Content

Chapter 1 Layer 3 Forward Configuration

Explanation:

The layer 3 switch in this chapter represents the a general sense of router or wireless controller which is running routing protocol.

Switch supports Layer 3 forwarding which forwards Layer 3 protocol packets (IP packets) across VLANs. Such forwarding uses IP addresses, when a interface receives an IP packet, it will perform a lookup in its own routing table and decide the operation according to the lookup result. If the IP packet is destined to another subnet reachable from this switch, then the packet will be forwarded to the appropriate interface. Switch can forward IP packets by hardware, the forwarding chip of switch have a host route table and default route table. Host route table stores host routes to connect to the switch directly; default route table stores network routes (after aggregation algorithm process).

If the route (either host route or network route) for forwarding unicast traffic exists in the forwarding chip, the forwarding of traffic will be completely handled by hardware. As a result, forwarding efficiency can be greatly improved, even to wire speed.

1.1 Layer 3 Interface

1.1.1 Introduction to Layer 3 Interface

Layer 3 interface can be created on switch. The Layer 3 interface is not a physical interface but a virtual interface. Layer 3 interface is built on VLANs. The Layer 3 interface can contain one or more layer 2 ports which belong to the same VLAN, or contain no layer 2 ports. At least one of the Layer 2 ports contained in Layer 3 interface should be in UP state for Layer 3 interface in UP state, otherwise, Layer 3 interface will be in DOWN state. All layer 3 interfaces in the switch use the same MAC address by default, this address is selected from the reserved MAC address while creating Layer 3 interface. The Layer 3 interface is the base for layer 3 protocols. The switch can use the IP addresses set in the layer 3 interfaces to communicate with the other devices via IP. The switch can forward IP packets between different Layer 3 interfaces. Loopback interface belongs to Layer 3 interface.

1.1.2 Layer 3 Interface Configuration Task List

Layer 3 Interface Configuration Task List:

1. Create Layer 3 interface
2. Bandwidth for Layer 3 Interface configuration
3. Configure VLAN interface description
4. Open or close the VLAN interface

1. Create Layer 3 Interface

Command	Explanation
Global Mode	
interface vlan *<vlan-id>* **no interface vlan *<vlan-id>***	Creates a VLAN interface (VLAN interface is a Layer 3 interface); the no command deletes the VLAN interface (Layer 3 interface) created in the switch.
interface loopback *<loopback-id>* **no interface loopback *<loopback-id>***	Creates a Loopback interface then enter the loopback Port Mode; the no command deletes the Loopback interface created in the switch.

2. Bandwidth for Layer 3 Interface configuration

Command	Explanation
VLAN Interface Mode	
bandwidth *<bandwidth>* **no bandwidth**	Configure the bandwidth for Layer 3 Interface. The no command recovery the default value.

3. Configure VLAN interface description

Command	Explanation
VLAN Interface Mode	
description *<text>* **no description**	Configure the description information of VLAN interface. The no command will cancel the description information of VLAN interface.

4. Open or close the vlan interface

Command	Explanation
VLAN Interface Mode	
shutdown **no shutdown**	Open or close the vlan interface.

1.2 IP Configuration

1.2.1 Introduction to IPv4, IPv6

IPv4 is the current version of global universal Internet protocol. The practice has proved that IPv4 is simple, flexible, open, stable, strong and easy to implement while collaborating well with various protocols of upper and lower layers. Although IPv4 almost has not been changed since it was established in 1980's, it has kept growing to the current global scale with the promotion of Internet. However, as Internet infrastructure and Internet application services continue boosting, IPv4 has shown its deficiency when facing the present scale and complexity of Internet.

IPv6 refers to the sixth version of Internet protocol which is the next generation Internet protocol designed by IETF to replace the current Internet protocol version 4 (IPv4). IPv6 was specially developed to make up the shortages of IPv4 addresses so that Internet can develop further.

The most important problem IPv6 has solved is to add the amount of IP addresses. IPv4 addresses have nearly run out, whereas the amount of Internet users has been increasing in geometric series. With the greatly and continuously boosting of Internet services and application devices (Home and Small Office Network, IP phone and Wireless Service Information Terminal which make use of Internet,) which require IP addresses, the supply of IP addresses turns out to be more and more tense. People have been working on the problem of shortage of IPv4 addresses for a long time by introducing various technologies to prolong the lifespan of existing IPv4 infrastructure, including Network Address Translation(NAT for short), and Classless Inter-Domain Routing(CIDR for short), etc.

Although the combination of CIDR, NAT and private addressing has temporarily mitigated the problem of IPv4 address space shortage, NAT technology has disrupted the end-to-end model which is the original intention of IP design by making it necessary for router devices that serve as network intermediate nodes to maintain every connection status which increases network delay greatly and decreases network performance. Moreover, the translation of network data packet addresses baffles the end-to-end network security check, IPSec authentication header is such an example.

Therefore, in order to solve all kinds of problems existing in IPv4 comprehensively, the next generation Internet Protocol IPv6 designed by IETF has become the only feasible solution at present.

First of all, the 128 bits addressing scheme of IPv6 Protocol can guarantee to provide

enough globally unique IP addresses for global IP network nodes in the range of time and space. Moreover, besides increasing address space, IPv6 also enhanced many other essential designs of IPv4.

Hierarchical addressing scheme facilitates Route Aggregation, effectively reduces route table entries and enhances the efficiency and expansibility of routing and data packet processing.

The header design of IPv6 is more efficient compared with IPv4. It has less data fields and takes out header checksum, thus expedites the processing speed of basic IPv6 header. In IPv6 header, fragment field can be shown as an optional extended field, so that data packets fragmentation process won't be done in router forwarding process, and Path MTU Discovery Mechanism collaborates with data packet source which enhances the processing efficiency of router.

Address automatic configuration and plug-and-play is supported. Large amounts of hosts can find network routers easily by address automatic configuration function of IPv6 while obtaining a globally unique IPv6 address automatically as well which makes the devices using IPv6 Internet plug-and-play. Automatic address configuration function also makes the readdressing of existing network easier and more convenient, and it is more convenient for network operators to manage the transformation from one provider to another.

Support IPSec. IPSec is optional in IPv4, but required in IPv6 Protocol. IPv6 provides security extended header, which provides end-to-end security services such as access control, confidentiality and data integrity, consequently making the implement of encryption, validation and Virtual Private Network easier.

Enhance the support for Mobile IP and mobile calculating devices. The Mobile IP Protocol defined in IETF standard makes mobile devices movable without cutting the existing connection, which is a network function getting more and more important. Unlike IPv4, the mobility of IPv6 is from embedded automatic configuration to get transmission address (Care-Of-Address); therefore it doesn't need Foreign Agent. Furthermore, this kind of binding process enables Correspondent Node communicate with Mobile Node directly, thereby avoids the extra system cost caused by triangle routing choice required in IPv4.

Avoid the use of Network Address Translation. The purpose of the introduction of NAT mechanism is to share and reuse same address space among different network segments. This mechanism mitigates the problem of the shortage of IPv4 address temporally; meanwhile it adds the burden of address translation process for network device and application. Since the address space of IPv6 has increased greatly, address translation becomes unnecessary, thus the problems and system cost caused by NAT deployment are solved naturally.

Support extensively deployed Routing Protocol. IPv6 has kept and extended the supports for existing Internal Gateway Protocols (IGP for short), and Exterior Gateway Protocols (EGP for short). For example, IPv6 Routing Protocol such as RIPng, OSPFv3, IS-ISv6 and MBGP4+, etc.

Multicast addresses increased and the support for multicast has enhanced. By dealing with IPv4 broadcast functions such as Router Discovery and Router Query, IPv6 multicast has completely replaced IPv4 broadcast in the sense of function. Multicast not only saves network bandwidth, but enhances network efficiency as well.

1.2.2 IP Configuration

Layer 3 interface can be configured as IPv4 interface, IPv6 interface.

1.2.2.1 IPv4 Address Configuration

IPv4 address configuration task list:

1. Configure the IPv4 address of three-layer interface

1. Configure the IPv4 address of three-layer interface

Command	Explanation
VLAN Interface Configuration Mode	
ip address *<ip-address>* *<mask>* [secondary] **no ip address [*<ip-address>* *<mask>*]**	Configure IP address of VLAN interface; the **no ip address [*<ip-address>* *<mask>*]** command cancels IP address of VLAN interface.

1.2.2.2 IPv6 Address Configuration

The configuration Task List of IPv6 is as follows:

1. IPv6 basic configuration
   (1) Configure interface IPv6 address
   (2) Configure IPv6 static routing
2. IPv6 Neighbor Discovery Configuration
   (1) Configure DAD neighbor solicitation message number
   (2) Configure send neighbor solicitation message interval
   (3) Enable and disable router advertisement
   (4) Configure router lifespan

(5) Configure router advertisement minimum interval

(6) Configure router advertisement maximum interval

(7) Configure prefix advertisement parameters

(8) Configure static IPv6 neighbor entries

(9) Delete all entries in IPv6 neighbor table

(10) Set the hoplimit of sending router advertisement

(11) Set the mtu of sending router advertisement

(12) Set the reachable-time of sending router advertisement

(13) Set the retrans-timer of sending router advertisement

(14) Set the flag representing whether information other than the address information will be obtained via DHCPv6

(15) Set the flag representing whether the address information will be obtained via DHCPv6

3. IPv6 Tunnel configuration

(1) Create/Delete Tunnel

(2) Configure tunnel description

(3) Configure Tunnel Source

(4) Configure Tunnel Destination

(5) Configure Tunnel Next-Hop

(6) Configure Tunnel Mode

(7) Configure Tunnel Routing

1. IPv6 Basic Configuration

(1) Configure interface IPv6 address

Command	Explanation
Interface Configuration Mode	
ipv6 address *<ipv6-address/prefix-length>* [eui-64] **no ipv6 address *<ipv6-address/prefix-length>***	Configure IPv6 address, including aggregatable global unicast addresses, site-local addresses and link-local addresses. The **no ipv6 address *<ipv6-address/prefix-length>*** command cancels IPv6 address.

(2) Set IPv6 Static Routing

Command	Explanation
Global mode	

ipv6 route <ipv6-prefix/prefix-length> {<nexthop-ipv6-address>|<interface-type interface-number> | {<nexthop-ipv6-address> <interface-type interface-number>}} [distance] **no ipv6 route <ipv6-prefix/prefix-length> {<nexthop-ipv6-address>|<interface-type interface-number> |{<nexthop-ipv6-address> <interface-type interface-number>}} [distance]**	Configure IPv6 static routing. The no command cancels IPv6 static routing.

2. IPv6 Neighbor Discovery Configuration

(1) Configure DAD Neighbor solicitation Message number

Command	Explanation
Interface Configuration Mode	
ipv6 nd dad attempts <value> **no ipv6 nd dad attempts**	Set the neighbor query message number sent in sequence when the interface makes duplicate address detection. The no command resumes default value (1).

(2) Configure Send Neighbor solicitation Message Interval

Command	Explanation
Interface Configuration Mode	
ipv6 nd ns-interval <*seconds*> **no ipv6 nd ns-interval**	Set the interval of the interface to send neighbor query message. The NO command resumes default value (1 second).

(3) Enable and disable router advertisement

Command	Explanation
Interface Configuration Mode	
ipv6 nd suppress-ra **no ipv6 nd suppress-ra**	Forbid IPv6 Router Advertisement. The NO command enables IPv6 router advertisement.

(4) Configure Router Lifespan

Command	Explanation
Interface Configuration Mode	
ipv6 nd ra-lifetime <*seconds*> **no ipv6 nd ra-lifetime**	Configure Router advertisement Lifespan. The NO command resumes default value (1800 seconds).

(5) Configure router advertisement Minimum Interval

Command	Description
Interface Configuration Mode	
ipv6 nd min-ra-interval <seconds> **no ipv6 nd min-ra-interval**	Configure the minimum interval for router advertisement. The NO command resumes default value (200 seconds).

(6) Configure router advertisement Maximum Interval

Command	Explanation
Interface Configuration Mode	
ipv6 nd max-ra-interval <*seconds*> **no ipv6 nd max-ra-interval**	Configure the maximum interval for router advertisement. The NO command resumes default value (600 seconds).

(7) Configure prefix advertisement parameters

Command	Explanation
Interface Configuration Mode	
ipv6 nd prefix ***<ipv6-address/prefix-length>*** ***<valid-lifetime>*** ***<preferred-lifetime>*** **[off-link]** **[no-autoconfig]** **no ipv6 nd prefix** ***<ipv6-address/prefix-length>*** ***<valid-lifetime>*** ***<preferred-lifetime>*** **[off-link]** **[no-autoconfig]**	Configure the address prefix and advertisement parameters of router. The NO command cancels the address prefix of routing advertisement.

(8) Configure static IPv6 neighbor Entries

Command	Explanation
Interface Configuration Mode	

ipv6 neighbor *<ipv6-address>* *<hardware-address>* interface *<interface-type interface-name>*	Set static neighbor table entries, including neighbor IPv6 address, MAC address and two-layer port.
no ipv6 neighbor *<ipv6-address>*	Delete neighbor table entries.

(9) Delete all entries in IPv6 neighbor table

Command	Explanation
Admin Mode	
clear ipv6 neighbors	Clear all static neighbor table entries.

(10) Set the hoplimit of sending router advertisement

Command	Explanation
Interface Configuration Mode	
ipv6 nd ra-hoplimit <value>	Set the hoplimit of sending router advertisement.

(11) Set the mtu of sending router advertisement

Command	Explanation
Interface Configuration Mode	
ipv6 nd ra-mtu <value>	Set the mtu of sending router advertisement.

(12) Set the reachable-time of sending router advertisement

Command	Explanation
Interface Configuration Mode	
ipv6 nd reachable-time <seconds>	Set the reachable-time of sending router advertisement.

(13) Set the retrans-timer of sending router advertisement

Command	Explanation
Interface Configuration Mode	
ipv6 nd retrans-timer <seconds>	Set the retrans-timer of sending router advertisement.

(14) Set the flag representing whether information other than the address information will be obtained via DHCPv6.

Command	Explanation
Interface Configuration Mode	

ipv6 nd other-config-flag	Set the flag representing whether information other than the address information will be obtained via DHCPv6.

(15) Set the flag representing whether the address information will be obtained via DHCPv6

Command	Explanation
Interface Configuration Mode	
ipv6 nd managed-config-flag	Set the flag representing whether the address information will be obtained via DHCPv6.

3. IPv6 Tunnel Configuration

(1) Add/Delete tunnel

Command	Explanation
Global mode	
interface tunnel <*tnl-id*> **no interface tunnel <*tnl-id*>**	Create a tunnel. The NO command deletes a tunnel.

(2) Configure tunnel description

Command	Explanation
Tunnel Configuration Mode	
description <*desc*> **no description**	Configure tunnel description. The NO command deletes the tunnel description.

(3) Configure tunnel source

Command	Explanation
Tunnel Configuration Mode	
tunnel source { <*ipv4-address*> | **<*ipv6-address*>|** **<*interface-name*> }** **no tunnel source**	Configure tunnel source end IPv4/IPv6 address. The NO command deletes the IPv4/IPv6 address of tunnel source end.

(4) Configure Tunnel Destination

Command	Explanation
Tunnel Configuration Mode	

tunnel destination {<ipv4-address> | <ipv6-address>} **no tunnel destination**	Configure tunnel destination end IPv4/IPv6 address. The NO command deletes the IPv4/IPv6 address of tunnel destination end.

(5) Configure Tunnel Next-Hop

Command	Explanation
Tunnel Configuration Mode	
tunnel nexthop <ipv4-address> **no tunnel nexthop**	Configure tunnel next-hop IPv4 address. The NO command deletes the IPv4 address of tunnel next-hop end.

(6) Configure Tunnel Mode

Command	Explanation
Tunnel Configuration Mode	
tunnel mode [[gre] | ipv6ip [6to4 | isatap]] **no tunnel mode**	Configure tunnel mode. The NO command clears tunnel mode.

(7) Configure Tunnel Routing

Command	Explanation
Global mode	
ipv6 route <ipv6-address/prefix-length> {<interface-type interface-number> | tunnel <tnl-id>} **no ipv6 route <ipv6-address/prefix-length> {<interface-type interface-number> | tunnel <tnl-id>}**	Configure tunnel routing. The NO command clears tunnel routing.

1.2.3 IP Configuration Examples

1.2.3.1 Configuration Examples of IPv4

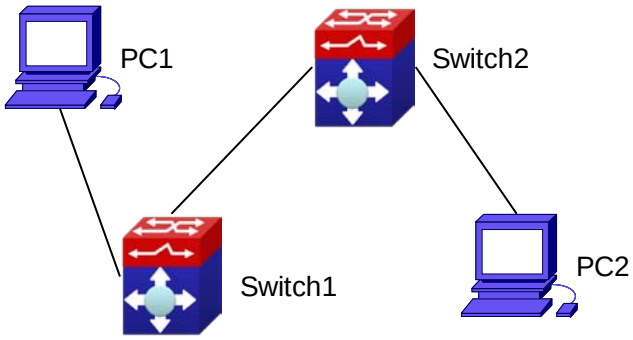


Fig 1-1 IPv4 configuration example

The user's configuration requirements are: Configure IP address of different network segments on Switch1 and Switch2, configure static routing and validate accessibility using ping function.

Configuration Description:

1. Configure two VLANs on Switch1, namely, VLAN1 and VLAN2.
2. Configure IPv4 address 192.168.1.1 255.255.255.0 in VLAN1 of Switch1, and configure IPv4 address 192.168.2.1 255.255.255.0 in VLAN2.
3. Configure two VLANs on Switch2, respectively VLAN2 and VLAN3.
4. Configure IPv4 address 192.168.2.2 255.255.255.0 in VLAN2 of Switch2, and configure IPv4 address 192.168.3.1 255.255.255.0 in VLAN3.
5. The IPv4 address of PC1 is 192.168.1.100 255.255.255.0, and the IPv4 address of PC2 is 192.168.3.100 255.255.255.0.
6. Configure static routing 192.168.3.0/24 on Switch1, and configure static routing 192.168.1.0/24 on Switch2.
7. Ping each other among PCs.

Note: First make sure PC1 and Switch1 can access each other by ping, and PC2 and Switch2 can access each other by ping.

The configuration procedure is as follows:

```
Switch1(config)#interface vlan 1
Switch1(Config-if-Vlan1)#ip address 192.168.1.1 255.255.255.0
Switch1(config)#interface vlan 2
Switch1(Config-if-Vlan2)#ip address 192.168.2.1 255.255.255.0
Switch1(Config-if-Vlan2)#exit
Switch1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2

Switch2(config)#interface vlan 2
Switch2(Config-if-Vlan2)#ip address 192.168.2.2 255.255.255.0
Switch2(config)#interface vlan 3
Switch2(Config-if-Vlan3)#ip address 192.168.3.1 255.255.255.0
```

Switch2(Config-if-Vlan3)#exit

Switch2(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1

1.2.3.2 Configuration Examples of IPv6

Example 1:

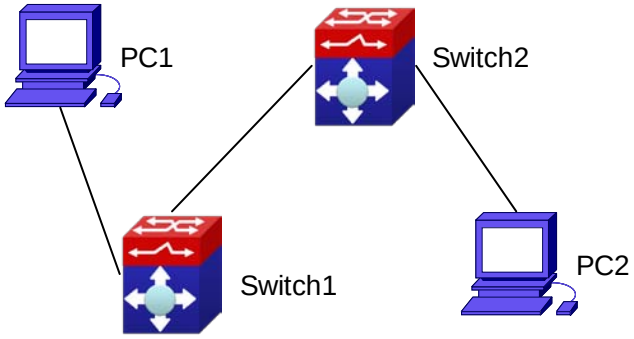


Fig 1-2 IPv6 configuration example

The user's configuration requirements are: Configure IPv6 address of different network segments on Switch1 and Switch2, configure static routing and validate reachability using ping6 function.

Configuration Description:

1. Configure two VLANs on Switch1, namely, VLAN1 and VLAN2.
2. Configure IPv6 address 2001::1/64 in VLAN1 of Switch1, and configure IPv6 address 2002::1/64 in VLAN2.
3. Configure 2 VLANs on Switch2, namely, VLAN2 and VLAN3.
4. Configure IPv6 address 2002::2/64 in VLAN2 of Switch2, and configure IPv6 address 2003::1/64 in VLAN3.
5. The IPv6 address of PC1 is 2001::11/64, and the IPv6 address of PC2 is 2003::33/64.
6. Configure static routing 2003:33/64 on Switch1, and configure static routing 2001::11/64 on Switch2.
7. ping6 each other among PCs.

Note: First make sure PC1 and Switch1 can access each other by ping, and PC2 and Switch2 can access each other by ping.

The configuration procedure is as follows:

Switch1(Config)#interface vlan 1

Switch1(Config-if-Vlan1)#ipv6 address 2001::1/64

Switch1(Config)#interface vlan 2

Switch1(Config-if-Vlan2)#ipv6 address 2002::1/64

Switch1(Config-if-Vlan2)#exit

```
Switch1(Config)#ipv6 route 2003::33/64 2002::2

Switch2(Config)#interface vlan 2
Switch2(Config-if-Vlan2)#ipv6 address 2002::2/64
Switch2(Config)#interface vlan 3
Switch2(Config-if-Vlan3)#ipv6 address 2003::1/64
Switch2(Config-if-Vlan3)#exit
Switch2(Config)#ipv6 route 2001::33/64 2002::1

Switch1#ping6 2003::33
```

Configuration result:

```
Switch1#show run
interface Vlan1
 ipv6 address 2001::1/64
!
interface Vlan2
 ipv6 address 2002::2/64
!
interface Loopback
 mtu 3924
!
ipv6 route 2003::/64 2002::2
!
no login
!
end

Switch2#show run
interface Vlan2
 ipv6 address 2002::2/64
!
interface Vlan3
 ipv6 address 2003::1/64
!
interface Loopback
 mtu 3924
!
ipv6 route 2001::/64 2002::1
```

!

no login

!

End

Example 2:

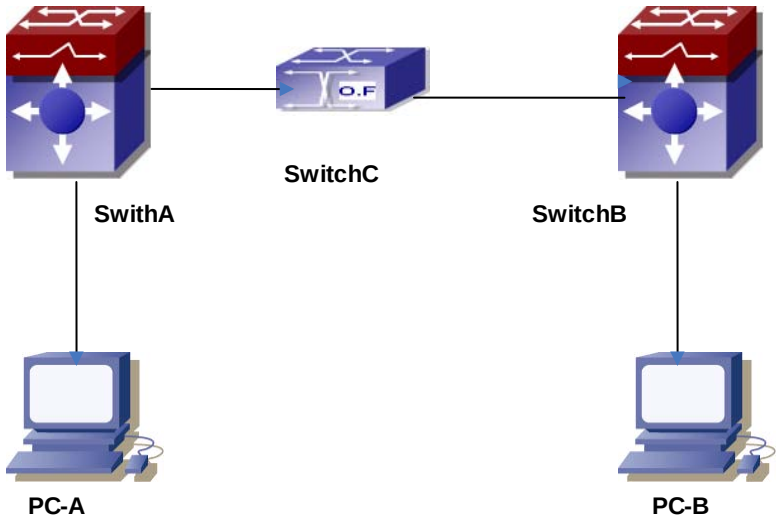


Fig 1-3 IPv6 tunnel

This case is IPv6 tunnel with the following user configuration requirements: SwitchA and SwitchB are tunnel nodes, dual-stack is supported. SwitchC only runs IPv4, PC-A and PC-B communicate.

Configuration Description:

1. Configure two vlans on SwitchA, namely, VLAN1 and VLAN2. VLAN1 is IPv6 domain, VLAN2 connects to IPv4 domain.
2. Configure IPv6 address 2002:caca:ca01:2::1/64 in VLAN1 of SwitchA and turn on RA function, configure IPv4 address 202.202.202.1 in VLAN2.
3. Configure two VLANs on SwitchB, namely, VLAN3 and VLAN4, VLAN4 is IPv6 domain, and VLAN3 connects to IPv4 domain.
4. Configure IPv6 address 2002:cbcb:cb01:2::1/64 in VLAN4 of SwitchB and turn on RA function, configure IPv4 address 203.203.203.1 on VLAN3.
5. Configure tunnel on SwitchA, the source IPv4 address of the tunnel is 202.202.202.1, the tunnel routing is ::/0
6. Configure tunnel on SwitchB, the source IPv4 address of the tunnel is 203.203.203.1, and the tunnel routing is ::/0
7. Configure two VLANs on SwitchC, namely, VLAN2 and VLAN3. Configure IPv4

address 202.202.202.202 on VLAN2 and configure IPv4 address 203.203.203.203 on VLAN3.

8. PC-A and PC-B get the prefix of 2002 via SwitchA and SwitchB to configure IPv6 address automatically.
9. On PC-A, ping IPv6 address of PC-B

The configuration procedure is as follows:

SwitchA(Config-if-Vlan1)#ipv6 address 2002:caca:ca01:2::1/64
SwitchA(Config-if-Vlan1)#no ipv6 nd suppress-ra
SwitchA(Config-if-Vlan1)#interface vlan 2
SwitchA(Config-if-Vlan2)#ipv4 address 202.202.202.1 255.255.255.0
SwitchA(Config-if-Vlan1)#exit
SwitchA(config)# interface tunnel 1
SwitchA(Config-if-Tunnel1)#tunnel source 202.202.202.1
SwitchA(Config-if-Tunnel1)#tunnel destination 203.203.203.1
SwitchA(Config-if-Tunnel1)#tunnel mode ipv6ip
SwitchA(config)#ipv6 route ::/0 tunnel1

SwitchB(Config-if-Vlan4)#ipv6 address 2002:cbcb:cb01::2/64
SwitchB(Config-if-Vlan4)#no ipv6 nd suppress-ra
SwitchB (Config-if-Vlan3)#interface vlan 3
SwitchB (Config-if-Vlan2)#ipv4 address 203.203.203.1 255.255.255.0
SwitchB (Config-if-Vlan1)#exit
SwitchB(config)#interface tunnel 1
SwitchB(Config-if-Tunnel1)#tunnel source 203.203.203.1
SwitchB(Config-if-Tunnel1)#tunnel destination 202.202.202.1
SwitchB(Config-if-Tunnel1)#tunnel mode ipv6ip
SwitchB(config)#ipv6 route ::/0 tunnel1

1.2.4 IPv6 Troubleshooting

☞ The router lifespan configured should not be smaller than the Send Router advertisement Interval. If the connected PC has not obtained IPv6 address, you should check RA announcement switch (the default is turned off).

1.3 IP Forwarding

1.3.1 Introduction to IP Forwarding

Gateway devices can forward IP packets from one subnet to another; such forwarding uses routes to find a path. IP forwarding of switch is done with the participation of hardware, and can achieve wire speed forwarding. In addition, flexible management is provided to adjust and monitor forwarding. Switch supports aggregation algorithm enabling/disabling optimization to adjust generation of network route entry in the switch chip and view statistics for IP forwarding and hardware forwarding chip status.

1.3.2 IP Route Aggregation Configuration Task

IP route aggregation configuration task:

1. Set whether IP route aggregation algorithm with/without optimization should be used

1. Set whether IP route aggregation algorithm with/without optimization should be used

Command	Explanation
Global Mode	
ip fib optimize **no ip fib optimize**	Enables the switch to use optimized IP route aggregation algorithm; the "**no ip fib optimize**" disables the optimized IP route aggregation algorithm.

1.4 URPF

1.4.1 Introduction to URPF

URPF (Unicast Reverse Path Forwarding) introduces the RPF technology applied in multicast to unicast, so to protect the network from the attacks which is based on source address cheat.

When switch receives the packet, it will search the route in the route table using the source address as the destination address which is acquired from the packet. If the found router exit interface does not match the entrance interface acquired from this packet, the switch will consider this packet a fake packet and discard it.

In Source Address Spoofing attacks, attackers will construct a series of messages with fake source addresses. For applications based on IP address verification, such attacks may allow unauthorized users to access the system as some authorized ones, or even the administrator. Even if the response messages can't reach the attackers, they will also damage the targets.

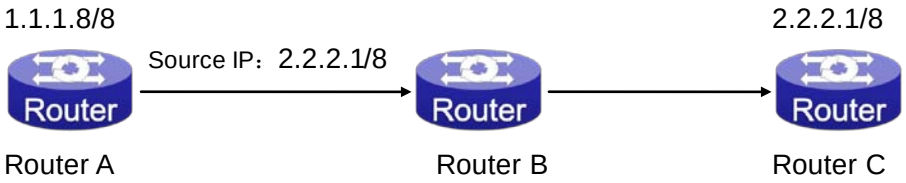


Fig 1-4 URPF application situation

In the above figure, Router A sends requests to the server Router B by faking messages whose source address are 2.2.2.1/8 .In response, Router B will send the messages to the real ”2.2.2.1/8”. Such illegal messages attack both Router B and Router C. The application of URPF technology in the situation described above can avoid the attacks based on the Source Address Spoofing.

1.4.1.1 IPv6 URPF Operating Mechanism

At present the UPRF relies on the ACL function provided by the switch chips.

Firstly, globally enable the URPF function to monitor the changes in the router table: create a corresponding URPF permit ACL rule for each router in the router table FIB. In URPF strict mode, the format of ACL rules is: the source address segments of inbound packets + the ingress interface VID of inbound packets. The source address segments of inbound packets are in correspondence with the destination address segments in the FIB router table entries, while the ingress interface VID of inbound packets with the egress interface VID in the FIB router table entries. In URPF loose mode, the format of ACL rules is the source address segments of inbound packets, which are in correspondence with destination address segments in the FIB router table entries.

After enabling URPF on the port: bind the port to RUPF rules, and create the default hardware for DENY ALL rule distribution.

The above operations will guarantee that, when data reach the port, only those match the rules can pass through it with all others dumped.

The present corresponding ACL rule privilege is low, not blocking all kinds of protocol packets; hence, enabling this function will not affect the normal operation of routing protocols of the switch.

1.4.2 URPF Configuration Task Sequence

1. Enable URPF
2. Enable URPF on port
3. Display and debug URPF relevant information

1. Globally enable URPF

Command	Explanation
Global mode	
urpf enable **no urpf enable**	Globally enable and disable URPF.

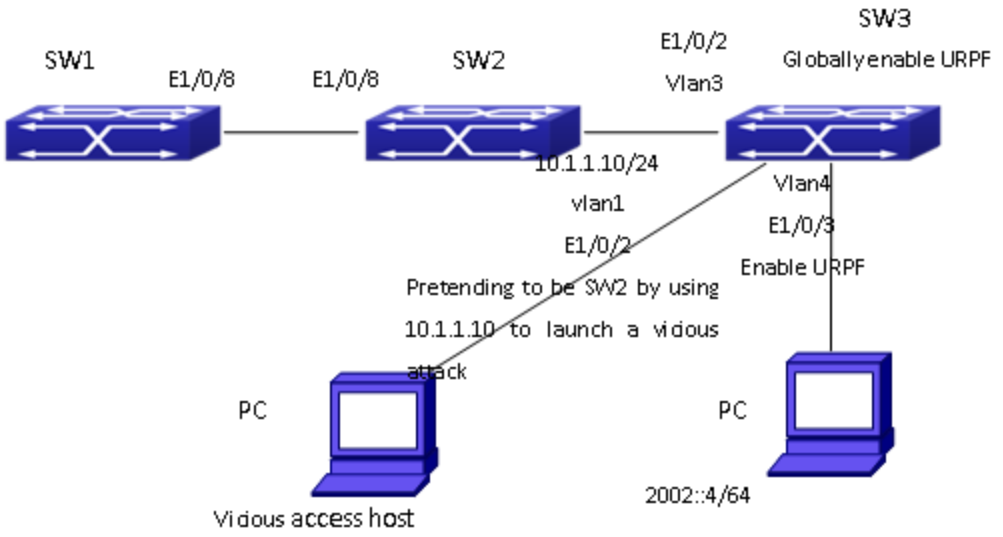
2. Enable URPF on port

Command	Explanation
Port mode	
ip urpf enable {loose | strict} {allow-default-route } **no ip urpf enable**	Enable and disable URPF on port.

3. Display and debug URPF relevant information

Command	Explanation
Admin mode	
debug urpf {notice | warn | error|} **no debug urpf {notice | warn | error|}**	Enable the URPF debug function to display error information if failures occur during the installation of URPF rules.
Admin and Config Mode	
show urpf	Display which interfaces have been enabled with URPF function.
show urpf rule ipv4 num interface ethernet IFNAME	Display the number of IPv4 rules bonded to the port.
show urpf rule ipv6 num interface ethernet IFNAME	Display the number of IPv6 rules bonded to the port.
show urpf rule ipv4 interface ethernet IFNAME	Display the details of IPv4 rules bonded to the port.
show urpf rule ipv6 interface ethernet IFNAME	Display the details of IPv6 rules bonded to the port.

1.4.3 URPF Typical Example



In the network, topology shown in the graph above, IP URPF function is enabled on SW3. When there is someone in the network pretending to be someone else by using his IP address to launch a vicious attack, the switch will drop all the attacking messages directly through the hardware FFP function.

Enable the URPF function in SW3 Ethernet1/0/3.

SW3 configuration task sequence:

Switch3#config

Switch3(config)#urpf enable

Switch3(config)#interface ethernet 1/0/3

Switch3(Config-If-Ethernet1/0/3)#ip urpf enable strict

1.4.4 URPF Troubleshooting

Proper operation of the URPF protocol depends greatly on whether the corresponding URPF rules can be applied correctly. If after the URPF configuration is done and the function does not meet the expectation:

- ☞ Check if the switch has been configured with the rules conflicting with URPF (URPF priority is lower than ACL), the ACL rules will validate if confliction exits.
- ☞ Check whether there is a relative route in the FIB table. Only when one is found, can the ACL rules be distributed to the port.
- ☞ Check if the hardware ACL performance is full which lead to the newly generated route can not be applied with ACL rules.
- ☞ If all configurations are normal but URPF still can't operate as expected, please enable the URPF debug function and use the "show urpf" command and other commands which display the rule number and details to observe whether the created URPF rules are correct, and send the result to the technology service

center.

1.5 ARP

1.5.1 Introduction to ARP

ARP (Address Resolution Protocol) is mainly used to resolve IP address to Ethernet MAC address. Switch supports both dynamic ARP and static ARP configuration.Furthermore, switch supports the configuration of proxy ARP for some applications. For instance, when an ARP request is received on the port, requesting an IP address in the same IP segment of the port but not the same physical network, if the port has enabled proxy ARP, the port would reply to the ARP with its own MAC address and forward the actual packets received. Enabling proxy ARP allows machines physically separated but of the same IP segment ignores the physical separation and communicate via proxy ARP interface as if in the same physical network.

1.5.2 ARP Configuration Task List

ARP Configuration Task List:

1. Configure static ARP
2. Configure proxy ARP
3. Clear dynamic ARP
4. Select hash arithmetic
5. Clear the statistic information of ARP messages

1. Configure static ARP

Command	Explanation
VLAN Interface Mode	
arp <*ip_address*> <*mac_address*> **{interface [ethernet] <portName>}** **no arp <ip_address>**	Configures a static ARP entry; the no command deletes a ARP entry of the specified IP address.

2. Configure proxy ARP

Command	Explanation
VLAN Interface Mode	
ip proxy-arp **no ip proxy-arp**	Enables the proxy ARP function for Ethernet ports: the no command disables the proxy ARP.

3. Clear dynamic ARP

Command	Explanation
Admin mode	
clear arp-cache	Clear the dynamic ARP learnt by the switch.

4. Select hash arithmetic

Command	Explanation
Global mode	
l3 hashselect [<crc16l|crc16u|crc32l|crc32u|lsb>]	Set the hash arithmetic of the layer 3 table. This command refers to ARP table list storage in the hardware, the implement need to guide by the technique specialist. The detail information please refer to the interrelated Command Guide.

5. Clear the statistic information of ARP message

Command	Explanation
Admin mode	
clear arp traffic	Clear the statistic information of ARP messages of the switch.

1.5.3 ARP Troubleshooting

If ping from the switch to directly connected network devices fails, the following can be used to check the possible cause and create a solution.

- ☞ Check whether the corresponding ARP has been learned by the switch.
- ☞ If ARP has not been learned, then enabled ARP debugging information and view the sending/receiving condition of ARP packets.
- ☞ Defective cable is a common cause of ARP problems and may disable ARP learning.

Chapter 2 ARP Scanning Prevention Function Configuration

2.1 Introduction to ARP Scanning Prevention Function

ARP scanning is a common method of network attack. In order to detect all the active hosts in a network segment, the attack source will broadcast lots of ARP messages in the segment, which will take up a large part of the bandwidth of the network. It might even do large-traffic-attack in the network via fake ARP messages to collapse of the network by exhausting the bandwidth. Usually ARP scanning is just a preface of other more dangerous attack methods, such as automatic virus infection or the ensuing port scanning, vulnerability scanning aiming at stealing information, distorted message attack, and DOS attack, etc.

Since ARP scanning threatens the security and stability of the network with great danger, so it is very significant to prevent it. Switch provides a complete resolution to prevent ARP scanning: if there is any host or port with ARP scanning features is found in the segment, the switch will cut off the attack source to ensure the security of the network.

There are two methods to prevent ARP scanning: port-based and IP-based. The port-based ARP scanning will count the number to ARP messages received from a port in a certain time range, if the number is larger than a preset threshold, this port will be “down”. The IP-based ARP scanning will count the number to ARP messages received from an IP in the segment in a certain time range, if the number is larger than a preset threshold, any traffic from this IP will be blocked, while the port related with this IP will not be “down”. These two methods can be enabled simultaneously. After a port or an IP is disabled, users can recover its state via automatic recovery function.

To improve the effect of the switch, users can configure trusted ports and IP, the ARP messages from which will not be checked by the switch. Thus the load of the switch can be effectively decreased.

2.2 ARP Scanning Prevention Configuration Task Sequence

1. Enable the ARP Scanning Prevention function.
2. Configure the threshold of the port-based and IP-based ARP Scanning

Prevention

3. Configure trusted ports
4. Configure trusted IP
5. Configure automatic recovery time
6. Display relative information of debug information and ARP scanning

1. Enable the ARP Scanning Prevention function.

Command	Explanation
Global configuration mode	
anti-arpscan enable **no anti-arpscan enable**	Enable or disable the ARP Scanning Prevention function globally.

2. Configure the threshold of the port-based and IP-based ARP Scanning Prevention

Command	Explanation
Global configuration mode	
anti-arpscan port-based threshold *<threshold-value>* **no anti-arpscan port-based threshold**	Set the threshold of the port-based ARP Scanning Prevention.
anti-arpscan ip-based threshold *<threshold-value>* **no anti-arpscan ip-based threshold**	Set the threshold of the IP-based ARP Scanning Prevention.

3. Configure trusted ports

Command	Explanation
Port configuration mode	
anti-arpscan trust *<port | supertrust-port>* **no anti-arpscan trust *<port | supertrust-port>***	Set the trust attributes of the ports.

4. Configure trusted IP

Command	Explanation
Global configuration mode	

anti-arpscan trust ip <*ip-address*> [<*netmask*>] **no anti-arpscan trust ip <*ip-address*> [<*netmask*>]**	Set the trust attributes of IP.

5. Configure automatic recovery time

Command	Explanation
Global configuration mode	
anti-arpscan recovery enable **no anti-arpscan recovery enable**	Enable or disable the automatic recovery function.
anti-arpscan recovery time <*seconds*> **no anti-arpscan recovery time**	Set automatic recovery time.

6. Display relative information of debug information and ARP scanning

Command	Explanation
Global configuration mode	
anti-arpscan log enable **no anti-arpscan log enable**	Enable or disable the log function of ARP scanning prevention.
anti-arpscan trap enable **no anti-arpscan trap enable**	Enable or disable the SNMP Trap function of ARP scanning prevention.
show anti-arpscan [trust <*ip* | *port* | *supertrust-port*> | prohibited <*ip* | *port*>]	Display the state of operation and configuration of ARP scanning prevention.
Admin Mode	
debug anti-arpscan <*port* | *ip*> **no debug anti-arpscan <*port* | *ip*>**	Enable or disable the debug switch of ARP scanning prevention.

2.3 ARP Scanning Prevention Typical Examples

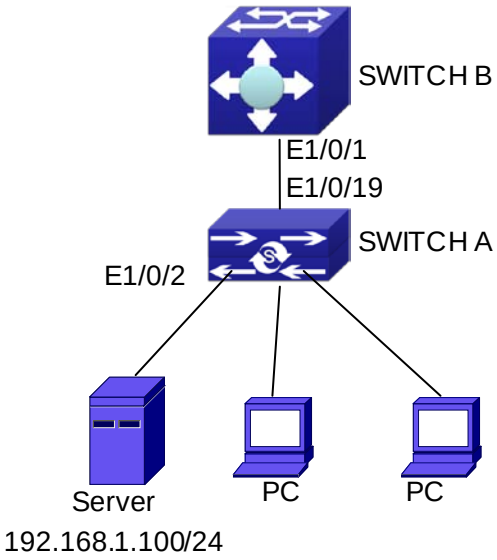


Fig 2-1 ARP scanning prevention typical configuration example

In the network topology above, port E1/0/1 of SWITCH B is connected to port E1/0/19 of SWITCH A, the port E1/0/2 of SWITCH A is connected to file server (IP address is 192.168.1.100/24), and all the other ports of SWITCH A are connected to common PC. The following configuration can prevent ARP scanning effectively without affecting the normal operation of the system.

SWITCH A configuration task sequence:

SwitchA(config)#anti-arpscan enable

SwitchA(config)#anti-arpscan recovery time 3600

SwitchA(config)#anti-arpscan trust ip 192.168.1.100 255.255.255.0

SwitchA(config)#interface ethernet1/0/2

SwitchA (Config-If-Ethernet1/0/2)#anti-arpscan trust port

SwitchA (Config-If-Ethernet1/0/2)#exit

SwitchA(config)#interface ethernet1/0/19

SwitchA (Config-If-Ethernet1/0/19)#anti-arpscan trust supertrust-port

Switch A(Config-If-Ethernet1/0/19)#exit

SWITCHB configuration task sequence:

Switch B(config)# anti-arpscan enable

SwitchB(config)#interface ethernet1/0/1

SwitchB(Config-If-Ethernet1/0/1)#anti-arpscan trust port

SwitchB(Config-If-Ethernet1/0/1)exit

2.4 ARP Scanning Prevention Troubleshooting Help

☞ ARP scanning prevention is disabled by default. After enabling ARP scanning prevention, users can enable the debug switch, "**debug anti-arpscan**", to view debug information.

Chapter 3 Prevent ARP, ND Spoofing Configuration

3.1 Overview

3.1.1 ARP (Address Resolution Protocol)

Generally speaking, ARP (RFC-826) protocol is mainly responsible of mapping IP address to relevant 48-bit physical address, that is MAC address, for instance, IP address is 192.168.0.1, network card Mac address is 00-03-0F-FD-1D-2B. What the whole mapping process is that a host computer send broadcast data packet involving IP address information of destination host computer, ARP request, and then the destination host computer send a data packet involving its IP address and Mac address to the host, so two host computers can exchange data by MAC address.

3.1.2 ARP Spoofing

In terms of ARP Protocol design, to reduce redundant ARP data communication on networks, even though a host computer receives an ARP reply which is not requested by itself, it will also insert an entry to its ARP cache table, so it creates a possibility of “ARP spoofing”. If the hacker wants to snoop the communication between two host computers in the same network (even if are connected by the switches), it sends an ARP reply packet to two hosts separately, and make them misunderstand MAC address of the other side as the hacker host MAC address. In this way, the direct communication is actually communicated indirectly among the hacker host computer. The hackers not only obtain communication information they need, but also only need to modify some information in data packet and forward successfully. In this sniff way, the hacker host computer doesn’t need to configure intermix mode of network card, that is because the data packet between two communication sides are sent to hacker host computer on physical layer, which works as a relay.

3.1.3 How to prevent void ARP/ND Spoofing

There are many sniff, monitor and attack behaviors based on ARP protocol in networks, and most of attack behaviors are based on ARP spoofing, so it is very important to prevent ARP spoofing. ARP spoofing accesses normal network environment by

counterfeiting legal IP address firstly, and sends a great deal of counterfeited ARP application packets to switches, after switches learn these packets, they will cover previously corrected IP, mapping of MAC address, and then some corrected IP, MAC address mapping are modified to correspondence relationship configured by attack packets so that the switch makes mistake on transfer packets, and takes an effect on the whole network. Or the switches are made used of by vicious attackers, and they intercept and capture packets transferred by switches or attack other switches, host computers or network equipment.

What the essential method on preventing attack and spoofing switches based on ARP in networks is to disable switch automatic update function; the cheater can't modify corrected MAC address in order to avoid wrong packets transfer and can't obtain other information. At one time, it doesn't interrupt the automatic learning function of ARP. Thus it prevents ARP spoofing and attack to a great extent.

ND is neighbor discovering protocol in IPv6 protocol, and it's similar to ARP on operation principle, therefore we do in the same way as preventing ARP spoofing to prevent ND spoofing and attack.

3.2 Prevent ARP, ND Spoofing configuration

The steps of preventing ARP, ND spoofing configuration as below:

1. Disable ARP, ND automatic update function
2. Disable ARP, ND automatic learning function
3. Changing dynamic ARP, ND to static ARP, ND

1. Disable ARP, ND automatic update function

Command	Explanation
Global Mode and Port Mode	
ip arp-security updateprotect **no ip arp-security updateprotect** **ipv6 nd-security updateprotect** **no ipv6 nd-security updateprotect**	Disable and enable ARP, ND automatic update function.

2. Disable ARP, ND automatic learning function

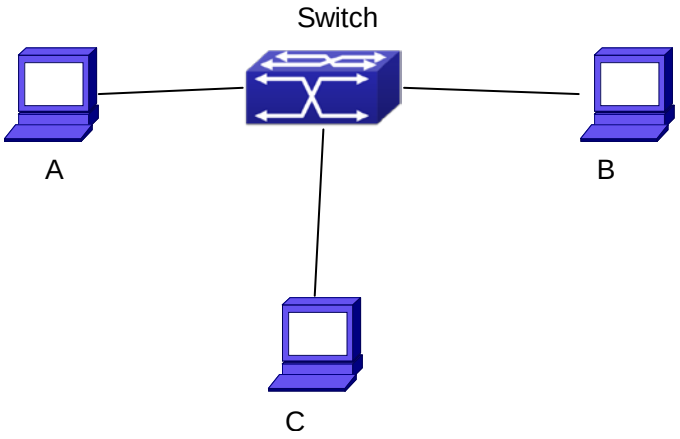
Command	Explanation
Global mode and Interface Mode	

ip arp-security learnprotect **no ip arp-security learnprotect** **ipv6 nd-security learnprotect** **no ipv6 nd-security learnprotect**	Disable and enable ARP, ND automatic learning function.

3. Function on changing dynamic ARP, ND to static ARP, ND

Command	Explanation
Global Mode and Port Mode	
ip arp-security convert **ipv6 nd-security convert**	Change dynamic ARP, ND to static ARP, ND.

3.3 Prevent ARP, ND Spoofing Example



Equipment Explanation

Equipment	Configuration	Quality
switch	IP:192.168.2.4; IP:192.168.1.4; mac: 00-00-00-00-00-04	1
A	IP:192.168.2.1; mac: 00-00-00-00-00-01	1
B	IP:192.168.1.2; mac: 00-00-00-00-00-02	1
C	IP:192.168.2.3; mac: 00-00-00-00-00-03	some

There is a normal communication between B and C on above diagram. A wants switch to forward packets sent by B to itself, so need switch sends the packets transfer from B to A. firstly A sends ARP reply packet to switch, format is: 192.168.2.3, 00-00-00-00-00-01, mapping its MAC address to C's IP, so the switch changes IP address when it updates ARP list., then data packet of 192.168.2.3 is transferred to 00-00-00-00-00-01 address (A MAC address).

In further, a transfers its received packets to C by modifying source address and

destination address, the mutual communicated data between B and C are received by A unconsciously. Because the ARP list is update timely, another task for A is to continuously send ARP reply packet, and refreshes switch ARP list.

So it is very important to protect ARP list, configure to forbid ARP learning command in stable environment, and then change all dynamic ARP to static ARP, the learned ARP will not be refreshed, and protect for users.

```
Switch#config
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)#arp 192.168.2.1 00-00-00-00-00-01 interface eth 1/0/2
Switch(Config-If-Vlan1)#interface vlan 2
Switch(Config-If-Vlan2)#arp 192.168.1.2 00-00-00-00-00-02 interface eth 1/0/2
Switch(Config-If-Vlan2#interface vlan 3
Switch(Config-If-Vlan3)#arp 192.168.2.3 00-00-00-00-00-03 interface eth 1/0/2
Switch(Config-If-Vlan3)#exit
Switch(Config)#ip arp-security learnprotect
Switch(Config)#
Switch(config)#ip arp-security convert
```

If the environment changing, it enable to forbid ARP refresh, once it learns ARP property, it wont be refreshed by new ARP reply packet, and protect use data from sniffing.

```
Switch#config
Switch(config)#ip arp-security updateprotect
```

Chapter 4 ARP GUARD Configuration

4.1 Introduction to ARP GUARD

There is serious security vulnerability in the design of ARP protocol, which is any network device, can send ARP messages to advertise the mapping relationship between IP address and MAC address. This provides a chance for ARP cheating. Attackers can send ARP REQUEST messages or ARP REPLY messages to advertise a wrong mapping relationship between IP address and MAC address, causing problems in network communication. The danger of ARP cheating has two forms: 1. PC4 sends an ARP message to advertise that the IP address of PC2 is mapped to the MAC address of PC4, which will cause all the IP messages to PC2 will be sent to PC4, thus PC4 will be able to monitor and capture the messages to PC2; 2. PC4 sends ARP messages to advertise that the IP address of PC2 is mapped to an illegal MAC address, which will prevent PC2 from receiving the messages to it. Particularly, if the attacker pretends to be the gateway and do ARP cheating, the whole network will be collapsed.

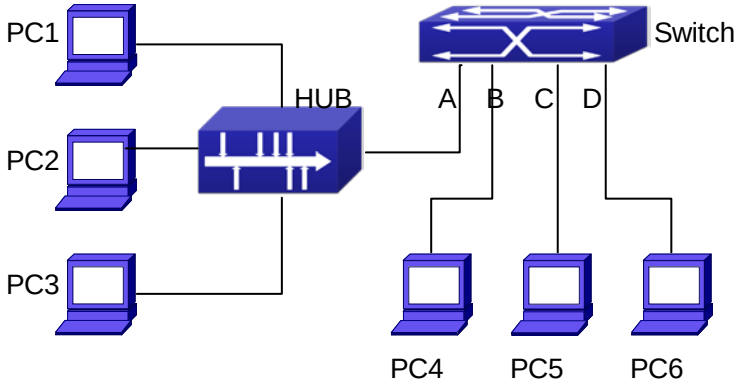


Fig 4-1 ARP GUARD schematic diagram

We utilize the filtering entries of the switch to protect the ARP entries of important network devices from being imitated by other devices. The basic theory of doing this is that utilizing the filtering entries of the switch to check all the ARP messages entering through the port, if the source address of the ARP message is protected, the messages will be directly dropped and will not be forwarded.

ARP GUARD function is usually used to protect the gateway from being attacked. If all the accessed PCs in the network should be protected from ARP cheating, then a large number of ARP GUARD address should be configured on the port, which will take up a big part of FFP entries in the chip, and as a result, might affect other applications. So this will be improper. It is recommended that adopting FREE RESOURCE related accessing

scheme. Please refer to relative documents for details.

4.2 ARP GUARD Configuration Task List

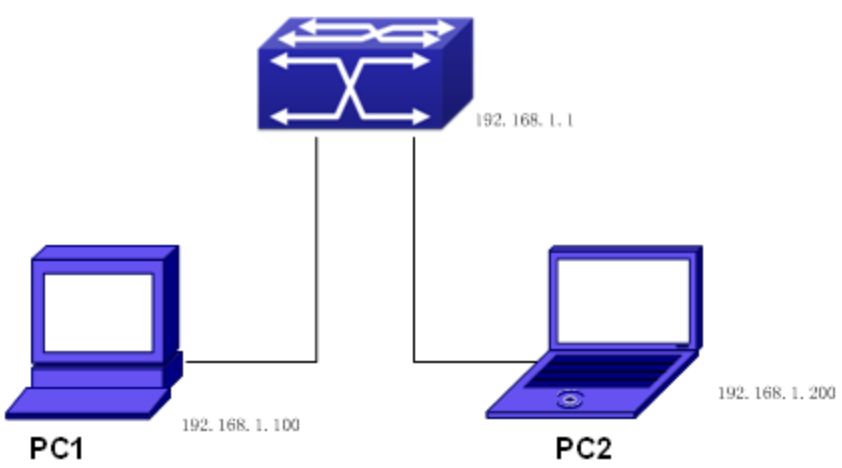
1. Configure the protected IP address

Command	Explanation
Port configuration mode	
arp-guard ip <addr> **no arp-guard ip <addr>**	Configure/delete ARP GUARD address

Chapter 5 ARP Local Proxy Configuration

5.1 Introduction to ARP Local Proxy function

In a real application environment, the switches in the aggregation layer are required to implement local ARP proxy function to avoid ARP cheating. This function will restrict the forwarding of ARP messages in the same vlan and thus direct the L3 forwarding of the data flow through the switch.



As shown in the figure above, PC1 wants to send an IP message to PC2, the overall procedure goes as follows (some non-arp details are ignored)

1. Since PC1 does not have the ARP of PC2, it sends and broadcasts ARP request.

2. Receiving the ARP message, the switch hardware will send the ARP request to CPU instead of forwarding this message via hardware, according to new ARP handling rules.

3. With local ARP proxy enabled, the switch will send ARP reply message to PC1 (to fill up its mac address)

4. After receiving the ARP reply, PC1 will create ARP, send an IP message, and set the destination MAC of the Ethernet head as the MAC of the switch.

5. After receiving the ip message, the switch will search the router table (to create router cache) and distribute hardware entries.

6. If the switch has the ARP of PC2, it will directly encapsulate the Ethernet head and send the message (the destination MAC is that of PC2)

7. If the switch does not have the ARP of PC2, it will request it and then send the ip message.

This function should cooperate with other security functions. When users configure local ARP proxy on an aggregation switch while configuring interface isolation function on the layer-2 switch connected to it, all ip flow will be forwarded on layer 3 via the aggregation switch. And due to the interface isolation, ARP messages will not be forwarded within the vlan, which means other PCs will not receive it.

5.2 ARP Local Proxy Function Configuration Task List

1. Enable/disable ARP local proxy function

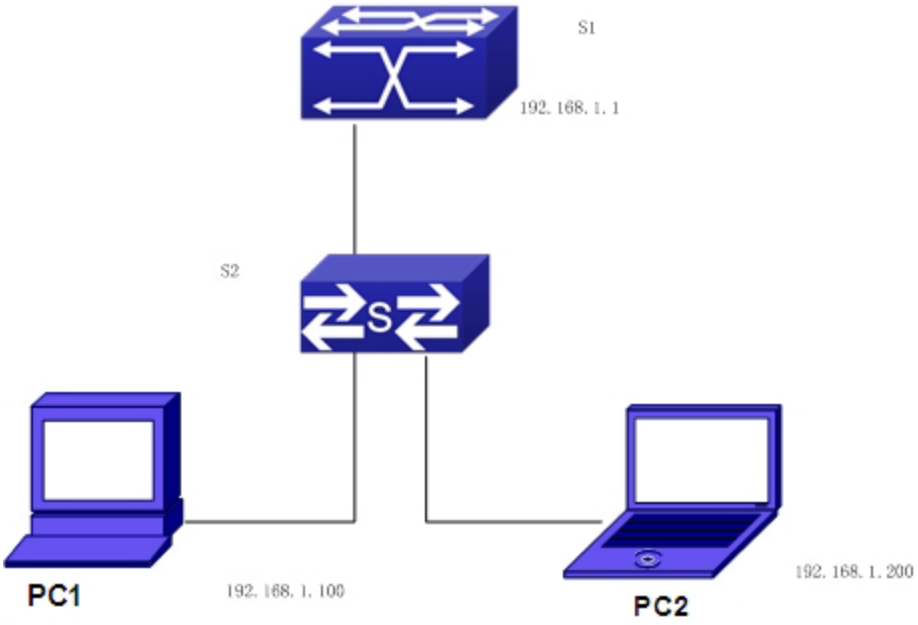
1. Enable/disable ARP local proxy function

Command	Explanation
Interface vlan mode	
ip local proxy-arp **no ip local proxy-arp**	Enable or disable ARP local proxy function.

5.3 Typical Examples of ARP Local Proxy Function

As shown in the following figure, S1 is a medium/high-level layer-3 switch supporting ARP local proxy, S2 is layer-2 access switches supporting interface isolation.

Considering security, interface isolation function is enabled on S2. Thus all downlink ports of S2 is isolated from each other, making all ARP messages able to be forwarded through S1. If ARP local proxy is enabled on S1, then all interfaces on S1 isolate ARP while S1 serves as an ARP proxy. As a result, IP flow will be forwarded at layer 3 through S1 instead of S2.



We can configure as follows:

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip address 192.168.1.1 255.255.255.0

Switch(Config-if-Vlan1)#ip local proxy-arp

Switch(Config-if-Vlan1)#exit

5.4 ARP Local Proxy Function Troubleshooting

ARP local proxy function is disabled by default. Users can view the current configuration with display command. With correct configuration, by enabling debug of ARP, users can check whether the ARP proxy is normal and send proxy ARP messages.

In the process of operation, the system will show corresponding prompts if any operational error occurs.

Chapter 6 Gratuitous ARP Configuration

6.1 Introduction to Gratuitous ARP

Gratuitous ARP is a kind of ARP request that is sent by the host with its IP address as the destination of the ARP request.

The basic working mode for the switch is as below: The Layer 3 interfaces of the switch can be configured to advertise gratuitous ARP packets period or the switch can be configured to enable to send gratuitous ARP packets in all the interfaces globally.

The purpose of gratuitous ARP is as below:

1. To reduce the frequency that the host sends ARP request to the switch. The hosts in the network will periodically send ARP requests to the gateway to update the MAC address of the gateway. If the switch advertises gratuitous ARP requests, the host will not have to send these requests. This will reduce the frequency the hosts' sending ARP requests for the gateway's MAC address.
2. Gratuitous ARP is a method to prevent ARP cheating. The switch's advertising gratuitous ARP request will force the hosts to update its ARP table cache. Thus, forged ARP of gateway cannot function.

6.2 Gratuitous ARP Configuration Task List

1. Enable gratuitous ARP and configure the interval to send gratuitous ARP request
2. Display configurations about gratuitous ARP

1. Enable gratuitous ARP and configure the interval to send gratuitous ARP request.

Command	Explanation
Global Configuration Mode and Interface Configuration Mode.	
ip gratuitous-arp <*5-1200*> **no ip gratuitous-arp**	To enable gratuitous ARP and configure the interval to send gratuitous ARP request. The no command cancels the gratuitous ARP.

2. Display configurations about gratuitous ARP

Command	Explanation
Admin Mode and Configuration Mode	
show ip gratuitous-arp [interface vlan *<1-4094>*]	To display configurations about gratuitous ARP.

6.3 Gratuitous ARP Configuration Example

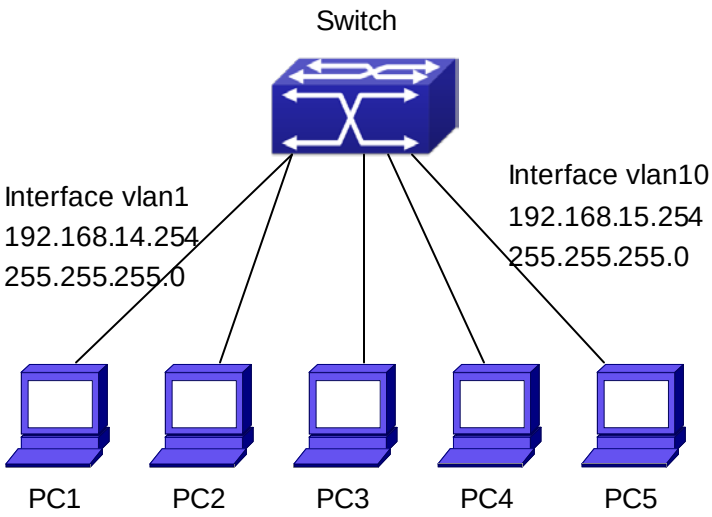


Fig 6-1 Gratuitous ARP Configuration Example

For the network topology shown in the figure above, interface VLAN10 whose IP address is 192.168.15.254 and network address mask is 255.255.255.0 in the switch system. Three PCs – PC3, PC4, PC5 are connected to the interface. The IP address of interface VLAN 1 is 192.168.14.254, its network address mask is 255.255.255.0. Two PCs – PC1 and PC2 are connected to this interface. Gratuitous ARP can be enabled through the following configuration:

1. Configure two interfaces to use gratuitous ARP at one time.

Switch(config)#ip gratuitous-arp 300
Switch(config)#exit

2. Configure gratuitous ARP specifically for only one interface at one time.

Switch(config)#interface vlan 10
Switch(Config-if-Vlan10)#ip gratuitous-arp 300
Switch(Config-if-Vlan10)#exit
Switch(config) #exit

6.4 Gratuitous ARP Troubleshooting

Gratuitous ARP is disabled by default. And when gratuitous ARP is enabled, the debugging information about ARP packets can be retrieved through the command debug ARP send.

If gratuitous ARP is enabled in global configuration mode, it can be disabled only in global configuration mode. If gratuitous ARP is configured in interface configuration mode, the configuration can only be disabled in interface configuration mode.

Chapter 7 ND Snooping Configuration

7.1 Introduction to ND Snooping

The purpose of developing ND snooping module: using Control Packet Snooping (CPS) mechanism, that means to detect the validity of access packets through the method which bind the source IPv6 address and the anchor information, so as to permit the matched packets and drop the unmatched packets that will control access of the direct connected IPv6 nodes. The development of this module requirement refers to IPv6 NDP and 《Control Packet Snooping Based Binding draft-bi-savi-cps-00》 draft. ND snooping adopts the "first-come first-serve" of the 《First-Come First-Serve Source-Address Validation Implementation draft-ietf-savi-fcfs-01》 draft that means to set up the first bound nodes as the legality nodes, and it is a principle to check the validity of the nodes.

ND snooping is mostly applied to the access device (such as layer 2 switch, wireless access node). The access device creates the binding information table of link-local nodes (the binding refers to the IPv6 address and the port ID and the MAC address of the nodes) according to the NDP packets received from theses ports, then creates the rules of FFP (Fast Filter Processor) hardware drive according to the binding information table, and implements the access control of the link-local nodes.

7.2 ND Snooping Basic Configuration

ND Snooping Configuration Task List:

1. Enable or disable the monitor function of ND Snooping
2. Configure the lifetime of ND Snooping
    1) Set the binding lifetime of SAC_BOUND state
    2) Set the binding lifetime of SAC_START state
    3) Set the binding lifetime of SAC-QUERY state
3. The binding function of ND Snooping
    1) Configure the dynamic binding policy of ND Snooping address
    2) Add a static binding
    3) Configure the max number of IPv6 addresses that can be bound to the same MAC address
    4) Set the max binding number for the ports
    5) Clear all dynamic bindings of ND Snooping
4. Set the trust port of the switch

1. Enable or disable the monitor function of ND Snooping

Command	Expalnation
Global mode	
ipv6 nd snooping enable **no ipv6 nd snooping enable**	Enable or disable ND Snooping globally.
Port mode	
ipv6 nd snooping user-control **no ipv6 nd snooping user-control**	Enable or disable ND Snooping in a port.

2. Configure the lifetime of ND Snooping

Command	Explanation
Global mode	
[no] ipv6 nd snooping max-sac-lifetime <*max-sac-lifetime*>	Reset the binding lifetime as <*max-sac-lifetime*> or 2 hours for SAC_BOUND.
[no] ipv6 nd snooping max-dad-delay <*max-dad-delay*>	Reset the binding lifetime as <*max-dad-delay*> or 1 second for SAC_START.
[no] ipv6 nd snooping max-dad-prepare-delay <*max-dad-prepare-delay*>	Reset the binding lifetime as <*max-dad-prepare-delay*> half a second for SAC_QUERY.

3. The binding function of ND Snooping

Command	Explanation
Global mode	
ipv6 nd snooping policy {bind-eui64-address | bind-non-eui64-address} **no ipv6 nd snooping policy**	Configure the dynamic binding policy of ND Snooping address.
ipv6 nd snooping static-binding <*ipv6-address*> hardware-address <*hardware-address*> interface <*interface-name*> **no ipv6 nd snooping static-binding <*ipv6-address*>**	Add a static binding.

ipv6 nd snooping mac-binding-limit <*number*> **no ipv6 nd snooping mac-binding-limit**	Configure the max number of IPv6 addresses that can be bound to the same MAC address.
Port mode	
ipv6 nd snooping port-binding-limit <*binding-number*> **no ipv6 nd snooping port-binding-limit**	Set the binding number for the ports. The binding number only limits the dynamic binding number of the ports, do not limit the static binding number of the ports.
Admin mode	
clear ipv6 nd snooping binding [<*interface-name*>]	Clear all static binding of ND Snooping.

4. Set the trust port of the switch

Command	Explanation
Global mode	
ipv6 nd snooping trust **no ipv6 nd snooping trust**	Set the trust port of the switch.

7.3 ND Snooping Example

Typical example:

The application environment of ND Snooping, the figure is as follows:

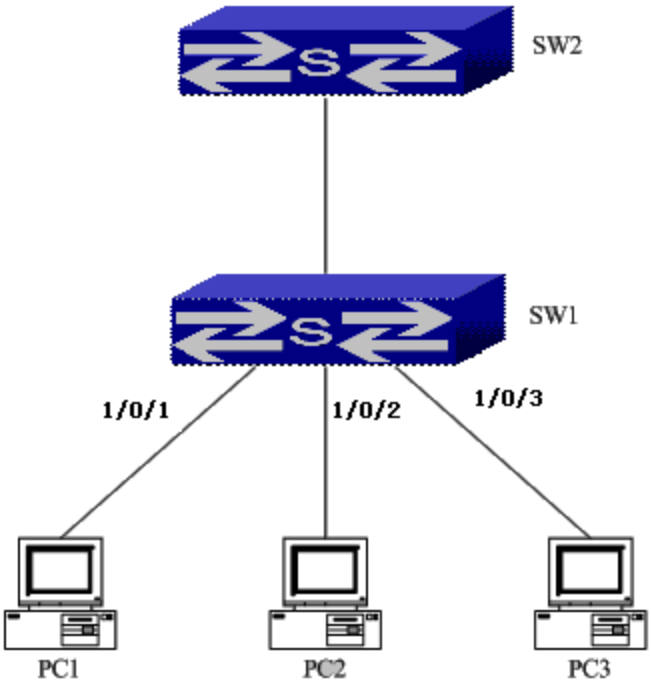


Fig 7-1 ND Snooping typical configuration

The configuration explanation:

SW2 is layer 3 switch, it connect to the layer 2 switch SW1, and enable IPv6 function and RA function;

SW1 is layer 2 switch, it enables IPv6 function and ND Snooping, and enable the control function of ND snooping on the ports which connect three PC nodes.

PC1, PC2, PC3 are three PCs, each PC installed IPv6 protocol and directly connect SW1, the direct ports are 1/0/1, 1/0/2, 1/0/3.

Layer 2 switch SW1 enabled ND Snooping. PC1, PC2 and PC3 correctly receive RA router advertisement packets from SW2. According to the link prefix 2001::/64 of RA packets, three PCs create IPv6 addresses automatically, they are:

PC1: FE80::2AA:FF:FE9A:4CA2, 2001::2AA:FF:FE9A:4CA2, 2001::23:4A:1122:C411;

PC2: FE80::2BB:FF:FE9A:4CA2, 2001::2BB:FF:FE9A:4CA2, 2001::32:4B:2211:11C4;

PC3: FE80::2CC:FF:FE9A:4CA2, 2001::2CC:FF:FE9A:4CA2, 2001::22:4A:1133:C422;

At the same time, three PCs send the DAD (duplicate address detect) NS packets to the link-local, ND Snooping module receives DAD NS packets and set up the corresponding dynamic binding table according to these packets , the table is as follows:

IPv6 address	MAC address	Port ID
FE80::2AA:FF:FE9A:4CA2	02-AA-00-9A-4C-A2	1/0/1
2001::2AA:FF:FE9A:4CA2	02-AA-00-9A-4C-A2	1/0/1
2001::23:4A:1122:C411	02-AA-00-9A-4C-A2	1/0/1
FE80:: BB:FF:FE9A:4CA2	02-BB-00-9A-4C-A2	1/0/2

2001::2BB:FF:FE9A:4CA2	02-BB-00-9A-4C-A2	1/0/2
2001::32:4B:2211:11C4	02-BB-00-9A-4C-A2	1/0/2
FE80:: CC:FF:FE9A:4CA2	02-CC-00-9A-4C-A2	1/0/3
2001::2CC:FF:FE9A:4CA2	02-CC-00-9A-4C-A2	1/0/3
2001::22:4A:1133:C422	02-CC-00-9A-4C-A2	1/0/3

If three PCs do not receive the responding DAD NA packets in the set time, then port 1/0/1, port 1/0/2, port 1/0/3 send to the FFP hardware drive binding entries according to the dynamic binding table. After that, these port will detect the source addresses of the received data packet, if it match the binding entries, then the IPv6 packet are allowed to pass, otherwise, the IPv6 packet are denied.

Configuration steps:

SW1:

SW1(config)# ipv6 nd snooping enable

SW1(config)# interface vlan 1

SW1(config-if-vlan1)# ipv6 address 2001::1/64

SW1(config)# interface ethernet 1/0/1; 1/0/2; 1/0/3

SW1(config-if-port-range)# ipv6 nd snooping user-control

SW2:

SW2(config)# interface vlan 1

SW2(config-if-vlan1)# ipv6 address 2001::2/64

SW2(config-if-vlan1)# no ipv6 nd suppress-ra

7.4 ND Snooping Troubleshooting

If there is any problem happens when using ND Snooping, please check whether the problem is caused by the following reasons:

- ☞ Whether ipv6 nd snooping enable is enabled globally and ipv6 nd snooping user-control is configured in the port.
- ☞ Use debug ipv6 nd snooping to check whether the switch can correctly receive and process the relative packets.
- ☞ After the switch connects PC and enables ND Snooping function, it can not set up the binding except the port that connects to PC is shutdown/no shutdown.

Chapter 8 Keepalive Gateway Configuration

8.1 Introduction to Keepalive Gateway

Ethernet port is used to process backup or load balance, for the reason that it is a broadcast channel, it may not detect the change of physical signal and fails to get to down when the gateway is down. Keepalive Gateway is introduced to detect the connectivity to the higher-up gateway, in the case that a Ethernet port connect with a higher-up gateway to form a point-to-point network topology.

For example: router connects optical terminal device and the line is up all the time, While the line between moden and remote gateway is down, it is necessary to use a effective method to detect whether the remote gateway is reachable. At present, detect gateway connectivity by sending ARP request to gateway on time, if ARP resolution is failing, shutdown the interface, if ARP resolution is successful, keep the interface up.

Only layer 3 switch supports keepalive gateway function.

8.2 Keepalive Gateway Configuration Task List

1. Enable or disable keepalive gateway, configure the interval period that ARP request packet is sent and the retry-count after detection is failing
2. Show keepalive gateway and IPv4 running status of the interface

1. Enable or disable keepalive gateway, configure the interval period that ARP request packet is sent and the retry-count after detection is failing

Command	Explanation
Interface mode	
keepalive gateway <ip-address> [{<interval-seconds> | msec <interval-millisecond >} [retry-count]] **no keepalive gateway**	Enable keepalive gateway, configure IP address of gateway, the interval period that ARP request packet is sent, and the retry-count after detection is failing, the no command disables the function.

2. Show keepalive gateway and IPv4 running status of interface

Command	Explanation

Admin and configuration mode	
show keepalive gateway [interface-name]	Show keepalive running status of the specified interface, if there is no interface is specified, show keepalive running status of all interfaces.
show ip interface [interface-name]	Show IPv4 running status of the specified interface, if there is no interface is specified, show IPv4 running status of all interfaces.

8.3 Keepalive Gateway Example

Fig 8-1 keepalive gateway typical example

In above network topology, interface address of interface vlan10 is 1.1.1.1 255.255.255.0 for gateway A, interface address of interface vlan100 is 1.1.1.2 255.255.255.0 for gateway B, gateway B supports keepalive gateway function, the configuration in the following:

1. Adopt the default interval that ARP packet is sent and the retry-count after detection is failing (the default interval is 10s, the default retry-count is 5 times)

Switch(config)#interface vlan 100
Switch(config-if-vlan100)#keepalive gateway 1.1.1.1
Switch(config-if-vlan100)#exit

2. Configure the interval that ARP packet is sent and the retry-count after detection is failing manually.

Switch(config)#interface vlan 100

Switch(config-if-vlan100)#keepalive gateway 1.1.1.1 3 3
Switch(config-if-vlan100)#exit

Send ARP detection once 3 seconds to detect whether gateway A is reachable, after 3 times detection is failing, gateway A is considered to be unreachable.

8.4 Kepalive Gteway Troubleshooting

If there is any problem happens when using keepalive gateway function, please check whether the problem is caused by the following reasons:

- ☞ Make sure the device is layer 3 switch, layer 2 switch does not support keepalive gateway
- ☞ The detection method is used to point-to-point topology mode only
- ☞ Detect IPv4 accessibility by the method, so the detection result only affects IPv4 traffic, other traffic such as IPv6 is not affected
- ☞ Physical state of interface only controlled by physical signal
- ☞ Interface can't run IPv4 after determine gateway is not reachable, so all relative IPv4 routes are deleted and IPv4 route protocol can't establish the neighbor on the interface