour 1 minute 30 second
```

```
total sa and sa group is 2
```

We can see that two IPsec tunnels are set up between Device1 and Device2.

#View the tunnel setup information on Device2.

```
Device2#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 70      STATE_QUICK_R2      150.255.24.29   139.255.24.29   139.255.24.29
 69      STATE_MAIN_R3       150.255.24.29   139.255.24.29   139.255.24.29
 68      STATE_QUICK_R2      151.255.24.24   129.255.169.15  129.255.169.15
 67      STATE_MAIN_R3       151.255.24.24   129.255.169.15  129.255.169.15
Device2#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  101.0.0.0/24  100.0.0.0/24  ip  any  any
policy name : subflow-1610612757, the parent policy name : policy1
 f (src, dst, protocol, src port, dst port) :  101.0.0.0/24  100.0.0.0/24  ip  any  any
 local tunnel endpoint : 151.255.24.24 remote tunnel endpoint : 129.255.169.15 , fabric
lpu-node : 0
 the pairs of ESP ipsec sa : id : 68, algorithm : SM1 HMAC-SHA1-96
  inbound esp ipsec sa :  spi : 0xb404106a(3020165226)
     current input 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28638/4294967295
     uptime is 0 hour 2 minute 42 second
  outbound esp ipsec sa :  spi : 0x6c911061(1821446241)
     current output 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28638/4294967295
     uptime is 0 hour 2 minute 42 second
 local tunnel endpoint : 150.255.24.29 remote tunnel endpoint : 139.255.24.29 , fabric
lpu-node : 0
 the pairs of ESP ipsec sa : id : 70, algorithm : SM1 HMAC-SHA1-96
  inbound esp ipsec sa :  spi : 0x8672106b(2255622251)
     current input 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28648/4294967295
     uptime is 0 hour 2 minute 32 second
```

outbound esp ipsec sa : spi : 0x903e1062(2419986530)

current output 0 packets, 0 kbytes

encapsulation mode : Tunnel

replay protection : ON

remaining lifetime (seconds/kbytes) : 28648/4294967295

uptime is 0 hour 2 minute 32 second

total sa and sa group is 2

We can see that two IPsec tunnels are set up between Device2 and Device1.

#On Device1, view the information of the route automatically added to the peer protect network.

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 100.0.0.0/24 is directly connected, 00:29:10, gigabitethernet1

S 101.0.0.0/24 [1/10] via 151.255.24.24, 00:05:59, gigabitethernet0

[1/10] via 150.255.24.29, 00:05:49, gigabitethernet2

C 127.0.0.0/8 is directly connected, 30:31:38, lo0

C 129.255.169.0/24 is directly connected, 30:30:31, gigabitethernet0

C 139.255.24.0/24 is directly connected, 05:23:17, gigabitethernet2

S 150.255.24.0/24 [1/10] via 139.255.24.38, 05:14:53, gigabitethernet2

S 151.255.24.0/24 [1/10] via 129.255.169.38, 00:08:28, gigabitethernet0

We can see that 101.0.0.0/24 is the static route automatically added for IPsec on Device1.

#On Device2, view the information of the route automatically added to the peer protect network.

Device2#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

S 100.0.0.0/24 [1/10] via 129.255.169.15, 00:06:03, gigabitethernet0

[1/10] via 139.255.24.29, 00:05:52, gigabitethernet2

```
C   101.0.0.0/24 is directly connected, 00:29:11, gigabitethernet1
C   127.0.0.0/8 is directly connected, 44:01:05, lo0
S   129.255.255.0/24 [1/10] via 151.255.24.38, 00:09:04, gigabitethernet0
S   139.255.24.0/24 [1/10] via 150.255.24.38, 05:14:39, gigabitethernet2
C   150.255.24.0/24 is directly connected, 05:22:59, gigabitethernet2
C   151.255.24.0/24 is directly connected, 01:18:52, gigabitethernet0
```

We can see that 100.0.0.0/24 is the static route automatically added for IPsec on Device2.

#PC1 can communicate with PC2 and PC3 normally via the two IPsec tunnels between Device1 and Device2; the packet is protected by two IPsec tunnels tun1 and tun2.

9.3.4. Configure Ipsec Backup Gateway

Network Requirements

1. gigabitethernet0 of Device2 and Device3 are added to VRRP group1; Device1 sets up the IPsec tunnel with the virtual address of VRRP, protecting the data communication of the network where PC1 and PC2 are located.
2. gigabitethernet1 of Device2 and Device3 are added to VRRP group2; the gateway of PC2 points to the virtual address of VRRP2.
3. IPsec proposal security protocol adopts ESP; IKE proposal and IPsec proposal encryption algorithm adopts 3DES; authentication algorithm adopts MD5.

Network Topology

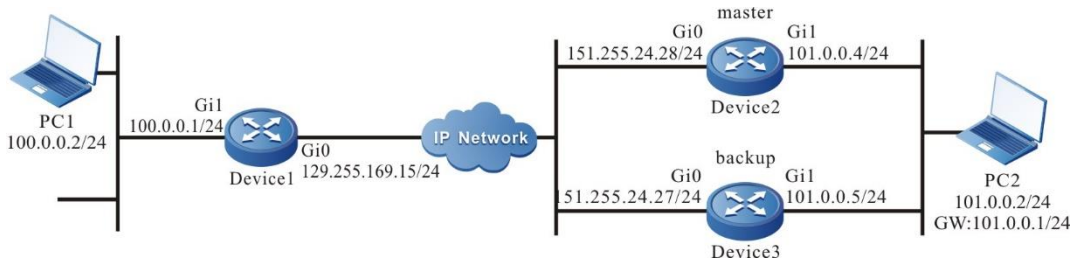


Figure 9-4 Networking of configuring the IPsec backup gateway

Configuration Steps

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

Step 2: Configure the VRRP group.

#On Device2, add VRRP group 1; add gigabitethernet0 to VRRP group 1; the virtual address of VRRP group1 is 151.255.24.29 and the priority is 110.

```
Device2#configure terminal
Device2(config)#interface gigabitethernet 0
Device2(config-if-gigabitethernet0)#vrrp 1 ip 151.255.24.29
Device2(config-if-gigabitethernet0)#vrrp 1 priority 110
Device2(config-if-gigabitethernet0)#exit
```

#On Device2, add VRRP group 2; add gigabitethernet1 to VRRP group 2; the virtual address of VRRP group2 is 101.0.0.1 and the priority is 110. Configure Track on VRRP group 2, monitor the interface gigabitethernet0 and configure the priority to reduce by 20.

```
Device2(config)#interface gigabitethernet 1
Device2(config-if-gigabitethernet1)#vrrp 2 ip 101.0.0.1
Device2(config-if-gigabitethernet1)#vrrp 2 priority 110
Device2(config-if-gigabitethernet1)#vrrp 2 track gigabitethernet 0 20
Device2(config-if-gigabitethernet1)#exit
```

#On Device3, add VRRP group 1; add gigabitethernet0 to VRRP group 1; the virtual address of VRRP group1 is 151.255.24.29.

```
Device3#configure terminal
Device3(config)#interface gigabitethernet 0
Device3(config-if-gigabitethernet0)#vrrp 1 ip 151.255.24.29
Device3(config-if-gigabitethernet0)#exit
```

#On Device3, add VRRP group 2; add gigabitethernet1 to VRRP group 2; the virtual address of VRRP group2 is 101.0.0.1.

```
Device3(config)#interface gigabitethernet 1
Device3(config-if-gigabitethernet1)#vrrp 2 ip 101.0.0.1
Device3(config-if-gigabitethernet1)#exit
```

Step 3: Configure the IKE and IPSec proposal.

#On Device1, configure the IKE proposal ikepro, use the encryption algorithm 3DES, authentication algorithm MD5; configure IPsec proposal ippro, use the ESP security protocol, use the encryption algorithm 3DES, and authentication algorithm MD5.

```
Device1#configure terminal
Device1(config)#crypto ike proposal ikepro
Device1(config-ike-prop)#encryption 3des
Device1(config-ike-prop)#integrity md5
Device1(config-ike-prop)#exit
Device1(config)#crypto ipsec proposal ippro
Device1(config-ipsec-prop)#esp 3des md5
Device1(config-ipsec-prop)#exit
```

#On Device2, configure the IKE proposal ikepro, use the encryption algorithm 3DES, authentication algorithm MD5; configure IPsec proposal ippro, use the ESP security protocol, use the encryption algorithm 3DES, and authentication algorithm MD5.

```
Device2(config)#crypto ike proposal ikepro
Device2(config-ike-prop)#encryption 3des
Device2(config-ike-prop)#integrity md5
Device2(config-ike-prop)#exit
Device2(config)#crypto ipsec proposal ippro
Device2(config-ipsec-prop)#esp 3des md5
```

```
Device2(config-ipsec-prop)#exit
```

#On Device3, configure the IKE proposal ikepro, use the encryption algorithm 3DES, authentication algorithm MD5; configure IPsec proposal ippro, use the ESP security protocol, use the encryption algorithm 3DES, and authentication algorithm MD5.

```
Device3(config)#crypto ike proposal ikepro
Device3(config-ike-prop)#encryption 3des
Device3(config-ike-prop)#integrity md5
Device3(config-ike-prop)#exit
Device3(config)#crypto ipsec proposal ippro
Device3(config-ipsec-prop)#esp 3des md5
Device3(config-ipsec-prop)#exit
```

Step 4: Configure the pre-share key.

#On Device1, configure the pre-share key, key is admin and permit all peers to use the key.

```
Device1(config)#crypto ike key admin any
```

#On Device2, configure the pre-share key, key is admin and permit all peers to use the key.

```
Device2(config)#crypto ike key admin any
```

#On Device3, configure the pre-share key, key is admin and permit all peers to use the key.

```
Device3(config)#crypto ike key admin any
```

Step 5: Configure the IPSec tunnel.

#On Device1, configure the tunnel tun; use the address of gigabitethernet0 as the local address of the tunnel; configure the peer address of the tunnel as the virtual address of the VRRP group 1 as 151.255.24.29; configure the authentication mode as the pre-share key authentication; the IKE proposal uses ikepro; the IPsec proposal uses ippro; enable the auto initiating negotiation.

```
Device1(config)#crypto tunnel tun
Device1(config-tunnel)#local address 129.255.169.15
Device1(config-tunnel)#peer address 151.255.24.29
Device1(config-tunnel)#set authentication preshared
Device1(config-tunnel)#set ike proposal ikepro
Device1(config-tunnel)#set ipsec proposal ippro
Device1(config-tunnel)#set auto-up
Device1(config-tunnel)#exit
```

#On Device2, configure the tunnel tun; use the virtual address of VRRP group 1 as the local address of the tunnel; configure the peer of the tunnel as any; the IKE proposal uses ikepro; the IPsec proposal uses ippro.

```
Device2(config)#crypto tunnel tun
```

```
Device2(config-tunnel)#local address 151.255.24.29
Device2(config-tunnel)#peer any
Device2(config-tunnel)#set ike proposal ikepro
Device2(config-tunnel)#set ipsec proposal ippro
Device2(config-tunnel)#exit
```

#On Device3, configure the tunnel tun; use the virtual address of VRRP group 1 as the local address of the tunnel; configure the peer of the tunnel as any; the IKE proposal uses ikepro; the IPsec proposal uses ippro.

```
Device3(config)#crypto tunnel tun
Device3(config-tunnel)#local address 151.255.24.29
Device3(config-tunnel)#peer any
Device3(config-tunnel)#set ike proposal ikepro
Device3(config-tunnel)#set ipsec proposal ippro
Device3(config-tunnel)#exit
```

Step 6: Configure the IPSec policy.

#On Device1, configure IPSec policypolicy1, protecting the IP communication from network 100.0.0.0/24 to network 101.0.0.0/24; associate the tunnel tun; add the route to the peer protect network automatically.

```
Device1(config)#crypto policy policy1
Device1(config-policy)#flow 100.0.0.0 255.255.255.0 101.0.0.0 255.255.255.0 ip tunnel tun
Device1(config-policy)#set reverse-route
Device1(config-policy)#exit
```

#On Device2, configure IPSec policypolicy1, protecting the IP communication from network 101.0.0.0/24 to network 100.0.0.0/24; associate the tunnel tun; add the route to the peer protect network automatically.

```
Device2(config)#crypto policy policy1
Device2(config-policy)#flow 101.0.0.0 255.255.255.0 100.0.0.0 255.255.255.0 ip tunnel tun
Device2(config-policy)#set reverse-route
Device2(config-policy)#exit
```

#On Device3, configure IPSec policy policy1, protecting the IP communication from network 101.0.0.0/24 to network 100.0.0.0/24; associate the tunnel tun; add the route to the peer protect network automatically.

```
Device3(config)#crypto policy policy1
Device3(config-policy)#flow 101.0.0.0 255.255.255.0 100.0.0.0 255.255.255.0 ip tunnel tun
Device3(config-policy)#set reverse-route
```

```
Device3(config-policy)#exit
```

Step 7: Check the result.

#On Devie1, view the tunnel setup information.

```
Device1#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 101    STATE_QUICK_I2       129.255.169.15  151.255.24.29   151.255.24.29
 100    STATE_MAIN_I4        129.255.169.15  151.255.24.29   151.255.24.29
Device1#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  100.0.0.0/24  101.0.0.0/24  ip  any  any
 local tunnel endpoint : 129.255.169.15 remote tunnel endpoint : 151.255.24.29 , fabric
lpu-node : 0
 the pairs of ESP ipsec sa : id : 101, algorithm : 3DES HMAC-MD5-96
  inbound esp ipsec sa :  spi : 0x6b5a106e(1801064558)
    current input 0 packets, 0 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28543/4294967295
    uptime is 0 hour 4 minute 17 second
  outbound esp ipsec sa :  spi : 0x12931077(311627895)
    current output 0 packets, 0 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28543/4294967295
    uptime is 0 hour 4 minute 17 second

total sa and sa group is 1
```

We can see that Device1 sets up the tunnel with Device2 successfully.

#On Device2, execute the **show vrrp** command to view that the status of VRRP group 1 and VRRP group 2 as Master; view the tunnel setup information.

```
Device2#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 88     STATE_QUICK_R2       151.255.24.29   129.255.169.15  129.255.169.15
 87     STATE_MAIN_R3        151.255.24.29   129.255.169.15  129.255.169.15
Device2#show crypto ipsec sa
policy name : policy1
```

f (src, dst, protocol, src port, dst port) : 101.0.0.0/24 100.0.0.0/24 ip any any

policy name : subflow-1610612761, the parent policy name : policy1

f (src, dst, protocol, src port, dst port) : 101.0.0.0/24 100.0.0.0/24 ip any any

local tunnel endpoint : 151.255.24.29 remote tunnel endpoint : 129.255.169.15 , fabric lpu-node : 0

the pairs of ESP ipsec sa : id : 88, algorithm : 3DES HMAC-MD5-96

inbound esp ipsec sa : spi : 0x12931077(311627895)

current input 0 packets, 0 kbytes

encapsulation mode : Tunnel

replay protection : ON

remaining lifetime (seconds/kbytes) : 28465/4294967295

uptime is 0 hour 5 minute 35 second

outbound esp ipsec sa : spi : 0x6b5a106e(1801064558)

current output 0 packets, 0 kbytes

encapsulation mode : Tunnel

replay protection : ON

remaining lifetime (seconds/kbytes) : 28465/4294967295

uptime is 0 hour 5 minute 35 second

total sa and sa group is 1

We can see that Device2 sets up the tunnel with Device1 successfully.

#On Device1, view the information of the route automatically added to the peer protect network.

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 129.255.24.38 to network 0.0.0.0

S 0.0.0.0/0 [1/10] via 129.255.169.38, 03:34:03, gigabitethernet0

C 100.0.0.0/24 is directly connected, 00:10:07, gigabitethernet1

S 101.0.0.0/24 [1/10] via 151.255.24.29, 00:07:47, gigabitethernet0

C 127.0.0.0/8 is directly connected, 76:28:40, lo0

C 129.255.169.0/16 is directly connected, 03:40:50, gigabitethernet1

We can see that 101.0.0.0/24 on Device1 is the static route automatically added for IPsec.

#On Device2, view the information of the route automatically added to the peer protect network.

```
Device2#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 151.255.24.38 to network 0.0.0.0

S   0.0.0.0/0 [1/10] via 151.255.24.38, 00:10:46, gigabitethernet0
S   100.0.0.0/24 [1/10] via 129.255.169.15, 00:08:43, gigabitethernet0
C   101.0.0.0/24 is directly connected, 00:10:09, gigabitethernet1
C   127.0.0.0/8 is directly connected, 89:59:00, lo0
C   151.255.24.0/24 is directly connected, 00:10:46, gigabitethernet0
```

We can see that 100.0.0.0/24 on Device2 is the static route automatically added for IPsec.

#PC1 can ping PC2 via the IPsec tunnel between Device1 and Device2 and the packet is protected by the IPsec tunnel.

#gigabitethernet0 on Device2 fails. On Device3, execute the **show vrrp** command to view that the status of the VRRP group 1 and VRRP group 2 are switched to Master; The tunnel of Device1 with Device2 is disconnected via the DPD detection; Device1 and Device3 set up the IPsec tunnel; on Device3, view the tunnel setup information.

```
Device3#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 40      STATE_QUICK_R2      151.255.24.29   129.255.169.15  129.255.169.15
 39      STATE_MAIN_R3       151.255.24.29   129.255.169.15  129.255.169.15
Device3#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  101.0.0.0/24  100.0.0.0/24  ip  any  any
policy name : subflow-1610612736, the parent policy name : policy1
 f (src, dst, protocol, src port, dst port) :  101.0.0.0/24  100.0.0.0/24  ip  any  any
 local tunnel endpoint : 151.255.24.29 remote tunnel endpoint : 129.255.169.15 , fabric lpu-node : 0
 the pairs of ESP ipsec sa : id : 40, algorithm : 3DES HMAC-MD5-96
  inbound esp ipsec sa :  spi : 0xb1852065(2978291813)
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28603/4294967295
     uptime is 0 hour 3 minute 17 second
  outbound esp ipsec sa :  spi : 0xc842106f(3359772783)
     current output 0 packets, 0 kbytes
     encapsulation mode : Tunnel
```

```
        replay protection : ON
        remaining lifetime (seconds/kbytes) : 28603/4294967295
        uptime is 0 hour 3 minute 17 second

    total sa and sa group is 1
```

We can see that Device3 and Device1 set up the Ipsec tunnel successfully.

#On Device1, view the tunnel setup information.

```
    Device1#show crypto ike sa
    sa-id   negotiation-state    localaddr       peeraddr        peer-identity
     103     STATE_QUICK_I2      129.255.169.15  151.255.24.29    151.255.24.29
     102     STATE_MAIN_I4       129.255.169.15  151.255.24.29    151.255.24.29

    Device1#show crypto ipsec sa
    policy name : policy1
     f (src, dst, protocol, src port, dst port) :  100.0.0.0/24  101.0.0.0/24  ip  any  any
     local tunnel endpoint : 129.255.169.15 remote tunnel endpoint : 151.255.24.29 , fabric
    lpu-node : 0
     the pairs of ESP ipsec sa : id : 103, algorithm : 3DES HMAC-MD5-96
      inbound esp ipsec sa :  spi : 0xc842106f(3359772783)
        current input 0 packets, 0 kbytes
        encapsulation mode : Tunnel
        replay protection : ON
        remaining lifetime (seconds/kbytes) : 28681/4294967295
        uptime is 0 hour 1 minute 59 second
      outbound esp ipsec sa :  spi : 0xb1852065(2978291813)
        current output 0 packets, 0 kbytes
        encapsulation mode : Tunnel
        replay protection : ON
        remaining lifetime (seconds/kbytes) : 28681/4294967295
        uptime is 0 hour 1 minute 59 second

    total sa and sa group is 1
```

We can see that Device1 and Device3 set up the Ipsec tunnel successfully.

#On Device1, view the information of the route automatically added to the peer protect network.

```
    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 129.255.24.38 to network 0.0.0.0

S   0.0.0.0/0 [1/10] via 129.255.169.38, 04:00:23, gigabitethernet0
C   100.0.0.0/24 is directly connected, 00:19:04, gigabitethernet1
S   101.0.0.0/24 [1/10] via 151.255.24.29, 00:05:29, gigabitethernet0
C   127.0.0.0/8 is directly connected, 76:55:00, lo0
C   129.255.169.0/24 is directly connected, 04:07:10, gigabitethernet0
```

We can see that 101.0.0.0/24 on Device1 is the static route automatically added for IPsec.

#On Device31, view the information of the route automatically added to the peer protect network.

```
Device3#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 151.255.24.38 to network 0.0.0.0

S   0.0.0.0/0 [1/10] via 151.255.24.38, 00:37:02, gigabitethernet
S   100.0.0.0/24 [1/10] via 129.255.169.15, 00:06:31, gigabitethernet0
C   101.0.0.0/24 is directly connected, 00:12:05, gigabitethernet1
C   127.0.0.0/8 is directly connected, 70:25:17, lo0
C   151.255.24.0/24 is directly connected, 00:37:02, gigabitethernet0
```

We can see that 100.0.0.0/24 on Device3 is the static route automatically added for IPsec.

PC1 can ping PC2 via the IPsec tunnel between Device1 and Device3 and the packet is protected by the IPsec tunnel.

gigabitethernet0 on Device2 restores the connection; on Device2, execute the **show vrrp** command to view that the status of VRRP group1 and VRRP group 2 is switched to Master; the tunnel of Device1 with Device3 is disconnected via the DPD detection; Device1 and Device2 set up the IPsec tunnel; View the tunnel setup information on Device2.

```
Device2#show crypto ike sa
sa-id   negotiation-state     localaddr       peeraddr        peer-identity
 90      STATE_QUICK_R2       151.255.24.29    129.255.169.15   129.255.169.15
 89      STATE_MAIN_R3        151.255.24.29    129.255.169.15   129.255.169.15
Device2#show crypto ipsec sa
policy name : policy1
  f (src, dst, protocol, src port, dst port) :  101.0.0.0/24  100.0.0.0/24  ip  any  any
policy name : subflow-1610612762, the parent policy name : policy1
```

```
 f (src, dst, protocol, src port, dst port) :  101.0.0.0/24  100.0.0.0/24  ip  any  any
 local tunnel endpoint : 151.255.24.29 remote tunnel endpoint : 129.255.169.15 ,
fabric lpu-node : 0
 the pairs of ESP ipsec sa : id : 90, algorithm : 3DES HMAC-MD5-96
  inbound esp ipsec sa :  spi : 0xe6331078(3862106232)
     current input 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 27188/4294967295
     uptime is 0 hour 26 minute 52 second
  outbound esp ipsec sa :  spi : 0x1c3b1070(473632880)
     current output 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 27188/4294967295
     uptime is 0 hour 26 minute 52 second


total sa and sa group is 1
```

We can see that Device2 sets up the tunnel with Device1 successfully.

#On Devie1, view the tunnel setup information.

```
Device1#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 105     STATE_QUICK_I2      129.255.169.15  151.255.24.29   151.255.24.29
 104     STATE_MAIN_I4       129.255.169.15  151.255.24.29   151.255.24.29
Device1#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  100.0.0.0/24  101.0.0.0/24  ip  any  any
 local tunnel endpoint : 129.255.169.15 remote tunnel endpoint : 151.255.24.29 ,
fabric lpu-node : 0
 the pairs of ESP ipsec sa : id : 105, algorithm : 3DES HMAC-MD5-96
  inbound esp ipsec sa :  spi : 0x1c3b1070(473632880)
     current input 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28546/4294967295
     uptime is 0 hour 4 minute 14 second
  outbound esp ipsec sa :  spi : 0xe6331078(3862106232)
     current output 0 packets, 0 kbytes
```

```
encapsulation mode : Tunnel
replay protection : ON
remaining lifetime (seconds/kbytes) : 28546/4294967295
uptime is 0 hour 4 minute 14 second


total sa and sa group is 1
```

We can see that Device1 sets up the tunnel with Device2 successfully.

#PC1 can ping PC2 via the IPsec tunnel between Device1 and Device2 and the packet is protected by the IPsec tunnel.

9.3.5. Configure GRE OVER IPsec

Network Requirements

1. Device1 and Device2 first set up the IPsec tunnel and then set up the GRE tunnel; the GRE tunnel is protected by IPsec;
2. Device1 and Device2 enable OSPF and can learn the OSPF route advertised by the peer;
3. IPsec proposal security protocol adopts ESP; IKE proposal and IPsec proposal emcryption algorithm adopts 3DES and the authentication algorithm adopts MD5.

Network Topology

Figure 9-5 Networking of configuring GRE OVER IPsec

Device	Interface	IP address	Device	Interface	IP address
Device1	Gi0	129.255.169.15/24	Device2	Gi0	151.255.24.24/24
	Gi1	100.0.0.1/24		Gi1	101.0.0.1/24
	Loopback0	102.0.0.1/24		Loopback0	103.0.0.1/24
	Tunnel1	10.0.0.1/24		Tunnel1	10.0.0.2/24

Configuration Steps

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

Step 2: Configure OSPF.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
```

```
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 101.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

Step 3: Configure the IKE and IPSec proposal.

#On Device1, configure the IKE proposal ikepro, use the encryption algorithm 3DES, authentication algorithm MD5; configure IPsec proposal ippro, use the encryption algorithm 3DES, and authentication algorithm MD5.

```
Device1(config)#crypto ike proposal ikepro
Device1(config-ike-prop)#encryption 3des
Device1(config-ike-prop)#integrity md5
Device1(config-ike-prop)#exit
Device1(config)#crypto ip proposal ippro
Device1(config-ipsec-prop)#esp 3des md5
Device1(config-ipsec-prop)#exit
```

#On Device2, configure the IKE proposal ikepro, use the encryption algorithm 3DES, authentication algorithm MD5; configure IPsec proposal ippro, use the encryption algorithm 3DES, and authentication algorithm MD5.

```
Device2(config)#crypto ike proposal ikepro
Device2(config-ike-prop)#encryption 3des
Device2(config-ike-prop)#integrity md5
Device2(config-ike-prop)#exit
Device2(config)#crypto ipsec proposal ippro
Device2(config-ipsec-prop)#esp 3des md5
Device2(config-ipsec-prop)#exit
```

Step 4: Configure the pre-share key.

#On Device1, configure the pre-share key, key is admin and permit all peers to use the key.

```
Device1(config)#crypto ike key admin any
```

#On Device2, configure the pre-share key, key is admin and permit all peers to use the key.

```
Device2(config)#crypto ike key admin any
```

Step 5: Configure the IPSec tunnel.

#On Device1, configure the tunnel tun; use the address of gigabitethernet0 as the local address of the tunnel; configure the peer address of the tunnel as 151.255.24.24; configure the authentication mode as the pre-share key authentication; the IKE proposal uses ikepro; the IPsec proposal uses ippro; enable the auto initiating negotiation.

```
Device1(config)#crypto tunnel tun
Device1(config-tunnel)#local address 129.255.169.15
Device1(config-tunnel)#peer address 151.255.24.24
Device1(config-tunnel)#set authentication preshared
Device1(config-tunnel)#set ike proposal ikepro
Device1(config-tunnel)#set ipsec proposal ippro
Device1(config-tunnel)#set auto-up
Device1(config-tunnel)#exit
```

#On Device2, configure the tunnel tun; use the address of gigabitethernet0 as the local address of the tunnel; configure the peer address of the tunnel as any; the IKE proposal uses ikepro; the IPsec proposal uses ippro.

```
Device2(config)#crypto tunnel tun
Device2(config-tunnel)#local address 151.255.24.24
Device2(config-tunnel)#peer any
Device2(config-tunnel)#set ike proposal ikepro
Device2(config-tunnel)#set ipsec proposal ippro
Device2(config-tunnel)#exit
```

Step 6: Configure the IPSec policy.

#On Device1, configure IPSec policy policy1, protecting the IP communication from network 102.0.0.0/24 to network 103.0.0.0/24; associate the tunnel tun.

```
Device1(config)#crypto policy policy1
Device1(config-policy)#flow 102.0.0.0 255.255.255.0 103.0.0.0 255.255.255.0 ip tunnel tun
Device1(config-policy)#exit
```

#On Device2 configure IPSec policy policy1, protecting the IP communication from network 1030.0.0/24 to network 1020.0.0/24; associate the tunnel tun.

```
Device2(config)#crypto policy policy1
Device2(config-policy)#flow 103.0.0.0 255.255.255.0 102.0.0.0 255.255.255.0 ip tunnel tun
Device2(config-policy)#exit
```

Step 7: Configure the GRE tunnel.

#On Device1, configure the GRE tunnel, the source address is 102.0.0.1, the destination address is 103.0.0.1, and the IP address is 10.0.0.1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel source 102.0.0.1
Device1(config-if-tunnel1)#tunnel destination 103.0.0.1
Device1(config-if-tunnel1)#ip address 10.0.0.1 255.255.255.0
Device1(config-if-tunnel1)#exit
```

#On Device2 configure the GRE tunnel, the source address is 1030.0.1, the destination address is 1020.0.1, and the IP address is 10.0.0.2

```
Device2(config)#interface tunnel 1
Device2(config-if-tunnel1)#tunnel source 103.0.0.1
Device2(config-if-tunnel1)#tunnel destination 102.0.0.1
Device2(config-if-tunnel1)#ip address 10.0.0.2 255.255.255.0
Device2(config-if-tunnel1)#exit
```

Step 8: Check the result.

#On Device1, view the GRE tunnel information.

```
Device1#show tunnel 1
Tunnel 1:
  Tunnel mode is gre ip
    Gre checksum validation is disabled
    Gre key is not set
    Gre keepalive is disabled
  Source ipv4 address is 102.0.0.1(Source ipv4 address is up on source interface loopback0)
  Destination ipv4 address is 103.0.0.1
  Tunnel state is up
  Encapsulation vrf is global(0x0)
  TTL(time-to-live) is 255
TOS(type of service) is not set
Send keepalive request: 0
Recv keepalive response: 0
Recv keepalive request: 0
Send keepalive response: 0
Send keepalive fail: 0
```

Send register request: 0

Recv register response: 0

Recv register request: 0

Send register response: 0

Send resolution request: 0

Recv resolution response: 0

Recv resolution request: 0

Send resolution response: 0

Send purge request: 0

Recv purge response: 0

Recv purge request: 0

Send purge response: 0

Send error packet: 0

Recv error packet: 0

Send redirect packet: 0

Recv redirect packet: 0

Send nhrp fail: 0

total(1)

We can see that the tunnel status is UP on Device1.

#On Device2, view the GRE tunnel information.

Device2# show tunnel 1

Tunnel 1:

Tunnel mode is gre ip

Gre checksum validation is disabled

Gre key is not set

Gre keepalive is disabled

Source ipv4 address is 103.0.0.1(Source ipv4 address is up on source interface loopback0)

Destination ipv4 address is 102.0.0.1

Tunnel state is up

Encapsulation vrf is global(0x0)

TTL(time-to-live) is 255

TOS(type of service) is not set

Send keepalive request: 0

Recv keepalive response: 0

Recv keepalive request: 0

Send keepalive response: 0

Send keepalive fail: 0
Send register request: 0
Recv register response: 0
Recv register request: 0
Send register response: 0
Send resolution request: 0
Recv resolution response: 0
Recv resolution request: 0
Send resolution response: 0
Send purge request: 0
Recv purge response: 0
Recv purge request: 0
Send purge response: 0
Send error packet: 0
Recv error packet: 0
Send redirect packet: 0
Recv redirect packet: 0
Send nhrp fail: 0
total(1)

We can see that the tunnel status is UP on Device2

#On Device1, view the IPsec tunnel setup information.

```
Device1#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 546    STATE_QUICK_I2      129.255.169.15  151.255.24.24   151.255.24.24
 545    STATE_MAIN_I4       129.255.169.15  151.255.24.24   151.255.24.24
Device1#sh crypto ipsec sa
policy name : policy1
  f (src, dst, protocol, src port, dst port) :  102.0.0.0/24  103.0.0.0/24  ip  any  any
  local tunnel endpoint : 129.255.169.15 remote tunnel endpoint : 151.255.24.24 , fabric lpu-node : 0
  the pairs of ESP ipsec sa : id : 546, algorithm : 3DES HMAC-MD5-96
    inbound esp ipsec sa :  spi : 0x5eb6107a(1588990074)
       current input 16 packets, 1 kbytes
       encapsulation mode : Tunnel
       replay protection : ON
       remaining lifetime (seconds/kbytes) : 28636/4294967293
       uptime is 0 hour 2 minute 44 second
```

```
    outbound esp ipsec sa :  spi : 0x29831048(696455240)
      current output 16 packets, 1 kbytes
      encapsulation mode : Tunnel
      replay protection : ON
      remaining lifetime (seconds/kbytes) : 28636/4294967293
      uptime is 0 hour 2 minute 44 second

  total sa and sa group is 1
```

We can see that Device1 sets up the tunnel with Device2 successfully.

#On Device2, view the IPsec tunnel setup information

```
Device2#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 4       STATE_QUICK_R2      151.255.24.24   129.255.169.15  129.255.169.15
 3       STATE_MAIN_R3       151.255.24.24   129.255.169.15  129.255.169.15
Device2#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  103.0.0.0/24  102.0.0.0/24  ip  any  any
policy name : subflow-1610612737, the parent policy name : policy1
 f (src, dst, protocol, src port, dst port) :  103.0.0.0/24  102.0.0.0/24  ip  any  any
 local tunnel endpoint : 151.255.24.24 remote tunnel endpoint : 129.255.169.15 , fabric
lpu-node : 0
 the pairs of ESP ipsec sa : id : 4, algorithm : 3DES HMAC-MD5-96
  inbound esp ipsec sa :  spi : 0x29831048(696455240)
    current input 16 packets, 1 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28643/4294967293
    uptime is 0 hour 2 minute 37 second
  outbound esp ipsec sa :  spi : 0x5eb6107a(1588990074)
    current output 16 packets, 1 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28643/4294967293
    uptime is 0 hour 2 minute 37 second

  total sa and sa group is 1
```

We can see that Device2 sets up the tunnel with Device1 successfully.

#View the route table on 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 129.255.24.38 to network 0.0.0.0

S   0.0.0.0/0 [1/10] via 129.255.169.38, 48:42:54, gigabitethernet0
C   10.0.0.0/24 is directly connected, 00:31:41, tunnel1
C   100.0.0.0/24 is directly connected, 16:30:29, gigabitethernet1
O   101.0.0.0/24 [110/11112] via 10.0.0.2, 00:29:55, tunnel1
C   102.0.0.0/24 is directly connected, 02:03:16, loopback0
C   127.0.0.0/8 is directly connected, 121:37:32, lo0
C   129.255.169.0/24 is directly connected, 48:49:41, gigabitethernet0
```

We can see that Device1 learns the OPSF route 101.0.0.0/24 advertised by the peer.

#On Device2, view the route table.

```
Device2#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 151.255.24.38 to network 0.0.0.0

S   0.0.0.0/0 [1/10] via 151.255.24.38, 02:36:59, gigabitethernet0
C   10.0.0.0/24 is directly connected, 00:29:59, tunnel1
O   100.0.0.0/24 [110/11112] via 10.0.0.1, 00:29:48, tunnel1
C   101.0.0.0/24 is directly connected, 15:25:33, gigabitethernet1
C   103.0.0.0/24 is directly connected, 01:58:29, loopback0
C   127.0.0.0/8 is directly connected, 15:26:28, lo0
C   151.255.24.0/24 is directly connected, 02:36:59, gigabitethernet0
```

We can see that Device2 learns the OSPF route 100.0.0.0/24 advertised by the peer.

9.3.6. Configure IPsec Policy VRF Isolation

Network Requirements

- IPSec tunnel is established between Device1 and Device2 in tunnel mode, PC1 and PC2 are in VRF 1, and PC3 and PC4 are in VRF 2.
- IPSec tunnel protects the data communication between PC1 and PC2 in VRF 1 and between PC3 and PC4 in VRF 2.

- IPSec proposal security protocol adopts ESP, IKE proposal and IPsec proposal encryption algorithm adopt 3DES, and authentication algorithm adopts MD5..

Network Topology

Figure 9-6 Networking of configuring IPsec policy to isolate VRF

Configuration Steps

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

Step 2: Configure VRF.

#On Device1, create VRF1 and VRF2.

```
Device1#configure terminal
Device1(config)#ip vrf 1
Device1(config-vrf)#rd 100:1
Device1(config-vrf)#exit
Device1(config)#ip vrf 2
Device1(config-vrf)#rd 200:1
Device1(config-vrf)#exit
```

#On Device2, create VRF1 and VRF2.

```
Device2#configure terminal
Device2(config)#ip vrf 1
Device2(config-vrf)#rd 100:1
Device2(config-vrf)#exit
Device2(config)#ip vrf 2
Device2(config-vrf)#rd 200:1
Device2(config-vrf)#exit
```

#Configure the gigabitethernet1.1 sub interface of Device1 to join VRF1, and the gigabitethernet1.2 sub interface to join VRF2.

```
Device1(config)#interface gigabitethernet 1.1
Device1(config-if-gigabitethernet1.1)#encapsulation dot1q 1
Device1(config-if-gigabitethernet1.1)#ip vrf forwarding 1
Device1(config-if-gigabitethernet1.1)#ip address 10.0.0.1 255.255.255.0
Device1(config-if-gigabitethernet1.1)#exit
Device1(config)#interface gigabitethernet 1.2
```

```
Device1(config-if-gigabitethernet1.2)#encapsulation dot1q 2
Device1(config-if-gigabitethernet1.2)#ip vrf forwarding 2
Device1(config-if-gigabitethernet1.2)#ip address 11.0.0.1 255.255.255.0
Device1(config-if-gigabitethernet1.2)#exit
```

#Configure the gigabitethernet1.1 sub interface of Device2 to join VRF1, and the gigabitethernet1.2 sub interface to join VRF2.

```
Device2(config)#interface gigabitethernet 1.1
Device2(config-if-gigabitethernet1.1)#encapsulation dot1q 1
Device2(config-if-gigabitethernet1.1)#ip vrf forwarding 1
Device2(config-if-gigabitethernet1.1)#ip address 10.1.1.1 255.255.255.0
Device2(config-if-gigabitethernet1.1)#exit
Device2(config)#interface gigabitethernet 1.2
Device2(config-if-gigabitethernet1.2)#encapsulation dot1q 2
Device2(config-if-gigabitethernet1.2)#ip vrf forwarding 2
Device2(config-if-gigabitethernet1.2)#ip address 11.1.1.1 255.255.255.0
Device2(config-if-gigabitethernet1.2)#exit
```

Step 3: Configure IKE, IPsec proposal.

#Configure IKE proposal ikepro on Device1, use encryption algorithm 3DES and authentication algorithm MD5; Configure IPSec proposal ippro, and use encryption algorithm 3DES and authentication algorithm MD5.

```
Device1(config)#crypto ike proposal ikepro
Device1(config-ike-prop)#encryption 3des
Device1(config-ike-prop)#integrity md5
Device1(config-ike-prop)#exit
Device1(config)#crypto ip proposal ippro
Device1(config-ipsec-prop)#esp 3des md5
Device1(config-ipsec-prop)#exit
```

#Configure IKE proposal ikepro on Device2, use encryption algorithm 3DES and authentication algorithm MD5; Configure IPSec proposal ippro, and use encryption algorithm 3DES and authentication algorithm MD5.

```
Device2(config)#crypto ike proposal ikepro
Device2(config-ike-prop)#encryption 3des
Device2(config-ike-prop)#integrity md5
Device2(config-ike-prop)#exit
Device2(config)#crypto ipsec proposal ippro
Device2(config-ipsec-prop)#esp 3des md5
Device2(config-ipsec-prop)#exit
```

Step 4: Configure the pre-share key.

#On Device1, configure the pre-share key, the key is admin, and permit all peers to use the key.

```
Device1(config)#crypto ike key admin any
```

#On Device2, configure the pre-share key, the key is admin, and permit all peers to use the key.

```
Device2(config)#crypto ike key admin any
```

Step 5: Configure the IPsec tunnel.

#Configure tunnel Tun on Device1, use the address of gigabitethernet0 as the local address of the tunnel, configure the peer address of the tunnel as 151.255.24.24, and configure the authentication method as pre shared key authentication. IKE proposal uses ikepro and IPSec proposal uses ippro, and enable auto negotiation.

```
Device1(config)#crypto tunnel tun
Device1(config-tunnel)#local address 129.255.169.15
Device1(config-tunnel)#peer address 151.255.24.24
Device1(config-tunnel)#set authentication preshared
Device1(config-tunnel)#set ike proposal ikepro
Device1(config-tunnel)#set ipsec proposal ippro
Device1(config-tunnel)#set auto-up
Device1(config-tunnel)#exit
```

#Configure tunnel tun on Device2, use the address of gigabitethernet0 as the local address of the tunnel, configure the peer of the tunnel as any, IKE proposal uses ikepro, and IPSec proposal uses ippro.

```
Device2(config)#crypto tunnel tun
Device2(config-tunnel)#local address 151.255.24.24
Device2(config-tunnel)#peer any
Device2(config-tunnel)#set ike proposal ikepro
Device2(config-tunnel)#set ipsec proposal ippro
Device2(config-tunnel)#exit
```

Step 6: Configure IPsec policy.

#Configure IPSec policy policy1 on Device1 to protect the IP communication from network 10.0.0.0/24 to network 10.1.1.0/24 in VRF1, associate the tunnel tun, and automatically add the route to the peer protection network.

```
Device1(config)#crypto policy policy1
Device1(config-policy)#flow vrf 1 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0 ip ipv4-tunnel tun
Device1(config-policy)#set reverse-route
Device1(config-policy)#exit
```

#Configure IPSec policy policy2 on Device1 to protect the IP communication from network 11.0.0.0/24 to network 11.1.1.0/24 in VRF2, associate the tunnel tun, and automatically add the route to the peer protection network.

```
Device1(config)#crypto policy policy2
Device1(config-policy)#flow vrf 2 11.0.0.0 255.255.255.0 11.1.1.0 255.255.255.0 ip ipv4-tunnel tun
Device1(config-policy)#set reverse-route
Device1(config-policy)#exit
```

#Configure IPSec policy policy1 on Device2 to protect the IP communication from network 10.0.0.0/24 to network 10.1.1.0/24 in VRF1, associate the tunnel tun, and automatically add the route to the peer protection network.

```
Device2(config)#crypto policy policy1
Device2(config-policy)#flow vrf 1 10.1.1.0 255.255.255.0 10.0.0.0 255.255.255.0 ip ipv4-tunnel tun
Device2(config-policy)#set reverse-route
Device2(config-policy)#exit
```

#Configure IPSec policy policy2 on Device2 to protect the IP communication from network 11.0.0.0/24 to network 11.1.1.0/24 in VRF2, associate the tunnel tun, and automatically add the route to the peer protection network.

```
Device2(config)#crypto policy policy2
Device2(config-policy)#flow vrf 2 11.1.1.0 255.255.255.0 11.0.0.0 255.255.255.0 ip ipv4-tunnel tun
Device2(config-policy)#set reverse-route
Device2(config-policy)#exit
```

Note:

- When multiple source network segments need to be protected on the central device Device2, the source network segment can be configured as any.

Step 7: Check the result.

#On Device1, view the setup information of the tunnel.

```
Device1#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 15      STATE_QUICK_I2      129.255.169.15  151.255.24.24   151.255.24.24
 14      STATE_QUICK_I2      129.255.169.15  151.255.24.24   151.255.24.24
 13      STATE_MAIN_I4       129.255.169.15  151.255.24.24   151.255.24.24
Device1#show crypto ipsec sa
policy name : policy1
  f (src, dst, protocol, src port, dst port) :  10.0.0.0/24  10.1.1.0/24  ip  any  any
  local tunnel endpoint : 129.255.169.15 remote tunnel endpoint : 151.255.24.24 , fabric lpu-node : 0
  vrf name: 1 id: 1
```

```
    the pairs of ESP ipsec sa : id : 14, algorithm : 3DES HMAC-MD5-96
  inbound esp ipsec sa :  spi : 0x481e4627(1209943591)
    current input 0 packets, 0 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28666/4294967295
    uptime is 0 hour 2 minute 14 second
  outbound esp ipsec sa :  spi : 0x1f5f81c6(526352838)
    current output 0 packets, 0 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28666/4294967295
    uptime is 0 hour 2 minute 14 second
policy name : policy2
 f (src, dst, protocol, src port, dst port) :  11.0.0.0/24  11.1.1.0/24  ip  any  any
  local tunnel endpoint : 129.255.169.15 remote tunnel endpoint : 151.255.24.24 , fabric
lpu-node : 0
 vrf name: 2 id: 2
    the pairs of ESP ipsec sa : id : 15, algorithm : 3DES HMAC-MD5-96
  inbound esp ipsec sa :  spi : 0xc8ef4628(3371124264)
    current input 0 packets, 0 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28666/4294967295
    uptime is 0 hour 2 minute 14 second
  outbound esp ipsec sa :  spi : 0x993a81c7(2570748359)
    current output 0 packets, 0 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 28666/4294967295
    uptime is 0 hour 2 minute 14 second
```

It can be seen that Device1 and Device2 successfully established IPSec tunnel.

#View tunnel establishment information on Device2.

```
Device2#show crypto ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 5      STATE_QUICK_R2       151.255.24.24   129.255.169.15  129.255.169.15
 4      STATE_QUICK_R2       151.255.24.24   129.255.169.15  129.255.169.15
```

```
 3       STATE_MAIN_R3        151.255.24.24     129.255.169.15    129.255.169.15
Device2#show crypto ipsec sa
policy name : policy1
  f (src, dst, protocol, src port, dst port) :  10.1.1.0/24  10.0.0.0/24  ip  any  any
policy name : subflow-1610612742, the parent policy name : policy1
f (src, dst, protocol, src port, dst port) :  10.1.1.0/24  10.0.0.0/24  ip  any  any
    local tunnel endpoint : 151.255.24.24 remote tunnel endpoint : 129.255.169.15 , fabric
lpu-node : 0
  vrf name: 1 id: 1
       the pairs of ESP ipsec sa : id : 4, algorithm : 3DES HMAC-MD5-96
    inbound esp ipsec sa :  spi : 0x1f5f81c6(526352838)
       current input 0 packets, 0 kbytes
       encapsulation mode : Tunnel
       replay protection : ON
       remaining lifetime (seconds/kbytes) : 28557/4294967295
       uptime is 0 hour 4 minute 3 second
    outbound esp ipsec sa :  spi : 0x481e4627(1209943591)
       current output 0 packets, 0 kbytes
       encapsulation mode : Tunnel
       replay protection : ON
       remaining lifetime (seconds/kbytes) : 28557/4294967295
       uptime is 0 hour 4 minute 3 second
policy name : policy2
  f (src, dst, protocol, src port, dst port) :  11.1.1.0/24  11.0.0.0/24  ip  any  any
policy name : subflow-1610612743, the parent policy name : policy2
f (src, dst, protocol, src port, dst port) :  11.1.1.0/24  11.0.0.0/24  ip  any  any
  local tunnel endpoint : 151.255.24.24 remote tunnel endpoint : 129.255.169.15 , fabric
lpu-node : 0
  vrf name: 2 id: 2
       the pairs of ESP ipsec sa : id : 5, algorithm : 3DES HMAC-MD5-96
    inbound esp ipsec sa :  spi : 0x993a81c7(2570748359)
       current input 0 packets, 0 kbytes
       encapsulation mode : Tunnel
       replay protection : ON
       remaining lifetime (seconds/kbytes) : 28557/4294967295
       uptime is 0 hour 4 minute 3 second
    outbound esp ipsec sa :  spi : 0xc8ef4628(3371124264)
       current output 0 packets, 0 kbytes
```

encapsulation mode : Tunnel

replay protection : ON

remaining lifetime (seconds/kbytes) : 28557/4294967295

uptime is 0 hour 4 minute 3 second

It can be seen that Device2 and Device1 successfully established IPSec tunnel.

#View the information about the route automatically added to the peer protection network on Device1.

Device1#show ip route vrf 1

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 10.0.0.0/24 is directly connected, 00:00:04, gigabitethernet1.1

S 10.1.1.0/24 [1/10] via 151.255.24.24, 00:05:04, gigabitethernet0

Device1#show ip route vrf 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

C 11.0.0.0/24 is directly connected, 00:00:10, gigabitethernet1.2

S 11.1.1.0/24 [1/10] via 151.255.24.24, 00:05:06, gigabitethernet0

It can be seen that 10.1.1.0/24 on Device1 is the static route automatically added by IPSec in VRF1, and 11.1.1.0/24 is the static route automatically added by IPSec in VRF2.

#View the route information automatically added to the peer protection network on Device2.

Device2#show ip route vrf 1

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 10.0.0.0/24 [1/10] via 129.255.169.15, 00:07:16, gigabitethernet0

C 10.1.1.0/24 is directly connected, 00:42:38, gigabitethernet1.1

Device2#show ip route vrf 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

S   11.0.0.0/24 [1/10] via 129.255.169.15, 00:08:08, gigabitethernet0
C   11.1.1.0/24 is directly connected, 00:43:31, gigabitethernet1.2
```

It can be seen that 10.0.0.0/24 on Device2 is the static route automatically added by IPSec in VRF1, and 11.0.0.0/24 is the static route automatically added by IPSec in VRF2.

#PC1 can ping PC2 through the IPSec tunnel between Device1 and Device2, and the packet is protected by the IPSec tunnel.

```
Device1#show crypto ipsec sa policy policy1
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  10.0.0.0/24  10.1.1.0/24  ip  any  any
 local tunnel endpoint : 129.255.169.15 remote tunnel endpoint : 151.255.24.24 , fabric lpu-node : 0
 vrf name: 1 id: 1
    the pairs of ESP ipsec sa : id : 14, algorithm : 3DES HMAC-MD5-96
  inbound esp ipsec sa :  spi : 0x481e4627(1209943591)
    current input 4 packets, 0 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 27575/4294967294
    uptime is 0 hour 20 minute 25 second
  outbound esp ipsec sa :  spi : 0x1f5f81c6(526352838)
    current output 4 packets, 0 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 27575/4294967294
    uptime is 0 hour 20 minute 25 second
```

It can be seen that the packet on Device1 is encapsulated by IPSec tunnel.

#PC3 can ping PC4 through the IPSec tunnel between Device1 and Device2, and the packet is protected by the IPSec tunnel.

```
Device1#show crypto ipsec sa policy policy2
policy name : policy2
 f (src, dst, protocol, src port, dst port) :  11.0.0.0/24  11.1.1.0/24  ip  any  any
 local tunnel endpoint : 129.255.169.15 remote tunnel endpoint : 151.255.24.24 , fabric lpu-node : 0
```

```
vrf name: 2 id: 2
    the pairs of ESP ipsec sa : id : 15, algorithm : 3DES HMAC-MD5-96
 inbound esp ipsec sa :  spi : 0xc8ef4628(3371124264)
    current input 4 packets, 0 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 27474/4294967294
    uptime is 0 hour 22 minute 6 second
 outbound esp ipsec sa :  spi : 0x993a81c7(2570748359)
    current output 4 packets, 0 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 27474/4294967294
    uptime is 0 hour 22 minute 6 second
```

It can be seen that the packet on device1 is encapsulated by IPSec tunnel.

9.3.7. Configure Protecting IPv6 Packet by IPsec Tunnel Mode

Network Requirements

- IPSec tunnel is established between Device1 and Device2 in tunnel mode to protect the data communication of the IPv6 network where PC1 and PC2 are located.
- In the proposal, ESP is used as the security protocol, IKE proposal and IPsec proposal encryption algorithm adopt 3DES, and the authentication algorithm adopts SHA1.

Network Topology

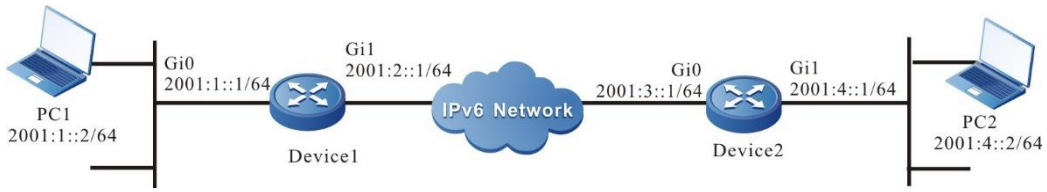


Figure 9-7Networking of configuring IPsec tunnel mode to protect the IPv6 packet

Configuration Steps

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

Step 2: Configure IKE, IPsec proposal.

#Configure IKE proposal ikepro on Device1, use encryption algorithm 3DES and authentication algorithm SHA1; Configure IPSec proposal ippro, use ESP security protocol, use encryption algorithm 3DES and authentication algorithm SHA1.

```
Device1#configure terminal
Device1(config)#crypto ike proposal ikepro
Device1(config-ike-prop)#encryption 3des
Device1(config-ike-prop)#integrity sha1
```

```
Device1(config-ike-prop)#exit
Device1(config)#crypto ipsec proposal ippro
Device1(config-ipsec-prop)#esp 3des sha1
Device1(config-ipsec-prop)#exit
```

#Configure IKE proposal ikepro on Device2, use encryption algorithm 3DES and authentication algorithm SHA1; Configure IPSec proposal ippro, use ESP security protocol, use encryption algorithm 3DES and authentication algorithm SHA1.

```
Device2#configure terminal
Device2(config)#crypto ike proposal ikepro
Device2(config-ike-prop)#encryption 3des
Device2(config-ike-prop)#integrity sha1
Device2(config-ike-prop)#exit
Device2(config)#crypto ipsec proposal ippro
Device2(config-ipsec-prop)#esp 3des sha1
Device2(config-ipsec-prop)#exit
```

Step 3: Configure the pre-share key.

#On Device1, configure the pre-shared key, the key is admin, and permit all peers to use the key.

```
Device1(config)#crypto ike key admin any
```

#On Device2, configure the pre-shared key, the key is admin, and permit all peers to use the key.

```
Device2(config)#crypto ike key admin any
```

Step 4: Configure the IPsec tunnel.

#Configure tunnel Tun on Device1, use the IPv6 address of gigabitethernet0 as the local address of the tunnel, configure the peer address of the tunnel as 2001:3::1, and configure the authentication method as pre shared key authentication. IKE proposal uses ikepro and IPSec proposal uses ippro, and enable auto negotiation.

```
Device1(config)#crypto ipv6-tunnel tun
Device1(config-tunnel)#local address 2001:2::1
Device1(config-tunnel)#peer address 2001:3::1
Device1(config-tunnel)#set authentication preshared
Device1(config-tunnel)#set ike proposal ikepro
Device1(config-tunnel)#set ipsec proposal ippro
Device1(config-tunnel)#set auto-up
Device1(config-tunnel)#exit
```

#Configure tunnel tun on Device2, use the IPv6 address of gigabitethernet0 as the local address of the tunnel, configure the peer of the tunnel as any, IKE proposal uses ikepro, and IPSec proposal uses ippro.

```
Device2(config)#crypto ipv6-tunnel tun
Device2(config-tunnel)#local address 2001:3::1
Device2(config-tunnel)#peer any
Device2(config-tunnel)#set ike proposal ikepro
Device2(config-tunnel)#set ipsec proposal ippro
Device2(config-tunnel)#exit
```

Step 5: Configure the IPSec policy.

#Configure IPSec policy policy1 on Device1 to protect the IPv6 communication from network 2001:1::/64 to network 2001:4::/64 in VRF1, associate the tunnel tun, and automatically add the route to the peer protection network.

```
Device1(config)#crypto ipv6-policy policy1
Device1(config-policy)#flow 2001:1::/64 2001:4::/64 ipv6 ipv6-tunnel tun
Device1(config-policy)#set reverse-route
Device1(config-policy)#exit
```

#Configure IPSec policy policy1 on Device2 to protect the IPv6 communication from network 2001:1::/64 to network 2001:4::/64 in VRF1, associate the tunnel tun, and automatically add the route to the peer protection network.

```
Device2(config)#crypto ipv6-policy policy1
Device2(config-policy)#flow 2001:4::/64 2001:1::/64 ipv6 ipv6-tunnel tun
Device2(config-policy)#set reverse-route
Device2(config-policy)#exit
```

Step 6: Check the result.

#On Device1, view the setup information of the tunnel.

```
Device1#show crypto ike sa
sa-id   negotiation-state    localaddr      peeraddr       peer-identity
 9      STATE_QUICK_I2      2001:2::1      2001:3::1      2001:3::1
 8      STATE_MAIN_I4       2001:2::1      2001:3::1      2001:3::1
Device1#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  2001:1::/64  2001:4::/64 ipv6  any  any
 local tunnel endpoint : 2001:2::1 remote tunnel endpoint : 2001:3::1, fabric lpu-node :
0
 the pairs of ESP ipsec sa : id : 9, algorithm : 3DES HMAC-SHA1-96
  inbound esp ipsec sa :  spi : 0x229b88f7(580618487)
     current input 0 packets, 0 kbytes
     encapsulation mode : Tunnel
     replay protection : ON
```

```
    remaining lifetime (seconds/kbytes) : 27225/4294967295
    uptime is 0 hour 26 minute 15 second
  outbound esp ipsec sa :  spi : 0x3b71859d(997295517)
    current output 0 packets, 0 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 27225/4294967295
    uptime is 0 hour 26 minute 15 second


total sa and sa group is 1
```

It can be seen that Device1 and Device2 successfully established IPSec tunnel.

#View the tunnel establishment information on Device2.

```
Device2#show crypto ike sa
sa-id   negotiation-state    localaddr      peeraddr       peer-identity
 24      STATE_QUICK_R2      2001:3::1      2001:2::1      2001:2::1
 23      STATE_MAIN_R3       2001:3::1      2001:2::1      2001:2::1
Device2#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  2001:4::/64  2001:1::/64 ipv6  any  any
policy name : subflow-1610612736, the parent policy name : policy1
 f (src, dst, protocol, src port, dst port) :  2001:4::/64  2001:1::/64 ipv6  any  any
 local tunnel endpoint : 2001:3::1 remote tunnel endpoint : 2001:2::1, fabric lpu-node :
0
 the pairs of ESP ipsec sa : id : 24, algorithm : 3DES HMAC-SHA1-96
  inbound esp ipsec sa :  spi : 0x3b71859d(997295517)
    current input 0 packets, 0 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 27175/4294967295
    uptime is 0 hour 27 minute 5 second
  outbound esp ipsec sa :  spi : 0x229b88f7(580618487)
    current output 0 packets, 0 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 27175/4294967295
    uptime is 0 hour 27 minute 5 second
```

```
total sa and sa group is 1
```

It can be seen that Device2 and Device1 successfully established IPSec tunnel.

#View the information about the route automatically added to the peer protection network on Device2.

```
Device2#show ipv6 route
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


L   ::1/128 [0/0]
      via ::, 5d:23:52:02, lo0
S   2001:1::/64 [1/10]
      via 2001:2::1, 00:27:51, gigabitethernet0
S   2001:2::/64 [1/10]
      via 2001:3::2, 00:27:58, gigabitethernet0
C   2001:3::/64 [0/0]
      via ::, 00:46:58, gigabitethernet0
L   2001:3::1/128 [0/0]
      via ::, 00:46:57, lo0
C   2001:4::/64 [0/0]
      via ::, 00:46:50, gigabitethernet1
L   2001:4::1/128 [0/0]
      via ::, 00:46:49, lo0
```

It can be seen that 2001:1:: / 64 on Device2 automatically adds static routes for IPSec.

#PC1 can ping PC2 through the IPSec tunnel between Device1 and Device2, and the packet is protected by the IPSec tunnel.

9.3.8. Configure Protecting IPv6 Packet by IPsec Transmission Mode

Network Requirements

- IPSec tunnel is established between Device1 and Device2 in transmission mode to protect the data communication between Device1 and Device2.
- In the proposal, the security protocol uses AH and ESP, AH protocol authentication algorithm adopts MD5, IKE proposal and IPsec proposal encryption algorithm adopts 3DES, and the authentication algorithm adopts SHA1.

Network Topology

Figure 9-8 Networking of configuring IPsec transmission mode to protect the IPv6 packet

Configuration Steps

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

Step 2: Configure IKE, IPsec proposal.

#Configure IKE proposal ikepro on Device1, use encryption algorithm 3DES and authentication algorithm SHA1; Configure IPSec proposal ippro, use ESP security protocol, use encryption algorithm 3DES, authentication algorithm SHA1, use the AH security protocol, authentication algorithm MD5, and use the transmission mode.

```
Device1#configure terminal
Device1(config)#crypto ike proposal ikepro
Device1(config-ike-prop)#encryption 3des
Device1(config-ike-prop)#integrity sha1
Device1(config-ike-prop)#exit
Device1(config)#crypto ipsec proposal ippro
Device1(config-ipsec-prop)#esp 3des sha1
Device1(config-ipsec-prop)#ah md5
Device1(config-ipsec-prop)#mode transport
Device1(config-ipsec-prop)#exit
```

#Configure IKE proposal ikepro on Device2, use encryption algorithm 3DES and authentication algorithm SHA1; Configure IPSec proposal ippro, use ESP security protocol, use encryption algorithm 3DES, authentication algorithm SHA1, use the AH security protocol, authentication algorithm MD5, and use the transmission mode.

```
Device2#configure terminal
Device2(config)#crypto ike proposal ikepro
Device2(config-ike-prop)#encryption 3des
Device2(config-ike-prop)#integrity sha1
Device2(config-ike-prop)#exit
Device2(config)#crypto ipsec proposal ippro
Device2(config-ipsec-prop)#esp 3des sha1
Device2(config-ipsec-prop)#ah md5
Device2(config-ipsec-prop)#mode transport
Device2(config-ipsec-prop)#exit
```

Step 3: Configure the pre-share key.

#On Device1, configure the pre-shared key, the key is admin, and permit all peers to use the key.

```
Device1(config)#crypto ike key admin any
```

#On Device2, configure the pre-shared key, the key is admin, and permit all peers to use the key.

```
Device2(config)#crypto ike key admin any
```

Step 4: Configure the IPsec tunnel.

#Configure tunnel Tun on Device1, use the IPv6 address of gigabitethernet0 as the local address of the tunnel, configure the peer address of the tunnel as 2001:3::1, and configure the authentication method as pre shared key authentication. IKE proposal uses ikepro and IPSec proposal uses ippro, and enable auto negotiation.

```
Device1(config)#crypto ipv6-tunnel tun
Device1(config-tunnel)#local interface gigabitethernet1
Device1(config-tunnel)#peer address 2001:3::1
Device1(config-tunnel)#set authentication preshared
Device1(config-tunnel)#set ike proposal ikepro
Device1(config-tunnel)#set ipsec proposal ippro
Device1(config-tunnel)#set auto-up
Device1(config-tunnel)#exit
```

#Configure tunnel tun on Device2, use gigabitethernet0 as the local interface of the tunnel, configure the peer of the tunnel as any, IKE proposal uses ikepro, and IPSec proposal uses ippro.

```
Device2(config)#crypto ipv6-tunnel tun
Device2(config-tunnel)#local interface gigabitethernet0
Device2(config-tunnel)#peer any
Device2(config-tunnel)#set ike proposal ikepro
Device2(config-tunnel)#set ipsec proposal ippro
Device2(config-tunnel)#exit
```

Step 5: Configure the IPSec policy.

#Configure IPSec policy policy1 on Device1 to protect the IPv6 communication from Device1 2001:2::1 to Device2 2001:3::1, and associate the tunnel tun.

```
Device1(config)#crypto ipv6-policy policy1
Device1(config-policy)#flow host 2001:2::1 host 2001:3::1 ipv6 ipv6-tunnel tun
Device1(config-policy)#exit
```

#Configure IPSec policy policy1 on Device2 to protect the IPv6 communication from Device2 2001:3::1 to Device1 2001:2::1, and associate the tunnel tun.

```
Device2(config)#crypto ipv6-policy policy1
Device2(config-policy)#flow host 2001:3::1 host 2001:2::1 ipv6 ipv6-tunnel tun
Device2(config-policy)#exit
```

Step 6: Check the result.

#On Device1, view the setup information of the tunnel.

```
Device1#show crypto ike sa
sa-id   negotiation-state   localaddr      peeraddr       peer-identity
```

```
 13      STATE_QUICK_I2      2001:2::1       2001:3::1       2001:3::1
 12      STATE_MAIN_I4       2001:2::1       2001:3::1       2001:3::1
Device1#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  2001:2::1/128  2001:3::1/128 ipv6  any  any
 local tunnel endpoint : 2001:2::1 remote tunnel endpoint : 2001:3::1, fabric lpu-node :
0
 the pairs of AH ipsec sa : id : 13, algorithm : HMAC-MD5-96
  inbound ah ipsec sa :  spi : 0xb3cd88fa(3016591610)
     current input 0 packets, 0 kbytes
     encapsulation mode : Transport
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28703/4294967295
     uptime is 0 hour 1 minute 37 second
  outbound ah ipsec sa :  spi : 0x5b5859f(95782303)
     current output 0 packets, 0 kbytes
     encapsulation mode : Transport
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28703/4294967295
     uptime is 0 hour 1 minute 37 second
 local tunnel endpoint : 2001:2::1 remote tunnel endpoint : 2001:3::1, fabric lpu-node :
0
 the pairs of ESP ipsec sa : id : 13, algorithm : 3DES HMAC-SHA1-96
  inbound esp ipsec sa :  spi : 0xd35988f9(3545860345)
     current input 0 packets, 0 kbytes
     encapsulation mode : Transport
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28703/4294967295
     uptime is 0 hour 1 minute 37 second
  outbound esp ipsec sa :  spi : 0xd4bf85a0(3569321376)
     current output 0 packets, 0 kbytes
     encapsulation mode : Transport
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28703/4294967295
     uptime is 0 hour 1 minute 37 second

total sa and sa group is 1
```

It can be seen that Device1 and Device2 successfully established IPSec tunnel.

#View the tunnel establishment information on Device2.

```
Device2#show crypto ike sa
sa-id   negotiation-state     localaddr       peeraddr        peer-identity
 28      STATE_QUICK_R2       2001:3::1       2001:2::1       2001:2::1
 27      STATE_MAIN_R3        2001:3::1       2001:2::1       2001:2::1
Device2#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  2001:3::1/128  2001:2::1/128 ipv6  any  any
policy name : subflow-1610612738, the parent policy name : policy1
 f (src, dst, protocol, src port, dst port) :  2001:3::1/128  2001:2::1/128 ipv6  any  any
 local tunnel endpoint : 2001:3::1 remote tunnel endpoint : 2001:2::1, fabric lpu-node :
0
 the pairs of AH ipsec sa : id : 28, algorithm : HMAC-MD5-96
  inbound ah ipsec sa :  spi : 0x5b5859f(95782303)
     current input 0 packets, 0 kbytes
     encapsulation mode : Transport
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28647/4294967295
     uptime is 0 hour 2 minute 33 second
  outbound ah ipsec sa :  spi : 0xb3cd88fa(3016591610)
     current output 0 packets, 0 kbytes
     encapsulation mode : Transport
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28647/4294967295
     uptime is 0 hour 2 minute 33 second
 local tunnel endpoint : 2001:3::1 remote tunnel endpoint : 2001:2::1, fabric lpu-node :
0
 the pairs of ESP ipsec sa : id : 28, algorithm : 3DES HMAC-SHA1-96
  inbound esp ipsec sa :  spi : 0xd4bf85a0(3569321376)
     current input 0 packets, 0 kbytes
     encapsulation mode : Transport
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28647/4294967295
     uptime is 0 hour 2 minute 33 second
  outbound esp ipsec sa :  spi : 0xd35988f9(3545860345)
     current output 0 packets, 0 kbytes
     encapsulation mode : Transport
     replay protection : ON
```

```
remaining lifetime (seconds/kbytes) : 28647/4294967295
uptime is 0 hour 2 minute 33 second

total sa and sa group is 1
```

It can be seen that Device2 and Device1 successfully established IPSec tunnel.

#Device1 can ping Device2 through the IPSec tunnel, and the packet is protected by the IPSec tunnel.

```
Device1#ping 2001:3::1

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2001:3::1 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.
```

9.3.9. Configure IPsec Tunnel to Protect Packets of GRE OVER IPv6 Tunnel

Network Requirements

- Device1 and Device2 first establish IPSec tunnel to protect the packets of GRE over IPv6 Tunnel.
- Device1 and Device2 enable OSPFv3 and can learn OSPFv3 routes advertised by the peer.
- ESP is used as the security protocol in the proposal, IKE proposal and IPsec proposal encryption algorithm adopts 3DES, and the authentication algorithm adopts SHA1.

Network Topology

Figure 9-9Networking of configuring IPsec tunnel to protect the packets of the GRE OVER IPv6 tunnel

Device	Interface	IPv6 Address	Device	Interface	IPv6 Address
Device1	Gi0	2001:1::1/64	Device2	Gi0	2001:3::1/64
	Gi1	2001:2::1/64		Gi1	2001:4::1/64
	Loopback0	2001:5::1/64		Loopback0	2001:6::1/64
	Tunnel1	2001:7::1/64		Tunnel1	2001:7::2/64

Configuration Steps

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

Step 2: Configure IKE, IPsec proposal.

#Configure IKE proposal ikepro on Device1, use encryption algorithm 3DES and authentication algorithm SHA1; Configure IPSec proposal ippro, use ESP security protocol, use encryption algorithm 3DES, authentication algorithm SHA1.

```
Device1(config)#crypto ike proposal ikepro
Device1(config-ike-prop)#encryption 3des
Device1(config-ike-prop)#integrity sha1
Device1(config-ike-prop)#exit
Device1(config)#crypto ipsec proposal ippro
Device1(config-ipsec-prop)#esp 3des sha1
Device1(config-ipsec-prop)#exit
```

#Configure IKE proposal ikepro on Device2, use encryption algorithm 3DES and authentication algorithm SHA1; Configure IPSec proposal ippro, use ESP security protocol, use encryption algorithm 3DES, authentication algorithm SHA1.

```
Device2(config)#crypto ike proposal ikepro
Device2(config-ike-prop)#encryption 3des
Device2(config-ike-prop)#integrity sha1
Device2(config-ike-prop)#exit
Device2(config)#crypto ipsec proposal ippro
Device2(config-ipsec-prop)#esp 3des sha1
Device2(config-ipsec-prop)#exit
```

Step 3: Configure the pre-share key.

#On Device1, configure the pre-shared key, the key is admin, and permit all peers to use the key.

```
Device1(config)#crypto ike key admin any
```

#On Device2, configure the pre-shared key, the key is admin, and permit all peers to use the key.

```
Device2(config)#crypto ike key admin any
```

Step 4: Configure the IPsec tunnel.

#Configure tunnel Tun on Device1, use the address of gigabitethernet1 as the local address of the tunnel, configure the peer address of the tunnel as 2001:3::1, and configure the authentication method as pre shared key authentication. IKE proposal uses ikepro and IPSec proposal uses ippro, and enable auto negotiation.

#Configure tunnel tun on Device2, use gigabitethernet0 as the local interface of the tunnel, configure the peer of the tunnel as any, IKE proposal uses ikepro, and IPSec proposal uses ippro.

```
Device2(config)#crypto ipv6-tunnel tun
Device2(config-tunnel)#local address 2001:3::1
Device2(config-tunnel)#peer any
Device2(config-tunnel)#set ike proposal ikepro
Device2(config-tunnel)#set ipsec proposal ippro
Device2(config-tunnel)#exit
```

Step 5: Configure the IPsec policy.

#Configure IPSec policy policy1 on Device1 to protect the IPv6 communication from network 2001:5::/64 to network 2001:6::/64, and associate the tunnel tun.

```
Device1(config)#crypto ipv6-policy policy1
Device1(config-policy)#flow 2001:5::/64 2001:6::/64 ipv6 ipv6-tunnel tun
Device1(config-policy)#exit
```

#Configure IPSec policy policy1 on Device2 to protect the IPv6 communication from network 2001:6::/64 to network 2001:5::/64, and associate the tunnel tun.

```
Device2(config)#crypto ipv6-policy policy1
Device2(config-policy)#flow 2001:6::/64 2001:5::/64 ipv6 ipv6-tunnel tun
Device2(config-policy)#exit
```

Step 6: Configure the GRE OVER IPv6 tunnel.

#Configure GRE over IPv6 Tunnel on Device1. The source address is 2001:5:: 1, the destination address is 2001:6:: 1, and the IPv6 address is 2001:7::1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode gre ipv6
Device1(config-if-tunnel1)#tunnel source 2001:5::1
Device1(config-if-tunnel1)#tunnel destination 2001:6::1
Device1(config-if-tunnel1)#ipv6 address 2001:7::1/64
Device1(config-if-tunnel1)#exit
```

#Configure GRE over IPv6 Tunnel on Device2. The source address is 2001:6:: 1, the destination address is 2001:5:: 1, and the IPv6 address is 2001:7:: 2.

```
Device2(config)#interface tunnel 1
Device2(config-if-tunnel1)#tunnel mode gre ipv6
Device2(config-if-tunnel1)#tunnel source 2001:6::1
Device2(config-if-tunnel1)#tunnel destination 2001:5::1
Device2(config-if-tunnel1)#ipv6 address 2001:7::2/64
Device2(config-if-tunnel1)#exit
```

Step 7: Configure OSPFv3.

#On Device1, create OSPFv3 process.

```
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 100.0.0.1
Device1(config-ospf6)#exit
```

#On Device2, create OSPFv3 process.

```
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 101.0.0.1
Device2(config-ospf6)#exit
```

#On the interface Tunnel1 and gigabitethernet0 of Device1, configure OSPFv3.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#ipv6 router ospf 100 area 0
Device1(config-if-tunnel1)#exit
Device1(config)#interface gigabitethernet 0
Device1(config-if-gigabitethernet0)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0)#exit
```

#On the interface Tunnel1 and gigabitethernet1 of Device2, configure OSPFv3.

```
Device2(config)#interface tunnel 1
Device2(config-if-tunnel1)#ipv6 router ospf 100 area 0
Device2(config-if-tunnel1)#exit
Device2(config)#interface gigabitethernet 1
Device2(config-if-gigabitethernet1)#ipv6 router ospf 100 area 0
Device2(config-if-gigabitethernet1)#exit
```

Step 8: Check the result.

#On Device1, view the GRE OVER IPv6 tunnel information.

```
Device1#show tunnel 1
Tunnel 1:
  Tunnel mode is gre ipv6
    Gre checksum validation is disabled
    Gre key is not set
  Source ipv6 address is 2001:5::1(Source ipv6 address is up on source interface loopback0)
  Destination ipv6 address is 2001:6::1
  Tunnel state is up
  Encapsulation vrf is global(0x0)
```

TTL(time-to-live) is 255
TOS(type of service) is not set
Send keepalive request: 0
Recv keepalive response: 0
Recv keepalive request: 0
Send keepalive response: 0
Send keepalive fail: 0
Send register request: 0
Recv register response: 0
Recv register request: 0
Send register response: 0
Send resolution request: 0
Recv resolution response: 0
Recv resolution request: 0
Send resolution response: 0
Send purge request: 0
Recv purge response: 0
Recv purge request: 0
Send purge response: 0
Send error packet: 0
Recv error packet: 0
Send redirect packet: 0
Recv redirect packet: 0
Send nhrp fail: 0
total(1)

You can see that the tunnel status on Device1 is up.

#View GRE over IPv6 Tunnel information on Device2.

Device2#show tunnel 1
Tunnel 1:
Tunnel mode is gre ipv6
Gre checksum validation is disabled
Gre key is not set
Source ipv6 address is 2001:6::1(Source ipv6 address is up on source interface loopback0)
Destination ipv6 address is 2001:5::1
Tunnel state is up
Encapsulation vrf is global(0x0)

```
    TTL(time-to-live) is 255
  TOS(type of service) is not set
  Send keepalive request: 0
  Recv keepalive response: 0
  Recv keepalive request: 0
  Send keepalive response: 0
  Send keepalive fail: 0
  Send register request: 0
  Recv register response: 0
  Recv register request: 0
  Send register response: 0
  Send resolution request: 0
  Recv resolution response: 0
  Recv resolution request: 0
  Send resolution response: 0
  Send purge request: 0
  Recv purge response: 0
  Recv purge request: 0
  Send purge response: 0
  Send error packet: 0
  Recv error packet: 0
  Send redirect packet: 0
  Recv redirect packet: 0
  Send nhrp fail: 0
  total(1)
```

You can see that the tunnel status on Device2 is up.

#View IPSec tunnel establishment information on Device1.

```
  Device1#show crypto ike sa
  sa-id   negotiation-state    localaddr      peeraddr       peer-identity
   19      STATE_QUICK_I2      2001:2::1      2001:3::1      2001:3::1
   17      STATE_MAIN_I4       2001:2::1      2001:3::1      2001:3::1
  Device1#show crypto ipsec sa
  policy name : policy1
   f (src, dst, protocol, src port, dst port) :  2001:5::/64  2001:6::/64 ipv6  any  any
   local tunnel endpoint : 2001:2::1 remote tunnel endpoint : 2001:3::1, fabric lpu-node :
  0
   the pairs of ESP ipsec sa : id : 19, algorithm : 3DES HMAC-SHA1-96
```

```
    inbound esp ipsec sa :  spi : 0xa7b98900(2813954304)
      current input 176 packets, 22 kbytes
      encapsulation mode : Tunnel
      replay protection : ON
      remaining lifetime (seconds/kbytes) : 23109/4294967272
      uptime is 1 hour 34 minute 51 second
    outbound esp ipsec sa :  spi : 0x2deb85a5(770409893)
      current output 174 packets, 22 kbytes
      encapsulation mode : Tunnel
      replay protection : ON
      remaining lifetime (seconds/kbytes) : 23109/4294967272
      uptime is 1 hour 34 minute 51 second

  total sa and sa group is 1
```

It can be seen that Device1 and Device2 successfully established IPSec tunnel.

#View the IPSec tunnel establishment information on Device2.

```
Device2#show crypto ike sa
sa-id   negotiation-state    localaddr      peeraddr       peer-identity
 32      STATE_QUICK_R2      2001:3::1      2001:2::1      2001:2::1
 31      STATE_MAIN_R3       2001:3::1      2001:2::1      2001:2::1
Device2#show crypto ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  2001:6::/64  2001:5::/64 ipv6  any  any
policy name : subflow-1610612739, the parent policy name : policy1
 f (src, dst, protocol, src port, dst port) :  2001:6::/64  2001:5::/64 ipv6  any  any
 local tunnel endpoint : 2001:3::1 remote tunnel endpoint : 2001:2::1, fabric lpu-node :
0
 the pairs of ESP ipsec sa : id : 32, algorithm : 3DES HMAC-SHA1-96
  inbound esp ipsec sa :  spi : 0x2deb85a5(770409893)
    current input 180 packets, 22 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
    remaining lifetime (seconds/kbytes) : 23046/4294967272
    uptime is 1 hour 35 minute 54 second
  outbound esp ipsec sa :  spi : 0xa7b98900(2813954304)
    current output 182 packets, 23 kbytes
    encapsulation mode : Tunnel
    replay protection : ON
```

```
        remaining lifetime (seconds/kbytes) : 23046/4294967271
        uptime is 1 hour 35 minute 54 second

    total sa and sa group is 1
    It can be seen that Device2 and Device1 successfully established IPSec tunnel.
    #View the routing table on Device1.
    Device1#show ipv6 route
    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   ::/0 [1/10]
        via 2001:2::2, 19:28:07, gigabitethernet1
    L   ::1/128 [0/0]
        via ::, 6d:18:52:55, lo0
    C   2001:1::/64 [0/0]
        via ::, 19:50:57, gigabitethernet0
    L   2001:1::1/128 [0/0]
        via ::, 19:50:56, lo0
    C   2001:2::/64 [0/0]
        via ::, 19:50:40, gigabitethernet1
    L   2001:2::1/128 [0/0]
        via ::, 19:50:38, lo0
    O   2001:4::/64 [110/1001]
        via fe80::201:7aff:fe5e:6d81, 00:26:29, tunnel1
    C   2001:5::/64 [0/0]
        via ::, 01:35:25, loopback0
    L   2001:5::1/128 [0/0]
        via ::, 01:35:25, loopback0
    C   2001:7::/64 [0/0]
        via ::, 00:57:40, tunnel1
    L   2001:7::1/128 [0/0]
        via ::, 00:57:39, lo0
```

You can see that device1 learned OSPFv3 route 2001:4:: / 64 advertised by the peer.

#View the route table on Device2.

```
    Device2#show ipv6 route
```

```
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   ::/0 [1/10]
    via 2001:3::2, 01:02:28, gigabitethernet0
L   ::1/128 [0/0]
    via ::, 6d:18:55:20, lo0
O   2001:1::/64 [110/1001]
    via fe80::201:7aff:fe5e:6d4b, 00:29:04, tunnel1
C   2001:3::/64 [0/0]
    via ::, 19:50:16, gigabitethernet0
L   2001:3::1/128 [0/0]
    via ::, 19:50:14, lo0
C   2001:4::/64 [0/0]
    via ::, 01:59:53, gigabitethernet1
L   2001:4::1/128 [0/0]
    via ::, 01:59:52, lo0
C   2001:6::/64 [0/0]
    via ::, 01:37:45, loopback0
L   2001:6::1/128 [0/0]
    via ::, 01:37:45, loopback0
C   2001:7::/64 [0/0]
    via ::, 00:58:59, tunnel1
L   2001:7::2/128 [0/0]
    via ::, 00:58:57, lo0
```

You can see that Device2 learned OSPFv3 route 2001:1:: / 64 adveetised by the peer.

10. ACL CONFIGURATION

10.1. Overview

10.1.1. Overview of ACL

One ACL (Access Control List) comprises a series of rules. Each rule is one permit, refuse or remark sentence, stating the corresponding matching condition and action. The ACL rule filters the packets by matching some field in the packet.

ACL can comprise multiple rules. The matching content specified by each rule is different and the matching contents in different rules may overlap or conflict. ACL rule matching strictly complies with the order of the sequence from small to large. The rule with smaller sequence takes effect earlier. Sequence means the order number of the rule in the while ACL.

There is one rule of refusing all packets hidden after the last rule of the ACL and the sequence is larger than all the other rules in the ACL. The hidden rule is invisible and it drops the packets that do not match the previous rules, that is, when the packet does not match with the previous rules, it matches the default rule and is dropped.

According to the ACL usage, we can divide ACL to five kinds, that is, IP standard ACL, IP extended ACL, MAC standard ACL, MAC extended ACL, and Ethernet protocol ACL. ACL name can use the number and also can use the customized character string. When ACL name uses the number, the corresponding ACL type and number value range are as follows:

- IP standard ACL: 1-1000;
- IP extended ACL: 1001-2000;
- MAC standard ACL: 2001-3000;
- MAC extended ACL: 3001-4000;
- Ethernet protocol ACL: 4001-5000;

When the ACL name adopts the customized character string, all ACLs share one name space, that is, if IP standard ACL uses one name, the other ACL types cannot use the name.

ACL also can execute the corresponding action group according to the matching. For details, refer to “QoS Configuration Manual”.

10.1.2. Overview of Time Domain

The time domain is the set of the time segments. One time domain can contain zero to multiple time segments. The time range of the time domain is the union of the time segments.

The time segment has the following two kinds:

- Periodical time segment: Periodical time segment means to select one day or several days from Monday to Sunday, and the start time point to the end time point as the time segment, taking effect every week repeatedly.
- Absolute time segment: The absolute time segment means to take effect within the specified date and time range

The user usually has the following demands:

The PC of one network segment can access the server only in the work time of the work day (except for all holidays); in the afternoon of Saturday, permit all PCs to communicate with the external Internet.

The communication control demands based on the time can be met by binding time domain in the ACL or ACL rule.

10.2. ACL Function Configuration

Table 10-1 ACL function configuration list

Configuration Task	
Configure the IP standard ACL	Configure the IP standard ACL
	Configure the IP standard ACL named by numbers
Configure the IP extended ACL	Configure the IP extended ACL
	Configure the IP extended ACL named by numbers
Configure the MAC standard ACL	Configure the MAC standard ACL
	Configure the MAC standard ACL named by numbers
Configure the MAC extended ACL	Configure the MAC extended ACL
	Configure the MAC extended ACL named by numbers
Configure the Ethernet protocol ACL	Configure the Ethernet protocol ACL
	Configure the Ethernet protocol ACL named by numbers
Configure the quantity limitation of the ACL rules	Configure the quantity limitation of the ACL rules
Configure the reflexive access control list	Configure defining the reflexive access control list
	Configure referencing the reflexive access control list
	Configure the global age time of the reflexive rule
Configure the ACL logs	Configure the ACL logs
	Configure the ACL log level

Configuration Task	
Configure the ACL compiling	Configure the ACL compiling
	Configure ACL to prohibit compiling
	Configure the percentage of the system memory permitted to be occupied by the ACL compiling
Configure the time domain	Configure the time domain
	Configure the periodical time segment
	Configure the absolute time segment
	Configure the refresh period
	Configure the maximum time offset
	Configure the time domain to be bound with the ACL rule
	Configure the time domain to be bound with the ACL
Configure the ACL application	Configure IP ACL to be applied to the interface
	Configure MAC ACL to be applied to the interface
	Configure Ethernet protocol ACL to be applied to the bridge group

10.2.1. Configure IP Standard ACL

IP standard ACL makes the rules according to the source IP address to filter the packets and generate logs.

Configuration Condition

None

Configure IP Standard ACL

IP standard ACL name can use the number and also can use the customized character string. If the IP standard ACL name adopts the numbers, we can configure the maximum quantity limitation of ACL; if adopting the customized character string, there is no limitation for the maximum quantity of ACL. The user can select the ACL name as desired.

Table 10-2 Configure the IP standard ACL

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the IP standard ACL	**ip access-list standard** { *access-list-number* | *access-list-name* }	Mandatory By default, the IP standard ACL is not configured. The number range of the IP standard ACL is 1-1000.
Configure the permit rule of ACL	[*sequence*] **permit** { **any** | *source-addr source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*] [log]	Optional By default, the ACL permit rule is not configured.
Configure the refuse rule of ACL	[*sequence*] **deny** { **any** | *source-addr source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*] [log]	Optional By default, the refuse rule of ACL is not configured.
Configure the ACL remarks	[*sequence*] **remark** *comment*	Optional By default, the remarks of the ACL rule are not configured.

Note:

- When using the **ip access-list standard** command to create the IP standard ACL, the ACL can be created only after configuring the rules in the IP standard ACL configuration mode.
- Sequence means the order number of the rule in the ACL. ACL matches and filters the packet strictly according to the order from small sequence to large sequence. The rule with the small sequence first takes effect. When all rules do not match, execute the default drop action, that is, all the packets not permitted to pass are dropped.

Configure IP Standard ACL Named by Numbers

The IP standard ACL named by numbers can let the user identify the type of the ACL quickly. However, the IP standard ACL named by numbers has some limitations. For example, the ACL quantity is limited.

Table 10-3 Configure the IP standard ACL named by numbers

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the IP standard ACL named by numbers	**access-list** *access-list-number* { **permit** | **deny** } { **any** | *source-addr source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*] [log]	Mandatory By default, the IP standard ACL named by numbers is not configured. The sequence range of the IP standard ACL is 1-1000.
Configure the remarks of the IP standard ACL named by numbers	**access-list** *access-list-number* **remark** *comment*	Optional By default, the remarks of the IP standard ACL named by numbers are not configured.

Note:

- If the ACL with the specified sequence does not exist, create one new ACL and add new rules. If the ACL with the specified number exists, just add new rules.
- l3-action-group is used for the ace matching counting of the L2 switching port. If the ace configured with the option acts on the L3 port (ignore the status of l3-action-group), do not affect the matching of its ace.

10.2.2. Configure IP Extended ACL

IP extended ACL can make the classification rule according to the IP protocol number, source IP address, destination IP address, source TCP/UDP port number, destination TCP/UDP port number, packet priority, fragment tag, and TCP tag, so as to filter the packets, generate logs and reflexive list.

Configuration Condition

None

Configure IP Extended ACL

IP extended ACL name can use the number and also can use the customized character string. If the IP extended ACL name adopts the numbers, we can configure the maximum quantity limitation of ACL; if adopting the customized character string, there is no limitation for the maximum quantity of ACL. The user can select the ACL name as desired. IP extended ACL is richer, more correct, and more flexible than the contents defined by IP standard ACL.

Table 10-4 Configure the IP extended ACL

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the IP extended ACL	**ip access-list extended** { *access-list-number* | *access-list-name* }	Mandatory By default, IP extended ACL is not configured. The sequence range of the IP extended ACL is 1001-2000.
Configure the permit rule of ACL	[*sequence*] **permit** *protocol* { **any** | *source-addr source-wildcard* | **host** *source-addr* } [*operator source-port*] { **any** | *destination-addr destination-wildcard* | **host** *destination-addr* } [*operator destination-port*] [*icmp-type*] [*icmp-code*] [*igmp-type*] [**ack** / **fin** / **established** / **psh** / **rst** / **syn** / **urg**] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**ttl** *ttl-value*] [**log**] [**time-range** *time-range-name*] [**reflect** *reflect-list-name* [**timeout** *reflect-timeout-value*]]	Optional By default, the permit rule of ACL is not configured.

Step	Command	Description
Configure the refuse rule of ACL	[*sequence*] **deny** *protocol* { **any** | *source-addr source-wildcard* | **host** *source-addr* } [*operator source-port*] { **any** | *destination-addr destination-wildcard* | **host** *destination-addr* } [*operator destination-port*] [*icmp-type*] [*icmp-code*] [*igmp-type*] [**ack** / **fin** / **established / psh** / **rst** / **syn** / **urg**] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**ttl** *ttl-value*] [**log**] [**time-range** *time-range-name*] [**reflect** *reflect-list-name* [**timeout** *reflect-timeout-value*]]	Optional By default, the refuse rule of ACL is not configured.
Configure the ACL remarks	[*sequence*] **remark** *comment*	Optional By default, the remarks of the ACL are not configured.
Configure ACL to reference the reflexive list	[*sequence*] **evaluate** *reflect-list-name*	Optional By default, do not configure the ACL to reference reflexive list.

Note:

- When using the **ip access-list extended** command to create the IP extended ACL, the ACL can be created only after configuring the rules in the IP extended ACL configuration mode.
- Sequence means the order number of the rule in the ACL. ACL matches and filters the packet strictly according to the order from small sequence to large sequence. The rule with the small sequence first takes effect. When all rules do not match, execute the default drop action, that is, all the packets not permitted to pass are dropped.
- Only permit rule can use the reflect parameter to create the reflexive ACL.
- l3-action-group is used for the ace matching counting of the L2 switching port. If the ace configured with the option acts on the L3 port (ignore the status of l3-action-group), do not affect the matching of its ace.

Configure IP Extended ACL Named by Numbers

The IP extended ACL named by numbers can let the user identify the type of the ACL quickly. However, the IP extended ACL named by numbers has some limitations. For example, the ACL quantity is limited. IP extended ACL is richer, more correct, and more flexible than the contents defined by IP standard ACL.

Table 10-5 Configure the IP extended ACL named by numbers

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the IP extended ACL named by numbers	**access-list** *access-list-number* { **permit** | **deny** } *protocol* { **any** | *source-addr source-wildcard* | **host** *source-addr* } [*operator source-port*] { **any** | *destination-addr destination-wildcard* | **host** *destination-addr* } [*operator destination-port*] [*icmp-type*] [*icmp-code*] [*igmp-type*] [**ack** / **established** / **fin** / **psh** / **rst** / **syn** / **urg**] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**ttl** *ttl-value*] [**log**] [**time-range** *time-range-name*] [**reflect** *reflect-list-name* [**timeout** *reflect-timeout-value*]]	Mandatory By default, the IP extended ACL named by numbers is not configured. The sequence range of the IP extended ACL is 1001-2000.
Configure the remarks of the IP extended ACL named by numbers	**access-list** *access-list-number* **remark** *comment*	Optional By default, the remarks of the IP extended ACL named by numbers are not configured.

Step	Command	Description
Configure the ACL to reference the reflexive list	**access-list** *access-list-number* **evaluate** *reflect-list-name*	Optional By default, do not configure the ACL to reference the reflexive list rule.

Note:

- If the ACL with the specified sequence does not exist, create one new ACL and add new rules. If the ACL with the specified number exists, just add new rules.
- Only permit rule can use the reflect parameter to create the reflexive ACL.
- l3-action-group is used for the ace matching counting of the L2 switching port. If the ace configured with the option acts on the L3 port (ignore the status of l3-action-group), do not affect the matching of its ace.

10.2.3. Configure ipv6 Standard ACL

IPv6 standard ACL only makes rules according to the source IPv6 address to filter packets and generate logs.

Configuration Conditions

No

Configure IP Standard ACL

IPv6 standard ACL name uses the custom string. When a custom string is used, there is no limit to the number of ACLs that can be configured. The user can select the appropriate ACL name according to the actual situation.

Table10-2 Configure IPv6 standard ACL

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure IPv6 standard ACL	**ipv6 access-list standard** {*access-list-name* }	Mandatory By default, do not configure the IPv6 standard ACL.
Configure the ACL permit rule	[*sequence*] **permit** { **any** | *source-addr source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*] [**log**]	Optional By default, do not configure the ACL permit rule.

Step	Command	Description
Configure the ACL deny rule	[*sequence*] **deny** { **any** | *source-addr source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*] [**log**]	Optional By default, do not configure the ACL deny rule.
Configure the ACL remarks	[*sequence*] **remark** *comment*	Optional By default, do not configure the remarks of the ACL rule.

Note:

- When using the command **ipv6 access-list standard** to create an IPv6 standard ACL, the ACL can be created only after the rules are configured in the IPv6 standard ACL configuration mode.
- Sequence refers to the sequence number of the rule in the whole ACL. When ACL matches and filters packets, it strictly follows the order from small sequence number to large sequence number. The rule of small sequence number takes effect first. When all rules do not match, the default deny action will be executed, that is, all packets that are not allowed to pass will be discarded.
- l3-action-group: this option is used for ACE matching count of L2 switching port; If the ace configured with this option acts on the L3 interface (l3-action-group status is ignored), its ace matching will not be affected.
- The current IPv6 standard ACL does not support compiling.

10.2.4. Configure IPv6 Extended ACL

IPv6 extended ACL can make the classification rule according to the IP protocol number, source IP address, destination IP address, source TCP/UDP port number, destination TCP/UDP port number, packet priority, IP fragment tag, TCP tag, and PAYLOAD value, so as to match and process the packets.

Configuration Condition

None

Configure IPv6 Extended ACL

Table 10-3 Configure the IPv6 extended ACL

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the IPv6 extended ACL	**ipv6 access-list extended** { *access-list-number* | *access-list-name* }	Mandatory The value range of *access-list-number* is 7001-8000.
Configure the permit rule of ACL	[*sequence*] **permit** *protocol* { **any |** *source-addr source-prefix* **| host** *source-addr* } [*operator source-port*] { **any |** *destination-addr destination-prefix* **| host** *destination-addr* } [*icmp-type*] [*icmp-code*] [*igmp-type*] [*operator destination-port*] [**flow-label** *flow-label value*] [**ack / fin / psh / rst / syn / urg**] [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**payload** *operator payload-value*] [**time-range** *time-range-name*]	Optional Configure the permit rule to analyze and process the packet.
Configure the refuse rule of ACL	[*sequence*] **deny** *protocol* { **any |** *source-addr source-prefix* | **host** *source-addr* } [*operator source-port*] { **any** | *destination-addr destination-prefix* | **host** *destination-addr* } [*icmp-type*] [*icmp-code*] [*igmp-type*] [*operator destination-port*] [**flow-label** *flow-label value*] [**ack / fin / psh / rst / syn / urg] [precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**payload** *operator payload-value*] [**time-range** *time-range-name*]	Optional Configure the refuse rule to analyze and process the packet.

Step	Command	Description
Configure the ACL remarks	[*sequence*] **remark** *comment*	Optional Configure one remark. The remark does not take part in the matching of the packet, but just plays the role of remarking and isolating.

Note:

- When using the **ipv6 access-list extended** command to create the IPv6 extended ACL, the ACL can be created only after configuring the rules in the IPv6 extended ACL configuration mode.
- deny rule: By default, the IPv6 extended ACL permits the icmpv6 neighbor entry query packet to pass; for the IPv6 extended ACL rule, be careful to configure the rules, like **deny ipv6 any any**. If the user configured rule can deny icmpv6 neighbor entry query packet, the default rule cannot process the icmpv6 neighbor entry query packet, and icmpv6 neighbor entry query cannot succeed.

Configure IPv6 Extended ACL Named by Numbers

Table 10-4 Configure the IPv6 extended ACL named by numbers

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the IPv6 extended ACL named by numbers	access-list access-list-number { permit | deny } protocol { any | source-addr source-prefix | host source-addr } [operator source-port] { any | destination-addr destination-prefix | host destination-addr } [icmp-type] [icmp-code] [igmp-type] [operator destination-port] [flow-label flow-label value] [ack / fin / psh / rst / syn / urg] [precedence precedence] [dscp dscp] [fragments] [payload operator payload-value] [time-range time-range-name]	Mandatory

Step	Command	Description
Configure the remarks of the IPv6 extended ACL named by numbers	**access-list** *access-list-number* **remark** *comment*	Optional

Note:

- If the ACL with the specified sequence does not exist, create one new ACL and add new rules. If the ACL with the specified number exists, just add new rules.
- deny rule: By default, the IPv6 extended ACL permits the icmpv6 neighbor entry query packet to pass; for the IPv6 extended ACL rule, be careful to configure the rules, like **deny ipv6 any any**. If the user configured rule can deny icmpv6 neighbor entry query packet, the default rule cannot process the icmpv6 neighbor entry query packet, and icmpv6 neighbor entry query cannot succeed.

10.2.5. Configure MAC Standard ACL

MAC standard ACL makes the rules according to the source MAC address to filter the packets.

Configuration Condition

None

Configure MAC Standard ACL

MAC standard ACL name can use the number and also can use the customized character string. If the MAC standard ACL name adopts the numbers, we can configure the maximum quantity limitation of ACL; if adopting the customized character string, there is no limitation for the maximum quantity of ACL. The user can select the ACL name as desired.

Table 10-9 Configure the MAC standard ACL

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the MAC standard ACL	**mac access-list standard** { *access-list-number* | *access-list-name* }	Mandatory By default, the MAC standard ACL is not configured. The sequence range of the MAC standard ACL is 2001-3000.

Step	Command	Description
Configure the permit rule of ACL	[*sequence*] **permit** { **any** | *source-addr source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*]	Optional By default, the permit rule of ACL is not configured.
Configure the refuse rule of ACL	[*sequence*] **deny** { **any** | *source-addr source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*]	Optional By default, the refuse rule of ACL is not configured.
Configure the ACL remarks	[*sequence*] **remark** *comment*	Optional By default, the remarks of ACL are not configured.

Note:

- When using the **mac access-list standard** command to create the MAC standard ACL, the ACL can be created only after configuring the rules in the MAC standard ACL configuration mode.
- Sequence means the order number of the rule in the ACL. ACL matches and filters the packet strictly according to the order from small sequence to large sequence. The rule with the small sequence first takes effect. When all rules do not match, execute the default drop action, that is, all the packets not permitted to pass are dropped.

Configure MAC Standard ACL Named by Numbers

The MAC standard ACL named by numbers can let the user identify the type of the ACL quickly. However, the MAC standard ACL named by numbers has some limitations. For example, the ACL quantity is limited.

Table 10-10 Configure the MAC standard ACL named by numbers

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the MAC standard ACL named by numbers	**access-list** *access-list-number* { **permit** | **deny** } { **any** | *source-addr source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*]	Mandatory By default, the MAC standard ACL named by numbers is not configured. The sequence range of the MAC standard ACL is 2001-3000.
Configure the remarks of the MAC standard ACL named by numbers	**access-list** *access-list-number* **remark** *comment*	Optional By default, the remarks of the MAC standard ACL named by numbers are not configured.

Note:

- If the ACL with the specified sequence does not exist, create one new ACL and add new rules. If the ACL with the specified number exists, just add new rules.

10.2.6. Configure MAC Extended ACL

MAC extended ACL can make the classification rule according to the Ethernet protocol type, source MAC address, destination MAC address, VLAN ID, and 802.1p priority, so as to filter the packets.

Configuration Condition

None

Configure MAC Extended ACL

MAC extended ACL name can use the number and also can use the customized character string. If the MAC extended ACL name adopts the numbers, we can configure the maximum quantity limitation of ACL; if adopting the customized character string, there is no limitation for the maximum quantity of ACL. The user can select the ACL name as desired. MAC extended ACL is richer, more correct, and more flexible than the contents defined by MAC standard ACL.

Table 10-11 Configure the MAC extended ACL

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the MAC extended ACL	**mac access-list extended** { *access-list-number* | *access-list-name* }	Mandatory By default, MAC extended ACL is not configured. The sequence range of the MAC extended ACL is 3001-4000.
Configure the permit rule of ACL	[*sequence*] **permit** { **any** | *source-addr source-wildcard* | **host** *source-addr* } { **any** | *destination-addr destination-wildcard* | **host** *destination-addr* } [**ether-type** *type*] [**cos** *cos*] [**vlan-id** *vlan*] [**time-range** *time-range-name*]	Optional By default, the permit rule of ACL is not configured.
Configure the refuse rule of ACL	[*sequence*] **deny** { **any** | *source-addr source-wildcard* | **host** *source-addr* } { **any** | *destination-addr destination-wildcard* | **host** *destination-addr* } [**ether-type** *type*] [**cos** *cos*] [**vlan-id** *vlan*] [**time-range** *time-range-name*]	Optional By default, the refuse rule of ACL is not configured.
Configure the ACL remarks	[*sequence*] **remark** *comment*	Optional By default, the remarks of ACL are not configured.

Note:

- When using the **mac access-list extended** command to create the MAC extended ACL, the ACL can be created only after configuring the rules in the MAC extended ACL configuration mode.
- Sequence means the order number of the rule in the ACL. ACL matches and filters the packet strictly according to the order from small sequence to large sequence. The rule

with the small sequence first takes effect. When all rules do not match, execute the default drop action, that is, all the packets not permitted to pass are dropped.

Configure MAC Extended ACL Named by Numbers

The MAC extended ACL named by numbers can let the user identify the type of the ACL quickly. However, the MAC extended ACL named by numbers has some limitations. For example, the ACL quantity is limited. MAC extended ACL is richer, more correct, and more flexible than the contents defined by MAC standard ACL.

Table 10-12 Configure the MAC extended ACL named by numbers

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the MAC extended ACL named by numbers	**access-list** *access-list-number* { **permit** | **deny** } { **any** | *source-addr source-wildcard* | **host** *source-addr* } { **any** | *destination-addr destination-wildcard* | **host** *destination-addr* } [**ether-type** *type*] [**cos** *cos*] [**vlan-id** *vlan*] [**time-range** *time-range-name*]	Mandatory By default, the MAC extended ACL named by numbers is not configured. The sequence range of the MAC extended ACL is 3001-4000.
Configure the remarks of the MAC extended ACL named by numbers	**access-list** *access-list-number* **remark** *comment*	Optional By default, the remarks of the MAC extended ACL named by numbers are not configured.

Note:

- If the ACL with the specified sequence does not exist, create one new ACL and add new rules. If the ACL with the specified number exists, just add new rules.

10.2.7. Configure Ethernet protocol ACL

Configuration Condition

None

Configure the Ethernet protocol ACL

Ethernet protocol ACL makes the rule only according to the Ethernet protocol type, so as to filter the packets.

Table 10-5 Configure the Ethernet protocol ACL

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the Ethernet protocol ACL	**protocol access-list standard** { *access-list-number* }	Mandatory By default, do not configure the Ethernet protocol ACL. The number range of the Ethernet protocol ACL is 4001-5000.
Configure the ACL permit rule	[*sequence*] **permit** *type-code* [*type-wildcard*]	Optional By default, do not configure the ACL permit rule.
Configure the ACL refuse rule	[*sequence*] **deny** *type-code* [*type-wildcard*]	Optional By default, do not configure ACL refuse rule.
Configure the ACL remarks	[*sequence*] **remark** *comment*	Optional By default, do not configure the ACL rule remarks.

Note:

- When using the **protocol access-list standard** command to create the Ethernet protocol ACL, the ACL can be created only after configuring the rules in the Ethernet protocol ACL configuration mode.
- Sequence means the order number of the rule in the ACL. ACL matches and filters the packet strictly according to the order from small sequence to large sequence. The rule with the small sequence first takes effect. When all rules do not match, execute the default drop action, that is, all the packets not permitted to pass are dropped.
- Ethernet protocol ACL can only be applied by the bridge module and cannot be applied to the L3 Ethernet interface via the **access-group** command. For the bridge configuration, refer to “Bridge Configuration Manual”.

Configure Ethernet Protocol ACL Named by Numbers

The Ethernet protocol ACL rule named by numbers can let the user fast identify the type of the rule ACL.

Table 10-6 Configure Ethernet protocol ACL named by numbers

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure Ethernet protocol ACL named by numbers	**access-list** *access-list-number* { **permit | deny** } *type-code* [*type-wildcard*]	Mandatory By default, do not configure the Ethernet protocol ACL named by numbers. The number range of the Ethernet protocol ACL is 4001-5000.
Configure the remarks of the Ethernet protocol ACL named by numbers	**access-list** *access-list-number* **remark** *comment*	Optional By default, do not configure the remarks of the Ethernet protocol ACL named by numbers.

Note:

- If the ACL with the specified sequence does not exist, create one new ACL and add new rules. If the ACL with the specified number exists, just add new rules.
- Ethernet protocol ACL can only be applied by the bridge module and cannot be applied to the L3 Ethernet interface via the **access-group** command. For the bridge configuration, refer to “Bridge Configuration Manual”.

10.2.8. Configure Hybrid Extended ACL

Hybrid extended ACL can make the classification rule according to the source MAC address, destination MAC address, Ethernet type, IP protocol type, source IP address, destination IP address, packet priority, VLAN ID, and 802.1p priority, so as to filter the packets.

Configuration Condition

None

Configure Hybrid Extended ACL

Hybrid extended ACL name can use the number and also can use the customized character string. If the Hybrid extended ACL name adopts the numbers, we can configure the maximum quantity limitation of ACL; if adopting the customized character string, there is no limitation for the maximum quantity of ACL. The user can select the ACL name as desired. Hybrid extended ACL is richer, more correct, and more flexible than using the contents defined by IP ACL and MAC ACL separately.

Table 10-15 Configure the Hybrid extended ACL

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the Hybrid extended ACL	**hybrid access-list extended** { *access-list-number* | *access-list-name* }	Mandatory By default, Hybrid extended ACL is not configured. The sequence range of the Hybrid extended ACL is 5001-6000.
Configure the permit rule of ACL	[*sequence*] **permit** { **any** | *source-mac -addr source-wildcard* | **host** *source-mac-addr* } { **any** | *destination-mac-addr destination-wildcard* | **host** *destination-mac-addr* } [**cos** *cos*] [**vlan-id** *vlan*] [**time-range** *time-range-name*] **[egr-action-group** *egr-action-group-name*] [**ethter-type**] { *etherne-type* | *ipv4 protocol* } { **any** | *source-ip-addr source-wildcard* | **host** *source-ip-addr* } { **any** | *destination -ip-addr destination -wildcard* | **host** *destination-ip-addr* }**[precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**time-range** *time-range-name*] [**egr-action-group** *egr-action-group-name*]	Optional By default, the permit rule of ACL is not configured.

Step	Command	Description
Configure the refuse rule of ACL	[*sequence*] **deny** { **any** | *source-mac -addr source-wildcard* | **host** *source-mac-addr* } { **any** | *destination-mac-addr destination-wildcard* | **host** *destination-mac-addr* } [**cos** *cos*] [**vlan-id** *vlan*] [**time-range** *time-range-name*] **[egr-action-group** *egr-action-group-name*] [**ethter-type**] { *etherne-type* | *ipv4 protocol* } { **any** | *source-ip-addr source-wildcard* | **host** *source-ip-addr* } { **any** | *destination -ip-addr destination -wildcard* | **host** *destination-ip-addr* }**[precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**time-range** *time-range-name*] [**egr-action-group** *egr-action-group-name*]	Optional By default, the refuse rule of ACL is not configured.
Configure the ACL remarks	[*sequence*] **remark** *comment*	Optional By default, the remarks of ACL are not configured.

Note:

- When using the **hybrid access-list extended** command to create the Hybrid extended ACL, the ACL can be created only after configuring the rules in the Hybrid extended ACL configuration mode.
- Sequence means the order number of the rule in the ACL. ACL matches and filters the packet strictly according to the order from small sequence to large sequence. The rule with the small sequence first takes effect. When all rules do not match, execute the default drop action, that is, all the packets not permitted to pass are dropped.

Configure Hybrid Extended ACL Named by Numbers

The Hybrid extended ACL named by numbers can let the user identify the type of the ACL quickly. However, the Hybrid extended ACL named by numbers has some limitations. For example, the ACL quantity is limited.

Table 10-16 Configure the Hybrid extended ACL named by numbers

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the Hybrid extended ACL named by numbers	**access-list** *access-list-number* { **permit** | **deny** } { **any** | *source-mac -addr source-wildcard* | **host** *source-mac-addr* } { **any** | *destination-mac-addr destination-wildcard* | **host** *destination-mac-addr* } [**cos** *cos*] [**vlan-id** *vlan*] [**time-range** *time-range-name*] **[egr-action-group** *egr-action-group-name*] [**ethter-type**] { *etherne-type* | *ipv4 protocol* } { **any** | *source-ip-addr source-wildcard* | **host** *source-ip-addr* } { **any** | *destination -ip-addr destination -wildcard* | **host** *destination-ip-addr* }**[precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**time-range** *time-range-name*] [**egr-action-group** *egr-action-group-name*]	Mandatory By default, the Hybrid extended ACL named by numbers is not configured. The sequence range of the Hybrid extended ACL is 5001-6000.
Configure the remarks of the Hybrid extended ACL named by numbers	**access-list** *access-list-number* **remark** *comment*	Optional By default, the remarks of the Hybrid extended ACL named by numbers are not configured.

Note:

- If the ACL with the specified sequence does not exist, create one new ACL and add new rules. If the ACL with the specified number exists, just add new rules.

10.2.9. Configure Hybrid Advanced ACL

Hybrid advanced ACL can make the classification rule according to the source MAC address, destination MAC address, IP protocol type, source IP address, and destination IP address, so as to filter the packets.

Configuration Condition

None

Configure Hybrid Advanced ACL

Hybrid advanced ACL name can use the number and also can use the customized character string. If the Hybrid advanced ACL name adopts the numbers, we can configure the maximum quantity limitation of ACLs; if adopting the customized character string, there is no limitation for the maximum quantity of ACLs. The user can select the ACL name as desired. Hybrid advanced ACL is richer, more correct, and more flexible than using the contents defined by IP ACL and MAC ACL separately. Users can select hybrid extended AC or hybrid advanced ACL as needed.

Table 10-7 Configure Hybrid advanced ACL

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure Hybrid advanced ACL	**hybrid access-list advanced** { *access-list-number* | *access-list-name* }	Mandatory By default, Hybrid advanced ACL is not configured. The sequence range of the Hybrid advanced ACL is 9001-9100.
Configure the permit rule of ACL	[*sequence*] **permit** *protocol* { **any** | *source-ip-addr source-wildcard* | **host** *source-ip-addr* } { **any** | *source-mac-addr source-wildcard* | **host** *source-mac-addr* } { **any** | *destination -ip-addr destination -wildcard* | **host** *destination -ip-addr* } { **any** | *destination -mac-addr destination -wildcard* | **host** *destination -mac-addr* }	Optional By default, the permit rule of ACL is not configured.

Step	Command	Description
Configure the refuse rule of ACL	[*sequence*] **deny** *protocol* { **any** | *source-ip-addr source-wildcard* | **host** *source-ip-addr* } { **any** | *source-mac-addr source-wildcard* | **host** *source-mac-addr* } { **any** | *destination -ip-addr destination -wildcard* | **host** *destination -ip-addr* } { **any** | *destination -mac-addr destination -wildcard* | **host** *destination -mac-addr* }	Optional By default, the refuse rule of ACL is not configured.
Configure the ACL remarks	[*sequence*] **remark** *comment*	Optional By default, the remarks of ACL are not configured.

Note:

- When using the **hybrid access-list advanced** command to create the Hybrid advanced ACL, the ACL can be created only after configuring the rules in the Hybrid advanced ACL configuration mode.
- Sequence means the order number of the rule in the ACL. ACL matches and filters the packet strictly according to the order from small sequence to large sequence. The rule with the small sequence first takes effect. When all rules do not match, execute the default drop action, that is, all the packets not permitted to pass are dropped.

Configure Hybrid Advanced ACL Named by Numbers

The Hybrid advanced ACL named by numbers can let the user identify the type of the ACL quickly. However, the Hybrid advanced ACL named by numbers has some limitations. For example, the ACL quantity is limited, it is cumbersome for the user to identify ACL rules.

Table 10-18 Configure the Hybrid advanced ACL named by numbers

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the Hybrid advanced ACL named by numbers	**access-list** *access-list-number* { **permit** | **deny** } *protocol* { **any** | *source-ip-addr source-wildcard* | **host** *source-ip-addr* } { **any** | *source-mac-addr source-wildcard* | **host** *source-mac-addr* } { **any** | *destination -ip-addr destination -wildcard* | **host** *destination -ip-addr* } { **any** | *destination -mac-addr destination -wildcard* | **host** *destination -mac-addr* } [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**cos** *cos*] [**vlan-id** *vlan*] [**time-range** *time-range-name*]	Mandatory By default, the Hybrid advanced ACL named by numbers is not configured. The sequence range of the Hybrid extended ACL is 9001-9100.
Configure the remarks of the Hybrid advanced ACL named by numbers	**access-list** *access-list-number* **remark** *comment*	Optional By default, the remarks of the Hybrid advanced ACL named by numbers are not configured.

Note:

- If the ACL with the specified sequence does not exist, create one new ACL and add new rules. If the ACL with the specified number exists, just add new rules.

10.2.10. Configure ACL Conflict Detection

Configuration Conditions

Before configuring the ACL conflict detection function, first complete the following task:

- Configure ACL

Configure ACL Conflict Detection

Table 10-8 Configure ACL conflict detection

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable/disable the ACL conflict detection	**access-list rule-collision-detect** { **enable** | **disable** }	Mandatory By default, the ACL conflict detection function is enabled.

10.2.11. Configure ACL Rule Quantity Limitation

Configuration Condition

Before configuring the time domain function, first complete the following task:

- Configure ACL

Configure ACL Rule Quantity Limitation

After enabling the ACL rule quantity limitation, the maximum number of the rules that can be configured in one ACL is 1024.

Table 10-20 Configure the ACL rule quantity limitation

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Disable/enable the ACL rule quantity limitation	**access-list rule-limit** { **enable** | **disable** }	Mandatory By default, it is enabled, that is, the maximum number of the rules that can be configured in one ACL is 1024.

10.2.12. Configure Reflexive ACL

To ensure the network security, we can configure the reflexive ACL function to filter the IP packets based on the session. Only the response packets of the request packets initiated by the internal network can enter the internal network, while the request packets initiated by the external network cannot enter the internal network.

Configuration Condition

None

Define Reflexive ACL

Add the reflect option in the IP extended ACL rule to define the reflexive ACL.

Table 10-9 Define the reflexive ACL

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the IP extended ACL configuration mode	**ip access-list extended** { *access-list-number* | *access-list-name* }	Mandatory Enter the IP extended ACL configuration mode
Configure the ACL rule to define the reflexive ACL	[*sequence*] **permit** *protocol* { **any** | *source-addr source-wildcard* | **host** *source-addr* } [*operator source-port*] { **any** | *destination-addr destination-wildcard* | **host** *destination-addr* } [*operator destination-port*] [*icmp-type*] [*icmp-code*] [*igmp-type*] [**ack** / **fin** / **established** / **psh** / **rst** / **syn** / **urg**] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**ttl** *ttl-value*] [**log**] [**time-range** *time-range-name*] [**reflect** *reflect-list-name* [**timeout** *reflect-timeout-value*]]	Mandatory By default, do not define any reflexive ACL. The rule should carry the reflect option.

Configure Referencing Reflexive ACL

In the IP extended ACL rule, reference the reflexive ACL via the evaluate command.

Table 10-10 Configure referencing the reflexive ACL

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the IP extended ACL configuration mode	**ip access-list extended** { *access-list-number* | *access-list-name* }	Mandatory Enter the IP extended ACL configuration mode
Configure referencing the reflexive ACL	[*sequence*] **evaluate** *reflect-list-name*	Mandatory By default, do not reference the reflexive ACL.

Configure Global Age Time of Reflexive Rule

The generated reflexive ACL rule can be aged within the set time by configuring the global age time of the reflexive rule.

Table 10-11 Configure the global age time of the reflexive rule

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the global age time of the reflexive rule	**ip reflexive-list timeout** *live-time*	Mandatory By default, the global age time of the reflexive rule is 300s. The value range of the age time of the reflexive rule is 5-2147483647 and the unit is second.

Note:

- If the global age time of the reflexive rule and the age time of the single reflexive rule are configured at the same time, the age time of the single reflexive rule has higher priority.

10.2.13. Configure ACL Logs

In the configuration of the IP ACL, add the log option in the rule to record the log for the matching packets.

Configuration Condition

None

Configure ACL Logs

The contents of the log record includes the IP ACL name, the packet passed or dropped, IP protocol type, source/destination IP address, source/destination port number, and the number of the packets in the log recording period.

Table 10-12 Configure the ACL logs

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the IP ACL configuration mode	**ip access-list** { **extended | standard** } { *access-list-number* | *access-list-name* }	Mandatory Enter the IP ACL configuration mode
Configure the ACL logs	[*sequence*] { **permit** | **deny** } *protocol* { **any** | *source-addr source-wildcard* | **host** *source-addr* } [*operator source-port*] { **any** | *destination-addr destination-wildcard* | **host** *destination-addr* } [*operator destination-port*] [*icmp-type*] [*icmp-code*] [*igmp-type*] [**ack / established** / **fin** / **psh** / **rst** / **syn** / **urg**] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**ttl** *ttl-value*] [**log**] [**time-range** *time-range-name*] [**reflect** *reflect-list-name* [**timeout** *timeout-value*]]	Mandatory By default, do not configure the ACL logs. The former command is the configuration of the IP extended ACL rule; the latter is the configuration of the IP standard ACL rule. The rule should carry the **log** option.
	[*sequence*] { **permit** | **deny** } { **any** | *source-addr source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*]	

Configure ACL Log Level

The ACL log level decides to which terminal the ACL log is output and is affected by the whole system log setting.

Table 10-13 Configure the ACL log level

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the ACL log level	**access-list logging-level** *{* ***logging-level-value*** | ***console-only*** | ***file-only*** | ***trap-only*** *}*	Mandatory By default, the ACL log level is 6. The value range of the ACL log level: 1-7: The basic log level; for the log level, refer to “System Log Configuration Manual”. **console-only**: Specify the ACL log to be output to the console port; and the log level is set as 10. **file-only**: Specify the ACL log to be output to the flash file; the log level is set as 9. **trap-only**: Specify the ACL log to be output to the log server. The log level is set as 11.

Configure the Printing Interval of the ACL Log

The command is used to set the interval of printing the switch ACL log.

Table 10-14 Configure the interval of printing the ACL log

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the interval of printing the ACL log	**acl log interval** *minutes*	minutes: log the minutes of the printing interval (1-1040); the default value is 10 minutes.

The interval of printing the current route ACL log is the fixed 60s.

10.2.14. Configure ACL Compiling

Usually, the ACL packet matches the rules one by one until finding one matching rule. With the increasing complexity of the network application environment, the configured rules in the ACL are becoming more. ACL adopts the mode of matching by order and lots of rules increase the

delay of the packet forwarding. As a result, the forwarding performance of the device is reduced. ACL compiling solves the problem, speeding up the matching speed of the ACL packet and improving the ACL performance.

Configuration Condition

Before configuring the ACL compiling function, first complete the following task:

- Configure ACL.

Configure ACL Compiling

After configuring the ACL compiling, the matching time of the packet is fixed. No matter which rule in the ACL the packet matches with, the processing cost keeps constant. Therefore, when there are lots of ACL rules, compiling ACL can ensure the correct transmission time and small delay and jitter, maintaining the network stability.

Table 10-15 Configure the ACL compiling

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the ACL compiling	**access-list compile** [*access-list-number* | *access-list-name*] [part]	Mandatory By default, do not enable the ACL complete or fragment compiling for any IP ACL. The number range of IP ACL is 1-2000.

Note:

- The ACL compiling function only takes effect for the IP ACL. The part compiling is just applicable to the IP extended ACL. When there are many complicated ACE items, it is suggested to use the part compiling, and the compiling time is less than the complete compiling.
- The ACL complete compiling function compiles all ACEs in the ACL, and generates one compiling result. The ACL part compiling function compiles every 500 ACEs in the ACL and generates one compiling result. If there are no 500 ACEs, also compile once and generate one compiling result, and you can compile for eight times at most (There can be 4000 ACEs in one IP extended ACL at most).
- Compiling ACL needs several seconds to several minutes according to the ACL complexity and rule quantity. Compiling ACL needs large memory space. For the device whose memory is smaller than 128M, it is suggested not to use to the ACL compiling function.
- Considering the features of compiling ACL and system memory, it is suggested to enable the ACL compiling only for the ACL with more than 25 rules; for the ACL with less than 25 rules, do not need to enable the ACL compiling.

- We can use the ACL compiling function only for IP ACL. Usually, it is suggested to enable the ACL compiling for the specified IP ACL. It is not suggested to use the compiling command for all IP ACLs.
- If the IP ACL rules contain the following cases, the compiling cannot succeed:
- The wildcard mask of the source/destination IP address in the rule and the wildcard mask of the source/destination port are the irregular mask (that is, 1 in the mask are not successive).
- The rules contain the reference for the reflexive list.
- If the rule does not contain any one element of seven elements (source-addr, destination-addr, source-port, destination-port, protocol, fragments, tcp-flag), it cannot be compiled.
- The rule is bound with the time domain and the time domain status is Inactive.
- If the rule contains the remark rule, it also cannot be compiled.

Configure Forbidding ACL Compiling

If the global ACL compiling is enabled and when configuring new IP ACL, perform the compiling automatically. We can configure forbidding the ACL compiling for one ACL, avoiding the compiling for the IP ACL.

Table 10-16 Configure forbidding ACL compiling

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure forbidding ACL compiling	**access-list forbid-compile** { *access-list-number* | *access-list-name* }	Mandatory By default, do not forbid the ACL compiling for any IP ACL. The number range of IP ACL is 1-2000.

Note:

- Forbidding the ACL compiling function takes effect only for IP ACL.

Configure Percentage of System Memory Occupied by ACL Compiling

By default, the memory space occupied by compiling ACL cannot exceed 15% of the system memory. The percentage can be adjusted by the command. The memory percentage is one limitation, but not guarantee, that is, the memory occupied by compiling ACL cannot exceed 15% of the system memory, but if the memory occupied by the other modules and the reserved memory of the system already occupy more than 85% of the system memory, compiling ACL cannot get 15%.

Table 10-17 Configure the percentage of the system memory occupied by the ACL compiling

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the percentage of the system memory occupied by the ACL compiling	**access-list compile-memory limit-percent** *limit-percent-value*	Mandatory By default, the ACL compiling is permitted to occupy 15% of the system memory. The value range of the memory percentage occupied by the ACL compiling is 1-100.

10.2.15. Configure Time Domain

The time domain is the set of the time segments. One time domain can contain zero to multiple time segments. The time range of the time domain is the union of the time segments. The time domain can be bound with ACL or ACL rule, as the condition of whether ACL or ACL rule takes effect.

Configuration Condition

Before configuring the time domain function, first complete the following task:

- Configure ACL

Configure Time Domain

Configure whether the application object of the time domain is limited by the time domain. When it is enabled, the application object is limited by the time domain. On the contrary, it is not limited by the time domain.

Table 10-30 Configure the time domain

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure disabling/enabling the time domain	**set time-range** { **disable** | **enable** }	Mandatory By default, it is enabled.

Configure Periodical Time Segment

Periodical time segment: Periodical time segment means to select one day or several days from Monday to Sunday, and the start time point to the end time point as the time segment, taking effect every week repeatedly.

Table 10-31 Configure the periodical time segment

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the time domain	**time-range** *time-range-name*	Mandatory By default, do not configure the time domain.
Configure the periodical time segment	[sequence] **periodic** [{ *day-of-the-week* / *hh*:*mm* [:*ss*] } [**to** { *day-of-the-week* / *hh*:*mm* [:*ss*] }]]	Either By default, do not configure periodical time segment. The former command can specify the time range as one day (such as Monday) or several days (such as Monday,Friday). The latter command can specify the time range as every day, weekend, or workday.
	[*sequence*] **periodic** [[**weekdays** | **weekend** | **daily**] [*hh*:*mm* [:ss]] **to** [*hh*:*mm* [:ss]]]	

Note:

- If only inputting **periodic**, it indicates 00:00 to 23:59 from Monday to Friday.

Configure Absolute Time Segment

The absolute time segment means to take effect within the specified date and time range.

Table 10-32 Configure the absolute time segment

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the time domain	**time-range** *time-range-name*	Mandatory By default, do not configure the time domain.
Configure the absolute time segment of the time domain	[*sequence*] **absolute start** *hh*: *mm* [: *ss*] [*day* [*month* [*year*]]] **end** *hh*: *mm* [: *ss*] [*day* [*month* [*year*]]]	Mandatory By default, do not configure the absolute time segment of the time domain.

Configure Refresh Period

The status of time domain includes effective and ineffective. The status refresh period of the time domain is 1 minute by default. Automatically refresh according to the current system time. Therefore, when refreshing the status, there may be 0-60s delay compared with the system time.

Table 10-33 Configure the refresh period

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the refresh period of the time domain	**set time-range frequency** *frequency-number*	Mandatory The default value is 1. The refresh period is the interval between two refreshes and the unit is minute.

Configure Maximum Time Offset

The maximum offset means the maximum offset between accumulation time of the counter and the system time. Once the time statistics exceeds the offset, re-judge the status of the time domain and update during the next refreshing so that the time statistics is more correct.

Table 10-34 Configure the maximum time offset

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the maximum time offset of the time domain	**set time-range max-offset** *max-offset-number*	Mandatory The default value is 100. The unit of the time offset is second and the value range is 1-300.

Configure Time Domain and ACL Rule

When it is necessary to control one user to access the network resources within the specified time segment, we can set the ACL rule based on the time domain to filter the packets. Whether the time domain takes effect directly affects the associated ACL rule.

Table 10-35 Configure the time domain to be bound with the ACL rule

Step	Command	Description
Configure the binding with IP standard ACL rule	Refer to “Configure IP Standard ACL”	-
Configure the binding with IP extended ACL rule	Refer to “Configure IP Extended ACL”	-
Configure the binding with MAC standard ACL rule	Refer to “Configure MAC Standard ACL”	-
Configure the binding with MAC extended ACL rule	Refer to “Configure MAC Extended ACL”	-

Note:

- When the time domain bound with the ACL rule does not exist, the ACL rule is in the effective state.

Configure Time Domain and ACL Binding

When it is necessary to control one user to access the network resources within the specified time segment, we can set the ACL rule based on the time domain to filter the packets. Whether the time domain takes effect directly affects the rules contained in the whole ACL.

Table 10-36 Configure the time domain and ACL binding

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the time domain to be bound with IP ACL	**ip time-range** *time-range-name* **access-list** { *access-list-number* | *access-list-name* }	Mandatory By default, do not configure the time domain to be bound with IP ACL.
Configure the time domain to be bound with MAC ACL	**mac time-range** *time-range-name* **access-list** { *access-list-number* | *access-list-name* }	Mandatory By default, do not configure the time domain to be bound with MAC ACL.

Note:

- When the time domain bound with the ACL rule does not exist, the ACL rule is in the effective state.

10.2.16. Configure ACL to Support Connection Tracking Acceleration

By default, ACL supports flow table acceleration. You can switch to support connection tracking acceleration through the command. This function is effective for the ACL fast forwarding full path bound to the interface or other service reference ACL. It is a global command. When this function is enabled, all ACLs bound to the interfaces under the full path or ACLs referenced by other services will be switched from flow table acceleration to connection tracking acceleration. Support IP standard ACL, IP extended ACL, and IPv6 extended ACL.

Configuration Conditions

None

Configure ACL to Support Connection Tracking

Table 10-36 Configure ACL to support connection tracking

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable/disable ACL to support connection tracking	**[no] access-list accelerate mode connection**	Mandatory By default, it is disabled.

Note:

- This function does not take effect when the load balancing policy between CPU cores is per-packet.
- When the ACL rules have the following matching fields (TOS, precedence, DSCP, flow label, etc.), the packet matching is not accelerated by connection tracking, but matched one by one by ACL rules or ACL compiling.
- When the packet is not the first fragment and the packet descriptor does not carry L4 information and ICMP, it is matched one by one by ACL rules or matched by ACL compiling.

10.2.17. Configure ACL Application

IP ACL can be applied to the ingress and egress directions of the L3 interface; MAC ACL can be applied to the ingress and egress directions of the L3 interface; Ethernet protocol ACL can only be applied by the bridge module. For details, refer to “Bridge Configuration Manual”.

If ACL is applied to the ingress direction of the L3 interface, filter the packets (containing multicast and broadcast packets) at the ingress direction of the L3 interface whose destination is the local device and the L3 forwarded packets, no influence for the L2 forwarded packets. If ACL is applied to the egress direction of the L3 interface, filter the packets at the egress direction of the L3 interface starting from the local device and the L3 forwarded packets, no influence for the L2 forwarded packets. If the applied ACL does not exist, all packets are permitted.

Configuration Condition

Before configuring the ACL application function, first complete the following task:

- Configure ACL

Configure IP ACL to Be Applied to Interface

If IP ACL is applied to the ingress direction of the L3 interface, it will analyze and process the packets (containing multicast and broadcast packets) at the ingress direction of the L3 interface whose destination is the local device, no influence for the L2 forwarded packets. If IP ACL is applied to the egress direction of the L3 interface, it will analyze and process the packets at the egress direction of the L3 interface starting from the local device and the L3 forwarded packets, no influence for the L2 forwarded packets.

Table 10-37 Configure IP ACL to be applied to the interface

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

Step	Command	Description
Configure IP ACL to be applied to the L3 Ethernet interface	**ip access-group** { *access-list-number* | *access-list-name* } { **in** | **self** }	Mandatory By default, IP ACL is not applied to the L3 Ethernet interface.

Configure MAC ACL to Be Applied to Interface

If MAC ACL is applied to the ingress direction of the L3 interface, it will analyze and process the packets (containing multicast and broadcast packets) at the ingress direction of the L3 interface whose destination is the local device, no influence for the L2 forwarded packets. If MAC ACL is applied to the egress direction of the L3 interface, it will analyze and process the packets at the egress direction of the L3 interface starting from the local device and the L3 forwarded packets, no influence for the L2 forwarded packets.

Table 10-38 Configure MAC ACL to be applied to the interface

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure MAC ACL to be applied to the L3 interface	**mac access-group** { *access-list-number* | *access-list-name* } { **in** }	Mandatory By default, MAC ACL is not applied to the L3 interface.

Configure Ethernet Protocol ACL to Be Applied to Bridge Group

If the Ethernet protocol ACL is applied to the ingress direction of the L3 Ethernet interface of the bridge group, it will analyze and process all packets at the ingress direction of the interface. If the Ethernet protocol ACL is applied to the egress direction of the L3 interface of the bridge group, it will analyze and process the forwarded packets at the egress direction of the interface.

Table 10-18 Configure the Ethernet protocol ACL to be applied to the bridge group

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

Step	Command	Description
Enter the interface configuration mode	**interface** *interface-name*	-
Add the L3 interface to the bridge group	**bridge-group** *group-number*	Mandatory By default, L3 interface is not added to any bridge group.
Configure applying Ethernet protocol ACL to the L3 interface added to the bridge group	**bridge-group** *group-number* { **input-type-list** | **output-type-list** } *access-list-number*	Mandatory By default, the bridge interface is not configured with any Ethernet protocol ACL.

10.2.18. ACL Monitoring and Maintaining

Table 10-40 ACL Monitoring and Maintaining

Command	Description
show access-list compile-memory	Display the information about the memory occupied by the ACL compiling
show access-list [*access-list-number* | *access-list-name*]	Display the ACL configuration information
show access-list-reflexive	Display the current reflexive ACL rules
show access-lists { **interface** [[*interface-type*] / [**in** | **out | self**]] }	Display the ACL application information and the details of the ACL rules
show acl-log-count	Display the current generated ACL log quantity
show ip access-list [*access-list-number* | *access-list-name*]	Display the configuration information of IP ACL
show ip interface list	Display the information of the IP ACL applied to the interface

Command	Description
show mac access-list [*access-list-number* | *access-list-name*]	Configure the MAC ACL configuration information
show mac interface list	Display the information of the MAC ACL applied to the interface
show protocol access-list	Display the configuration information of Ethernet protocol ACL
show time-range [*time-range-name*]	Display the configuration and status information of the time domain
show access-list connection *[ipv4 | ipv6]* **table**	Display the connection tracking information

10.3. ACL Typical Configuration Example

10.3.1. Configure IP Standard ACL

Network Requirements

- The IP address of PC1 is 131.44.1.1/16; the IP address of PC2 is 131.44.2.1/16; the IP address of PC3 is 131.44.2.2/16;
- Configure the ACL rule on Device, permitting PC1 to access IP Network;
- Configure the ACL rule on Device, preventing the PCs of the segment 131.44.2.0/24 from accessing IP Network.

Network Topology

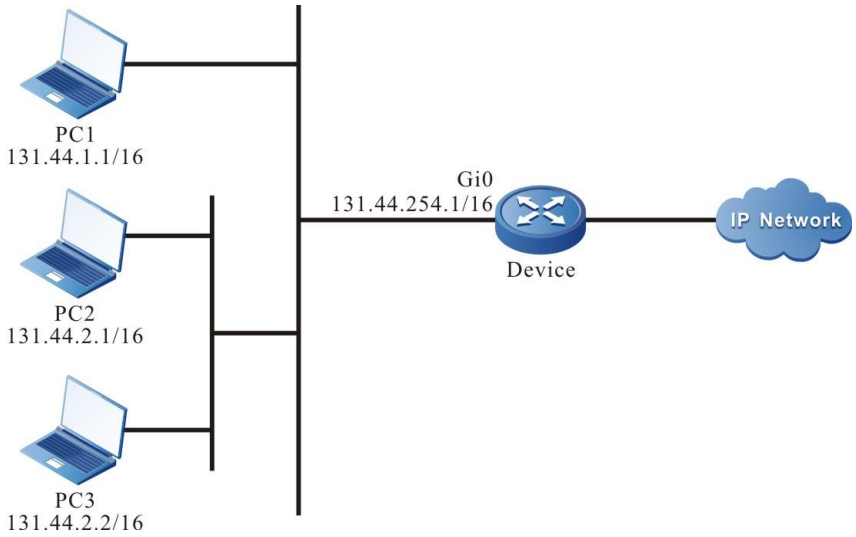


Figure 10–1 Networking of configuring IP standard ACL

Configuration Steps

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

Step 2: Configure ACL 1.

#Configure ACL 1 on Device.

```
Device#configure terminal
Device(config)#ip access-list  standard 1
```

#Configure the rule, permitting PC1 to access IP Network.

```
Device(config-std-nacl)#permit host 131.44.1.1
```

#Configure the rule, preventing the network segment 131.44.2.0/24 from accessing IP Network.

```
Device(config-std-nacl)#deny 131.44.2.0 0.0.0.255
Device(config-std-nacl)#exit
```

#View the information of the ACL 1 on Device.

```
Device#show ip access-list 1
ip access-list standard 1
 10 permit host 131.44.1.1
 20 deny 131.44.2.0 0.0.0.255
```

Step 3: Apply the configured ACL1 to the ingress direction of the interface gigabitethernet0.

#Configure Device.

```
Device(config)#interface gigabitethernet0
Device(config-if-gigabitethernet0)ip access-group 1 in
Device(config-if-gigabitethernet0)exit
```

#View the information of the ACL applied to the interface on Device.

```
Device#show access-lists interface gigabitethernet 0
-----------Interface-----Bind-----Instance--------------
Interface----------------Direction----AclType----AclName
gigabitethernet0        IN          IP        1
detail:
ip access-list standard 1
 10 permit host 131.44.1.1
 20 deny 131.44.2.0 0.0.0.255
```

Step 4: Check the result.

#PC1 can access IP Network; PC and PC3 cannot access IP Network.

10.3.2. Configure IP Extended ACL with Time Domain

Network Requirements

- The IP address of PC1 is 131.44.1.1/16; the IP address of PC2 is 131.44.1.2/16; the IP address of PC3 is 131.44.2.1/16;
- Configure the ACL rule on Device, permitting PC2 to access IP Network via FTP;
- Configure the ACL rule on Device, permitting PC1 to access IP Network in the specified time range;
- Configure the ACL rule on Device, preventing the PC of the segment 131.44.2.0/24 from accessing IP Network.

Network Topology

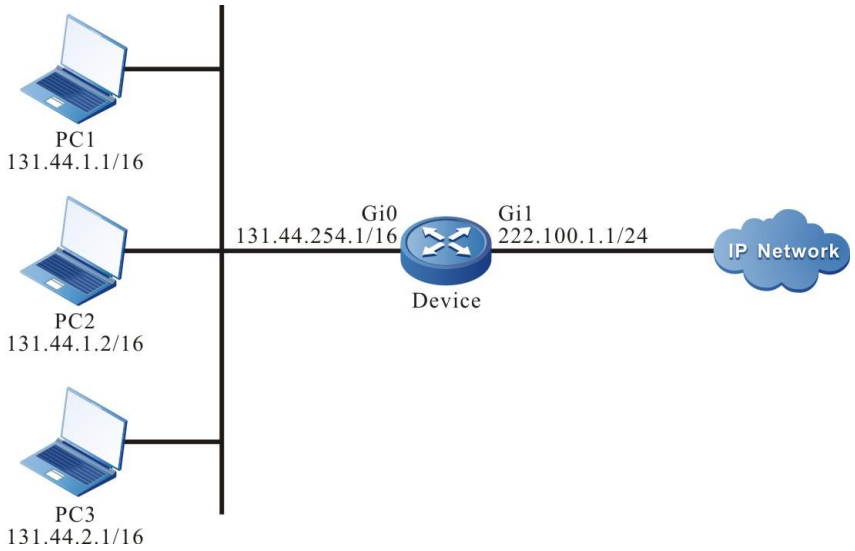


Figure 10-2 Networking of configuring IP extended ACL with time domain

Configuration Steps

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

Step 2: Configure the time domain time-range-work and the range of the time domain is 8:00 to 18:00 every day.

#Configure Device.

```
Device#configure terminal
Device(config)#time-range time-range-work
Device(config-time-range)#periodic daily 08:00 to 18:00
Device(config-time-range)#exit
```

#View the current system time on Device.

```
Device#show clock
UTC WED NOV 07 11:15:45 2012
```

#View the information of the defined time domain “time-range-work” on Device.

```
Device#show time-range time-range-work
Timerange name:time-range-work  (STATE:active)
```

```
10  periodic daily 08:00 to 18:00 (active)
```

Step 3: Configure the ACL 1001.

#Configure the ACL 1001 on Device.

```
Device(config)#ip access-list extended 1001
```

#Configure the rule, preventing the network segment 131.44.2.0/24 from accessing IP Network.

```
Device(config-ext-nacl)#deny ip 131.44.2.0 0.0.0.255 any
```

#Configure the rule, permitting PC2 to access IP Network via the FTP.

```
Device(config-ext-nacl)#permit tcp host 131.44.1.2 any eq ftp
Device(config-ext-nacl)#permit tcp host 131.44.1.2 any eq ftp-data
```

#Configure the rule, permitting PC1 to access IP Network in the defined time domain “time-range-work” range.

```
Device(config-ext-nacl)#permit ip host 131.44.1.1 any time-range time-range-work
Device(config-ext-nacl)#exit
```

#View the information of the ACL 1001 on Device.

```
Device#show ip access-list 1001
ip access-list extended 1001
 10 deny ip 131.44.2.0 0.0.0.255 any     0 matches
 20 permit tcp host 131.44.1.2 any eq ftp     0 matches
 30 permit tcp host 131.44.1.2 any eq ftp-data     0 matches
 40 permit ip host 131.44.1.1 any time-range time-range-work (active)     0 matches
```

Step 4: Apply the configured ACL 1001 to the egress direction of the interface gigabitethernet1.

#Configure Device.

```
Device(config)#interface gigabitethernet 1
Device(config-if-gigabitethernet1)#ip access-group 1001  out
```

#View the information of the ACL applied to the interface on Device.

```
Device#show access-lists interface gigabitethernet 1
-----------Interface-----Bind-----Instance--------------
Interface----------------Direction----AclType----AclName
gigabitethernet1        OUT        IP        1001
detail:
ip access-list extended 1001
 10 deny ip 131.44.2.0 0.0.0.255 any
 20 permit tcp host 131.44.1.2 any eq ftp
```

```
30 permit tcp host 131.44.1.2 any eq ftp-data
40 permit ip host 131.44.1.1 any time-range time-range-work (active)
```

Step 6: Check the result.

#PC1 can access IP Network from 08:00 to 18:00 of every day; PC2 can access IP Network via FTP; PC3 cannot access IP Network.

10.3.3. Configure IPv6 ACL

Network Requirements

- The IPv6 address of PC1 is 1000:100::1/32; the IPv6 address of PC2 is 1000:100::2/32; the IPv6 address of PC3 is 1000:100:1::3/32;
- Configure the ACL rule on Device, permitting PC1 to access Internet in the specified time range;
- Configure the ACL rule on Device, permitting PC2 to access Internet via TFTP;
- Configure the ACL rule on Device, preventing the PC of the segment 1000:100:1::/48 from accessing Internet.

Network Topology

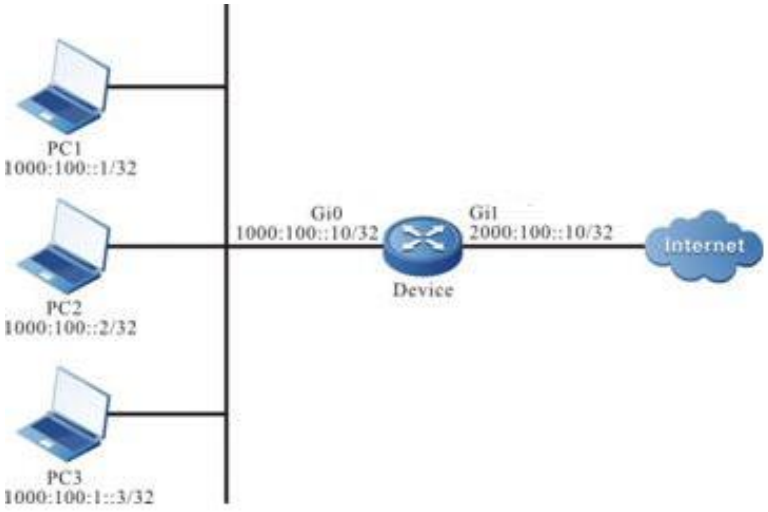


Figure 10-3 Networking of configuring IPv6 ACL

Configuration Steps

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

Step 2: Configure the time domain time-range-work and the range of the time domain is 8:00 to 18:00 every day.

#Configure Device.

```
Device#configure terminal
Device(config)#time-range time-range-work
Device(config-time-range)#periodic daily 8:00 to 18:00
```

```
Device(config-time-range)#exit
```

#On Device, view the information of the defined time domain time-range-work.

```
Device#show time-range time-range-work

Timerange name:time-range-work  (STATE:active)
 10  periodic daily 08:00 to 18:00 (active)
```

Step 3: Configure the IPv6 ACL 7001.

#On Device, configure IPv6 ACL 7001.

```
Device(config)#ipv6 access-list extended 7001
```

#Configure the rule, permitting PC1 to access Internet in the defined time domain time-range-work.

```
Device(config-v6-list)#permit ipv6 host 1000:100::1 any time-range time-range-work
```

#Configure the rule, permitting PC2 to access Internet via TFTP.

```
Device(config-v6-list)#permit udp host 1000:100::2 any eq tftp
```

#Configure the rule, preventing the segment 1000:100:1::/48 from accessing Internet.

```
Device(config-v6-list)#deny ipv6 1000:100:1::/48 any
Device(config-v6-list)#exit
```

#On Device, view the information of IPv6 ACL rule 7001.

```
Device#show ipv6 access-list 7001
ipv6 access-list extended 7001
 10 permit ipv6 host 1000:100::1 any time-range time-range-work (active)    0 matches
 20 permit udp host 1000:100::2 any eq tftp     0 matches
 30 deny ipv6 1000:100:1::/48 any     0 matches
```

Step 4: Configure IPv6 ACL 7001 to be applied to the ingress direction of the interface.

#Configure Device.

```
Device(config)#interface gigabitethernet 0
Device(config-if-gigabitethernet0)#ipv6 access-group 7001  in
Device(config-if-gigabitethernet0)#exit
```

#On Device, view the information of IPv6 ACL applied to the interface.

```
Device#show access-group bind interface
 Filter resource bind interface information
 ifName                    fwDirect bindType listName
 ********************************************************************************
```

```
gigabitethernet0            IN      IPV6    7001
*********************************************************************************
```

Step 5: Check the result.

#PC1 can access Internet from 08:00 to 18:00 of every day; PC2 can access Internet via TFTP; PC3 cannot access IP Network.

10.3.4. Configure Hardware Attack Detection Function

Configuration Condition

None

Configure Intercepting Packet with Same Source and Destination MAC

When the switching port of the device receives the packet with the same source and destination MAC, drop the packet.

Table 10-41 Configure intercepting the packet with the same source and destination MAC

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the packet with the same source and destination MAC	**ip mac intercept bad**	Mandatory By default, do not configure the function of intercepting the packet with the same source and destination MAC

Configure Intercepting Packet with Same Source and Destination IP

When the switching port of the device receives the packet with the same source and destination IP, drop the packet.

Table 10-42 Configure intercepting the packet with the same source and destination IP

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

Step	Command	Description
Configure intercepting the packet with the same source and destination IP	**ip intercept ipeq**	Mandatory By default, do not configure the function of intercepting the IP packet with the same source and destination IP.

Configure Intercepting TCP Packet with Same Source and Destination Port

When the switching port of the device receives the TCP packet with the same source and destination port, drop the packet.

Table 10-43 Configure intercepting the TCP packet with the same source and destination port

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the TCP packet with the same source and destination port	**ip tcp intercept porteq**	Mandatory By default, do not configure the function of intercepting the TCP packet with the same source and destination port.

Configure Intercepting UDP Packet with Same Source and Destination Port

When the switching port of the device receives the UDP packet with the same source and destination port, drop the packet.

Table 10-44 Configure intercepting the UDP packet with the same source and destination port

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

Step	Command	Description
Configure intercepting the UDP packet with the same source and destination port	**ip udp intercept porteq**	Mandatory By default, do not configure the function of intercepting the UDP packet with the same source and destination port.

Configure Intercepting Invalid TCP Packet

When the switching port of the device receives the invalid TCP packet, drop the packet.

The packet with any one of the following features is regarded as the invalid TCP packet. The features are as follows:

1. The TCP head length of the first fragmented packet is smaller than the configured value;
2. The flags and sequence number fields in the TCP head are both equal to 0;
3. The SYN and FIN in the flags field of the TCP head are set at the same time;
4. FIN, URG, and PSH in the flags field of the TCP head are set at the same time and the sequence number field is equal to 0;
5. The TCP fragment packet with the offset 1.

Table 10-45 Configure intercepting the invalid TCP packet

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the invalid TCP packet	**ip tcp intercept bad** [*length*]	Mandatory By default, do not configure the function of intercepting the invalid TCP packet.

Configure Intercepting Invalid ICMP Packet

When the switching port of the device receives the invalid ICMP packet, drop the packet.

The packet with any one of the following features is regarded as the invalid ICMP packet. The features are as follows:

1. The fragmented ICMP packet
2. ICMP ping packet, and the length exceeds the configured value.

Table 10-46 Configure intercepting the invalid ICMP packet

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the invalid ICMP packet	**ip icmp intercept bad** [**length** *value*]	Mandatory By default, do not configure the function of intercepting the invalid ICMP packet.

Configure TCP SYN Packet with Source Port Smaller than 1024

When the switching port of the device receives the TCP SYN packet with the source port is smaller than 1024, drop the packet.

Table 10-47 Configure intercepting the TCP SYN packet with the source port smaller than 1024

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the TCP SYN packet with the source port smaller than 1024	**ip tcp intercept sport-limit**	Mandatory By default, do not configure the function of intercepting the TCP SYN packet with the source port smaller than 1024.

10.3.5. Configure MAC Extended ACL

Network Requirements

- PC1, PC2, and IP Phone are connected to IP Network via Device.
- Configure the MAC extended ACL rule on Device2, realizing that the user of VLAN2 cannot access IP Network, and except for the voice users, the other users of VLAN3 all can access IP Network.

Network Topology

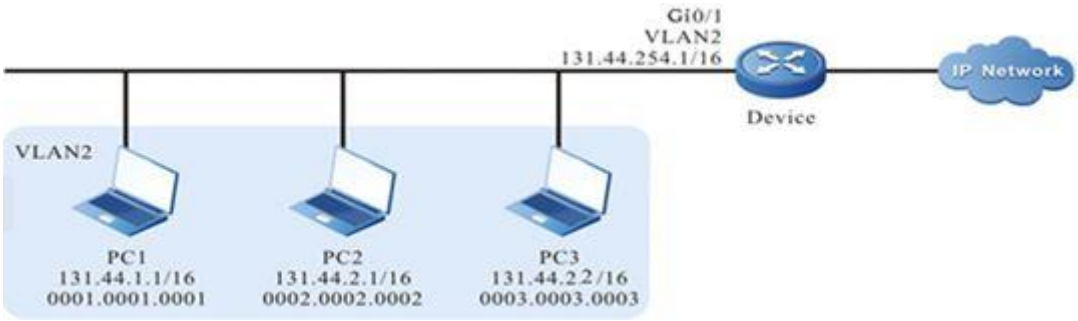


Figure 10–4 Networking of configuring the MAC extended ACL

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device2.

#Create VLAN2-3.

```
Device2#configure terminal
Device2(config)#vlan 2-3
```

#Configure the link type of port gigabitethernet0/1 as Hybrid, permitting the services of VLAN2-3 to pass.

```
Device2(config)#interface gigabitethernet0/1
Device2(config-if-gigabitethernet0/1)#switchport mode hybrid
Device2(config-if-gigabitethernet0/1)#switchport hybrid tagged vlan 2-3
Device2(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the corresponding VLAN interface and IP address on Device1 and Device2. (Omitted)

Step 3: Configure Voice-VLAN to set the COS value of the packet from IP Phone as 7 on Device1. (Omitted)

Step 4: Configure the MAC extended ACL.

#Configure the MAC extended ACL with serial number 3001 on Device2.

```
Device2(config)#mac access-list extended 3001
```

#Configure the rule, preventing the users in VLAN2 from accessing IP Network.

```
Devic2(config-ext-mac-nacl)#deny any any vlan-id 2
```

#Configure the rule, preventing the voice users in VLAN3 from accessing IP Network.

```
Device2(config-ext-mac-nacl)#deny any any cos 7 vlan-id 3
```

#Configure the rule, permitting the other users in VLAN3 to access IP Network.

```
Device2(config-ext-mac-nacl)#permit any any vlan-id 3
```

#View the information of the ACL with serial number 3001 on Device2.

```
Device2#show access-list 3001
```

```
mac access-list extended 3001
 10 deny any any vlan-id 2
 20 deny any any cos 7 vlan-id 3
 30 permit any any vlan-id 3
```

Step 5: Configure applying the MAC extended ACL.

#Apply the MAC extended ACL with serial number 3001 to the ingress of the port gigabitethernet0/1 on Device2.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#mac access-group 3001 in
Device2(config-if-gigabitethernet0/1)#exit
```

#View the information of the ACL applied to the port on Device2.

```
Device2#show acl-object interface
-----------Interface-----Bind-----Instance--------------
Interface----------------Direction----AclType----AclName
gi0/1              IN       MAC      3001
```

Step 6: Check the result.

#PC2 can access IP Network; PC1 and IP Phone cannot access IP Network.

Note:

- For the configuration of Voice-VLAN, refer to the Voice-VLAN chapter of the configuration manual.

10.3.6. Configure Hybrid Extended ACL

Network Requirements

- PC1, PC2, and PC3 are connected to IP Network via Device.
- Configure the Hybrid extended ACL rule, realizing that PC1 can access IP Network within the specified time, PC2 and PC3 cannot access IP Network.

Network Topology

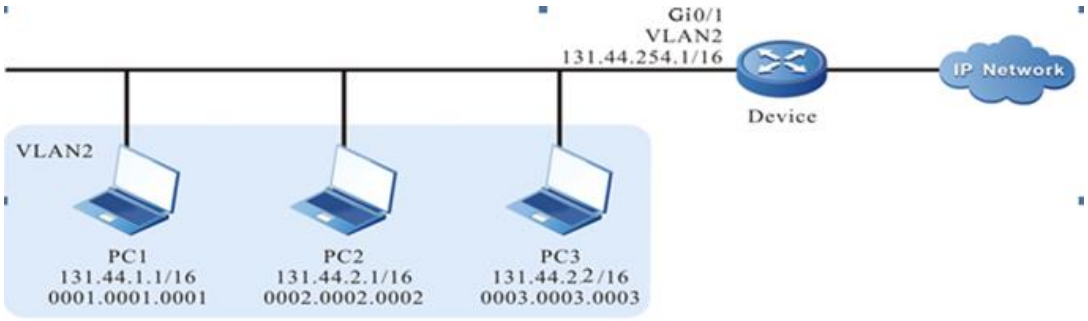


Figure 10-5 Networking of configuring Hybrid extended ACL

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device.

#Create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the corresponding VLAN interface and IP address on Device. (Omitted)

Step 3: Configure the time domain.

#Configure the time domain “time-range-work” on Device and the range is 08:00 to 18:00 every day.

```
Device(config)#time-range time-range-work
Device(config-time-range)#periodic daily 08:00 to 18:00
Device(config-time-range)#exit
```

#View the current system time on Device.

```
Device#show clock

UTC FRI APR 05 15:26:31 2013
```

#View the information of the defined time domain “time-range-work” on Device.

```
Device#show time-range time-range-work
Timerange name:time-range-work  (STATE:active)
  10  periodic daily 08:00 to 18:00 (active)
```

Step 4: Configure the Hybrid extended ACL list.

#Configure the Hybrid extended ACL with serial number 5001 on Device.

```
Device(config)#hybrid access-list extended 5001
```

#Configure the rule, preventing the network segment 131.44.2.0/24 from accessing IP Network.

```
Device(config-hybrid-nacl)#deny ip 131.44.2.0 0.0.0.255 any
```

#Configure the rule, permitting PC1 to access IP Network in the defined time domain “time-range-work” range.

```
Device(config-hybrid-nacl)#permit ip any host 0001.0001.0001 time-range time-range-work
```

#Configure the rule, permitting all packets from IP Network to pass Device.

```
Device(config-hybrid-nacl)#permit ip any any
Device(config-hybrid-nacl)#exit
```

#View the information of the ACL with serial number 5001 on Device.

```
Device#show hybrid access-list 5001
hybrid access-list extended 5001
 10 deny ip 131.44.2.0 0.0.0.255 any
 20 permit ip any host 0001.0001.0001 time-range time-range-work (active)
 30 permit ip any any
```

Step 5: Configure applying Hybrid extended ACL.

#Apply the Hybrid extended ACL with serial number 5001 to the ingress globally.

```
Device(config)#global hybrid access-group 5001 in
```

#View the information of the ACL applied globally on Device.

```
Device#show acl-object global
----------------Global-----Bind-----Instance-----------
Global-------------------Direction----AclType----AclName
global              IN        HYBRID    5001
```

11. SSAC

11.1. Overview

SSAC is the abbreviation of system-class security and access control. Access control refers to the different authorized access of the subject to the object itself or its resources according to some control policies or authorities. Access control is divided into two levels, physical access control and logical access control. There are three main logical access control modes: discretionary access control (DAC), mandatory access control (MAC) and role-based access control (RBAC). SSAC is implemented based on mandatory access control.

11.2. SSAC Function Configuration

Table 11-1 SSAC function configuration list

Configuration Tasks	
Configure te SSAC security mode	Configure SSAC security mode: strict/loose

11.2.1. Configure SSAC Mode

Configuration Conditions

None

Configure SSAC Security Mode

Table 11-2 Configure the security mode

Step	**Command**	**Description**
Enter the global configuration mode	**configure terminal**	-
Configure the security mode	**ssac mode** {*strict* | *loose*}	It can be configured as the strict mode or loose mode.

Step 6: Check the result.

#PC1 can access IP Network from 08:00 to 18:00 every day; PC2 and PC3 cannot access IP Network.

12. DPI

12.1. Overview

DPI is the abbreviation of deep packet inspection. It is a general framework module for string rule matching of packet application layer load, and generates rule matching results for L4-7 service module. Based on DPI depth detection, AVC, URL, CCF and object service functions are provided.

Application identification and visual control AVC are classified according to the application software used for flow. Each application has a unique ID, which is uniformly managed by the DPI process on the control plane. Application is a more advanced and accurate traffic classification method than service. Applications are layered. Currently, the L4 protocol processed by DPI is only TCP/UDP/ICMP, and L5 applications are defined on TCP/UDP. L6 or even L7 applications can continue to be defined on L5 applications. For example, we call ordinary web page access HTTP application (L5), and the traffic generated by using the mobile application "Sina News" will be recognized as the "Sina News mobile client" application (L6) hosted on HTTP. Some streaming media use UDP transmission and can be identified as a streaming media application (L5) hosted on UDP. The top-level application of a session is uniquely determined by the AVC module. This determined top-level application will be recorded in the packet to guide the actions of the AVC module, QoS module, etc. DPI identifies applications in the following ways:

Well known port protocol + optional parser confirmation: for example, port 80 is recognized as HTTP, and then the HTTP parser of DPI will further confirm the packet format. The first load packet after three handshakes must come from the request direction of the session and contain HTTP method. Not all well-known port applications have developed parsers, and those without them are directly identified.

The multi-channel protocol is identified based on the negotiation process, such as FTP, TFTP, sip, etc. First, the DPI confirms the FTP control channel application based on the fixed port (21) + FTP parser, and then the FTP parser continues to analyze the signaling interaction of the FTP control channel until the port/PASV instruction is found, you can know the expected connection (session) of the FTP data channel, and then confirm the FTP data channel application through the arrival of the expected connection packet.

Identification based on the way of defining load features: this definition can be preset by the application feature library or manually configured custom application. Custom application is a flexible supplement to customer site identification means. Refer to another term for explanation: "rules".

Traffic model identification: this identification method has not been developed for the DPI feature of the current version.

Finally, AVC provides users with packet processing actions defined based on applications and application groups, such as drop, reset, logging, etc.

URL classification is not a strict tree structure like application groups, but a classification evaluation. Each classification evaluation has (absolute) different severity grades. The URL module can execute the packet processing action according to the classification. If a session matches different classifications, it will execute the packet action configured by the most severe classification. The URL module has a common additional action: redirect. The URL module only detects HTTP traffic.

The content control and filtering CCF mainly matches the established keywords in the message load, and then performs blocking, erasure, logging and other actions according to the configuration. If a session matches different keywords, the packet actions of the keyword will be

executed one by one. Content filtering can detect UDP, TCP, HTTP, FTP, SMTP/POP3/IMAP4 and other traffic. The current version does not support mail applications

Object service is the classification of traffic based on port. Each service has a unique ID, which is uniformly managed by the DPI process on the control plane. For example, we classify the traffic of TCP destination port 80 as HTTP service, and the traffic of UDP destination port 53 as DNS service. In security policy, policy routing and other modules, services can be referenced to select different policies for different traffic. In particular, for a negotiation protocol (multi-channel protocol), such as FTP, both the traffic of the control channel and the data channel belong to the FTP service. The policy definition based on service traffic is easier to use and more practical than ACL, and its performance is better than AVC (no deep detection of load is required). In routers (rather than firewalls), it is often enough for customers to choose to use services. A flow can be determined by DPI as a predefined service and a custom service.

12.2. DPI Function Configuration

Table 12-1 DPI function configuration list

Configuration Tasks	
Configure the AVC function	Create application or application group
	Enable application
	Configure application popularity
	Configure the platform attributes of the application
	Configure the basic protocol type of the application
	Configure the application direction
	Configure the L4 protocol of the application
	Configure the destination address range of the application
	Configure the port matching range of the application
	Configure the features of the application
	Configure the description of the application

Configuration Tasks	
Configure the AVC function	Configure the combination relation of the application and application group
	Create application policy
	Configure the actions of the application and application group
	Configure the default action of the application policy
	Configure the description information of the application policy
Configure the URL function	Create URL classification
	Create the URL classification policy
	Configure the url classification rules
	Configure the action of the url classification
	Configure the default action of the url classification
	Configure the description information of the url classification
Configure the CCF function	Create the ccf rule
	Configure the L4 protocol of the ccf rule
	Configure the basic application of the ccf rule
	Configure the keyword of the ccf rule
	Configure the file type of the cf rule

Configuration Tasks	
Configure the CCF function	Create the ccf filter policy
	Configure the referencing relation and the policy action of the ccf rule and the policy
Configure the SERVICE function	Create the service or service group
	Configure the protocol rule of the service
	Configure the combination relation of the service and service group
	Configure the description information of the service or service group
Configure the DPI function	Configure the DPI detection switch
	Configure the feature library upgrade
Configure the DPI function	Configure referencing the DPI policy in the interface

12.2.1. Configure Application Identification and Visible Control AVC Function

AVC is the abbreviation of Application Visible and Control. It can carry out depth detection of packets and corresponding processing actions for different applications.

Configuration Conditions

None

Create Application Method List

Table 12-2 Create application method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create application	**avc application** *application-name*	Mandatory

Enable Application Method List

Table 12-3 Enable application method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application view	**avc application** *application-name*	Mandatory
Enable the application	**application enable**	By default, it is enabled.

Configure Application Popularity Method List

Table 12-4 Configure the application popularity method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application view	**avc application** *application-name*	Mandatory
Configure the application popularity	**application popular { high | normal | low }**	Optional By default, the popularity is normal.

Configure Application Platform Attribute Method List

Table 12-5 Configure the platform attribute method list of the application

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application view	**avc application** *application-name*	Mandatory
Step	**Command**	**Description**
Configure the platform attribute of the application	**application platform { windows | linux | android | ios }**	Optional By default, the platform attribute is linux.

Configure Application Basic Protocol Type Method List

Table 12-6 Configure the basic protocol type method list of the application

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application view	**avc application** *application-name*	Mandatory
Configure the basic protocol type of the application	**base-application { http position { uri | rawuri |subheader** *header-name-string* **| body } | https}**	Optional Configure the basic application protocol

Note:

- If the command is configure, signature must be configured.

Configure Direction Method List of Application

Table 12-7 Configure the direction method list of the application

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application view	**avc application** *application-name*	Mandatory
Configure the application direction	**direction { request | response }**	-

Configure L4 Protocol Method List of Application

Table 12-8 Configure the L4 protocol method list of the application

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application view	**avc application** *application-name*	Mandatory
Configure the L4 protocol of the application	**l4 protocol { tcp | udp }**	Optional As the effective condition of the avc application, the item is mandatory.

Configure Destination Address Range Method List of Application

Table 12-9 Configure the destination address range method list of the application

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application view	**avc application** *application-name*	Mandatory

Step	Command	Description
Configure the destination address range of the application	**destination { ip** *ip-address mask-length* **| ipv6** *ipv6-address prefix-length* **}**	Optional Configure the matching item of the destination address.

Note:

- At most 4 destination address commands can be configured for IPv4 and IPv6 respectively. In addition, perform the duplicate-check for the configured addresses.

Configure Destination Port Range Method List of Application

Table 12-10 Configure the destination port range method list of the application

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application view	**avc application** *application-name*	Mandatory
Configure the destination port range of the application	**port {** *port-num* **[** *secondary_port_num* **] | range** *start-port end-port* **}**	Optional

Configure Feature Method List of Application

Table 12-11 Configure the feature method list of the application

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application view	**avc application** *application-name*	Mandatory

Step	Command	Description
Configure the application feature	**signature pattern { text** *pattern-text-string* | **regex** *pattern-regex-string* **}**	Optional The feature can be text or regular expression

Note:

- This command is used to configure the feature pattern of the application object. The location of the pattern is specified in the base-application command.
- For text regular strings, two codes are supported when configuring Chinese: UTF-8 and GB18030. But it has the ability to recognize two Chinese codes. That is, the Chinese GB18030/UTF8 user inputs any code, and the data stream can be recognized by any code.
- Regular expressions do not support character sets, that is, if regular expressions are configured, the input formal expressions will not be coded. If you need to match the same Chinese encoded by different characters, you need to input different codes into regular expressions.

Configure Description Information Method List of Application

Table 12-12 Configure the description information method list of the application

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application view	**avc application** *application-name*	Mandatory
Configure the description information of the application	**description** *description*	Mandatory

Create Application Group Method List

Table 12-13 Create application group method list

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

Step	Command	Description
Create application group	**avc application-group** *application-group -name*	Mandatory

Configure Combination Relation Method List of Application and Application Group

Table 12-14 Configure the combination relation method list of the application and application group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application group view	**avc application-group** *application-group -name*	Mandatory
Configure the combination relation of the application and application group	**member { application** *application-name* **| application-group** *application-group-name***}**	Optional

Note:

- An application or application group object can only belong to one application group.
- Nested configuration is not allowed.

Configure Description Information Method List of Application Group

Table 12-15 Configure the description information method list of the application group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application group view	**avc application-group** *application-group -name*	Mandatory

Step	Command	Description
Configure the description information of the application group	**description** *description*	Mandatory

Create Application Control Policy Method List

Table 12-16 Create application method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create application control policy	**avc policy** *policy-name*	Mandatory

Configure Application Action Method List

Table 12-17 Configure the application action method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application control policy view	**avc policy** *policy-name*	Mandatory
Configure the application action	**application** *application-name* **{ permit | deny } [logging security-data {notifications | warnings | errors }]**	Optional

Configure Application Group Method List

Table 12-18 Configure the application group action method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application control policy view	**avc policy** *policy-name*	Mandatory
Configure the application group action	**application-group** *application-group-name* **{ permit | deny } [logging security-data {notifications | warnings | errors }]**	Optional

Configure Default Action Method List of Application Control Policy

Table 12-19 Configure the default action method list of the application control policy

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application control policy view	**avc policy** *policy-name*	Mandatory
Configure the default action of the application control policy	**default action { permit | deny } [logging security-data {notifications | warnings | errors }]**	Optional

Configure Description Information Method List of Application Control Policy

Table 12-20 Configure the description information method list of the application control policy

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the application control policy view	**avc policy** *policy-name*	Mandatory
Configure the description information of the application control policy	**description** *description*	Mandatory

12.2.2. Configure URL Classification and Filtering Function

Configuration Conditions

None

Create url Classification Method List

Table 12-21 Create usl classification method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create usl classification	**url-filter category user-defined** *category-name* **severity** *severity-level*	Mandatory

Note:

- Severity-level is the severity level of the classification. The higher the value, the higher the priority.
- Severity levels of different classifications cannot be the same.
- Different classifications are referenced by the same policy, and the classification contains the same URL rules. After the rule is hit, execute the action corresponding to the classification with high severity.

Configure Rule Method List of url Classification

Table 12-22 Configure the rule method list of the url classification

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the url category view	**url-filter category user-defined** *category-name* **severity** *severity-level*	Mandatory
Configure the rules of the url classification	**rule** *rule-id* host { **text** *host-text-string* | **regex** *host-regex-string* } [**uri** { **text** *uri-text-string* | **regex** *uri-regex-string* }]	Optional

Configure Description Information Method List of URL Classification

Table 12-23 Configure the rule method list of the url classification

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the url category view	**url-filter category user-defined** *category-name* **severity** *severity-level*	Mandatory
Configure the description information of the url classification	**description** *description*	Optional

Create url Classification Policy Method List

Table 12-24 Configure url classification policy method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create url classification policy	**url-filter policy** *policy-name*	Mandatory

Configure url Classification Action Method List

Table 12-25 Configure the action method list of the url classification

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the url category policy view	**url-filter policy** *policy-name*	Mandatory
Configure the url classification action	**category** *category-name* **action { permit | deny | reset } [logging security-data {notifications | warnings | errors }]**	Mandatory

Configure Default Action Method List of url Classification

Table 12-26 Configure the default action method list of the url classification

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the url category policy view	**url-filter policy** *policy-name*	Mandatory
Configure the default action of the url classification	**default action { permit | deny | reset } [logging security-data {notifications | warnings | errors }]**	Mandatory

12.2.3. Configure Content Control and Filtering CCF Function

The CCF (Content control and filter) function releases, discards, alters and replaces the specific string of the identified packet.

Configuration Conditions

None

Create ccf Rule Method List

Table 12-27 Create ccf rule list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create ccf rule	**ccf { keyword | file-type | event } rule** *rule-id*	Mandatory Configure the rule of keyword type, file type or event rule

Configure Basic Protocol Type Method List of ccf Rule

Table 12-28 Configure the basic protocol type method list of the ccf rule

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the ccf rule view	**ccf { keyword | file-type } rule** *rule-id*	Mandatory
Configure the basic protocol type of the ccf rule	**base-application { http position { uri | rawuri | subheader** *header-name-string* **| body } * |** **{ pop3 | smtp } position { subheader** *header-name-string* **| body } * | ftp}**	Mandatory Configure http/pop3/smtp/ftp basic application

Note:

- A ccf rule can only be configured with one basic application, and can be configured with up to four different positions (for example, four different subheaders can be configured, or three subheaders plus one body, there cannot be four bodies).
- Configure the basic application whose protocol type is FTP, and only process the FTP control channel packet.

- Only one basic application can be configured for a ccf rule.

Configure L4 Protocol Method List of ccf Rule

Table 12-29 Configure the L4 protocol method list of the ccf rule

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the ccf rule view	**ccf { keyword | file-type } rule** *rule-id*	Mandatory
Configure the L4 protocol of the ccf rule	**l4 protocol { tcp | udp }**	Optional As the effective condition of the ccf rule, the item is mandatory.

Configure Keyword Method List of ccf Rule

Table 12-30 Configure the keyword list of the ccf rule

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the ccf rule view	**ccf keyword rule** *rule-id*	Mandatory
Configure the keyword list of the ccf rule	**keyword { text** *pattern-text-string* **| regex** *pattern-regex-string* **}**	Optional As the effective condition of the ccf rule, the item is mandatory.

Note:

- This command is used to configure the keyword of the rule object. The keyword is a character string.
- Only two codes are supported in Chinese configuration: UTF-8 and GB18030. But it has the ability to recognize two Chinese codes. That is, the GB18030/UTF8 user inputs any code, and the data stream can be recognized by any code.

Configure File Type Method List of ccf Rule

Table 12-31 Configure the file type list of the ccf rule

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the ccf rule view	**ccf file-type rule** *rule-id*	Mandatory
Configure the file type lof the ccf rule	**file-type** *type-name*	Optional Configure the filtered file type.

Note:

- The first character must be ".", case insensitive, 2–7 characters.

Configure ccf Control Policy Method List

Table 12-32 Configure the ccf control policy method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the ccf control policy	**ccf policy** *policy-name*	Mandatory

Configure Black-whitelist Priority Method

Table 12-33 Configure the black/whitelist priority policy method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure black/whitelist priority	**rule match-prefer whitelist**	Mandatory

Configure Quantity Restriction Method of Mail Attachments

Table 12-34 Configure the quantity restriction method list of the mail attachments

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the ccf control policy	**ccf event rule** *rule-id*	Mandatory
Configure attachment quantity limitation	**mail attachment threshold** *num*	Mandatory

Configure Restriction Method of Mail Size

Table 12-35 Configure the mail size restriction method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the ccf control policy	**ccf event rule** *rule-id*	Mandatory
Configure the mail size restriction	**mail size threshold** *size*	Mandatory

Configure Application Action Method List

Table 12-36 Configure the reference relationship between ccf rules and policies and the list of policy action methods

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the ccf control policy view	**ccf policy** *policy-name*	Mandatory

Step	Command	Description
Configure the reference relationship between ccf rules and policies and the policy action	**rule** *id* **action { permit | deny | modify [offset** *offset_num*] **{ newstring** *newstring* **| character character length** *length* **} | replace { newstring** *newstring* **| character** *character* **}} [notifications | warnings | errors]**	Optional

Note:

- ccf filetype and ccf event rules only support permit and deny actions.

12.2.4. Configure OBJECT-SERVICE Function

Configuration Conditions

None

Create Service Method List

Table 12-37 Create service method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create service	**ip object-service** *object-service-name*	Mandatory

Configure Service TCP/UDP Protocol Rule Method List

Table 12-38 Configure service TCP/UDP protocol rule method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the service view	**ip object-service** *object-service-name*	Mandatory

Step	Command	Description
Configure the service TCP/UDP protocol rule	**protocol {udp | tcp} [source-port** *start-port* **[to** *end-port*] **| destination-port** *src-start-port* **[to** *src-end-port*]]	Mandatory

Configure Service ICMP Protocol Rule Method List

Table 12-39 Configure service ICMP protocol rule method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the service view	**ip object-service** *object-service-name*	Mandatory
Configure the service ICMP protocol rule	**protocol icmp [icmp-type** *type* **[icmp-code** *code-num1* **[to** *code-num2*]]]	Mandatory

Configure Service Other Protocol Rule Method List

Table 12-40 Configure service other protocol rule method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the service view	**ip object-service** *object-service-name*	Mandatory
Configure the other protocol rules of the service	**protocol other** *protocol-number*	Mandatory

Configure Description Information Method List of Service

Table 12-41 Configure the description information method list of the service

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the service view	**ip object-service** *object-service-name*	Mandatory
Configure the description information of the service	**description** *description*	Optional

Create Service Group Method List

Table 12-42 Create service group method list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create service group	**ip object-service-group** *object-service-group-name*	Mandatory

Configure Combination Relation of Service and Service Group

Table 12-43 Configure the combination relation of the service and service group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the service group view	**ip object-service-group** *object-service-group-name*	Mandatory
Configure the combination relation of the	**member { object-service**	Mandatory

Step	Command	Description
service and service group	*object-service-name*| **object-service-group** *object-service -group-name***}**	

Configure Description Information Method List of Service Group

Table 12-44 Configure the description information method list of the service group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the service view	**ip object-service-group** *object-service-group-name*	Mandatory
Configure the description information of the service group	**description** *description*	Optional

12.2.5. Configure DPI Function

Configure Referencing DPI In Interface

Table 12-45 Configure referencing DPI method list in the interface

Step	Command	Description
Enter privileged mode	**enable**	-
Configure referencing DPI in the interface	**dpi [ip | ipv6] apply {{ avc-policy | url-policy** | **ccf-policy }** *policy_name***}***	Mandatory Reference avc/url/ccf policy in the interface.

Note:

- Multiple different types of policies can be configured. Only one policy of each type can be configured.
- avc/url/ccf policies can be referenced by the interface and secp at the same time. If the referenced policies are different, the policies referenced under the interface take precedence.

12.2.6. Configure Feature Library Upgrade Function

Configuration Conditions

None

Configure Scheduled Upgrade Function of Feature Library

Table 12-46 Configure the scheduled upgrade method list of the feature library

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the server address	**dpi update server avc** *url*	Mandatory
Configure the scheduled upgrade time	**dpi update schedule avc { daily | weekly { Mon | Tue | Wed | Thu | Fri | Sat | Sun } }** *time*	Mandatory

Note:

- url only supports ftp, http type.

Configure Rollback Function of Feature Library

Table 12-47 Configure the rollback function of the feature library

Step	Command	Description
Enter privileged mode	**enable**	-
Configure the rollback function of the feature library	**dpi update rollback avc**	Mandatory

Configure Immediate Upgrade Function of Feature Library

Table 12-48 Configure the immediate upgrade function of the feature library

Step	Command	Description
Enter privileged mode	**enable**	-

Step	Command	Description
Configure the immediate upgrade function of the feature library	**dpi update instant avc**	Mandatory

Configure Restoring Factory Version of Feature Library

Table 12-49 Configure restoring the factory version of the feature library

Step	Command	Description
Enter privileged mode	**enable**	-
Configure restoring the factory version	**dpi update restore default avc**	Mandatory

Configure Local Upgrade Function of Feature Library

Table 12-50 Configure the local upgrade function of the feature library

Step	Command	Description
Enter privileged mode	**enable**	-
Restore the factory version	**dpi update local file avc** *filename*	Mandatory

12.2.7. DPI Monitoring and Maintaining

Table 12-51 AVC monitoring and maintaining method list

Command	Description
show avc { application [*application-name***] | application-group [***application-group-name***] }**	Display all or specified applications
show avc statistics	Display the statistics information of the avc filtering
clear avc statistics	Clear the statistics information of the avc filtering

Command	Description
show url statistics	Display the statistics information of the url filtering
clear url statistics	Clear the statistics information of the url filtering
clear ccf statistics	Clear the statistics information of the content filtering policy
show ccf statistics policy *policy-name* **lpu** *lpu-id* **[details rule** *rule-id***]**	Display statistics information of content filtering policies or specific rules under filtering policies. The statistics of the content filtering policy is the sum of the statistics of all referenced rules under the policy. When the user modifies the rule configuration, the statistics of the rule will be cleared, and the statistics of the corresponding filtering policy will be updated.
show object-service [*object-service-name***]**	Display all or specified services
show object-service-group [*object-service-group-name***]**	Display all or specified service groups
show version avc	Display the feature library version information
debug dpi {all | packet | error | engine | ctrl | http | https | avc | rule | url || option | update }	Enable all debug switches of the dpi module

12.3. DPI Typical Configuration Examples

12.3.1. Configure AVC Feature Library Upgrade

Network Requirements

- PC1 is the internal host, the Web Server is the web server on the public network, and Device is the NAT device. The internal source NAT dynamic port conversion is configured, and the IP route is reachable;
- Device upgrades the AVC feature library through the web server on the public network.

Network Topology

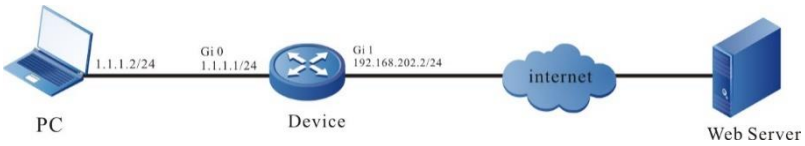


Figure 12-1 Configure regular upgrade of feature library through HTTP address

Configuration Steps

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

Step 2: Configure internal source NAT dynamic port conversion, and configure route to ensure that the PC can be connected to the external network.

#Configure the interface gigabitethernet0 as the inside interface of NAT.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0
Device(config-if-gigabitethernet0)#ip nat inside
Device(config-if-gigabitethernet0)#exit
```

#Configure the interface gigabitethernet1 as the outside interface of NAT.

```
Device(config)#interface gigabitethernet 1
Device(config-if-gigabitethernet1)#ip nat outside
Device(config-if-gigabitethernet1)#exit
```

#Configure the ACL 1001, only permitting the PCs in the 1.1.1.0/24 network segment of the internal private network to access the web server.

```
Device(config)#ip access-list extended 1001
Device(config-ext-nacl)#10 permit ip 1.1.1.0 0.0.0.255 any
Device(config-ext-nacl)#exit
```

#Configure the internal source NAT dynamic port conversion rules to convert the internal private network address 1.1.1.2 to the public network address.

```
Device(config)#ip nat inside source list 1001 interface gigabitethernet 1 overload
```

#Configure a gateway route to gateway 192.168.202.254.

```
Device(config)#ip route 0.0.0.0 0.0.0.0 192.168.202.254
```

Step 3: Configure the upgrade server address and scheduled upgrade cycle of the AVC feature library.

#Configure the server address of AVC upgrade feature library in the URL address mode of http:

```
Device(config)#dpi update server avc http://15.255.1.98/zhuabao/avc-1.0.0.dat
```

#Configure the regular upgrade cycle of AVC feature library, which starts at 9:00 a.m. every Monday with weekly intervals:

```
Device(config)#dpi update schedule avc weekly Mon 9:00
```

```
Device(config)#exit
```

Step 4: Check the result.

The version information before upgrading:

```
Device#show version avc
avc Update Information List:
------------------------------------------------------------
 Signature Update Result       : --

 Current Version:
  Signature Database Version    : 16777217
  Signature Database Size(byte) : 3274
  Update Time                   : 00:00:00 0000/00/00
  Issue Time of the Update File : 09:30:01 2019/05/30

 Backup Version:
  Signature Database Version    : 0
  Signature Database Size(byte) : 0
  Update Time                   : 00:00:00 0000/00/00
  Issue Time of the Update File : 00:00:00 0000/00/00
```

When reaching the scheduled upgrade time, the version information after the first upgrade is completed:

```
Device#show version avc
avc Update Information List:
------------------------------------------------------------
 Signature Update Result       : SUCCESS

 Current Version:
  Signature Database Version    : 2020051220
  Signature Database Size(byte) : 10335
  Update Time                   : 09:00:05 2020/05/25
  Issue Time of the Update File : 08:19:49 2020/05/12

 Backup Version:
  Signature Database Version    : 0
  Signature Database Size(byte) : 0
  Update Time                   : 00:00:00 0000/00/00
  Issue Time of the Update File : 00:00:00 0000/00/00
```

The console port of device will output the system log of AVC feature library upgrade success:

```
May 25 2020 09:00:05 DPI-Device MPU0 %DPI-UPDATE_RESULT_SUCC-5:Avc signature update success!
```

12.3.2. Configure HTTP Packet Filtering of AVC

Network Requirements

- PC1 and PC2 are internal hosts, web server is a web server on the public network, and device is a NAT device. Internal source NAT dynamic port conversion is configured, and IP route is reachable.
- Configure the HTTP packet filtering function of AVC on the device to discard or release specific HTTP packets and prevent or allow users to access specific websites or applications. For example: prevent PC1 from searching "youtube" on http://www.google.com/ website and record log information for discarded packets; allow PC2 to search other keywords, such as "mail" on http://www.google.com/, and record log information for released packets.

Network Topology

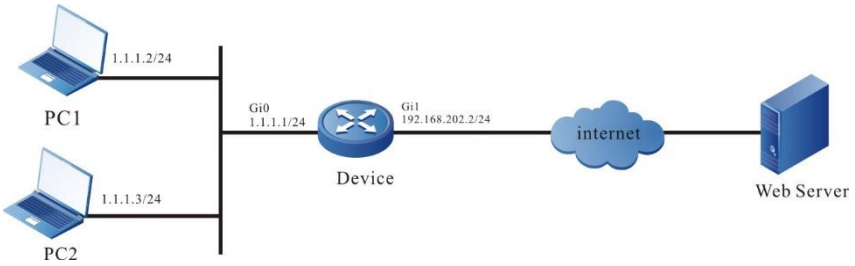


Figure 12-2 Networking of configuring the HTTP packet filtering of AVC

Configuration Steps

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

Step 2: Configure internal source NAT dynamic port conversion, and configure route to ensure that the PC can be connected to the external network.

#Configure the interface gigabitethernet0 as the inside interface of NAT.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0
Device(config-if-gigabitethernet0)#ip nat inside
Device(config-if-gigabitethernet0)#exit
```

#Configure the interface gigabitethernet1 as the outside interface of NAT.

```
Device(config)#interface gigabitethernet 1
Device(config-if-gigabitethernet1)#ip nat outside
Device(config-if-gigabitethernet1)#exit
```

#Configure the ACL 1001, only permitting the PCs in the 1.1.1.0/24 network segment of the internal private network to access the web server.

```
Device(config)#ip access-list extended 1001
Device(config-ext-nacl)#10 permit ip 1.1.1.0 0.0.0.255 any
```

```
Device(config-ext-nacl)#exit
```

#Configure the internal source NAT dynamic port conversion rules to convert the internal private network address 1.1.1.2 and 1.1.1.3 to the public network address.

```
Device(config)#ip nat inside source list 1001 interface gigabitethernet1 overload
```

#Configure a gateway route to gateway 192.168.202.254.

```
Device(config)#ip route 0.0.0.0 0.0.0.0 192.168.202.254
```

Step 3: Configure the HTTP packet filtering function of AVC.

#Configure the AVC application object as http, the L4 protocol as TCP, the L5 application protocol as HTTP, and the filter feature string as "youtube", which is located in the url field of the http packet.

```
Device(config)#avc application http
Device(config-application)#l4 protocol tcp
Device(config-application)#base-application http position uri
Device(config-application)#signature pattern text youtobe
Device(config-application)#exit
```

#Configure the avc application policy as http, the policy action as deny, and the log type as warnings; The default action is permit, and the log type is notifications.

```
Device(config)#avc policy http
Device(config-avc-policy)#application http deny logging security-data warnings
Device(config-avc-policy)#default action permit logging security-data notifications
Device(config-avc-policy)#exit
```

#Configure the security policy to reference the avc application policy http.

```
Device(config)#security policy 1
Device(config-security-policy)#action inspect avc-policy http
Device(config-security-policy)#exit
```

Step 4: Check the result: Verify whether the HTTP packet filtering of AVC is effective.

#PC1 accesses http://www.google.com/, and enter the string "youtobe" in the search box to match the action deny of the application object http. Web page access is blocked, and you can see that there are data log records on the serial port of Device. The action is deny and the log type is level-4 log: warnings.

```
Sep 20 2019 20:23:40 Device LPU0 %DPI-AVC-4:Protocol:tcp, source ip:1.1.1.2, source port:62377, destination ip:180.97.36.72, destination port:80 hit the avc policy http, application name: http, action: deny.
```

#PC2 accesses http://www.google.com/, and enter any string that does not match "youtobe" in the search box, such as "mail", which matches the default action permit of the application, web page access is allowed, and you can see that there are data log records on the serial port of Device, the action is permit, and the log type is level-5 log: notifications.

Sep 20 2019 20:23:40 Device LPU0 %DPI-AVC-5:Protocol:tcp, source ip:1.1.1.3, source port:62641, destination ip:183.3.226.111, destination port:36688 hit the avc policy http, default action: permit.

12.3.3. Configure FTP Packet Filtering of AVC

Network Requirements

- PC1 and PC2 are the internal host, the Ftp Server is the web server on the public network, and Device is the NAT device. The internal source NAT dynamic port conversion is configured, and the IP route is reachable;
- The FTP packet filtering function of AVC is configured on Device to discard or release specific FTP connection packets, such as prevent PC1 from downloading files with file names containing "secret" on the FTP server, and record log information for discarded packets; PC2 is allowed to download other files whose file name does not contain "secret" on the FTP server, and record log information for released packets.

Network Topology

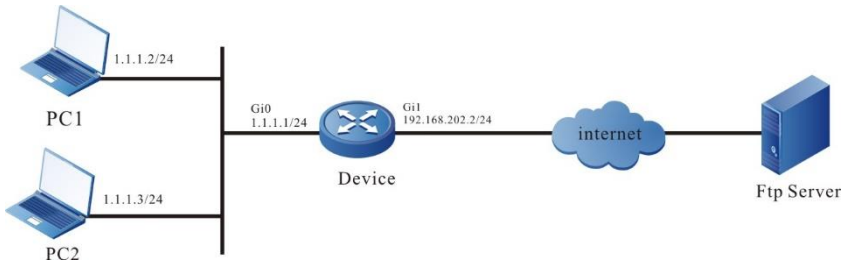


Figure 12-3 Networking of configuring the FTP packet filtering of AVC

Configuration Steps

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

Step 2: Configure internal source NAT dynamic port conversion, and configure route to ensure that the PC can be connected to the external network.

#Configure the interface gigabitethernet0 as the inside interface of NAT.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0
Device(config-if-gigabitethernet0)#ip nat inside
Device(config-if-gigabitethernet0)#exit
```

#Configure the interface gigabitethernet1 as the outside interface of NAT.

```
Device(config)#interface gigabitethernet 1
Device(config-if-gigabitethernet1)#ip nat outside
Device(config-if-gigabitethernet1)#exit
```

#Configure the ACL 1001, only permitting the PCs in the 1.1.1.0/24 network segment of the internal private network to access the web server.

```
Device(config)#ip access-list extended 1001
Device(config-ext-nacl)#10 permit ip 1.1.1.0 0.0.0.255 any
Device(config-ext-nacl)#exit
```

#Configure the internal source NAT dynamic port conversion rules to convert the internal private network address 1.1.1.2 and 1.1.1.3 to the public network address.

```
Device(config)#ip nat inside source list 1001 interface gigabitethernet 1 overload
#Configure a gateway route to gateway 192.168.202.254.
Device(config)#ip route 0.0.0.0 0.0.0.0 192.168.202.254
```

Step 3: Configure the FTP packet filtering function of AVC.

#Configure the avc application object as ftp, the L4 protocol as tcp, and the filter feature string as "secret".

```
Device(config)#avc application ftp
Device(config-application)#l4 protocol tcp
Device(config-application)#signature pattern text secret
Device(config-application)#exit
```

#Configure the avc application policy as ftp, the policy action as deny, and the log type as warnings; The default action is permit, and the log type is notifications.

```
Device(config)#avc policy ftp
Device(config-avc-policy)#application ftp deny logging security-data warnings
Device(config-avc-policy)#default action permit logging security-data notification
Device(config-avc-policy)#exit
```

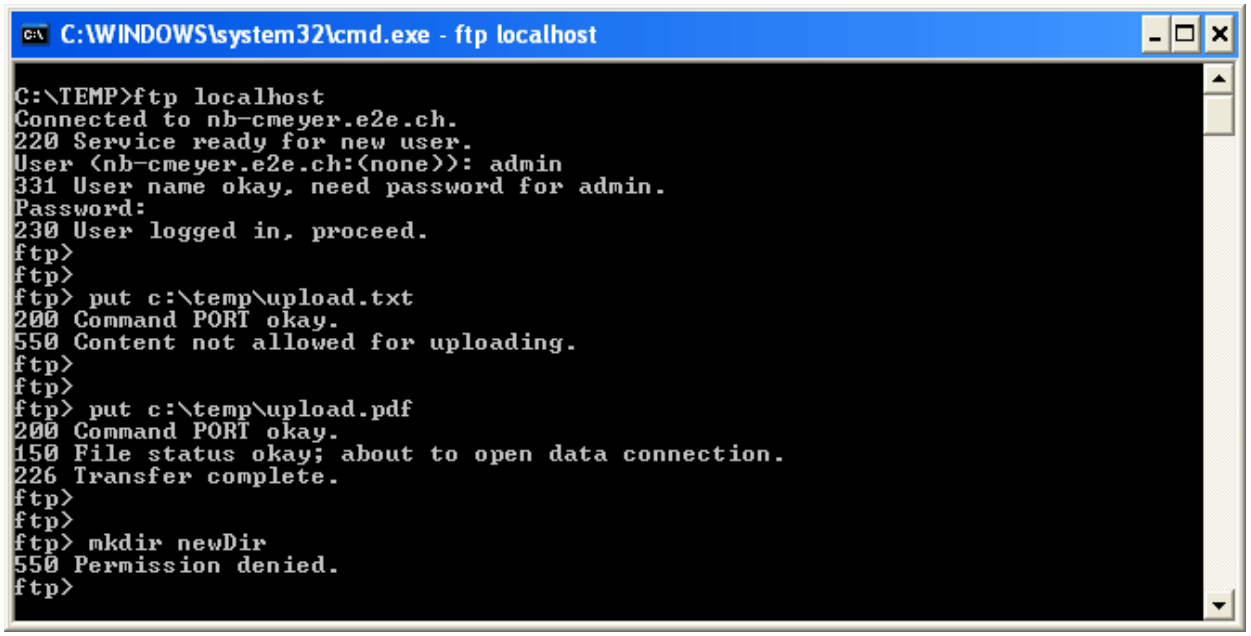
#Configure security policy to reference avc application policy ftp.

```
Device(config)#security policy 1
Device(config-security-policy)#action inspect avc-policy ftp
Device(config-security-policy)#exit
```

Step 4: Check the result: Verify whether the FTP packet filtering of AVC is effective.

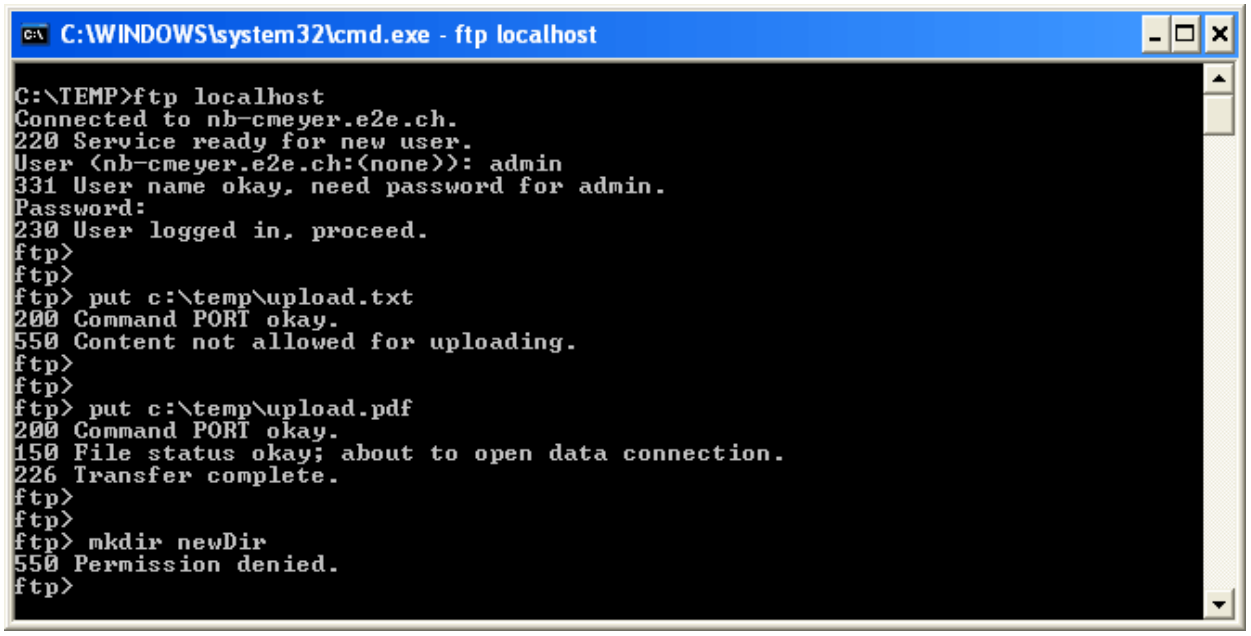
#PC1 uses the FTP client carried by windows to access FTP Server 192.168.202.230 (using the 3CDaemon server as the FTP server, where there are files secret-file.txt and normal.txt). Enter the user name: a and password: 123456. Prevent downloading the file secret-file.txt on PC1, match the action deny of application object a, and you can see that there are data logs on the serial port of Device, The action is deny, and the log type is level-4: warnings.

```
Sep 21 2019 03:00:14 Device LPU0 %DPI-AVC-4: Protocol:tcp, source ip:1.1.1.2, source port:63499, destination ip:192.168.202.230, destination port:21 hit the avc policy ftp, application name: ftp, action: deny.
```



#PC2 uses the FTP client carried by windows to access FTP Server 192.168.202.230 (there are files secret-file.txt and normal.txt on the server). Enter the user name: a and password: 123456. Permit downloading the file secret-file.txt on PC2, match the action permit of application, and you can see that there are data logs on the serial port of Device, The action is permit, and the log type is level-5: notifications.

> Sep 21 2019 03:00:14 Device LPU0 %DPI-AVC-5:Protocol:tcp, source ip:1.1.1.3, source port:63630, destination ip:192.168.202.230, destination port:21 hit the avc policy ftp, default action: permit.



12.3.4. Configure URL Classification Filtering

Network Requirements

- PC1 and PC2 are the internal host, the Web Server is the web server on the public network, and Device is the NAT device. The internal source NAT dynamic port conversion is configured, and the IP route is reachable;
- By configuring the URL classification filtering function on Device, specific http packets can be discarded or released to prevent or allow users to access specific websites, such as preventing PC1 from accessing Google domestic news network: http://news.google.com/ And record log information for blocked packets; when PC2 accesses Google International News Network: http://news.google.com/, the connection is reset (i.e. disconnect the connection immediately without waiting for a response), and record the log information for the reset packet; permit PC1 to access http://news.google.com/finance, and record the log information of the released packet.

Network Topology

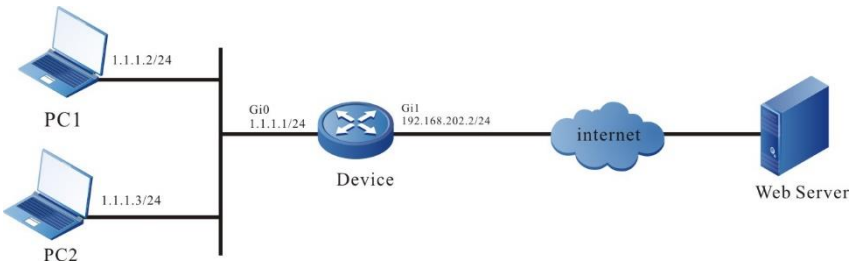


Figure 12-4 Networking of configuring URL filtering classification

Configuration Steps

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

Step 2: Configure internal source NAT dynamic port conversion, and configure route to ensure that the PC can be connected to the external network.

#Configure the interface gigabitethernet0 as the inside interface of NAT.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0
Device(config-if-gigabitethernet0)#ip nat inside
Device(config-if-gigabitethernet0)#exit
```

#Configure the interface gigabitethernet1 as the outside interface of NAT.

```
Device(config)#interface gigabitethernet 1
Device(config-if-gigabitethernet1)#ip nat outside
Device(config-if-gigabitethernet1)#exit
```

#Configure the ACL 1001, only permitting the PCs in the 1.1.1.0/24 network segment of the internal private network to access the web server.

```
Device(config)#ip access-list extended 1001
Device(config-ext-nacl)#10 permit ip 1.1.1.0 0.0.0.255 any
Device(config-ext-nacl)#exit
```

#Configure the internal source NAT dynamic port conversion rules to convert the internal private network address 1.1.1.2 and 1.1.1.3 to the public network address.

```
Device(config)#ip nat inside source list 1001 interface gigabitethernet 1 overload
#Configure a gateway route to gateway 192.168.202.254.
Device(config)#ip route 0.0.0.0 0.0.0.0 192.168.202.254
```

Step 3: Configure the URL classification filtering function.

#Configure the URL classification object as a, the severity level as 100, the host of the URL rule as text type, the filtering content as "news.google.com", the URI of the URL rule as text text type, and the filtering content as: "guonei".

```
Device(config)#url-filter category user-defined a severity 100
Device(config-url-category)#rule 1 host text news.google.com uri text guonei
Device(config-url-category)#exit
```

#Configure the URL classification object as b, the severity level as 200, the host of URL rule as text type, the filtering content as: "news.google.com", the URI of URL rule as text text type, and the filtering content as: "guoji".

```
Device(config)#url-filter category user-defined b severity 200
Device(config-url-category)#rule 1 host text news.google.com uri text guoji
Device(config-url-category)#exit
```

#Configure the URL classification policy as 1. The policy action is: the action of classification a is deny, and the record log type is warnings; The action of classification b is reset, and the log type is notifications. The default action is permit, and the log type is notifications.

```
Device(config)#url-filter policy 1
Device(config-url-policy)#category a action deny logging security-data warnings
Device(config-url-policy)#category b action reset logging security-data notifications
Device(config-url-policy)#default action permit logging security-data notifications
Device(config-url-policy)#exit
```

#Configure the security policy to reference the url classification policy 1.

```
Device(config)#security policy 1
Device(config-security-policy)#action inspect url-policy 1
Device(config-security-policy)#exit
```

Step 4: Check the result: Verify whether the URL classification filtering takes effect.

#PC1 cannot access http://news.google.com/guonei, match the action deny of URL classification object a, and you can see that there are data log records on the serial port of Device. The action is deny, and the log type is level-4 log: warnings.

```
Sep 21 2019 03:23:17 Device LPU0 %DPI-URL-4:Protocol:tcp, source ip:1.1.1.2, source port:65047, destination ip:180.97.36.72, destination port:80 hit the url policy 1, category name: a, action: deny.
```

#PC2 accesses http://news.google.com/guoji , match the action reset of URL classification object b, the connection is reset, and you can see that there are data log records on the serial port of Device. The action is reset, and the log type is level-5 log: notifications.

```
Sep 21 2019 03:23:17 Device LPU0 %DPI-URL-5:Protocol:tcp, source ip: 1.1.1.3 source port:49763, destination ip:119.97.145.90, destination port:80 hit the url policy 1, category name: b, action: reset.
```

#PC1 can access http://news.google.com/finance , match the default action permit of URL classification, and you can see that there are data logging records on the serial port of Device. The action is permit, and the log type is level-5 log: notifications.

```
Sep 21 2019 03:24:27 Device LPU0 %DPI-URL-5:Protocol:tcp, source ip: 1.1.1.2, source port:50007, destination ip:113.219.136.29, destination port:80, hit the url policy 1, default action: permit.
```

Note:

- The host of URL classification rule supports *wildcard, but multiple * cannot be configured continuously.
- When the same stream hits different URL classifications at the same time, the higher the severity value of the URL classification, the higher the priority.

12.3.5. Configure OBJECT-SERVICE Filtering

- PC1 and PC2 are the internal host, the Web Server is the web server on the public network, and Device is the NAT device. The internal source NAT dynamic port conversion is configured, and the IP route is reachable;
- By configuring the OBJECT-SERVICE filtering function on the device, PC1 is prevented from sending connection packets with TCP protocol and destination port 80 to the external network; prevent PC2 from pinging.

Network Topology

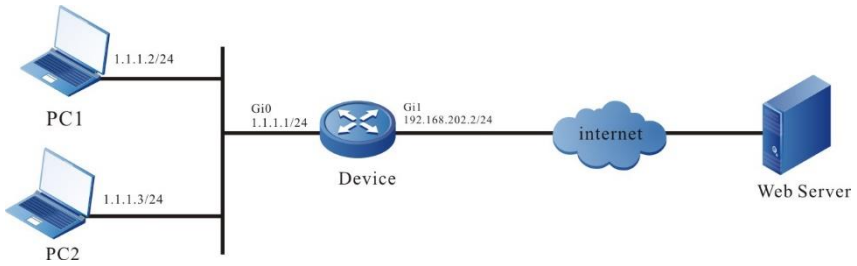


Figure 12-5 Networking of configuring OBJECT-SERVICE filtering

Configuration Steps

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

Step 2: Configure internal source NAT dynamic port conversion, and configure route to ensure that the PC can be connected to the external network.

#Configure the interface gigabitethernet0 as the inside interface of NAT.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0
Device(config-if-gigabitethernet0)#ip nat inside
Device(config-if-gigabitethernet0)#exit
```

#Configure the interface gigabitethernet1 as the outside interface of NAT.

```
Device(config)#interface gigabitethernet 1
Device(config-if-gigabitethernet1)#ip nat outside
Device(config-if-gigabitethernet1)#exit
```

#Configure the ACL 1001, only permitting the PCs in the 1.1.1.0/24 network segment of the internal private network to access the web server.

```
Device(config)#ip access-list extended 1001
Device(config-ext-nacl)#10 permit ip 1.1.1.0 0.0.0.255 any
Device(config-ext-nacl)#exit
```

#Configure the internal source NAT dynamic port conversion rules to convert the internal private network address 1.1.1.2 and 1.1.1.3 to the public network address.

```
Device(config)#ip nat inside source list 1001 interface gigabitethernet1 overload
```

#Configure a gateway route to gateway 192.168.202.254.

```
Device(config)#ip route 0.0.0.0 0.0.0.0 192.168.202.254
```

Step 3: Configure OBJECT-SERVICE filtering function.

#Configure the Object-Service object as 1, first configure the protocol type as TCP, the source port as 1 to 65535, and the destination port as 80; and then configure the protocol type as ICMP, ICMP type as 8, and ICMP code as 0 to 255.

```
Device(config)#ip object-service 1
Device(config-object-service)#protocol tcp source-port 1 to 65535 destination-port 80 to 80
Device(config-object-service)#protocol icmp icmp-type 8 icmp-code 0 to 255
Device(config-object-service)#exit
```

#Configure the security policy to match object service object 1, configure the security policy action as deny, and record the log type as notifications.

```
Device(config)#security policy 1
Device(config-security-policy)#match object-service 1
Device(config-security-policy)#action deny logging security-data notifications
Device(config-security-policy)#exit
```

Step 4: Check the result: verify whether the OBJECT-SERVICE filtering takes effect.

#PC1 cannot access http://www.google.com/, the security policy prevents PC1 from sending HTTP connection packet with TCP protocol and destination port 80 to the external network, and it can be seen that there are data log records on the serial port of Device, the action is deny, and the log type is level-5 log: notifications.

```
Sep 21 2019 03:32:56 Device LPU0 %SECP-SECP-5:Pkt from any to any (protocol:tcp,source-ip:1.1.1.2,destination-ip:178.255.83.1,source-port:50750,destination-port:80) hit the security policy 1, action: deny
```

#PC2 cannot ping www.google.com. The security policy prevents PC2 from sending ICMP packets to the external network, and it can be seen that there are data log records on the serial port of Device. The action is permit, and the log type is level-5 log: notifications.

```
Sep 21 2019 03:32:58 Device LPU0 %SECP-SECP-5:Pkt from any to any (protocol:
icmp,source-ip:1.1.1.3,destination-ip:180.97.33.108, id:1) hit the security policy 1, action:
deny.
```

12.3.6. Configure Referencing DPI Policy in the Interface

- PC1 and PC2 are the internal host, the Web Server is the web server on the public network, and Device is the NAT device. The internal source NAT dynamic port conversion is configured, and the IP route is reachable;
- Configure the DPI policy on the Gi0 interface of Device to filter AVC HTTP packets, so as to discard or release specific HTTP packets and prevent or allow users to access specific websites or applications. For example: prevent PC1 from http://www.google.com/ Search "youtobe" on the website and record log information for discarded packets; permit PC2 to search other keywords on http://www.google.com/, such as "taobao", and record log information for released packets.

Network Topology

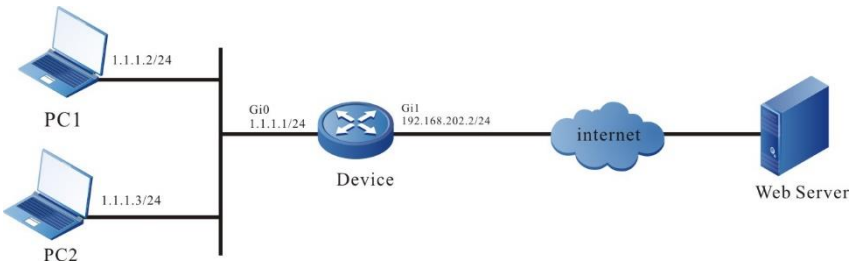


Figure 12-6 Networking of configuring the SERVICE filtering

Configuration Steps

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

Step 2: Configure internal source NAT dynamic port conversion, and configure route to ensure that the PC can be connected to the external network.

#Configure the interface gigabitethernet0 as the inside interface of NAT.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0
Device(config-if-gigabitethernet0)#ip nat inside
Device(config-if-gigabitethernet0)#exit
```

#Configure the interface gigabitethernet1 as the outside interface of NAT.

```
Device(config)#interface gigabitethernet 1
Device(config-if-gigabitethernet1)#ip nat outside
Device(config-if-gigabitethernet1)#exit
```

#Configure the ACL 1001, only permitting the PCs in the 1.1.1.0/24 network segment of the internal private network to access the web server.

```
Device(config)#ip access-list extended 1001
```

```
Device(config-ext-nacl)#10 permit ip 1.1.1.0 0.0.0.255 any
Device(config-ext-nacl)#exit
```

#Configure the internal source NAT dynamic port conversion rules to convert the internal private network address 1.1.1.2 and 1.1.1.3 to the public network address.

```
Device(config)#ip nat inside source list 1001 interface gigabitethernet 1 overload
#Configure a gateway route to gateway 192.168.202.254.
Device(config)#ip route 0.0.0.0 0.0.0.0 192.168.202.254
```

Step 3: Configure HTTP packet filtering function of AVC.

#Configure the AVC application object as http, the L4 protocol as TCP, the L5 application protocol as HTTP, and the filter feature string as "youtobe", which is located in the URI field of the HTTP packet.

```
Device(config)#avc application http
Device(config-application)#l4 protocol tcp
Device(config-application)#base-application http position uri
Device(config-application)#signature pattern text youtobe
Device(config-application)#exit
```

#Configure the AVC application policy as http, the policy action as deny, and the log type as warnings; The default action is permit, and the log type is notifications.

```
Device(config)#avc policy http
Device(config-avc-policy)#application http deny logging security-data warnings
Device(config-avc-policy)#default action permit logging security-data notifications
Device(config-avc-policy)#exit
```

#Configure referencing the avc application polict http in the interface.

```
Device(config)#interface gigabitethernet0
Device(config-if-gigabitethernet0)#dpi ip apply avc-policy http
Device(config-if-gigabitethernet0)#exit
```

Step 4: Check the result: Verify whether the DPI policy referenced under the interface (HTTP packet filtering of AVC) is effective.

#PC1 accesses http://www.google.com/, and enter the string "youtobe" in the search box to match the action deny of the application object http. Web page access is blocked, and you can see that there are data log records on the serial port of Device. The action is deny and the log type is level-4 log: warnings.

```
Sep 21 2019 06:36:55 Device LPU0 %DPI-AVC-4:Protocol:tcp, source ip:1.1.1.2, source port:62377, destination ip:180.97.36.72, destination port:80 hit the avc policy http, application name: http, action: deny.
```

#PC2 accesses http://www.google.com/, and enter any string that does not match "youtobe" in the search box, such as "taobao", which matches the default action permit of the application, web

page access is allowed, and you can see that there are data log records on the serial port of Device, the action is permit, and the log type is level-5 log: notifications.

```
Sep 21 2019 06:37:50 Device LPU0 %DPI-AVC-5:Protocol:tcp, source ip:1.1.1.3, source
port:62641, destination ip:183.3.226.111, destination port:36688 hit the avc policy http,
default action: permit.
```

Note:

- The difference between referencing DPI policy under the interface and referencing DPI in security policy: referencing DPI policy under the interface only monitors the traffic in and out of the interface, while referencing DPI policy in security policy is a global reference, which will monitor all traffic submitted to the local device.
- The DPI policies that can be configured and referenced under interface and security policy are AVC and URL. You can reference both policies or only one of them. If AVC and URL policies are referenced at the same time, the final execution action is the joint function result of the actions defined by the two policies. The reset execution priority of URL is the highest, deny is the second, and permission is the lowest.
- It is allowed to reference DPI policies under the interface and security policies at the same time. If they reference different policies, the policies referenced under the interface are preferred for matching; If only one of them references the DPI policy, the referenced policy can be used directly.

12.3.7. Configure CCF Keyword Rule Filtering and Altering

Network Requirements

- PC1 and PC2 are the internal host, the Mail Server is the mail server on the public network, and Device is the NAT device. The internal source NAT dynamic port conversion is configured, and the IP route is reachable;
- By configuring the CCF keyword filtering and altering function on the device, the mail containing specific keywords can be filtered and desensitized (i.e. altering function).

Network Topology

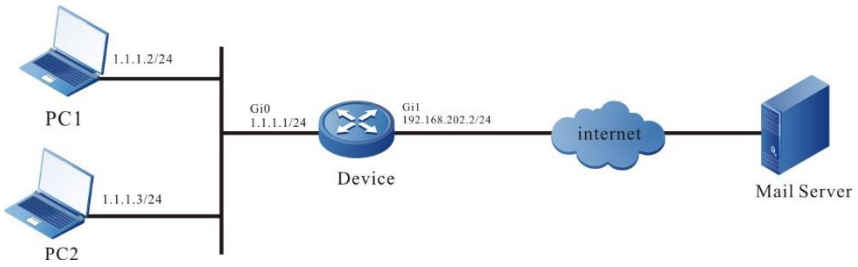


Figure 12-7 Networking of configuring the CCF mail filtering

Configuration Steps

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

Step 2: Configure internal source NAT dynamic port conversion, and configure route to ensure that the PC can be connected to the external network.

#Configure the interface gigabitethernet0 as the inside interface of NAT.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0
Device(config-if-gigabitethernet0)#ip nat inside
```

```
Device(config-if-gigabitethernet0)#exit
```

#Configure the interface gigabitethernet1 as the outside interface of NAT.

```
Device(config)#interface gigabitethernet 1
Device(config-if-gigabitethernet1)#ip nat outside
Device(config-if-gigabitethernet1)#exit
```

#Configure the ACL 1001, only permitting the PCs in the 1.1.1.0/24 network segment of the internal private network to access the web server.

```
Device(config)#ip access-list extended 1001
Device(config-ext-nacl)#10 permit ip 1.1.1.0 0.0.0.255 any
Device(config-ext-nacl)#exit
```

#Configure the internal source NAT dynamic port conversion rules to convert the internal private network address 1.1.1.2 and 1.1.1.3 to the public network address.

```
Device(config)#ip nat inside source list 1001 interface gigabitethernet1 overload
```

#Configure a gateway route to gateway 192.168.202.254.

```
Device(config)#ip route 0.0.0.0 0.0.0.0 192.168.202.254
```

Step 3: Configure CCF keyword rules to filter and desensitize mail.

#Configure CCF keyword rule 1, which is used to block users sending mail from "hello1".

```
Device(config)#ccf keyword rule 1
Device(config-ccf-keyword-rule)#l4 protocol tcp
Device(config-ccf-keyword-rule)#base-application smtp position subheader from
Device(config-ccf-keyword-rule)#keyword text hello1
Device(config-ccf-keyword-rule)#exit
```

#Configure CCF keyword rule 2 to alter the keyword "secret" contained in the subject of the email to "*".

```
Device(config)#ccf keyword rule 2
Device(config-ccf-keyword-rule)#l4 protocol tcp
Device(config-ccf-keyword-rule)#base-application smtp position subheader subject
Device(config-ccf-keyword-rule)#keyword text secret
Device(config-ccf-keyword-rule)#exit inspect ccf-policy mail
Device(config-security-policy)#exit
```

Step 4: Check the result: Verify whether the filtering and altering of the CCF keyword rule takes effect.

#PC1 user who opens Foxmail logs into mail account (taking the account hello1@dpi.com as an example) to forward by Device. Send one mail to other users, match the CCF keyword rule 1,hit the CCF policy mail, and you can see that there are data log records on the serial port of Device, the action is deny, the log type is level-4 log: warnings, and the e-mail sending fails.

```
May 20 2020 18:26:28 Device MPU0 %DPI-CCF-4:Protocol:tcp, source ip: 1.1.1.2,, source port:55803, destination ip: 112.97.36.72, destination port:25, hit the ccf policy mail, rule id: 1, action: deny.
```

#PC2 user who opens Foxmail logs into mail account (taking the account hello2@dpi.com as an example) to forward by Device. Send one mail whose subject contains secret to other users (such as hello3@dpi.com) , match the CCF keyword rule 2,hit the CCF policy mail, execute the replace action, and the log type is level-5 log: notifications. The printed data log is as follows:

```
May 20 2020 18:28:22 Device MPU0 %DPI-CCF-5:Protocol:tcp, source ip: 1.1.1.2,, source port:55803, destination ip: 112.97.36.72, destination port:25, hit the ccf policy mail, rule id: 2, action: replace.
```

#On the user hello3@dpi.com for receiving the mail, you can verify that “secret” in the subject of the received mail sent by hello2@dpi.com is altered to ******.

12.3.8. Configure CCF Event Rule Filtering

Network Requirements

- PC1 and PC2 are the internal host, the Mail Server is the mail server on the public network, and Device is the NAT device. The internal source NAT dynamic port conversion is configured, and the IP route is reachable;
- The event filtering function of CCF is configured on the device to filter specific mails (total mail size, number of attachments carried).

Network Topology

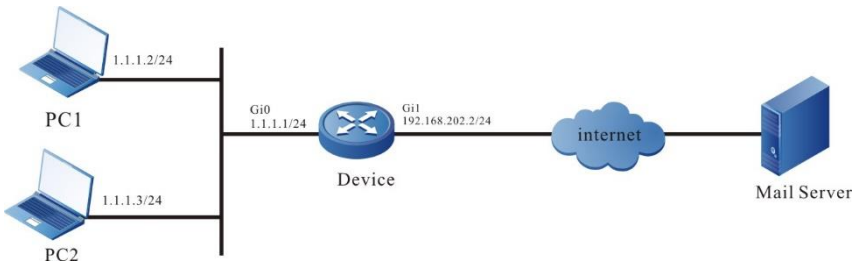


Figure 12-8 Networking of configuring CCF mail filtering

Configuration Steps

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

Step 2: Configure internal source NAT dynamic port conversion, and configure route to ensure that the PC can be connected to the external network.

#Configure the interface gigabitethernet0 as the inside interface of NAT.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0
Device(config-if-gigabitethernet0)#ip nat inside
Device(config-if-gigabitethernet0)#exit
```

#Configure the interface gigabitethernet1 as the outside interface of NAT.

```
Device(config)#interface gigabitethernet 1
Device(config-if-gigabitethernet1)#ip nat outside
Device(config-if-gigabitethernet1)#exit
```

#Configure the ACL 1001, only permitting the PCs in the 1.1.1.0/24 network segment of the internal private network to access the web server.

```
Device(config)#ip access-list extended 1001
Device(config-ext-nacl)#10 permit ip 1.1.1.0 0.0.0.255 any
Device(config-ext-nacl)#exit
```

#Configure the internal source NAT dynamic port conversion rules to convert the internal private network address 1.1.1.2 and 1.1.1.3 to the public network address.

```
Device(config)#ip nat inside source list 1001 interface gigabitethernet 1 overload
```

#Configure a gateway route to gateway 192.168.202.254.

```
Device(config)#ip route 0.0.0.0 0.0.0.0 192.168.202.254
```

Step 3: Configure CCF event rules to realize mail control function.

#Configure CCF event rule 1. The mail filtering rule is that the total mail capacity is greater than 5M and the number of attachments is greater than 3.

```
Device(config)# ccf event rule 1
Device(config-ccf-event-rule)#mail size threshold 5
Device(config-ccf-event-rule)#mail attachment threshold 3
Device(config-ccf-event-rule)#exit
```

#Configure CCF policy as mail, policy action as deny, and record log type as warnings.

```
Device(config)#ccf policy mail
Device(config-ccf-policy)#rule 1 action deny logging security-data warnings
Device(config-ccf-policy)#exit
```

#Configure the security policy to reference the CCF application policy mail.

```
Device(config)#security policy 1
Device(config-security-policy)#action inspect ccf-policy mail
Device(config-security-policy)#exit
```

Step 4: Check the result: Verify whether the event filtering rules of CCF take effect.

#When a user of PC1 sends an email with four attachments and a total size of 6M to other users through Device forwarding, it matches CCF event rule 1, hits CCF policy mail, and you can see that there are data log records on the serial port of Device, the action is deny, and the log type is level-4 log: warnings.

```
May 20 2020 18:26:28 Device MPU0 %DPI-CCF-4:Protocol:tcp, source ip: 1.1.1.2,, source port:55803, destination ip: 112.97.36.72, destination port:25, hit the ccf policy mail, rule id: 1, action: deny.
```

#When a user of PC2 sends an email with 3 attachments and a total size of 4M to other users through Device forwarding, it will not match CCF event rule 1, execute the default permit action, and will not print the data log.

13. ASPF

13.1. Overview

ASPF is the abbreviation of Advanced Stateful Packet Filter. Its main functions include the detection of application layer protocol, transport layer protocol, ICMP error message and TCP connection header packet, and dynamically determine whether packets are allowed to enter the internal network through the firewall according to the detection results. At the network edge, ASPF can provide more comprehensive and practical security policies for the enterprise internal network.

13.2. ASPF Function Configuration

Table 13-1 ASPF function configuration list

Configuration Task	
Configure the ASPF policy function	Create the ASPF policy
	Enable the ICMP error packet dropping function in the ASPF policy
	Enable the non-SYN TCP header packet dropping function in the ASPF policy
	Enable the FTP multi-channel protocol detection function in the ASPF policy

13.2.1. Configure ASPF Policy Function

The ASPF policy supports detecting the packets of the following three protocol states, and blocking or releasing them according to the detection:

1. The current packet is ICMP error packet, which can be configured to be discarded to prevent attacks;
2. The current packet is a non-SYN TCP header packet, which can be configured to be discarded to prevent attacks;
3. The current packet is an FTP protocol packet, which can be configured to be released to avoid being misidentified as unsafe packets.

Configuration Conditions

None

Create ASPF Policy

Table 13-2 Create the ASPF policy

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Create the ASPF polic	**aspf policy** *policy-id*	Mandatory

Enable ICMP Error Packet Dropping Function in ASPF Policy

Table 13-3 Enable the ICMP error packet dropping function in the ASPF policy

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the ASPF policy view	**aspf policy** *policy-id*	Mandatory
Enable the ICMP error packet dropping function	**icmp error drop**	Mandatory

Enable Non-SYN TCP Header Packet Dropping Function in ASPF Policy

Table 13-4 Enable non-SYN TCP header packet dropping function in the ASPF policy

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the ASPF policy view	**aspf policy** *policy-id*	Mandatory
Enable non-SYN TCP header packet dropping function in the ASPF policy	**tcp syn-check**	Mandatory

Enable FTP Multi-channel Protocol Detection Function in ASPF Policy

Table 13-5 Enable the FTP multi-channel protocol detection function in the ASPF policy

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the ASPF policy view	**aspf policy** *policy-id*	Mandatory
Enable the FTP multi-channel protocol detection function in the ASPF policy	**detect ftp**	Mandatory

13.2.2. ASPF Monitoring and Maintaining

Table 13-6 ASPF Monitoring and Maintaining

Command	Description
show aspf policy [*policy-id* | **all**]	Display the ASPF policy information
debug aspf {error | message |packet| all}	Enable the ASPF debugging switch

13.3. ASPF Typical Configuration Example

13.3.1. Configure TCP Non-SYN Header Packet and ICMP Error Packet Detection

Network Requirements

- Device is the edge device connecting the internal network and the external network. Local users PC1 and PC2 in the internal network access the server on the public network. Configure the ASPF policy on Device, add the device packet input interface Gi0 to the security domain with high security level, and the output interface GI1 to the security domain with low security level. ASPF and the security domain work together. The packets between the security domains are security checked by the security policy to realize the functions of ICMP error packet detection and TCP non-syn header packet discarding.

Network Topology

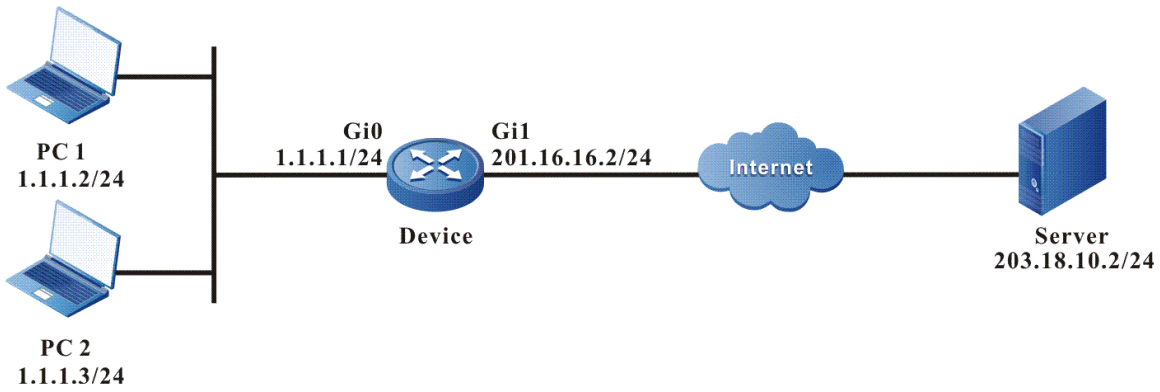


Figure 13-1 Networking of configuring TCP non-SYN header packet and ICMP error packet detection

Configuration Steps

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

Step 2: Configure the ASPF policy.

#Enable the ICMP error packet dropping function.

```
Device#configure terminal
Device(config)#aspf policy 1
Device(config-aspf-policy)#icmp error drop
Device(config-aspf-policy)#exit
```

#Enable TCP non-syn header packet detection function.

```
Device(config)# aspf policy 1
Device(config-aspf-policy)#tcp syn-check
Device(config-aspf-policy)#exit
```

Step 3: Configure the security policy and security domain.

#Configure the source security domain object zone1 and destination security domain object zone2.

```
Device(config)# security zone name zone1
Device(config-security-zone)#import interface gigabitethernet 0
Device(config-security-zone)#priority 80
Device(config-security-zone)#exit
Device(config)# security zone name zone2
Device(config-security-zone)#import interface gigabitethernet 1
Device(config-security-zone)#priority 60
Device(config-security-zone)#exit
```

#Configure the security policy to match the source security domain zone1 and the destination security domain zone2. The action is inspect aspf policy.

```
Device(config)#security policy 1
Device(config-security-policy)#match source security-zone zone1
Device(config-security-policy)#match destination security-zone zone2
Device(config-security-policy)#action inspect aspf-policy 1
Device(config-security-policy)#exit
```

Step 4: Check the result:

#View the ASPF configuration information of policy 1.

```
Device#show aspf policy 1
ASPF policy configuration:
Policy Id: 1
Policy description:
TCP SYN packet check: Enable
ICMP error message check: Enable
Inspected protocol:
```

#When the internal private networks PC1 and PC2 access the external network Server, Device can identify the forged ICMP error packet and discard it to avoid the malicious attack of ICMP, and the TCP header of non-syn packet will also be discarded.

#All kinds of connection packets from the external network cannot enter the internal network.

13.3.2. Configure ASPF to Enable ftp Data Channel Detection

Network Requirements

- Device is the edge device connecting the internal network and the external network. Local user PC in the internal network accesses the ftp server on the public network. Configure the ASPF policy on Device, add the device packet input interface Gi0 to the security domain with high security level, and the output interface Gi1 to the security domain with low security level. ASPF and the security domain work together. The packets between the security domains are security checked by the security policy to realize the ftp multi-channel protocol detection function.

Network Topology

Figure 13-2 Networking of configuring ASPF to enable ftp data channel detection

Configuration Steps

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

Step 2: Configure ASPF policy to enable the ftp data channel detection function.

```
Device#configure terminal
```

```
Device(config)#aspf policy 1
Device(config-aspf-policy)#detect ftp
Device(config-aspf-policy)#exit
```

Step 3: Configure the security policy and security domain.

#Configure the source security domain object zone1 and destination security domain object zone2.

```
Device(config)# security zone name zone1
Device(config-security-zone)#import interface gigabitethernet 0
Device(config-security-zone)#priority 80
Device(config-security-zone)#exit
Device(config)# security zone name zone2
Device(config-security-zone)#import interface gigabitethernet 1
Device(config-security-zone)#priority 60
Device(config-security-zone)#exit
```

#Configure the security policy to match the source security domain zone1 and the destination security domain zone2. The action is inspect aspf policy.

```
Device(config)#security policy 1
Device(config-security-policy)#match source security-zone zone1
Device(config-security-policy)#match destination security-zone zone2
Device(config-security-policy)#action inspect aspf-policy 1
Device(config-security-policy)#exit
```

Step 4: Check the result:

#View the ASPF configuration information of policy 1.

```
Device#show aspf policy 1
ASPF policy configuration:
Policy Id: 1
Policy description:
TCP SYN packet check: Disable
ICMP error message check: Disable
Inspected protocol:
ftp
```

#The internal private network PC transmits data through FTP from the interface of the security domain with high security level to the server of the interface of the security domain with low security level, uploads and downloads files successfully, and the expected connection of the data channel is established correctly.

```
Device#show connection ipv4 table
IPV4 connection table
```

```
Protocol  Source:port          Destination:port/other   State        Lifetime  Vrf
--------  --------------------  ----------------------   -------------  ----
----  --------
TCP       [1.1.1.2]:4945        [203.18.10.2]:21         tcp-time-wait    0      global
TCP       [203.18.10.2]:20      [1.1.1.2]:4946           tcp-time-wait    0      global
```

#The internal private network PC adopts the PASV mode to transmit data through FTP from the interface of the security domain with high security level to the server of the interface of the security domain with low security level, uploads and downloads files successfully, and the expected connection of the data channel is established correctly.

```
Device#show connection ipv4 table
IPV4 connection table
Protocol  Source:port          Destination:port/other   State        Lifetime  Vrf
--------  --------------------  ----------------------   -------------  ----
----  --------
TCP       [1.1.1.2]:49320       [203.18.10.2]:21         tcp-time-wait   79     global
TCP       [1.1.1.2]:38805       [203.18.10.2]:11656      tcp-time-wait   79     global
```

#The packets that initiate various connections from the external network cannot enter the internal network.

14. SECP

14.1. Overview

SECP is the abbreviation of security policy. Its function is to control the traffic forwarding and content security integrated detection of traffic. It can match a class of traffic by configuring broader security policy conditions, and then ensure network security through various content security functions.

14.2. SECP Function Configuration

Table 14-1 SECP function configuration list

Configuration Task	
Configure the security domain function	Create security domain
	Add interfaces in the security domain
	Configure the security level of the security domain
Configure the security policy function	Create security policy
	Configure security policy to match source domain
	Configure security policy to match destination domain
	Configure security policy to match the service or service group
	Configure the security policy to match time domain
	Configure the security policy to match source IP
	Configure the security policy to match destination IP
	Configure the action of the security policy
	Configure the description information of the security policy

14.2.1. Configure Security Domain Function

Security domain is a logical concept used to manage multiple interfaces with the same security requirements on firewall devices. At present, SECP can configure custom security domains and also provide the following four default security domains:

Untrust: usually used to define insecure networks such as the Internet. The security level is 5 and cannot be modified.

DMZ: DMZ (demilitarized zone) originated from the military. It is an area with partial control between strict military control area and loose public area. It refers to a security zone that is logically and physically separated from the internal network and the external network. It is usually used to define the area where the intranet server is located. Although this device is deployed in the intranet, it often needs to be accessed by the external network, which has great security risks. At the same time, it is generally not allowed to actively access the external network, so its security level is lower than that of trust, However, in the security zone higher than untrust, the security level is 50 and cannot be modified.

Trust: usually used to define the area where intranet end users are located. The security level is 85 and cannot be modified.

Local: The local area defines the device itself. All messages constructed and actively sent by the equipment can be considered to be sent from the local area. All messages requiring equipment response and processing (not only detection or direct forwarding) can be considered to be accepted by the local area. The security level is 100 and cannot be modified.

Configuration Conditions

None

Create Security Domain

Table 14-2 Create security domain

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create security domain	**security zone name** *zone-name*	Mandatory

Add Interfaces in Security Domain

Table 14-3 Add interfaces in the security domain

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the security domain view	**security zone name** *zone-name*	*zone-name* is the specified security domain.

Step	Command	Description
Add interfaces in the security domain	**import interface** *interface-name*	Mandatory

Note:

- One interface can only be added to one security domain.

Configure Security Level in Security Domain

Table 14-4 Configure the security level in the security domain

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the security domain view	**security zone name** *zone-name*	*zone-name* is the specified security domain name
Configure the security level in the security domain	**priority** *security-priority*	Mandatory

14.2.2. Configure Security Policy Function

Configuration Conditions

None

Create Security Policy

Table 14-5 Create the security policy

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create security policy	**security policy** *policy-id*	Mandatory

Note:

- The value of policy-id determines the priority of the security policy. The smaller the value, the higher the priority. When multiple security policies hit at the same time, select the security policy with higher priority to perform its actions.

Configure Security Policy to Match Source Domain

Table 14-6 Configure the security policy to match source domain

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the security policy view	**security policy** *policy-id*	*policy-id* is the ID of the specified security policy
Configure the security policy to match source domain	**match source security-zone** *zone-name*	Mandatory By default, the match item is any.

Note:

- The source domain is the source security domain. It is used to manage multiple input interfaces with the same security requirements.
- By default, the matching item is "any", indicating that the security policy does not care about the matching item. By default, the matching is successful.
- When the configured source domain does not exist, the item will fail to match and the security policy will not hit.

Configure Security Policy to Match Destination Domain

Table 14-7 Configure the security policy to match destination domain

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the security policy view	**security policy** *policy-id*	*policy-id* is the ID of the specified security policy
Configure the security policy to match destination domain	**match destination security-zone** *zone-name*	Mandatory By default, the match item is any.

Note:

- The destination domain is the destination security domain. It is used to manage multiple output interfaces with the same security requirements.
- By default, the matching item is "any", indicating that the security policy does not care about the matching item. By default, the matching is successful.

- When the configured destination domain does not exist, the item will fail to match and the security policy will not hit.

Configure Security Policy to Match Service or Service Group

Service is an application protocol type determined by the rules of protocol type and port number. It is a collection of one or several rules. A service group is a collection of services and service groups.

Table 14-8 Configure the security policy to match service or service group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the security policy view	**security policy** *policy-id*	*policy-id* is the ID of the specified security policy
Configure the security policy to match service or service group	**match { service** *service-name* **| service-group** *group-name***}**	Optional By default, the match item is any.

Note:

- By default, the matching item is "any", which means that the security policy does not care about the matching item. By default, the matching is successful.
- When the configured service or service group does not exist, the item will fail to match and the security policy will not hit.

Configure Security Policy to Match Time Domain

Table 14-9 Configure the security policy to match time domain

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the security policy view	**security policy** *policy-id*	*policy-id* is the ID of the specified security policy
Configure the security policy to match time domain	**match time-range** *time-name*	Mandatory

Note:

- By default, the security policy does not care about the matching item. By default, the matching is successful.
- When the configured time domain does not exist, the item will fail to match and the security policy will not hit.

Configure Security Policy to Match Source IP

Table 14-10 Configure the security policy to match source IP

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the security policy view	**security policy** *policy-id*	*policy-id* is the ID of the specified security policy
Configure the security policy to match source IP	**match source-ip** *ip-address* **mask** *masklen*	Mandatory

Note:

- By default, the security policy does not care about the matching item. By default, the matching is successful.

Configure Security Policy to Match Destination IP

Table 14-11 Configure the security policy to match destination IP

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the security policy view	**security policy** *policy-id*	*policy-id* is the ID of the specified security policy
Configure the security policy to match destination IP	**match destination-ip** *ip-address* **mask** *masklen*	Mandatory

Note:

- By default, the security policy does not care about the matching item. By default, the matching is successful.

Configure the Action of Security Policy

When configuring security policy actions, you can reference the packet depth detection function provided by the DPI module, namely avc policy, url policy, and aspf policy.

AVC is the abbreviation of Application Visible and Control. AVC policy can perform idepth detection and corresponding processing actions of the packet for different applications.

URL is short for Uniform Resource Locator. URL policy is used to control the URL accessed, that is, to allow or prohibit users from accessing web resources. It only supports URL filtering based on HTTP protocol.

ASPF is the abbreviation of Advanced Stateful Packet Filter. Its main functions include the detection for application layer protocol, transport layer protocol, ICMP error packet and TCP connection header packet, and dynamically determine whether packets are allowed to enter the internal network through the firewall according to the detection results.

Table 14-12 Configure the action of the security policy

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the security policy view	**security policy** *policy-id*	*policy-id* is the ID of the specified security policy
Configure the action of the security policy	**action {{permit | deny} [logging security-data { warnings | notifications | informational }] | inspect { avc-policy** *avc_policy_name* **| url-policy** *url_policy_name* **| aspf-policy** *aspf_policy_id* **}*}**	Optional By default, the item is permit.

Note:

- By default, this item is "permit", that is, the packet is released.
- When the configured action inspect object does not exist, it is equivalent to the default state. Otherwise, the detection of existing objects (url policy, avc policy or aspf policy) will continue.

14.2.3. SECP Monitoring and Maintaining

Table 14-13SECP monitoring and maintaining

Command	Description
show security statistics	Display all statistics information of SECP
clear security statistics	Clear all statistics information of SECP
debug security {all | message | packet}	Display the SECP debug information

14.3. SECP Typical Configuration Example

14.3.1. Configure SECP to Match Multiple Objects

Network Requirements

- PC1 and PC2 are internal hosts, Web Server is a web server on the public network, and Device is a NAT device. Configure internal source NAT dynamic port conversion, and IP route is reachable.
- Configure time domain objects, source and destination security domain objects and service objects on Device. Use SECP security policy 1 to match these objects, the action is deny, and the record log type is informational; Using SECP security policy 2, these objects do not match, the action is permit, and the log type is notifications, so as to discard or release specific connection packet.
- The packet sent by PC1 matches the security policy 1. The packet sent by PC2 matches the security policy 2.

Network Topology

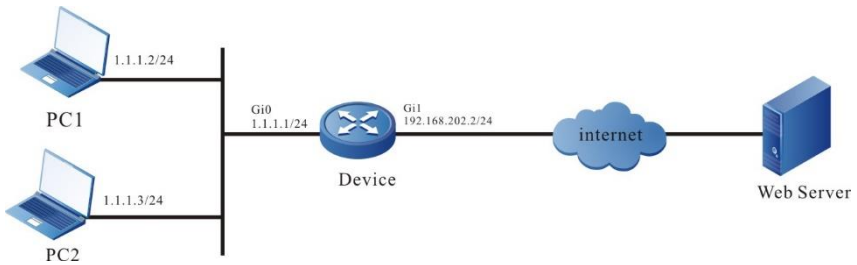


Figure 14-1 Networking of configuring secp to match multiple objects

Configuration Steps

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

Step 2: Configure internal source NAT dynamic port conversion, and configure route to ensure that the PC can be connected to the external network.

#Configure the interface gigabitethernet0 as the inside interface of NAT.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0
```

```
Device(config-if-gigabitethernet0)#ip nat inside
Device(config-if-gigabitethernet0)#exit
```

#Configure the interface gigabitethernet1 as the outside interface of NAT.

```
Device(config)#interface gigabitethernet 1
Device(config-if-gigabitethernet1)#ip nat outside
Device(config-if-gigabitethernet1)#exit
```

#Configure the ACL 1001, only permitting the PCs in the 1.1.1.0/24 network segment of the internal private network to access the web server..

```
Device(config)#ip access-list extended 1001
Device(config-ext-nacl)#10 permit ip 1.1.1.0 0.0.0.255 any
Device(config-ext-nacl)#exit
```

#Configure the internal source NAT dynamic port conversion rules to convert the internal private network address 1.1.1.2 and 1.1.1.3 to the public network address.

```
Device(config)#ip nat inside source list 1001 interface gigabitethernet 1 overload
```

#Configure a gateway route to gateway 192.168.202.254.

```
Device(config)#ip route 0.0.0.0 0.0.0.0 192.168.202.254
```

Step 3: Configure SECP to match multiple objects.

#Configure the time domain object 1.

```
Device(config)#time-range 1
Device(config-time-range)#periodic monday to friday
Device(config-time-range)#exit
```

#Configure source security domain object 1 and destination security domain object 2.

```
Device(config)#security zone name 1
Device(config-security-zone)#priority 1
Device(config-security-zone)#import interface gigabitethernet 0
Device(config-security-zone)#exit
Device(config)#security zone name 2
Device(config-security-zone)#priority 1
Device(config-security-zone)#import interface gigabitethernet 1
Device(config-security-zone)#exit
```

#Configure service object 1.

```
Device(config)#ip object-service 1
Device(config-object-service)#protocol tcp source-port 1 to 65535 destination-port 80 to 80
Device(config-object-service)#exit
```

#Configure security policy 1 to match the above objects, configure the action of security policy 1 as deny, and record the log as warnings; Security policy 2 does not match the above objects. Configure the action of security policy 2 as permit and record the log as notification.

```
Device(config)#security policy 1
Device(config-security-policy)#match time-range 1
Device(config-security-policy)#match source security-zone 1
Device(config-security-policy)#match destination security-zone 2
Device(config-security-policy)#match object-service 1
Device(config-security-policy)#action deny logging security-data  warnings
Device(config-security-policy)#exit
Device(config)#security policy 2
Device(config-security-policy)#action permit logging security-data  notifications
Device(config-security-policy)#exit
```

Step 4: Check the result: Verify whether SECP matching multiple objects takes effect.

#When the time domain object matched by PC1 fails, the security domain object matches, and the service object matches, the flow with the sending protocol of TCP and the destination port of 80 can successfully match the action deny of SECP security policy 1, and you can see that there are data log records on the serial port of Device, the action is deny, and the log type is level-4 log: warnings.

```
Sep 21 2019 03:52:54 Device LPU0 %SECP-SECP-4:Pkt from gigabitethernet0 to gigabitethernet1 (protocol:tcp,source-ip:1.0.0.103,destination-ip:116.211.153.241,source-port:65129,destination-port:80) hit the security policy 1, action: deny.
```

#When the time domain object matched by PC2 fails, or the security domain does not match, or the service object does not match, the flow with the sending protocol of UDP and the destination port of non-80 can successfully match the action pertmit of SECP security policy 2, and you can see that there are data log records on the serial port of Device, the action is permit, and the log type is level-5 log: notifications.

```
Sep 21 2019 03:53:12 Device LPU0 %SECP-SECP-5:Pkt from any to any (protocol:udp,source-ip:1.1.1.3,destination-ip:121.10.140.89,source-port:53594,destination-port:8270) hit the security policy 2, action: permit.
```

15. ATTACK DEFENSE

15.1. Overview

Attack defense is an important function to maintain network security. It judges whether the packet has attack characteristics by analyzing the packet content passing through the device, and implements certain preventive measures for the packet with attack characteristics according to the configuration, such as intercepting the attack packet, recording the attack packet log, adding the attack source to the blacklist, etc. By configuring the attack defense function on the device, on the one hand, it can avoid the abnormality of the device due to network attack and improve the anti-attack ability of the device; On the other hand, it can intercept the attack traffic forwarded by the device to prevent other devices on the network from working normally due to attacks.

15.2. Attack Defense Function Configuration

Table 15-1 Attack defense function configuration list

Configuration Task	
Configure single-packet attack defense function	Configure intercepting fraggle, fragment, frag-icmp, icmpv4-large, icmpv6-large, ping-of-death, smurf, src-dst-ip-equal, src-dst-mac-equal, src-ddst-port-equal, tcp-flag-seq-zero, tcp-hdr-incomplete, tcp-invalid-flags, tcp-land, tcp-syn-fin, teardrop, snork, udp-bomb, winnuke, traceroute, ip-option-source-route, ip-option-route-record, ip-option-time-stamp, icmp-redirect, icmp-unreachable, icmp-echoreply, icmp-sourcequench, icmp-echo, icmp-routeradvert, icmp-routersolicit, icmp-timxceed, icmp-paramprob, icmp-tstamp, icmp-tstampreply, icmp-ireq, icmp-ireqreply, icmp-maskreq, icmp-maskreply, icmpv6-unreachable, icmpv6-packetbig, icmpv6-timxceed, icmpv6-paramprob, icmpv6-echo, icmpv6-echoreply, icmpv6-routersolicit, icmpv6-routeradvert, icmpv6-neighborsolicit, icmpv6-neighboradvert, icmpv6-redirect, smac-zero, small-packet attack packets
Configure flood attack defense function	Configure to intercept the flood attack packets of tcp syn, tcp syn-ack, tcp ack, tcp fin, tcp rst, udp, icmp, icmpv6, dns, http types

Configuration Task	
Configure scan attack defense function	Configure to intercept the attack packets of IP scanning and port scanning
Configure URPF attack defense function	Configure the URPF check function
Configure the blacklist function	Configure the blacklist function to discard the packets of the corresponding source address

15.2.1. Configure Single-packet Attack Defense Function

Single-packet attack defense refers to judging whether the packet is aggressive by analyzing the characteristics of the packet passing through the device. Generally, it is only effective for the incoming packet with attack defense policy. After the single-packet attack defense function is configured, if the device detects that a packet is aggressive, it will output an alarm log, discard the packet, and make packet discarding statistics.

Configuration Conditions

None

Configure to Intercept Different Kinds of Single-packet Attack Defense Function

When an aggressive packet of the configured type is detected, the packet will be discarded and the discarded packet statistics will be carried out.

Table 15-2 Configure the single-packet attack

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure to intercept the specified type of single packet attack packet	**anti-attack detect { fraggle | fragment | frag-icmp | icmp-large [***max-length***] | icmpv6-large [***max-length***] | ping-of-death | src-dst-ip-equal | src-dst-mac-equal | src-dst-port-equal | smurf | tcp-flag-seq-zero | tcp-hdr-incomplete | tcp-invalid-flags | tcp-land | tcp-syn-fin | tear-drop | udp-snork | udp-bomb | winnuke | traceroute | ip-option-source-route | ip-option-record-route | ip-option-time-stamp | icmp-redirect | icmp-unreachable | icmp-echoreply | icmp-sourcequench | icmp-echo | icmp-routeradvert | icmp-routersolicit | icmp-timxceed | icmp-paramprob | icmp-tstamp | icmp-tstampreply | icmp-ireq | icmp-ireqreply | icmp-maskreq | icmp-maskreply | icmpv6-unreachable | icmpv6-packetbig | icmpv6-timxceed | icmpv6-paramprob | icmpv6-echo | icmpv6-echoreply | icmpv6-routersolicit | icmpv6-routeradvert | icmpv6-neighborsolicit | icmpv6-neighboradvert | icmpv6-redirect | smac-zero | small-packet [***mini-length***] }**	Mandatory The default value of *max-length* is 512. The default value of *mini-length* is 64. By default, the detection for the packet with the feature is not enabled.

Configure Single-packet Attack Defense Log Record

When the device detects the single-packet attack, it discards the packet and logs it at the same time.

Table 15-3 Configure the single-packet attack log output

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure to output the single-packet attack log	**attack-defense action logging detect**	Mandatory By default, do not enable the single-packet attack defense log.

15.2.2. Configure Flood Attack Defense Function

Flood attack is mainly used to protect the server from the impact of large traffic packets. It is generally applied to the interface of the device connected to the external network, and is only effective for the incoming packet on the interface with attack defense policy. After the flooding attack defense policy is applied to the interface, the interface is in the attack detection state. When it detects that the rate of a certain type of packets continues to exceed the specified trigger threshold, it considers that the interface has been flooded, enters the attack defense state, and starts the corresponding defense policy according to the configuration (output the alarm log, discard the packet, and add the attack source to the dynamic blacklist, where the blacklist takes effect after the traceability function is configured). When the device detects that the packet traffic of this type is lower than the threshold for 5 seconds, release the attack state and stop executing attack defense measures.

Configuration Conditions

- It is necessary to configure the attack defense policy, and configure the flood attack defense in the policy configuration mode.
- It is necessary to apply the attack defense policy to enable the flood attack defense detection in the policy.

Configure to Intercept Different Kinds of Flood Attack Defense

When the packet configured with flood detection type exceeds the threshold, take the corresponding preventive measures.

Table 15-4 Configure the flood attack defense

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the policy configuration mode	**attack-defense policy** *policy*	Mandatory Defense policies are distinguished by the policy name.
Configure flood detection type and defense action	**detect { tcp-syn | tcp-ack | tcp-syn-ack | tcp-fin | tcp-rst | udp | icmp | icmpv6 | dns | http } flood threshold** *threshold-value* **action { drop | blacklist }***	Mandatory By default, the corresponding type of flood attack detection is not enabled.

Configure Backtracking Attack Source Function during Flood Attack Detection

Trace the source of packets configured with flood attack defense type, and count the number of packets based on each source address.

Table 15-5 Configure the flood attack defense tracking function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the policy configuration mode	**attack-defense policy** *policy*	Mandatory
Configure the flood attack defense tracking function	**trace-type {source-ip | source-mac} max-count** *max-source-number*	Mandatory By default, the single source threshold is not checked according to the source address *max-source-number* configures the number of flood detection traceability. The source address nodes exceeding the number of traceability will not be traced

Configure to Apply Attack Defense Policy Globally

The configuration of flooding attack is implemented based on policy, and the configuration takes effect when the policy is applied.

Table 15-6 Configure to apply the attack defense policy globally

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure to apply the attack defense policy globally	**attack-defense global apply policy** *policy-name*	Mandatory By default, no attack defense policies are applied globally.

Configure to Apply Attack Defense Policy in the Interface

The configuration of flooding attack is based on policy, and the configuration takes effect when the policy is applied. The policy can be applied separately based on the interface. If the global applied policy and the configuration under the interface exist at the same time, the configuration under the interface takes precedence.

Table 15-7 Configure to apply the attack defense policy in the interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the interface to apply the attack defense policy	**attack-defense apply policy** *policy-name*	Mandatory By default, the interface does not apply the policy separately.

Configure Flood Attack Defense Log Records

When the device detects a flood attack, it takes defense policy and records the log at the same time.

Table 15-8 Configure to output flood attack logs

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure to output flood attack logs	**attack-defense action logging flood**	Mandatory By default, do not enable the flood attack defense log.

15.2.3. Configure Scan Attack Defense Function

Scanning attack defense mainly detects the detection behavior of network users by monitoring the rate of connection to the target system to prevent them from detecting the network state. It is generally applied to the interface of the device connected to the external network, and is only effective for the incoming packets on the interface where the attack defense policy is applied.

After scanning attack defense is configured, when the number of IPs accessed in the network or the number of ports accessed on a device exceeds the threshold, it is considered that a scanning attack has occurred in the network, the attack source is automatically detected and added to the dynamic blacklist, and the scanning attack defense log is output according to the configuration.

Configuration Conditions

- The attack defense policy needs to be configured. Scan the attack defense configuration in the policy configuration mode.
- Attack defense policy needs to be applied to enable scanning attack defense detection in the policy.

Configure Scanning Attack Defense Function

When the scan attack defense level is configured and the number of accessed destination addresses or ports of a destination address in the network exceeds the threshold, the scanning attack log is output or the attack source is added to the blacklist according to the configuration.

High indicates high-level defense, the number of destination IP addresses allowed to be accessed at the same time is 16, and the number of ports allowed to be accessed at the same destination address is 4; Medium refers to medium level defense, the number of destination IP addresses allowed to be accessed at the same time is 32, and the number of ports allowed to be accessed at the same destination address is 8; Low indicates low-level defense, the number of destination IP addresses allowed to be accessed at the same time is 64, and the number of ports allowed to be accessed at the same destination address is 16.

Table 15-9 Configure scanning attack defense function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Step	**Command**	**Description**
Enter the policy configuration mode	**attack-defense policy** *policy*	Mandatory
Configure scanning attack defense function	**detect scan level {high | medium | low} action blacklist**	Mandatory By default, do not enable the scanning attack detection.

Configure Scan Attack Defense Log Records

Record the log when the device detects a scan attack.

Table 15-10 Configure to output the scan attack log

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure to output the scan attack log	**attack-defense action logging scan**	Mandatory By default, do not enable scan attack defense log.

15.2.4. Configure URPF Attack Defense Function

URPF is a unicast reverse path forwarding technology, used to prevent attacks based on source address spoofing, such as DoS (denial of service) attacks based on source address spoofing and DDoS (distributed denial of service) attacks.

Configuration Conditions

- You need to enable the URPF function globally to make the URPF detection effective.

Configure Global URPF Function

After enabling the URPF function globally, the URPF function on the interface can take effect.

Table 15-11 Configure the global URPF function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the global URPF function	**ip urpf**	Mandatory By default, do not enable the URPF function globally.

Configure URPF Searching Default Route Function

When URPF finds the source route, it releases the packet that finds the source route as the default route by enabling the default route function.

Table 15-12 Configure URPF to permit default route

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure URPF to permit the default route	**ip urpf allow-default-route**	Mandatory By default, do not enable the function of checking the default route.

Configure URPF in Interface

URPF supports strict and loose modes. In the loose mode, URPF searches the route table for the source address of the received packet. If a route is found, the packet is allowed to pass through; In strict mode, the packet is allowed to pass only when the route is found and the outgoing interface is the same as the receiving interface of the packet.

Configure the URPF associated ACL under the interface. When the packet comes, check the URPF first. If the URPF check result is release, the packet will be released no matter whether the network segment matching the URPF associated ACL is permit or deny. Only the result of the URPF check is discard, then further determine whether the packet is released or discarded according to the permit and deny of the network segment matching the ACL.

Table 15-13 Configure the URPF check on the interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the URPF check on the interface	**ip urpf { loose | strict } [aclv4** *acl-name*] **[aclv6** *aclv6-name*]	Mandatory By default, the interface URPF function is not enabled.

Configure URPF Defense Log Records

When the device detects the URPF attack, perform the log recording.

Table 15-14 Configure the URPF log output

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the URPF log output	**attack-defense action logging urpf**	Mandatory By default, do not enable the URPF attack defense log.

15.2.5. Configure Blacklist Function

Blacklist function is an attack defense feature that filters packets according to the source IP or IPv6 address of the packet. Compared with the packet filtering function based on ACL (access control list), the way of packet matching in blacklist is simpler, which can realize high-speed filtering and effective shielding of packets. Blacklists can be added or deleted dynamically by the device or manually by the user.

Configuration Conditions

None

Configure Static Blacklist

The dynamic blacklist is dynamically added by flood attack defense, scanning attack defense and other functions, and the static blacklist is manually configured by the user. The blacklist on the routing device is implemented by software.

Table 15-15 Configure the static blacklist

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the static blacklist	**blacklist {ip** *ip-address* **| ipv6** *ipv6-address* **}**	Mandatory By default, do not configure the static blacklist.

15.2.6. Attack Defense Monitoring and Maintaining

Table 15-16 Attack defense monitoring and maintaining

Command	Description
clear attack-defense nullscan stastiscs	Clear the NULL SCAN statistics information on all members
clear anti-attack urpf statistic [member *member-ID* | **lpu** *lpu-ID***]**	Clear the URPF statistics information on the member
show anti-attack detect statistic [member *member-ID* | **lpu** *lpu-ID***]**	Display the single-packet attack statistics information
show anti-attack urpf statistic [member *member-ID* | **lpu** *lpu-ID***]**	Display the URPF statistics information
show attack-defense applied policy	Display the current applied attack defense policy
show attack-defense policy [*policy-name***]**	Display the attack defense policy configuration
show attack-defense flood [member *member-ID* | **lpu** *lpu-ID***] [interface** *interface-name***]**	Display the Flood attack defense status

Command	Description
show attack-defense scan { ip-scan | ipv6-scan | port-scan | ipv6-port-scan } [member *member-ID* | **lpu** *lpu-ID*]	Display the scan attack defense status
show attack-defense scan { statistic | ipv6-statistic } [member *member-ID* | **lpu** *lpu-ID*] **interface** *interface-name*	Display the scan attack defense status on the specified interface
show attack-defense trace [member *member-ID* | **lpu** *lpu-ID*] **[interface** *interface-name*]	Display the attack tracing status
show blacklist { ip | ipv6 | config | mac } [member *member-ID* | **lpu** *lpu-ID*]	Display the blacklist information
show attack-defense nullscan stastiscs [member *member-ID* | **lpu** *lpu-ID*]	Display the NULL SCAN statistics information

15.3. Attack Defense Typical Configuration Example

15.3.1. Configure Single-packet Attack Detection

Network Requirements

- The attacker accesses Device via the interface.
- Device configures the single packet attack detection function, alarms when an attack packet is detected, and discards the attack packet. Take the common Smurf attack, land attack and Ping of death attack as examples.

Network Topology

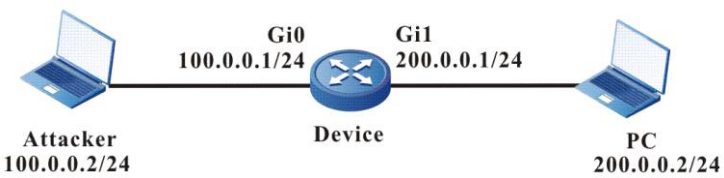


Figure 15-1 Networking of configuring single-packet attack detection

Configuration Steps

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

Step 2: On Device, configure Smurf, Land, Ping of death attack detection function, and enable the single-packet attack log switch.

#Configure the Smurf attack detection.

```
Device#configure terminal
Device(config)#anti-attack detect smurf
```

#Configure the Land attack detection.

```
Device(config)#anti-attack detect tcp-land
```

#Configure Ping of death attack detection.

```
Device(config)#anti-attack detect ping-of-death
```

#On Device, open the single-packet attack log switch.

```
Device(config)#attack-defense action logging detect
```

Step 3: Check the result:

#When the attacker initiates the Smurf, land, Ping of death attacks for the PC, if this function is not configured, the attack packet can be captured on the PC. After configuring this function, the attack packet cannot be captured on the PC, and the log and statistics can be viewed on Device.

#When Device is attacked by Smurf, the following log information is output:

```
%ANTIATTACK-DETECT_ATTACK-4: gigabitethernet0 detect attack, type smurf
```

#When Device is attacked by Land, the following log information is output:

```
%ANTIATTACK-DETECT_ATTACK-4: gigabitethernet0 detect attack, type tcp-land
```

#When Device is attacked by Ping of death, the following log information is output:

```
%ANTIATTACK-DETECT_ATTACK-4: gigabitethernet0 detect attack, type ping-of-death
```

#Execute the **show anti-attack detect statistic** command on Device to view the statistics information of the dropped attack packets.

```
Device#show anti-attack detect statistic
    detect-type            DropCount
    ------------------------------------------------
    fraggle                0
    fragment               0
    frag-icmp              0
    ping-of-death          125
    smurf                  87
    src-dst-ip-equal       0
    src-dst-mac-equal      0
    src-dst-port-equal     0
    tcp-flag-seq-zero      0
    tcp-hdr-incomplete     0
```

tcp-invalid-flag 0
tcp-syn-fin 0
tcp-land 456
tear-drop 0
udp-snork 0
udp-bomb 0
winnuke 0
traceroute 0
icmp-redirect 0
icmp-unreachable 0
icmp-echoreply 0
icmp-sourcequench 0
icmp-echo 0
icmp-routeradvert 0
icmp-routersolicit 0
icmp-timxceed 0
icmp-paramprob 0
icmp-tstamp 0
icmp-tstampreply 0
icmp-ireq 0
icmp-ireqreply 0
icmp-maskreq 0
icmp-maskreply 0
ip-option-source-route 0
ip-option-record-route 0
ip-option-time-stamp 0
icmpv6-unreachable 0
icmpv6-packetbig 0
icmpv6-timxceed 0
icmpv6-paramprob 0
icmpv6-echo 0
icmpv6-echoreply 0
icmpv6-routersolicit 0
icmpv6-routeradvert 0
icmpv6-neighborsolicit 0
icmpv6-neighboradvert 0
icmpv6-redirect 0

```
smac-zero              0
icmp-large             0
icmpv6-large           0
small-packet           0
```

Note:

- The software on the router handles all single-packet attack detection, which takes effect on the forwarded packet and local packet, and has log output and statistical information.
- The hardware processing single-packet attack detection on the switch is effective for both forwarding and local packets, and will not generate logs and statistics; the single packet attack detection processed by the software is only effective for the local packet, with log output and statistical information.
- The interface in the attack detection log output on the router is a L3 interface, and the interface in the attack detection log output on the switch is a L2 port.

15.3.2. Configure flood Attack Detection

Network Requirements

- Device accesses the IP network through gigabitethernet0.
- Device configures the flood attack detection function. When the corresponding characteristic type attack packet is detected, it outputs the alarm log and discards the attack packet. Take common TCP SYN Flood attacks and ICMP flood attacks as examples.

Network Topology

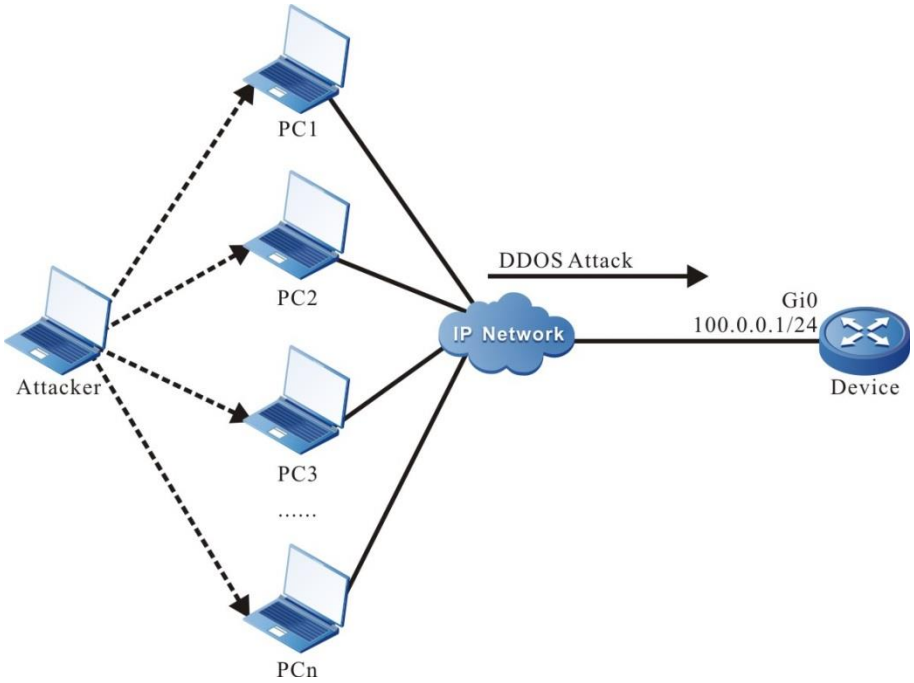


Figure 15-2 Networking of configuring flood attack detection

Configuration Steps

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

Step 2: Configure the attack defense policy a on Device, add the TCP SYN Flood and ICMP flood attack detection functions in the policy, and configure the attack traceability based on IP address.

```
Device(config)#attack-defense policy a
Device(config-anti-policy-a)#detect tcp-syn flood threshold 500 action drop
Device(config-anti-policy-a)#detect icmp flood threshold 500 action blacklist
Device(config-anti-policy-a)#trace-type source-ip max-count 5
Device(config-anti-policy-a)#exit
```

#On Device, globally apply attack defense policy a.

```
Device(config)#attack-defense global apply policy a
```

#On Device, open the flood attack log switch.

```
Device(config)#attack-defense action logging flood
```

Step 3: Check the result:

#View the currently applied attack defense policy on Device.

```
Device#show attack-defense applied policy
attack-defense policy a
 detect tcp-syn flood threshold 500 action drop
 detect icmp flood threshold 500 action blacklist
 trace-type source-ip max-count 5
```

#When an attacker initiates TCP SYN Flood and ICMP flood attacks on Device, view the flood attack log output on Device.

```
%ANTIATTACK-FLOOD_ATTACK-4:gigabitethernet0 detect attack, type tcp-syn.
%ANTIATTACK-FLOOD_IP_ATTACK-4:gigabitethernet0 detect attack, type icmp, ipaddr 100.0.0.2.
```

#View the attack traceability table entry on Device.

```
Device#show attack-defense trace
  Trace Info:
  IpAddr, Interface, LastRecvTime
    Type          DropCount       Token
  ------------------------------------------------------------
 100.0.0.2, gigabitethernet0, Mon May 04 16:55:46 2020
    tcp-syn       , 0             , 299
    icmp          , 0             , 0
 100.0.0.3, gigabitethernet0, Mon May 04 16:55:50 2020
    tcp-syn       , 0             , 250
    icmp          , 0             , 400
 100.0.0.4, gigabitethernet0, Mon May 04 16:55:50 2020
```

```
    tcp-syn       , 0           , 250
    icmp          , 0           , 400
  100.0.0.5, gigabitethernet0, Mon May 04 16:55:50 2020
    tcp-syn       , 0           , 250
    icmp          , 0           , 400
#On Device, view the flood attack defense status information.
Device#show attack-defense flood
  Flood Info:
    Type          DropCount      Token         LastRecvTime
-------------------------------------------------------------------------------
-----------
  gigabitethernet0
    tcp-syn       , 1851        , 50          , Mon May 04 16:55:50 2020
    icmp          , 0           , 100         , Mon May 04 16:55:46 2020
#View the dynamic blacklist items generated by traceability on Device.
Device#show blacklist ip
  Blacklist Info:
  IpAddr,              CreateTime,            Agetime
-----------------------------------------------------------------------
  100.0.0.2          ,    Mon May 04 16:55:47 2020     , 93
```

15.3.3. Configure Scan Attack Detection

Network Requirements

- Device accesses the IP network through gigabitethernet0.
- Device configures the scanning attack detection function, outputs the alarm log when IP scanning or port scanning is detected, adds the attack source to the blacklist, and intercepts all packets of the attack source before the blacklist aging.

Network Topology

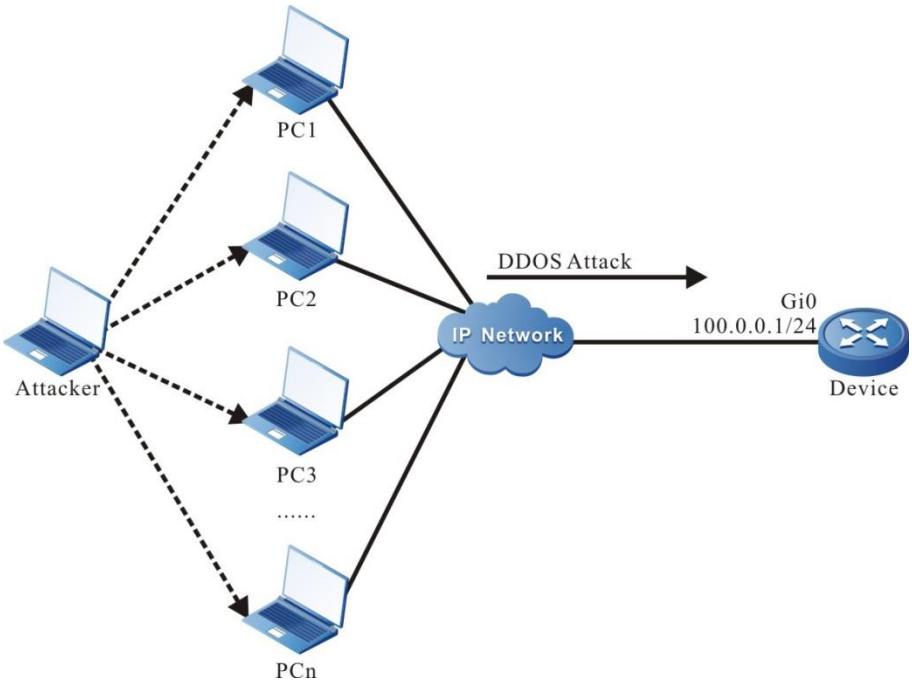


Figure 15-3 Networking of configuring scan attack detection

Configuration Steps

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

Step 2: Configure the attack defense policy a on Device, and configure the scan attack detection function in the policy. The scanning level is high.

```
Device(config)#attack-defense policy a
Device(config-anti-policy-a)#detect scan level high action blacklist
Device(config-anti-policy-a)#exit
```

#On Device, globally apply the attack defense policy a.

```
Device(config)#attack-defense global apply policy a
```

#On Device, open the scan attack log switch.

```
Device(config)#attack-defense action logging scan
```

Step 3: Check the result:

#On Device, view the current applied attack defense policy.

```
Device#show attack-defense applied policy
attack-defense policy a
 detect scan level high action blacklist
```

#When an attacker initiates a scanning attack on Device, view the scanning attack log output on Device.

```
%ANTIATTACK-SCAN_PORT_ATTACK-4:gigabitethernet0 detect port scan attack.
%ANTIATTACK-SCAN_PORT_ATTACK-4:Detect 100.0.0.2 is attacking the system.
```

%ANTIATTACK-SCAN_IP_ATTACK-4:gigabitethernet0 detect ip scan attack.

#On Device, view the IP scan entry.

```
Device#show attack-defense scan ip-scan
  IP Scan Statistic :
    sip              dip-count          interface
    ------------------------------------------------------------

    100.0.0.3          4              gigabitethernet0
    100.0.0.4          4              gigabitethernet0
    100.0.0.5          4              gigabitethernet0
    100.0.0.6          4              gigabitethernet0
    131.255.8.28        1              vlan1992
```

#On Device, view the Port scan entry.

```
Device#show attack-defense scan port-scan
  Port Scan Statistic :
    sip              dip              dport-count      interface
    ------------------------------------------------------------------------
-----------
    100.0.0.3          101.0.0.1          1            gigabitethernet0
    100.0.0.3          101.0.0.2          1            gigabitethernet0
        100.0.0.3          101.0.0.3          1            gigabitethernet0
    100.0.0.3          101.0.0.4          1            gigabitethernet0
        100.0.0.4          101.0.0.5          1            gigabitethernet0
    100.0.0.4          101.0.0.6          1            gigabitethernet0
        100.0.0.4          101.0.0.7          1            gigabitethernet0
    100.0.0.4          101.0.0.8          1            gigabitethernet0
    100.0.0.5          101.0.0.9          1            gigabitethernet0
    100.0.0.5          101.0.0.10         1            gigabitethernet0
        100.0.0.5          101.0.0.11         1            gigabitethernet0
    100.0.0.5          101.0.0.12         1            gigabitethernet0
        100.0.0.6          101.0.0.13         1            gigabitethernet0
    100.0.0.6          101.0.0.14         1            gigabitethernet0
        100.0.0.6          101.0.0.15         1            gigabitethernet0
    100.0.0.6          101.0.0.16         1            gigabitethernet0
```

#On Device, view the dynamic blacklist entry generated by scanning.

```
Device#show blacklist ip
Blacklist Info:
```

```
IpAddr,          CreateTime,          Agetime
-----------------------------------------------------------------
100.0.0.2        ,  Mon May 04 17:36:45 2020     , 94
```

Note:

- The flood attack and scan attack detection functions are effective for both local and forwarded packets on the router, and only local packets on the switch.
- Flood attack tracing or scanning attack will add to the dynamic blacklist after identifying the specific attack source. The aging time is 2min. Before the blacklist aging, all packets of the attack source will be intercepted.

15.3.4. Configure urpf Strict Mode

Network Requirements

- PC accesses Internet through Device.
- The gigabitethernet0 interface of Device configures URPF strict mode.
- The PC simulates the attacker to send an illegal packet with pseudo source address to access Internet, and the URPF function of Device discards this packet.

Network Topology

Figure 15-4 Networking of configuring URPF strict mode

Configuration Steps

Step 1: Configure the IP address and route of each interface. It is required that the PC can access the Internet through Device. (omitted)

Step 2: The interface gigabitethernet0 of Device configure the URPF strict mode.

#Enable the URPF function on Device and configure the URPF strict mode on the interface gigabitethernet0.

```
Device#configure terminal
Device(config)#ip urpf
Device(config)#interface gigabitethernet0
Device(config-if-gigabitethernet0)#ip urpf strict
Device(config-if-gigabitethernet0)#exit
Device(config)#exit
```

Step 3: Check the result:

#PC1 accesses Internet through Device, and the source address is 120.5.0.2.

There is a route to 120.5.0.2 on Device, and the route out interface is gigabitethernet0. The out interface of the route to the source address and the receiving interface of the packet are the same interface gigabitethernet0. Through URPF strict check, the packet is forwarded by Device, and PC1 can access Internet.

#PC1 simulates an attacker to send an illegal packet with a pseudo source address and accesses Internet through Device. The source address is 120.10.0.2.

There is no route to 120.10.0.2 on Device, URPF discards the packet, and PC1 cannot access Internet. The packet loss statistics of URPF are as follows:

```
Device#show anti-attack urpf statistic
    Interface            urpf4-DropCount      urpf6-DropCount
    ------------------------------------------------------------------
    gigabitethernet0        124                  0
```

15.3.5. Configure urpf Loose Mode

Network Requirements

- In the network environment, PC1 accesses PC2 through Device1, Device2 and Device3, and the response packet of PC2 reaches PC1 through Device3 and Device1.
- The interface gigabitethernet0 of Device3 configures the URPF loose mode.
- PC1 simulates an attacker to send an illegal packet with a pseudo source address to access PC2, and the URPF function of Device discards this packet.

Network Topology

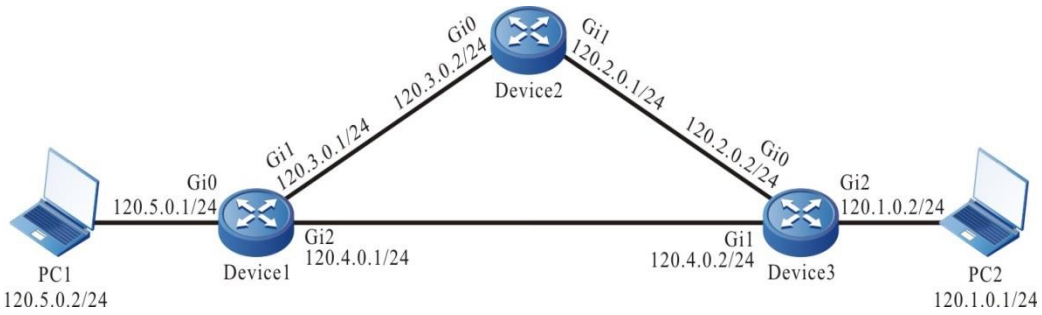


Figure 15-5 Networking of configuring the URPF loose mode

Configuration Steps

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

Step 2: Configure static route in the network so that PC1 accesses PC2 through Device1, Device2 and Device3. The response packet of PC2 reaches PC1 through Device3 and Device1.

#Configure the static route of Device1, Device2 and Device3, and construct the nework environment in the network requirements.

```
Device1#configure terminal
Device1(config)#ip route 120.1.0.0 255.255.255.0 120.3.0.2
Device1(config)#ip route 120.2.0.0 255.255.255.0 120.3.0.2
Device1(config)#exit

Device2#configure terminal
Device2(config)#ip route 120.1.0.0 255.255.255.0 120.2.0.2
Device2(config)#exit
```

Device3#configure terminal

Device3(config)#ip route 120.5.0.0 255.255.255.0 120.4.0.1

Device3(config)#exit

#View the route tables of Device1, Device2, and Device3.

Device1(config)#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

S 120.1.0.0/24 [1/10] via 120.3.0.2, 00:10:49, gigabitethernet1

S 120.2.0.0/24 [1/10] via 120.3.0.2, 00:11:19, gigabitethernet1

C 120.3.0.0/24 is directly connected, 00:19:15, gigabitethernet1

C 120.4.0.0/24 is directly connected, 00:15:00, gigabitethernet2

C 120.5.0.0/24 is directly connected, 00:07:36, gigabitethernet0

C 127.0.0.0/8 is directly connected, 357:23:02, lo0

Device2(config)#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

S 120.1.0.0/24 [1/10] via 120.2.0.2, 00:15:37, gigabitethernet1

C 120.2.0.0/24 is directly connected, 00:17:17, gigabitethernet1

C 120.3.0.0/24 is directly connected, 00:25:21, gigabitethernet0

C 127.0.0.0/8 is directly connected, 00:38:29, lo0

Device3(config)#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   120.1.0.0/24 is directly connected, 00:17:01, gigabitethernet2
C   120.2.0.0/24 is directly connected, 00:19:13, gigabitethernet0
C   120.4.0.0/24 is directly connected, 00:18:50, gigabitethernet1
S   120.5.0.0/24 [1/10] via 120.4.0.1, 00:17:19, gigabitethernet1
C   127.0.0.0/8 is directly connected, 00:26:16, lo0
```

Step 3: On the interface gigabitethernet0 of Device3, configure the URPF loose mode.

#Enable the URPF function on Device3 and configure the URPF loose mode on interface gigabitethernet0.

```
Device3#configure terminal
Device3(config)#ip urpf
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#ip urpf loose
Device3(config-if-gigabitethernet0)#exit
Device3(config)#exit
```

Step 4: Check the result:

#PC1 ping PC2

The ping request packet of PC1 reaches PC2 through Device1, Device2 and Device3; The ping response packet of PC2 reaches PC1 through Device3 and Device1.

#PC1 accesses PC2, and the source address is 120.5.0.2.

There is a route to 120.5.0.2 on Device3, and the out interface of the route is gigabitethernet1. Although the out interface gigabitethernet1 of the route to the source address and the receiving interface gigabitethernet0 of the packet are not the same interface, through the URPF loose mode function check, the packet is forwarded by Device3, PC1 can access PC2, and the response message of PC2 reaches PC1 through Device3 and Device1.

#PC1 simulates an attacker to send an illegal packet with a pseudo source address to access PC2. The source address is 120.10.0.2.

There is no route to 120.10.0.2 on Devic3, URPF discards the packet, and PC1 cannot access PC2. The packet loss statistics of URPF are as follows:

```
Device#show anti-attack urpf statistic
    Interface            urpf4-DropCount      urpf6-DropCount
    ------------------------------------------------------------------
    gigabitethernet0        456                  0
```

Note:

- The difference between the strict and loose modes of URPF is: in the loose mode, URPF will search the route table for the source IP address of the received packet. If a route is found, the message is allowed to pass through; In the strict mode, the packet is allowed to pass only when the route is found and the outgoing interface is the same as the receiving interface of the packet.
- The strict mode is generally applied, and the loose mode is applied to the network environment with "inconsistent back and forth paths" in similar cases.

- The URPF on the router is implemented by software detection, and the packet generated by this detection is discarded with log output and statistical information; The URPF on the switch is implemented by hardware, and the packet discarding caused by this detection will not generate logs and statistics.

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