FS.COM

FiberstoreOS

Security Configuration Guide

Contents

1 Configuring Port Security......6
1.1 Overview......6
1.2 Topology......7
1.3 Configurations......7
1.4 Validation......8
2 Configuring Vlan Security......9
2.1 Overview......9
2.2 Configuring vlan mac-limit......9
2.3 Configuring vlan mac learning......10
2.4 Validation......10
3 Configuring Time Range......11
3.1 Overview......11
3.2 Configuration......11
3.3 Validation......12
4 Configuring ACL......13
4.1 Overview......13
4.2 Terminology......13
4.3 Limitation......14
4.4 Configuration......14
4.5 Validation......17
5 Configuring Extend ACL......18
5.1 Overview......18
5.2 Terminology......18
5.3 Topology......19
5.4 Configuration......19
5.5 Validation......20
6 Configuring ACLv6......22
6.1 Overview......22
6.2 Terminology......22
6.3 Limitation......23
6.4 Topology......23
6.5 Configuration......23

6.6 Validation......25

7 Configuring Dot1x......26

7.1 Overview......26

7.2 Topology......27

7.3 Configuration......27

7.4 Validation......31

8 Configuring Guest VLAN......33

8.1 Overview......33

8.2 Topology......34

8.3 Configuration......35

8.4 Validation......36

9 Configuring Arp Inspection......41

9.1 Overview......41

9.2 Terminology......41

9.3 Topology......42

9.4 Configurations......43

9.5 Validation......44

10 Configuring DHCP Snooping......46

10.1 Overview......46

10.2 Topology......46

10.3 Configuration......47

10.4 Validation......48

11 Configuring IP Source Guard......50

11.1 Overview......50

11.2 Terminology......51

11.3 Topology......51

11.4 Configuration......52

11.5 Validation......53

12 Configuring RADIUS Authentication......54

12.1 Overview......54

12.2 Topology......54

12.3 Configuration......55

12.4 Validation......59

12.5 Display Results......60

13 Configuring Tacacs+......61

13.1 Overview......61

13.2 Topology......61

13.3 Configuration Steps......62

13.4 Configuration TACACS+ Server.. 62
13.5 Validation.. 63
13.6 Display Results.. 64

14 Configuring Port Isolate...65
14.1 Overview... 65
14.2 Topology... 65
14.3 Configuration... 66

15 Configuring Private-vlan...67
15.1 Overview... 67
15.2 Topology... 67
15.3 Configuration... 68
15.4 Validation.. 69

16 Configuring DDOS..70
16.1 Overview... 70
16.2 Topology... 71
16.3 Configuration... 71
16.4 Validation.. 73

17 Configuring Key Chain..74
17.1 Overview... 74
17.2 Configurations...74
17.3 Validation.. 75

18 Configuring Port-Block..75
18.1 Overview... 75
18.2 Configurations...76
18.3 Validation.. 76

Figures

Figure 1-1 Port Security topology....7

Figure 4-1 ACL.... 15

Figure 5-1 Extend ACL.... 19

Figure 7-1 Dot1x Basic topology.... 27

Figure 7-2 Select "Settings" -> "System"....30

Figure 7-3 Configure the shared-key, authorization port and account port....31

Figure 7-4 Add user name and password on the server....31

Figure 8-1 supplicant is not 802.1x capable....34

Figure 8-2 supplicant is 802.1x capable and authenticated....35

Figure 9-1 ARP Inspection Topology....42

Figure 10-1 DHCP Snooping Topology....47

Figure 11-1 IP Source Guard....52

Figure 12-1 RADIUS authentication application....54

Figure 12-2 Configure IP address.... 56

Figure 12-3 Ping test.... 57

Figure 12-4 Open software on server....57

Figure 12-5 Set system....58

Figure 12-6 Add user....58

Figure 12-7 Ping test.... 59

Figure 12-8 Telnet test....60

Figure 13-1 TACACS+ authentication application.... 61

Figure 13-2 Ping result....63

Figure 13-3 Telnet result.... 64

Figure 14-1 Basic topology for port-isolate.... 65

Figure 15-1 Basic topology for private vlan.... 67

Figure 16-1 DDos prevent topology....71

1 Configuring Port Security

1.1 Overview

Port security feature is used to limit the number of "secure" MAC addresses learnt on a particular interface. The interface will forward packets only with source MAC addresses that match these secure addresses. The secure MAC addresses can be created manually, or learnt automatically. After the number of secure MAC addresses reaches the limit for the number of secure MAC addresses, new MAC address can't be learnt or configured on the interface. if the interface then receives a packet with a source MAC address that is different with any of the secure addresses, it is considered as a security violation.

Port security feature also binds a MAC to a port so that the port does not forward packets with source addresses that are outside of defined addresses. If a MAC addresses configured or learnt on a secure port attempts to access another port, this is also considered as a security violation.

Two types of secure MAC addresses are supported:

Static secure MAC addresses: These are manually configured by the interface configuration command switchport port-security mac-address MAC.

Dynamic secure MAC addresses: These are dynamically learnt.

If a security violation occurs, the packets to be forwarded will be dropped.

1.2 Topology

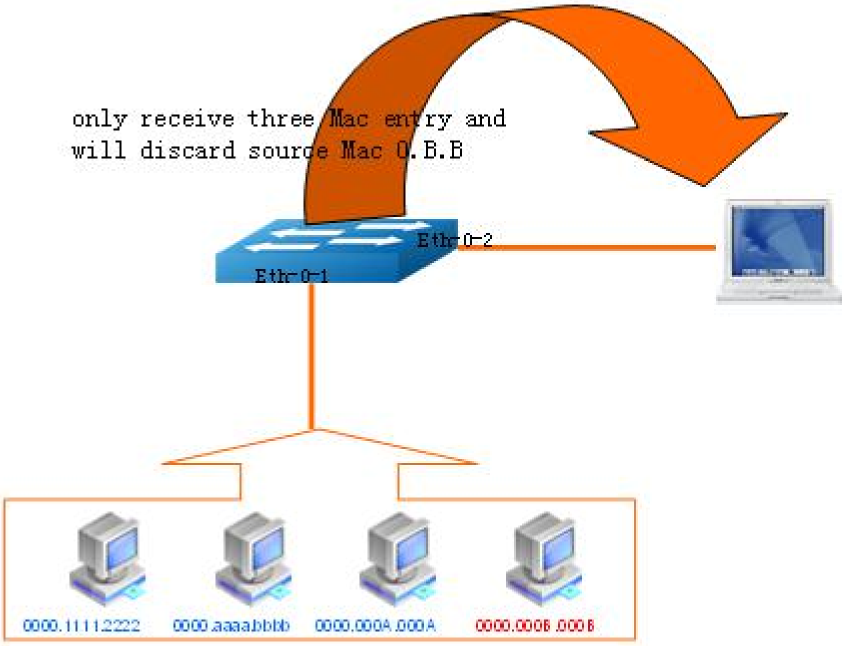


Figure 1-1 Port Security topology

1.3 Configurations

Following these steps to enable and configure port security.

Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1)to be configured and enter the Interface mode
Switch(config-if)# switchport	Configure Layer2 interface
Switch(config-if)# switchport port-security	Enable port security on the port
Switch(config-if)# switchport port-security maximum 3	Set maximum secure MAC addresses for this interface
Switch(config-if)# switchport port-security mac-address 0000.1111.2222 vlan 1	Add a secure MAC address 0000.1111.2222 for this interface
Switch(config-if)# switchport port-security mac-address 0000.aaaa.bbbb vlan 1	Add a secure MAC address 0000.aaaa.bbbb for this interface
Switch(config-if)# switchport port-security violation restrict	Set port security violation mode
Switch(config-if)# end	Return to privileged EXEC mode
Switch# show port-security	Verify the configuration

1.4 Validation

```
Switch# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolationMode
               (Count)        (Count)
---------------------------------------------------------------
  eth-0-1           3             2       restrict
```

```
Switch# show port-security address-table
          Secure MAC address table
--------------------------------------------------------
Vlan    Mac Address       Type                 Ports
----    -----------       -------              -------
1       0000.1111.2222    SecureConfigured     eth-0-1
1       0000.aaaa.bbbb    SecureConfigured     eth-0-1
```

```
Switch# show port-security interface eth-0-1
Port security                    : enabled
Violation mode                       : discard packet and log
Maximum MAC addresses                : 3
Total MAC addresses                  : 2
Static configured MAC addresses  : 2
```

2 Configuring Vlan Security

2.1 Overview

Vlan security feature is used to limit the total number of MAC addresses learnt in a particular vlan. The MAC addresses can be added manually, or learnt automatically. After the device reaches the limit for the number of MAC addresses on the vlan, if the vlan receives a packet with an unknown source MAC address, the configured action will take effect.

Two types of MAC addresses are supported:

- Static MAC addresses: These are manually configured by users.
- Dynamic MAC addresses: These are dynamically learnt.

Three types of actions are supported:

- Discard: Packet with an unknown source MAC address from the vlan will be discarded and its source MAC address will not be learnt.
- Warn: Packet with an unknown source MAC address from the vlan will be discarded, its source MAC address will not be learnt, but warning log will be printed in syslog.
- Forward: Packets from the vlan will be forwarded without MAC learning or warning log.

2.2 Configuring vlan mac-limit

Follow these steps to configure vlan mac-limit.

Switch# configure terminal	Enter the Configure mode
Switch(config)# vlan database	Enter the Vlan mode
Switch(config)# vlan 2	Create vlan 2
Switch(config-vlan)# vlan 2 mac-limit maximum 100	Configure maximum of MAC addresses in vlan 2

Switch(config-vlan)# vlan 2 mac-limit action discard	Configure action as “discard”
Switch(config-vlan)#end	Return to privileged EXEC mode
Switch# show vlan-security	Verify the configuration

2.3 Configuring vlan mac learning

Follow these steps to configure vlan mac learning.

Switch# configure terminal	Enter the Configure mode
Switch(config)# vlan database	Enter the Vlan mode
Switch(config)# vlan 2	Create a vlan
Switch(config-vlan)# vlan 2 mac learning disable	Disable mac learning on vlan 2
Switch(config-vlan)# end	Return to privileged EXEC mode
Switch# show vlan-security	Verify the configuration

2.4 Validation

Switch# show vlan-security

```
Vlan  learning-en  max-mac-count  cur-mac-count  action
-------------------------------------------------------
2     Disable      100            0              Discard
```

3 Configuring Time Range

3.1 Overview

A time range is created that defines specific absolute times or periodic times of the day and week in order to implement time-based function, such as ACLs. The time range is identified by a name and then referenced by a function, which by itself has no relevance. Therefore, the time restriction is imposed on the function itself. The time range relies on the system clock.

3.2 Configuration

Create an absolute time range

Switch# configure terminal	Enter the Configure mode
Switch(config)# time-range test-absolute	Create a time-range and enter time-range configure mode
Switch(config-tm-range)# absolute start 1:1:2 jan 1 2012 end 1:1:3 jan 7 2012	Create absolute time range
Switch(config-tm-range)# end	Exit time range configure mode

Create a periodic time range

Switch# configure terminal	Enter the Configure mode
Switch(config)# time-range test-periodic	Create a time-range and enter time-range configure mode
Switch(config-tm-range)# periodic 1:1 mon to 1:1 wed	Create periodic time range
Switch(config-tm-range)# end	Exit time range configure mode

3.3 Validation

DUT1# show time-range

```
time-range test-absolute
   absolute start 01:01:02 Jan 01 2012 end 01:01:03 Jan 07 2012
time-range test-periodic
   periodic 01:01 Mon to 01:01 Wed
```

4 Configuring ACL

4.1 Overview

Access control lists (ACLs) classify traffic with the same characteristics. The ACL can have multiple access control entries (ACEs), which are commands that match fields against the contents of the packet. ACLs can filter packets received on interface by many fields such as ip address, mac address and deny or permit the packets.

4.2 Terminology

The following terms and concepts are used to describe ACL.

Access control entry (ACE)

Each ACE includes an action element (permit or deny) and a filter element based on criteria such as source address, destination address, protocol, and protocol-specific parameters.

MAC ACL

MAC ACL can filter packet by mac-sa and mac-da, and the mac-address can be masked, or configured as host id, or configured as any to filter all MAC addresses. MAC ACL can also filter other L2 fields such as COS, VLAN-ID, INNER-COS, INNER-VLAN-ID, L2 type, L3 type.

IPv4 ACL

IPv4 ACL can filter packet by ip-sa and ip-da, and ip-address can be masked, or configured as host id, or configured as any to filter all IPv4 address. IPv4 ACL can also filter other L3 fields such as DSCP, L4 protocol and L4 fields such as TCP port, UDP port, and so on.

Time Range

Time range can define a period of time only between which the ACE can be valid if the ACE is associated to the time range.

4.3 Limitation

If the incoming packet has only one vlan tag, the fields inner-cos and inner-vlan-id will be set to value 0 default, so the configuration with inner-vlan and inner-cos may have different effect between situation that packet has one vlan tag and that packet has two vlan tags.

4.4 Configuration

In this example, use MAC ACL on interface eth-0-1, to permit packets with source mac 0000.0000.1111 and deny any other packets. Use IPv4 ACL on interface eth-0-2, to permit packets with source ip 1.1.1.1/24 and deny any other packets.

Topology

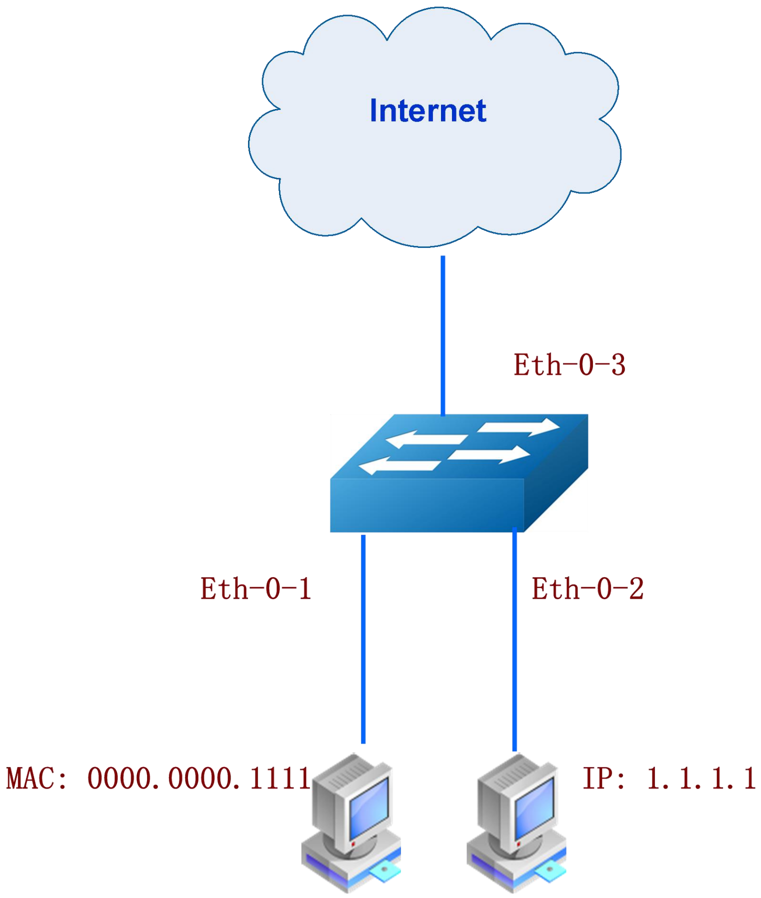


Figure 4-1 ACL

Configuration ACL details

Switch# configure terminal	Enter configuration mode
Switch(config)#mac access-list mac	Define a MAC ACL and enter ACL configuration mode
Switch(config-mac-acl)# permit src-mac host 0000.0000.1111 dest-mac any	Config ACE to permit packet with source mac address 0000.0000.1111
Switch(config-mac-acl)# deny src-mac any dest-mac any	Config ACE to deny any packets
Switch(config-mac-acl)# exit	Exit ACL configuration mode
Switch(config)# ip access-list ipv4	Define an IPv4 ACL and enter ACL configuration mode

Switch(config-ip-acl)# permit any 1.1.1.1 0.0.0.255 any	Config ACE to permit subnet 1.1.1.1/24
Switch(config-ip-acl)# deny any any any	Config ACE to deny any packets
Switch(config-ip-acl)# exit	Exit ACL configuration mode

Apply ACL

Switch# configure terminal	Enter configuration mode
Switch(config)# class-map cmap1	Create a class-map cmap1 and enter class-map configuration mode
Switch(config-cmap)# match access-group mac	Define the match criterion (match mac ACL) to classify traffic
Switch(config-cmap)# exit	Exit class-map configuration mode
Switch(config)# policy-map pmap1	Create a policy map pmap1 and enter policy-map configuration mode
Switch(config-pmap)# class cmap1	Define a traffic classification(match cmap1), and enter policy-map class configuration mode
Switch(config-pmap-c)# exit	Exit policy-map class configuration mode
Switch(config-pmap)# exit	Exit policy-map configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# service-policy input pmap1	Apply service-policy pmap1 on interface with ingress direction
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# class-map cmap2	Create a class-map cmap2 and enter class-map configuration mode
Switch(config-cmap)# match access-group ipv4	Define the match criterion (match ACL ipv4) to classify traffic
Switch(config-cmap)# exit	Exit class-map configuration mode
Switch(config)# policy-map pmap2	Create a policy map pmap2 and enter policy-map configuration mode
Switch(config-pmap)# class cmap2	Define a traffic classification(match cmap2), and enter policy-map class configuration mode
Switch(config-pmap-c)# exit	Exit policy-map class configuration mode
Switch(config-pmap)# exit	Exit policy-map configuration mode
Switch(config-if)# interface eth-0-2	Enter interface configuration mode
Switch(config-if)# service-policy input pmap2	Apply service-policy pmap2 on interface with ingress direction

4.5 Validation

The result of show running-config is as follows.

Switch# show running-config

```
mac access-list mac
  10 permit src-mac host 0000.0000.1111 dest-mac any
  20 deny src-mac any dest-mac any
!

ip access-list ipv4
  10 permit any 1.1.1.0 0.0.0.255 any
  20 deny any any any
!
class-map match-any cmap1
 match access-group mac
!
class-map match-any cmap2
 match access-group ipv4
!
policy-map pmap1
 class cmap1
!
policy-map pmap2
 class cmap2
!
interface eth-0-1
 service-policy input pmap1
!
interface eth-0-2
 service-policy input pmap2
!
```

5 Configuring Extend ACL

5.1 Overview

Extend IPv4 ACL combines MAC filters with IP filters in one access list. Different from MAC and IP ACL, extend ACL can access-control all packets (IP packets and non-IP packets). Extend ACL supported extend IPv4 ACL.

5.2 Terminology

Following is a brief description of terms and concepts used to describe the extend ACL

Extend IPv4 ACL

Extend IPv4 ACL takes advantages of MAC ACL and IPv4 ACL, which combines MAC ACE with IPv4 ACE in an ACL to provide more powerful function of access-controlling traverse packets.

Filter packets by mac-sa and mac-da, and the mac-address can be masked, or configured as host id, or configured as any to filter all MAC addresses. Other L2 fields, such as COS, VLAN-ID, INNER-COS, INNER-VLAN-ID, L2 type, L3 type, can also be filtered by MAC ACE.

Filter packets by ip-sa and ip-da, and ip-address can be masked, or configured as host id, or configured as any to filter all IPv4 address. Other L3 fields such as DSCP , L4 protocol and L4 fields, such as TCP port, UDP port, can also be filtered by IPv4 ACE.

The MAC ACE and IPv4 ACE in an extend IPv4 ACL can be configured alternately in arbitrary order which is completely specified by user.

5.3 Topology

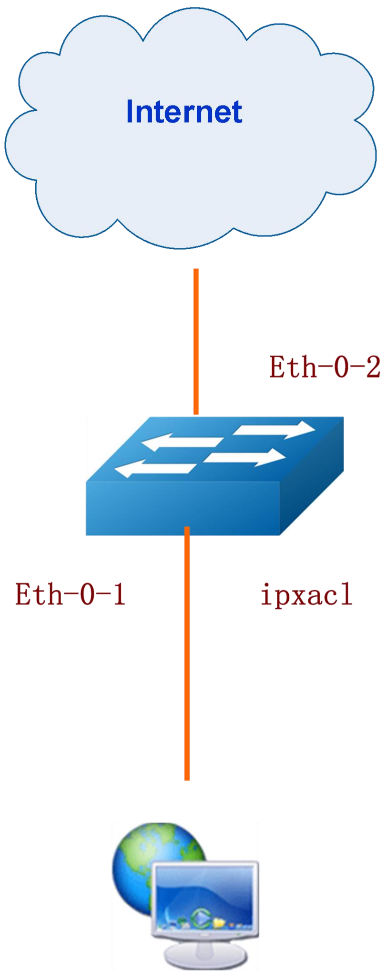


Figure 5-1 Extend ACL

5.4 Configuration

In this example, use extend IPv4 ACL on interface eth-0-1, to permit packets with source mac 0000.0000.1111 and cos value of 2, permit all TCP packets, and deny any other packets.

ACL configure details

Switch# configure terminal	Enter configuration mode
Switch(config)# ip access-list ipxacl extend	Define an extend IPv4 ACL and enter extend IP ACL configuration mode.
Switch(config-ex-ip-acl)# permit src-mac host 0000.0000.1111 dest-mac any cos 2	Config ACE to permit packet with source mac address 0000.0000.1111 and cos value of 2.

Switch(config-ex-ip-acl)# permit tcp any any	Config ACE to permit all TCP packets.
Switch(config-ex-ip-acl)# deny src-mac any dest-mac any	Config ACE to deny any packets.
Switch(config-ex-ip-acl)# exit	Exit extend IP ACL configuration mode.

Interface details

Switch# configure terminal	Enter configuration mode
Switch(config)# class-map cmap	Create a class-map cmap and enter class-map configuration mode
Switch(config-cmap)# match access-group ipxacl	Define the match criterion (match ACL ipxacl) to classify traffic
Switch(config-cmap)# exit	Exit class-map configuration mode
Switch(config)# policy-map pmap	Create a policy map pmap and enter policy-map configuration mode
Switch(config-pmap)# class cmap	Define a traffic classification(match cmap), and enter policy-map class configuration mode
Switch(config-pmap-c)# exit	Exit policy-map class configuration mode
Switch(config-pmap)# exit	Exit policy-map configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# service-policy input pmap	Apply service-policy pmap on interface with ingress direction
Switch(config-if)# exit	Exit interface configuration mode

5.5 Validation

The result of **show running-config** is as follows.

```
Switch# show running-config
ip access-list ipxacl extend
  10 permit src-mac host 0000.0000.1111 dest-mac any cos 2
  20 permit tcp any any
  30 deny src-mac any dest-mac any
!
class-map match-any cmap
 match access-group ipxacl
!
policy-map pmap
```

```
 class cmap
!
interface eth-0-1
 service-policy input pmap
```

```
Switch# show access-list ip
ip access-list ipxacl extend
  10 permit src-mac host 0000.0000.1111 dest-mac any cos 2
  20 permit tcp any any
  30 deny src-mac any dest-mac any
```

6 Configuring ACLv6

6.1 Overview

Access control lists for IPv6 (ACLv6) classify traffic with the same characteristics. The ACLv6 can have multiple access control entries (ACEs), which are commands that match fields against the contents of the packet. ACLv6 can filter packets received on interface by many fields such as ipv6 address and deny or permit the packets.

6.2 Terminology

The following terms and concepts are used to describe ACLv6.

Access control entry (ACE)

Each ACE includes an action element (permit or deny) and a filter element based on criteria such as source address, destination address, protocol, and protocol-specific parameters.

IPv6 ACL

IPv6 ACL can filter packet by ipv6-sa and ipv6-da, and ipv6-address can be masked, or configured as host id, or configured as any to filter all IPv6 address. IPv6 ACL can also filter other L3 fields such as L4 protocol and L4 fields such as TCP port, UDP port, and so on.

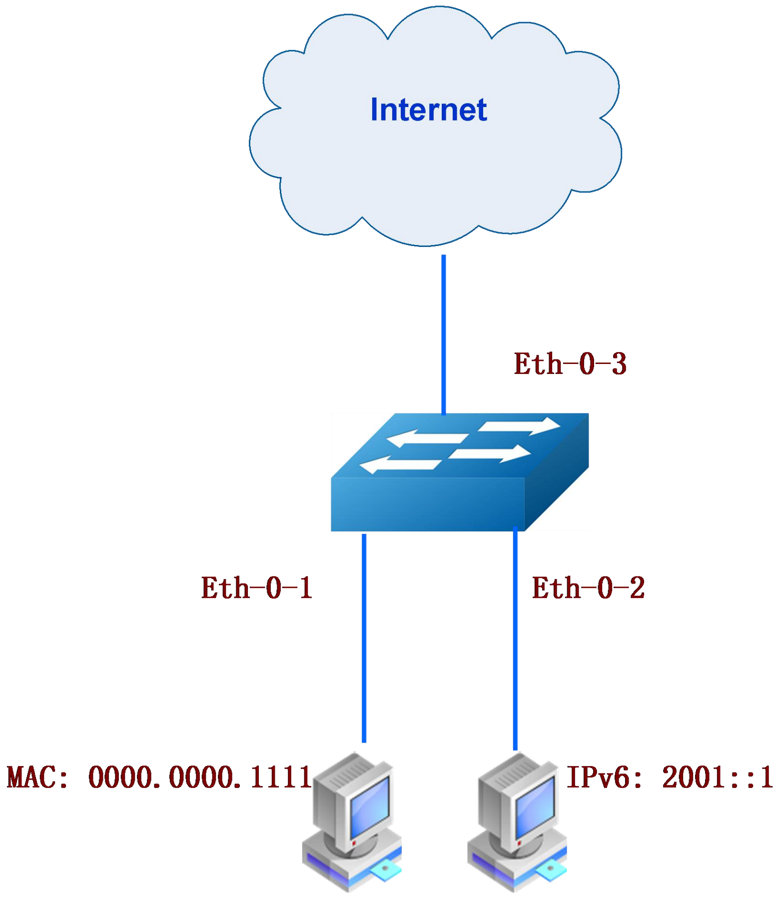
Time Range

Time range can define a period of time only between which the ACE can be valid if the ACE is associated to the time range.

6.3 Limitation

If IPv6 is enabled globally, the IPv6 packet will not obey the MAC ACL rules.

6.4 Topology



6.5 Configuration

In this example, use MAC ACL on interface eth-0-1, to permit not IPv6 packets with source mac 0000.0000.1111 and deny any other not IPv6 packets. Use IPv6 ACL on interface eth-0-2, to permit packets with source ip 2001::/64 and deny any other packets.

Configuration ACL details

Switch# configure terminal	Enter configuration mode
Switch# ipv6 enable	Enable IPv6 feature globally
Switch(config)#mac access-list mac	Define a MAC ACL and enter ACL configuration mode
Switch(config-mac-acl)# permit src-mac host 0000.0000.1111 dest-mac any	Config ACE to permit packet with source mac address 0000.0000.1111
Switch(config-mac-acl)# deny src-mac any dest-mac any	Config ACE to deny any packets
Switch(config-mac-acl)# exit	Exit ACL configuration mode
Switch(config)# ipv6 access-list ipv6	Define an IPv6 ACL and enter ACL configuration mode
Switch(config-ipv6-acl)# permit any 2001::/64 any	Config ACE to permit subnet 2001::/64
Switch(config-ipv6-acl)# deny any any any	Config ACE to deny any packets
Switch(config-ipv6-acl)# exit	Exit ACL configuration mode

Apply ACL

Switch# configure terminal	Enter configuration mode
Switch(config)# class-map cmap1	Create a class-map cmap1 and enter class-map configuration mode
Switch(config-cmap)# match access-group mac	Define the match criterion (match mac ACL) to classify traffic
Switch(config-cmap)# exit	Exit class-map configuration mode
Switch(config)# policy-map pmap1	Create a policy map pmap1 and enter policy-map configuration mode
Switch(config-pmap)# class cmap1	Define a traffic classification(match cmap1), and enter policy-map class configuration mode
Switch(config-pmap-c)# exit	Exit policy-map class configuration mode
Switch(config-pmap)# exit	Exit policy-map configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# service-policy input pmap1	Apply service-policy pmap1 on interface with ingress direction
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# class-map cmap2	Create a class-map cmap2 and enter class-map configuration mode

Switch(config-cmap)# match access-group ipv6	Define the match criterion (match ACL ipv6) to classify traffic
Switch(config-cmap)# exit	Exit class-map configuration mode
Switch(config)# policy-map pmap2	Create a policy map pmap2 and enter policy-map configuration mode
Switch(config-pmap)# class cmap2	Define a traffic classification(match cmap2), and enter policy-map class configuration mode
Switch(config-pmap-c)# exit	Exit policy-map class configuration mode
Switch(config-pmap)# exit	Exit policy-map configuration mode
Switch(config-if)# interface eth-0-2	Enter interface configuration mode
Switch(config-if)# service-policy input pmap2	Apply service-policy pmap2 on interface with ingress direction

6.6 Validation

The result of show running-config is as follows.

Switch# show running-config

```
mac access-list mac
  10 permit src-mac host 0000.0000.1111 dest-mac any
  20 deny src-mac any dest-mac any
!

ipv6 access-list ipv6
  10 permit any 2001::/64 any
  20 deny any any any
!
class-map match-any cmap1
 match access-group mac
!
class-map match-any cmap2
 match access-group ipv6
!
policy-map pmap1
 class cmap1
!
policy-map pmap2
 class cmap2
!
interface eth-0-1
 service-policy input pmap1
!
interface eth-0-2
 service-policy input pmap2
!
```

7 Configuring Dot1x

7.1 Overview

IEEE 802 Local Area Networks are often deployed in environments that permit unauthorized devices to be physically attached to the LAN infrastructure, or Permit unauthorized users to attempt to access the LAN through equipment already attached.

Port-based network access control makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.

With 802.1X port-based authentication, the devices in the network have specific roles:

- **Client**: the device (PC) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1X-compliant client softwares, such as *xsupplicant* in Linux.
- **Authentication serve**r: performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service

  (RADIUS) security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- **Switch**(edge switch or wireless access point): controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulation the EAP frames and Interacting with the authentication server. When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP Frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client. We can also config dot1x in routed port.

7.2 Topology

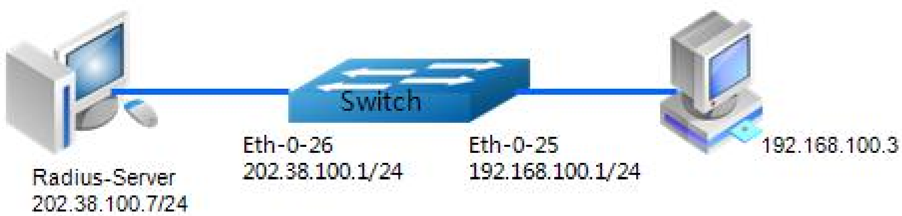


Figure 7-1 Dot1x Basic topology

7.3 Configuration

To use the auto negative mode in switch port, the Switch's configuration is as follow.

Switch# configure terminal	Enter the Configure mode
Switch(config)# dot1x system-auth-ctrl	Globally enable the dot1x authentication control
Switch(config)# interface eth-0-25	Specify the interface to be configured and enter the Interface mode

Switch(config)# switchport mode access	Set Eth-0-25 to access mode
Switch(config-if)# dot1x port-control auto	Enable dot1x port control on the interface, and Allow port client to negotiate authentication
Switch(config-if)# no shutdown	Make interface UP
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# interface vlan 1	Enter interface vlan 1
Switch(config-if)# ip address 192.168.100.1/24	Set vlan 1 ip address
Switch(config)# interface eth-0-26	Specify the interface to be configured and enter the Interface mode
Switch(config-if)# no switchport	Change interface to a routed port
Switch(config-if)# ip address 202.38.100.1/24	Configure IP address for this interface
Switch(config-if)# no shutdown	Make interface UP
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# radius-server host 202.38.100.7	Configure IPv4 address for radius server
Switch(config)# radius-server host 2001:1000::1	Configure IPv6 address for radius server
Switch(config)# radius-server key test	Configure the shared encryption key of RADIUS server
Switch(config)# end	Exit the Configure mode
Switch# show dot1x	Verify management dot1x configuration
Switch# show dot1x interface eth-0-25	Verify management dot1x configuration on interface eth-0-25

To use the auto negative mode in routed port, the Switch's configuration is as follow.

Switch# configure terminal	Enter the Configure mode
Switch(config)# dot1x system-auth-ctrl	Globally enable the dot1x authentication control
Switch(config)# interface eth-0-25	Specify the interface to be configured and enter the Interface mode
Switch(config-if)# no switchport	Change interface to a routed port
Switch(config-if)# ip address 192.168.100.1/24	Configure IP address for this interface
Switch(config-if)# dot1x port-control auto	Enable dot1x port control on the interface, and Allow port client to negotiate authentication

Switch(config-if)# no shutdown	Make interface UP
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# interface eth-0-26	Specify the interface to be configured and enter the Interface mode
Switch(config-if)# no switchport	Change interface to a routed port
Switch(config-if)# ip address 202.38.100.1/24	Configure IP address for this interface
Switch(config-if)# no shutdown	Make interface UP
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# radius-server host 202.38.100.7	Configure IPv4 address for radius server
Switch(config)# radius-server host 2001:1000::1	Configure IPv6 address for radius server
Switch(config)# radius-server key test	Configure the shared encryption key of RADIUS server
Switch(config)# end	Exit the Configure mode
Switch# show dot1x	Verify management dot1x configuration
Switch# show dot1x interface eth-0-25	Verify management dot1x configuration on interface eth-0-25

To use the force- authorized mode, the Switch's configuration is as follow.

Switch# configure terminal	Enter the Configure mode
Switch(config)# dot1x system-auth-ctrl	Globally enable the dot1x authentication control
Switch(config)# interface eth-0-25	Specify the interface to be configured and enter the Interface mode
Switch(config-if)# dot1x port-control force-authorized	Enable dot1x port control on the interface, and force the status always be authorized
Switch(config-if)# no shutdown	Make interface UP
Switch(config-if)# end	Exit the Interface mode
Switch# show dot1x	Verify management dot1x configuration
Switch# show dot1x interface eth-0-25	Verify management dot1x configuration on interface eth-0-25

The optional parameter setting is as follow.

Switch#configure terminal	Enter the Configure mode.

Switch(config)# radius-server deadtime 10	Set the wait time for re-activating RADIUS server
Switch(config)# radius-server retransmit 5	Set the maximum failed RADIUS requests sent to server
Switch(config)# radius-server timeout 10	Set the timeout value for no response from RADIUS server
Switch(config)# interface eth-0-25	Specify the interface to be configured and enter the Interface mode.
Switch(config-if)# dot1x max-reauth-req 5	Specify the number of reauthentication attempts before becoming unauthorized
Switch(config-if)# dot1x protocol-version 1	Set the protocol version
Switch(config-if)# dot1x quiet-period 120	Specify the quiet period in the HELD state
Switch(config-if)# dot1x reauthentication	Enable reauthentication on a por
Switch(config-if)# dot1x timeout re-authperiod 1800	Specify the seconds between reauthorization attempts
Switch(config-if)# dot1x timeout server-timeout 60	Specify the authentication server response timeout
Switch(config-if)# dot1x timeout supp-timeout 60	Specify the supplicant response timeout
Switch(config-if)# dot1x timeout tx-period 60	Specify the Seconds between successive request ID attempts

The Server's software setting and configuration in detail refers to Figure 7-2, Figure 7-3 and Figure 7-4.

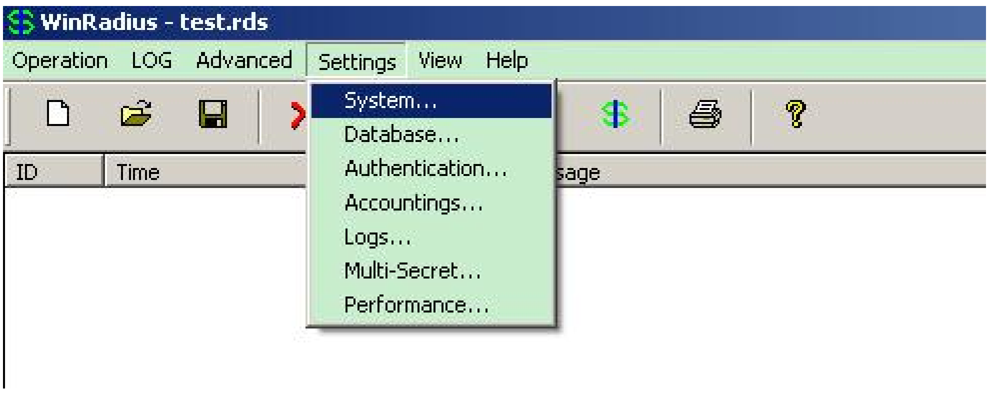


Figure 7-2 Select "Settings" -> "System"

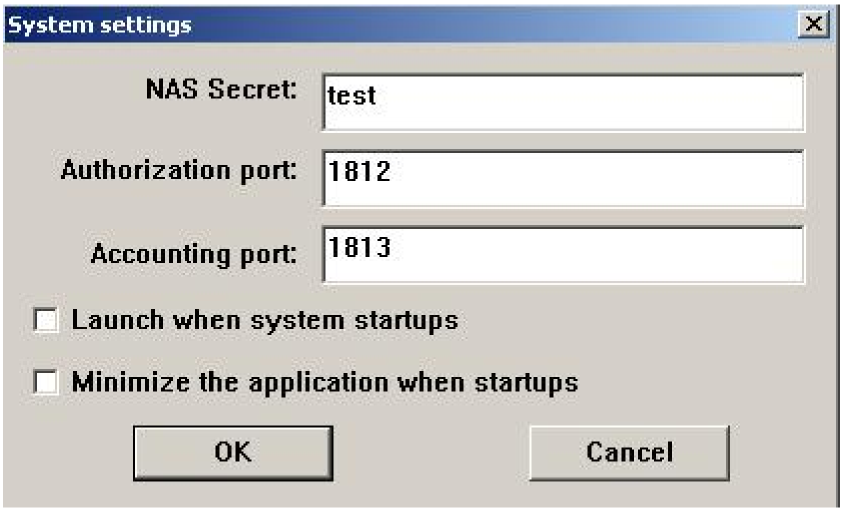


Figure 7-3 Configure the shared-key, authorization port and account port

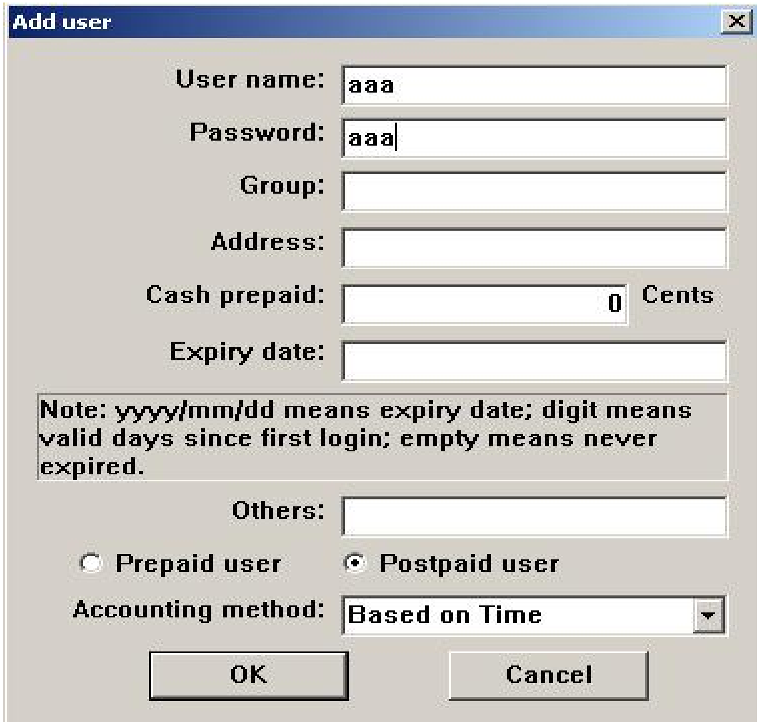


Figure 7-4 Add user name and password on the server

7.4 Validation

The result of show dot1x is as follows.

Switch# show dot1x

```
802.1X Port-Based Authentication Enabled
  RADIUS server address: 2001:1000::1:1812
  Next radius message ID: 0
  RADIUS server address: 202.38.100.7:1812
  Next radius message ID: 0

Switch# show dot1x interface eth-0-25
802.1X info for interface eth-0-25
  Supplicant name: aaa
  Supplicant address: 0011.11e1.9a3f
  portEnabled: true - portControl: Auto
  portStatus: Authorized - currentId: 42
  reAuthenticate: disabled
  reAuthPeriod: 3600
  abort:F fail:F start:F timeout:F success:T
  PAE: state: Authenticated - portMode: Auto
  PAE: reAuthCount: 0 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle - reqCount: 0 - idFromServer: 41
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
```

The result of show radius-server is as follows.

```
Switch# show radius-server
=====================================
802.1X session on interface eth-0-25:
current radius server:
 retransmit count  : 1
 server address    : 202.38.100.7:1812
 socket descriptor : 15
 last state        :
radius servers in dead list:
 N/A
=====================================
```

8 Configuring Guest VLAN

8.1 Overview

You can configure a guest VLAN for each 802.1x port on the switch to provide limited services to clients (for example, how to download the 802.1x client). These clients might be upgrading their system for 802.1x authentication, and some hosts, such as Windows 98 systems, might not be 802.1x-capable.

When the authentication server does not receive a response to its EAPOL request/identity frame, clients that are not 802.1x-capable are put into the guest VLAN for the port, if one is configured. However, the server does not grant 802.1x-capable clients that fail authentication access to the network. Any number of hosts is allowed access when the switch port is moved to the guest VLAN.

The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

8.2 Topology

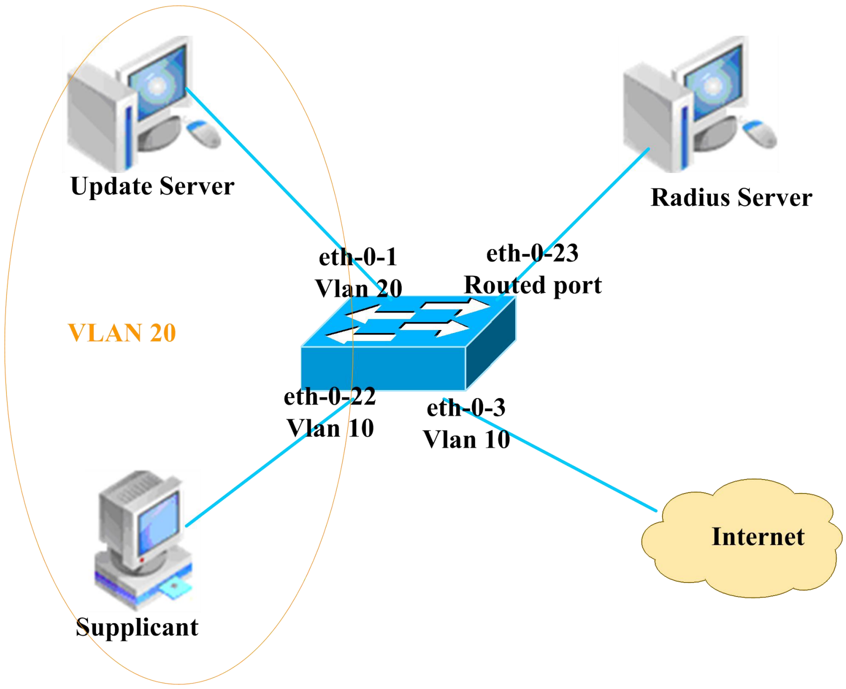


Figure 8-1 supplicant is not 802.1x capable

NOTE

In the above topology, eth-0-22 is an IEEE 802.1X enabled port, and it is in the native VLAN 10, the configured guest VLAN for this port is VLAN 20. So clients that are not 802.1X capable will be put into VLAN 20 after the authenticator had send max EAPOL request/identity frame but got no response.

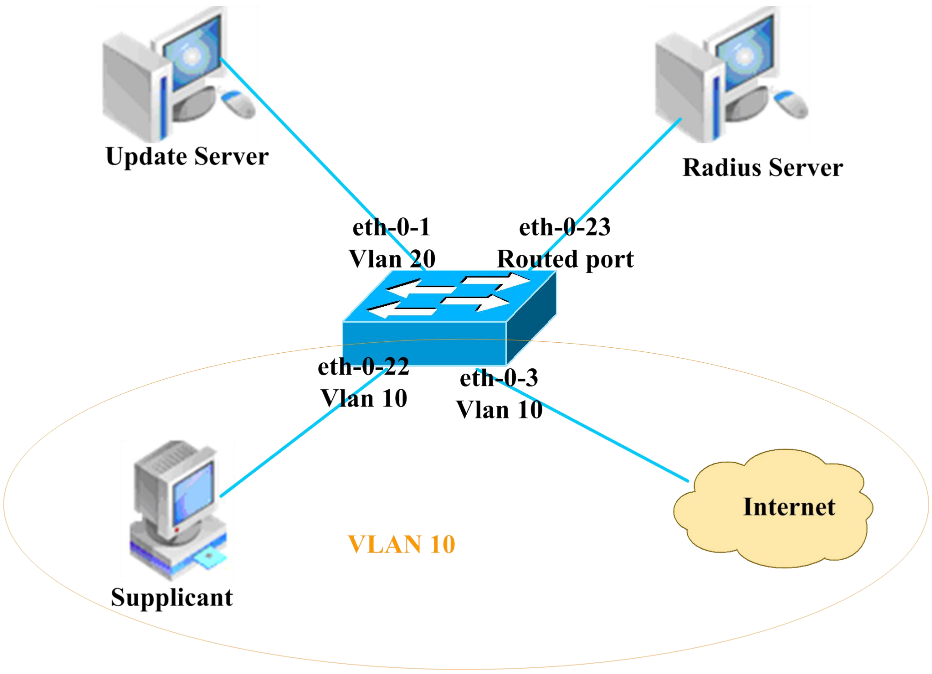


Figure 8-2 supplicant is 802.1x capable and authenticated

NOTE

We use remote linux Radius server as authenticate server, the server's address is 202.38.100.7, and the IP address for the connected routed port eth-0-23 is 202.38.100.1. When the client is authenticated by the radius server, then it can access the public internet which is also in VLAN 10.

8.3 Configuration

To use the auto negative mode in switch port, the Switch's configuration is as follow.

Switch# configure terminal	Enter the Configure mode
Switch(config)# vlan database	Enter the vlan database
Switch(config-vlan)# vlan 10	Create vlan 10
Switch(config-vlan)# vlan 20	Create vlan 20
Switch(config-vlan)# exit	Exit vlan database
Switch(config)# dot1x system-auth-ctrl	Globally enable the dot1x authentication control.
Switch(config)# interface eth-0-22	Specify the interface to be configured and enter the Interface mode

Switch(config-if)# switchport mode access	Set Eth-0-22 to access mode
Switch(config-if)# switchport access vlan 10	Add the port to native vlan 10
Switch(config-if)# dot1x port-control auto	Enable dot1x port control on the interface, and Allow port client to negotiate authentication.
Switch(config-if)# no shutdown	Make interface UP
Switch(config-if)# dot1x guest vlan 20	Configure the port with guest vlan 20
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# interface eth-0-23	Specify the interface to be configured and enter the Interface mode
Switch(config-if)# no switchport	Change interface to a routed port
Switch(config-if)# ip address 202.38.100.1/24	Configure IP address for this interface
Switch(config-if)# no shutdown	Make interface UP
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# radius-server host 202.38.100.7	Configure IP address for radius server
Switch(config)# radius-server key test	Configure the shared encryption key of RADIUS server
Switch(config)# end	Exit the Configure mode
Switch# show dot1x	Verify management dot1x configuration
Switch# show dot1x interface eth-0-22	Verify management dot1x configuration on interface eth-0-22

8.4 Validation

Init state

```
Switch# show running-config
dot1x system-auth-ctrl
radius-server host 202.38.100.7 key test
vlan database
 vlan 10,20
!
interface eth-0-22
 switchport access vlan 10
 dot1x port-control auto
 dot1x guest-vlan 20
```

```
!
interface eth-0-23
 no switchport
 ip address 202.38.100.1/24
!
```

```
Switch# show dot1x interface eth-0-22
802.1X info for interface eth-0-22
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 1
  reAuthenticate: disabled
  reAuthPeriod: 3600
  Guest VLAN:20
  abort:F fail:F start:F timeout:F success:F
  PAE: state: Connecting - portMode: Auto
  PAE: reAuthCount: 1 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle - reqCount: 0 - idFromServer: 19
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
```

```
Switch# show vlan brief
VLAN ID  Name             State   STP ID  DSCP    Member ports
                                                  (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ======= ========================
1       default          ACTIVE  0       Disable eth-0-1(u) eth-0-2(u)
                                                 eth-0-3(u) eth-0-4(u)
                                                 eth-0-5(u) eth-0-6(u)
                                                 eth-0-7(u) eth-0-8(u)
                                                 eth-0-9(u) eth-0-10(u)
                                                 eth-0-11(u) eth-0-12(u)
                                                 eth-0-13(u) eth-0-14(u)
                                                 eth-0-15(u) eth-0-16(u)
                                                 eth-0-17(u) eth-0-18(u)
                                                 eth-0-19(u) eth-0-20(u)
                                                 eth-0-21(u) eth-0-24(u)
                                                 eth-0-25(u) eth-0-26(u)
                                                 eth-0-27(u) eth-0-28(u)
                                                 eth-0-29(u) eth-0-30(u)
                                                 eth-0-31(u) eth-0-32(u)
                                                 eth-0-33(u) eth-0-34(u)
                                                 eth-0-35(u) eth-0-36(u)
                                                 eth-0-37(u) eth-0-38(u)
                                                 eth-0-39(u) eth-0-40(u)
                                                 eth-0-41(u) eth-0-42(u)
                                                 eth-0-43(u) eth-0-44(u)
                                                 eth-0-45(u) eth-0-46(u)
                                                 eth-0-47(u) eth-0-48(u)
10      VLAN0010         ACTIVE  0       Disable eth-0-22(u)
20      VLAN0020         ACTIVE  0       Disable
Client in guest VLAN
```

Switch# show dot1x interface eth-0-22

```
802.1X info for interface eth-0-22
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 2
  reAuthenticate: disabled
  reAuthPeriod: 3600
  Guest VLAN:20(Port Authorized by guest vlan)
  abort:F fail:F start:F timeout:F success:F
  PAE: state: Connecting - portMode: Auto
  PAE: reAuthCount: 2 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle - reqCount: 0 - idFromServer: 19
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
```

Switch# show vlan brief

```
VLAN ID  Name             State   STP ID  DSCP    Member ports
                                                  (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ======= ========================
1       default          ACTIVE  0       Disable eth-0-1(u) eth-0-2(u)
                                                 eth-0-3(u) eth-0-4(u)
                                                 eth-0-5(u) eth-0-6(u)
                                                 eth-0-7(u) eth-0-8(u)
                                                 eth-0-9(u) eth-0-10(u)
                                                 eth-0-11(u) eth-0-12(u)
                                                 eth-0-13(u) eth-0-14(u)
                                                 eth-0-15(u) eth-0-16(u)
                                                 eth-0-17(u) eth-0-18(u)
                                                 eth-0-19(u) eth-0-20(u)
                                                 eth-0-21(u) eth-0-24(u)
                                                 eth-0-25(u) eth-0-26(u)
                                                 eth-0-27(u) eth-0-28(u)
                                                 eth-0-29(u) eth-0-30(u)
                                                 eth-0-31(u) eth-0-32(u)
                                                 eth-0-33(u) eth-0-34(u)
                                                 eth-0-35(u) eth-0-36(u)
                                                 eth-0-37(u) eth-0-38(u)
                                                 eth-0-39(u) eth-0-40(u)
                                                 eth-0-41(u) eth-0-42(u)
                                                 eth-0-43(u) eth-0-44(u)
                                                 eth-0-45(u) eth-0-46(u)
                                                 eth-0-47(u) eth-0-48(u)
10      VLAN0010         ACTIVE  0       Disable
20      VLAN0020         ACTIVE  0       Disable eth-0-22(u)
Client is authenticated
```

Switch# show dot1x interface eth-0-22

```
802.1X info for interface eth-0-22
  Supplicant name: ychen
  Supplicant address: ae38.3288.f046
  portEnabled: true - portControl: Auto
  portStatus: Authorized - currentId: 6
```

```
  reAuthenticate: disabled
  reAuthPeriod: 3600
  Guest VLAN:20
  abort:F fail:F start:F timeout:F success:T
  PAE: state: Authenticated - portMode: Auto
  PAE: reAuthCount: 0 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle - reqCount: 0 - idFromServer: 5
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
```

Switch# show vlan brief

```
VLAN ID  Name             State   STP ID  DSCP    Member ports
                                                  (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ======= ========================
1       default          ACTIVE  0       Disable eth-0-1(u) eth-0-2(u)
                                                 eth-0-3(u) eth-0-4(u)
                                                 eth-0-5(u) eth-0-6(u)
                                                 eth-0-7(u) eth-0-8(u)
                                                 eth-0-9(u) eth-0-10(u)
                                                 eth-0-11(u) eth-0-12(u)
                                                 eth-0-13(u) eth-0-14(u)
                                                 eth-0-15(u) eth-0-16(u)
                                                 eth-0-17(u) eth-0-18(u)
                                                 eth-0-19(u) eth-0-20(u)
                                                 eth-0-21(u) eth-0-24(u)
                                                 eth-0-25(u) eth-0-26(u)
                                                 eth-0-27(u) eth-0-28(u)
                                                 eth-0-29(u) eth-0-30(u)
                                                 eth-0-31(u) eth-0-32(u)
                                                 eth-0-33(u) eth-0-34(u)
                                                 eth-0-35(u) eth-0-36(u)
                                                 eth-0-37(u) eth-0-38(u)
                                                 eth-0-39(u) eth-0-40(u)
                                                 eth-0-41(u) eth-0-42(u)
                                                 eth-0-43(u) eth-0-44(u)
                                                 eth-0-45(u) eth-0-46(u)
                                                 eth-0-47(u) eth-0-48(u)
10      VLAN0010         ACTIVE  0       Disable eth-0-22(u)
20      VLAN0020         ACTIVE  0       Disable
```

Switch# show dot1x

```
802.1X Port-Based Authentication Enabled
  RADIUS server address: 202.38.100.7:1812
  Next radius message ID: 0
```

Switch# show dot1x statistics

```
=====================================
802.1X statistics for interface eth-0-22
  EAPOL Frames Rx: 52 - EAPOL Frames Tx: 4270
  EAPOL Start Frames Rx: 18 - EAPOL Logoff Frames Rx: 2
  EAP Rsp/Id Frames Rx: 29 - EAP Response Frames Rx: 3
```

```
EAP Req/Id Frames Tx: 3196 - EAP Request Frames Tx: 3
Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
EAPOL Last Frame Version Rx: 2 - EAPOL Last Frame Src: ae38.3288.f046
```

9 Configuring Arp Inspection

9.1 Overview

ARP inspection is a security feature that validates ARP packets in a network. ARP inspection intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from some man-in-the-middle attacks. ARP inspection ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

- Intercept all ARP requests and responses on untrusted ports.
- Verify that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination.
- Drop invalid ARP packets.
- ARP inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On entrusted interfaces, the switch forwards the packet only if it is valid.

9.2 Terminology

Following is a brief description of terms and concepts used to describe the ARP Inspection:

DHCP Snooping

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. This feature builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.

Address Resolution Protocol (ARP)

ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. For example, Host B wants to send information to Host A , but it does not have the MAC address of Host A in its ARP cache. Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. All hosts within the broadcast domain receive the ARP request, and Host A responds with its MAC address.

9.3 Topology

This figure is the networking topology for testing ARP Inspection functions.

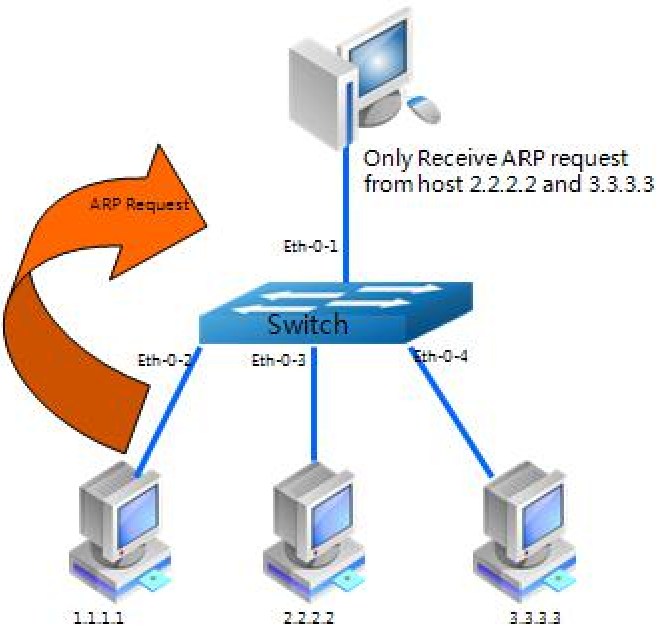


Figure 9-1 ARP Inspection Topology

9.4 Configurations

Create vlan

Switch#configure terminal	Enter the Configure mode
Switch(config)# vlan database	Configure VLAN database
Switch(config-vlan)# vlan 2	Create vlan 2
Switch(config-vlan)# exit	Exit the vlan Configure mode
Switch(config)# exit	Exit the Configure mode

Add interface to vlan

Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-1	Enter the Interface Configure mode and begin to configure port eth-0-1
Switch(config-if)# switchport access vlan 2	Add the port to vlan 2
Switch(config-if)# interface eth-0-2	Begin to configure port eth-0-2
Switch(config-if)# switchport access vlan 2	Add the port to vlan 2
Switch(config-if)# interface eth-0-3	Begin to configure port eth-0-3
Switch(config-if)# switchport access vlan 2	Add the port to vlan 2
Switch(config-if)# interface eth-0-4	Begin to configure port eth-0-4
Switch(config-if)# switchport access vlan 2	Add the port to vlan 2
Switch(config-if)# exit	Exit the Interface Configure mode

Configure ARP Inspection

Switch(config)# interface eth-0-1	Enter the Interface Configure mode and begin to configure port eth-0-1
Switch(config-if)# ip arp inspection trust	Configure the port to trust status.(usually configure the connection between switches as trusted)
Switch(config-if)#exit	Exit the Interface Configure mode
Switch(config)# ip arp inspection vlan 2	Enable ARP Inspection on VLAN 2

Switch(config)# ip arp inspection validate src-mac ip dst-mac	Validate source MAC address, IP and destination MAC address in ARP packet

Add ARP ACL

Switch(config)# arp access-list test	Create arp access-list of test
Switch(config-arp-acl)# deny request ip host 1.1.1.1 mac any	Add an ACL item of deny the ARP request with ip 1.1.1.1
Switch(config-arp-acl)# exit	Exit the ARP ACL Configure mode
Switch(config)# ip arp inspection filter test vlan 2	Enable the ARP ACL on VLAN 2
Switch(config)# exit	Exit the Configure mode

9.5 Validation

Check the configuration of ARP Inspection on switch A.

Switch# show ip arp inspection

```
Source Mac Validation        : Enabled
Destination Mac Validation   : Enabled
IP Address Validation        : Enabled

Vlan     Configuration     ACL Match     Static ACL
=================================================================
2        enabled             test

Vlan     ACL Logging     DHCP Logging
=================================================================
2        deny              deny

Vlan     Forwarded      Dropped     DHCP Drops     ACL Drops
=================================================================
2        0                0             0               0

Vlan     DHCP Permits     ACL Permits     Source MAC Failures
=================================================================
2        0                  0                  0

Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
=================================================================
2       0                      0                              0
```

Show the log information of ARP Inspection on switch A

Switch# show ip arp inspection log

```
Total Log Buffer Size : 32
Syslog rate : 5 entries per 1 seconds.
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
```

10 Configuring DHCP Snooping

10.1 Overview

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. The DHCP snooping feature performs the following activities:

- Validate DHCP messages received from untrusted sources and filters out invalid messages.
- Build and maintain the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.
- Utilize the DHCP snooping binding database to validate subsequent requests from untrusted hosts.
- Other security features, such as dynamic ARP inspection (DAI), also use information stored in the DHCP snooping binding database. DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs. The DHCP snooping feature is implemented in software basis. All DHCP messages are intercepted in the BAY and directed to the CPU for processing.

10.2 Topology

This figure is the networking topology for testing DHCP snooping functions. We need two Linux boxes and one switch to construct the test bed.

- Computer A is used as a DHCP server.
- Computer B is used as a DHCP client.
- Switch A is used as a DHCP Snooping box.

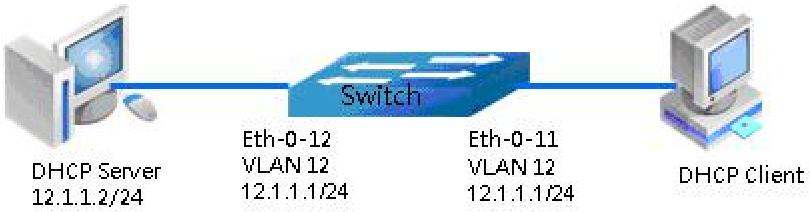


Figure 10-1 DHCP Snooping Topology

10.3 Configuration

Configure vlan

Switch# configure terminal	Enter the Configure mode
Switch(config)# vlan database	Configure VLAN database.
Switch(config-vlan)# vlan 12	Create vlan 12
Switch(config-vlan)# exit	Exit to the Configure mode

Configure interface eth-0-12

Switch(config)# interface eth-0-12	Enter the Interface Configure mode
Switch(config-if)# switchport	Make sure the port is switch port
Switch(config-if)# switchport access vlan 12	Add the port to vlan 12
Switch(config-if)# dhcp snooping trust	Trust all dhcp packets from this port
Switch(config-if)# no shutdown	Make sure the port is enabled
Switch(config-if)# exit	Exit the Interface Configure mode

Configure interface eth-0-11

Switch(config)# interface eth-0-11	Enter the Interface Configure mode
Switch(config-if)# switchport	Make sure the port is switch port
Switch(config-if)# switchport access vlan 12	Add the port to vlan 12
Switch(config-if)# no shutdown	Make sure the port is enabled

Switch(config-if)# exit	Exit the Interface Configure mode

Configure interface for vlan 12

Switch(config)# interface vlan 12	Enter the Interface Configure mode
Switch(config-if)# ip address 12.1.1.1/24	Set ip address for interface vlan 12
Switch(config-if)# exit	Exit the Interface Configure mode

Configure DHCP snooping feature

Switch(config)# dhcp snooping verify mac-address	Verify mac address of dhcp packets

Enable DHCP snooping global feature

Switch(config)# service dhcp enable	Enable dhcp services
Switch(config)# dhcp snooping	Enable dhcp snooping feature
Switch(config)# dhcp snooping vlan 12	Enable dhcp snooping feature on vlan 12

10.4 Validation

Step 1 Check the interface configuration.

```
Switch(config)# show running-config interface eth-0-12
!
interface eth-0-12
 dhcp snooping trust
 switchport access vlan 12
!
```

```
Switch(config)# show running-config interface eth-0-11
!
interface eth-0-11
 switchport access vlan 12
!
```

Step 2 Check the dhcp service status.

```
Switch# show services
Networking services configuration:
Service Name          Status
============================================================
dhcp                    enable
```

Step 3 Print dhcp snooping configuration to check current configuration.

```
Switch# show dhcp snooping config
dhcp snooping service: enabled
dhcp snooping switch: enabled
Verification of hwaddr field: enabled
Insertion of relay agent information (option 82): disable
Relay agent information (option 82) on untrusted port: not allowed
dhcp snooping vlan 11-12
```

Step 4 Show dhcp snooping statistics.

```
Switch# show dhcp snooping statistics
DHCP snooping statistics:
============================================================
DHCP packets                              17
BOOTP packets                             0

Packets forwarded                        30
Packets invalid                           0
Packets MAC address verify failed      0
Packets dropped                           0
```

Step 5 Show dhcp snooping binding information.

```
Switch# show dhcp snooping binding all
DHCP snooping binding table:

VLAN MAC Address    Interface  Lease(s)   IP Address
============================================================
12   0016.76a1.7ed9 eth-0-11   691190     12.1.1.65
```

11 Configuring IP Source Guard

11.1 Overview

IP source guard prevents IP spoofing by allowing only the IP addresses that are obtained through DHCP snooping on a particular port. Initially, all IP traffic on the port is blocked except for the DHCP packets that are captured by DHCP snooping. When a client receives a valid IP address from the DHCP server, an access control list (ACL) is installed on the port that permits the traffic from the IP address. This process restricts the client IP traffic to those source IP addresses that are obtained from the DHCP server; any IP traffic with a source IP address other than that in the ACL's permit list is filtered out. This filtering limits the ability of a host to attack the network by claiming a neighbor host's IP address.

IP source guard uses source IP address filtering, which filters the IP traffic that is based on its source IP address. Only the IP traffic with a source IP address that matches the IP source binding entry is permitted. A port's IP source address filter is changed when a new DHCP-snooping binding entry for a port is created or deleted. The port ACL is modified and reapplied in the hardware to reflect the IP source binding change. By default, if you enable IP source guard without any DHCP-snooping bindings on the port, a default ACL that denies all IP traffic is installed on the port. When you disable IP source guard, any IP source filter ACL is removed from the port.

Also IP source guard can use source IP and MAC address Filtering. When IP source guard is enabled with this option, IP traffic is filtered based on the source IP and Mac addresses. The switch forwards traffic only when the source IP and MAC addresses match an entry in the IP source binding table. If not, the switch drops all other types of packets except DHCP packet.

The switch also supports to have IP, MAC and VLAN Filtering. When IP source guard is enabled with this option, IP traffic is filtered cased on the source IP and MAC addresses. The switch forwards traffic only when the source IP, MAC addresses and VLAN match an entry in the IP source binding table.

11.2 Terminology

The following terms and concepts are used to describe the IPsourceguard:

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

DHCP Snooping

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. This feature builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.

ACL

Access control list.

11.3 Topology

This figure is the networking topology for testing IP source guard functions.

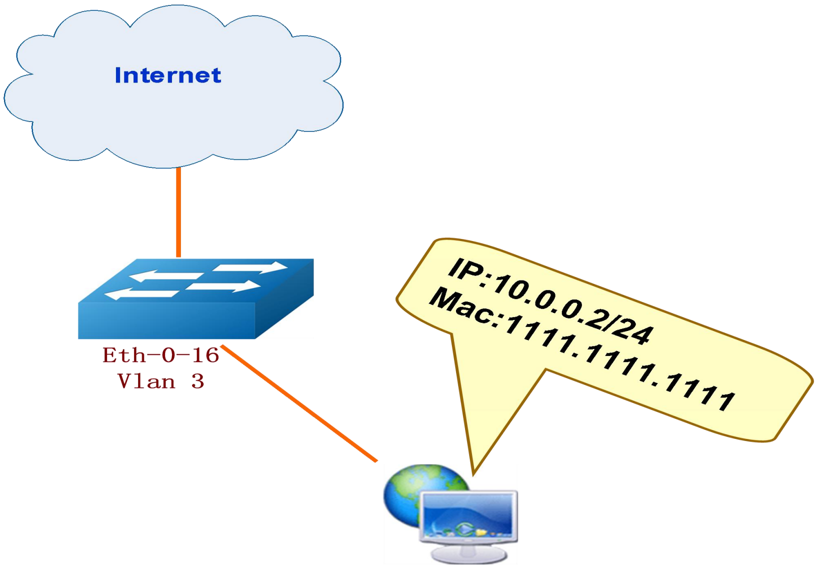


Figure 11-1 IP Source Guard

11.4 Configuration

Switch's configuration is as follow.

Create vlan and add interface to vlan

Switch# configure terminal	Enter the Configure mode
Switch(config)# vlan database	Configure VLAN database
Switch(config-vlan)# vlan 3	Create vlan 3
Switch(config-vlan)# exit	Exit the Vlan Configure mode
Switch(config)# interface eth-0-16	Enter the Interface Configure mode
Switch(config-if)# switchport	Make sure the port is switch port
Switch(config-if)# no shutdown	Turn on the interface
Switch(config-if)# switchport access vlan 3	Add the port to vlan 3
Switch(config-if)# exit	Exit the Interface Configure mode

Configure IP source guard

Switch(config)# ip source maximal binding number per-port 15	Set maximal binding number per-port (optional, the default number is 10)
Switch(config)# ip source binding mac 1111.1111.1111 vlan 3 ip 10.0.0.2 interface eth-0-16	Add static IP source guard binding item
Switch(config)# interface eth-0-16	Enter the Interface Configure mode
Switch(config-if)# ip verify source ip	Enable IP source guard feature on interface eth-0-16 (enable IP filtering)
Switch(config-if)# exit	Exit the Interface Configure mode

Delete or clear IP source guard

Switch(config)# no ip source binding mac 1111.1111.1111 vlan 3 ip 10.0.0.2 interface eth-0-16	Delete static IP source guard binding item
Switch(config)# clear ip source binding entries interface eth-0-16	Clear all ip source binding entries which is binding to interface eth-0-16
Switch(config)# clear ip source binding entries vlan 3	Clear all ip source binding entries which is binding to vlan 3
Switch(config)# clear ip source binding entries	Clear all ip source binding entries

11.5 Validation

The result of show ip source binding is as follows.

Check the config of interface eth-0-16.

DUT#show running-config interface eth-0-16

```
!
interface eth-0-16
 ip verify source ip
 switchport access vlan 3
```

12 Configuring RADIUS Authentication

12.1 Overview

Authentication verifies users before they are allowed access to the network and network services. System can use AAA authentication methods and Non-AAA authentication methods. RADIUS Authentication is one of AAA authentication methods. RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS is widely used protocol in network environments. It is commonly used for embedded network devices such as routers, modem servers, switches, etc. RADIUS clients run on support routers and switches. Clients send authentication requests to a central RADIUS server, which contains all user authentication and network service access information.

12.2 Topology

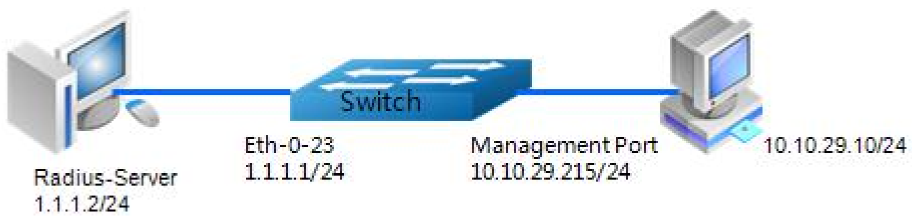


Figure 12-1 RADIUS authentication application

Figure 12-1is the networking topology for RADIUS authentication functions. We need one Switch and two computers for this test.

One computer as RADIUS server, it ip address of the eth0 interface is 1.1.1.2/24.

Switch has RADIUS authentication function. The ip address of interface eth-0-23 is 1.1.1.1/24. The management ip address of switch is 10.10.29.215, management port is connected the PC for test login, PC's ip address is 10.10.29.10.

12.3 Configuration

Configuration enable AAA on switch

Switch# configure terminal	Enter the Configure mode
Switch(config)# aaa new-model	Enable AAA on switch
Switch(config)# aaa authentication login radius-login radius local	Configuration authentication login method list. "radius-login" is the login
Switch(config)# radius-server host 1.1.1.2 auth-port 1819 key keyname	Configuration RADIUS server parameter
Switch(config)# radius-server host 2001:1000::1 auth-port 1819 key keyname	(Optional) Configuration RADIUS server parameter
Switch(config)# interface eth-0-23	Enter the interface mode
Switch(config-if)# no switchport	Change the port to L3 port
Switch(config-if)# ip address 1.1.1.1/24	Set ip address
Switch(config-if)# quit	Exit the Interface Configure mode
Switch(config)# line vty 0 7	enter line configuration mode
Switch(config-line)# login authentication radius-login Switch(config-line)# privilege level 4 Switch(config-line)# no line-password	configuration line authentication

Configuring PC and WinRADIUS

Step 1 Set ip address on RADIUS Server, show as Figure 12-2.

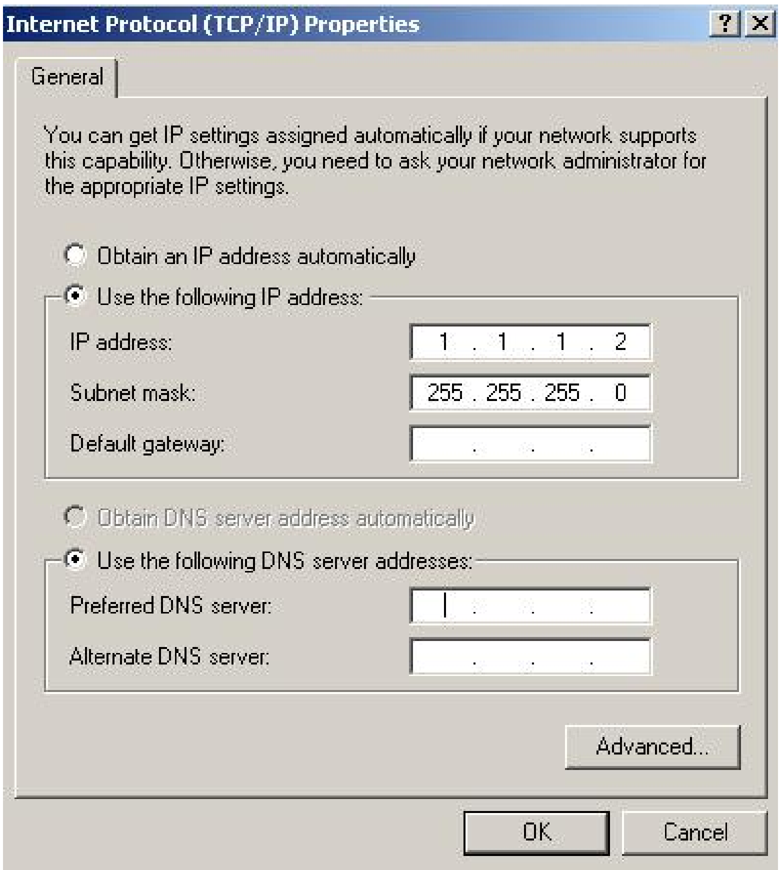


Figure 12-2 Configure IP address

Step 2 Test Ping Between Server and Switch, show as Figure 12-3.

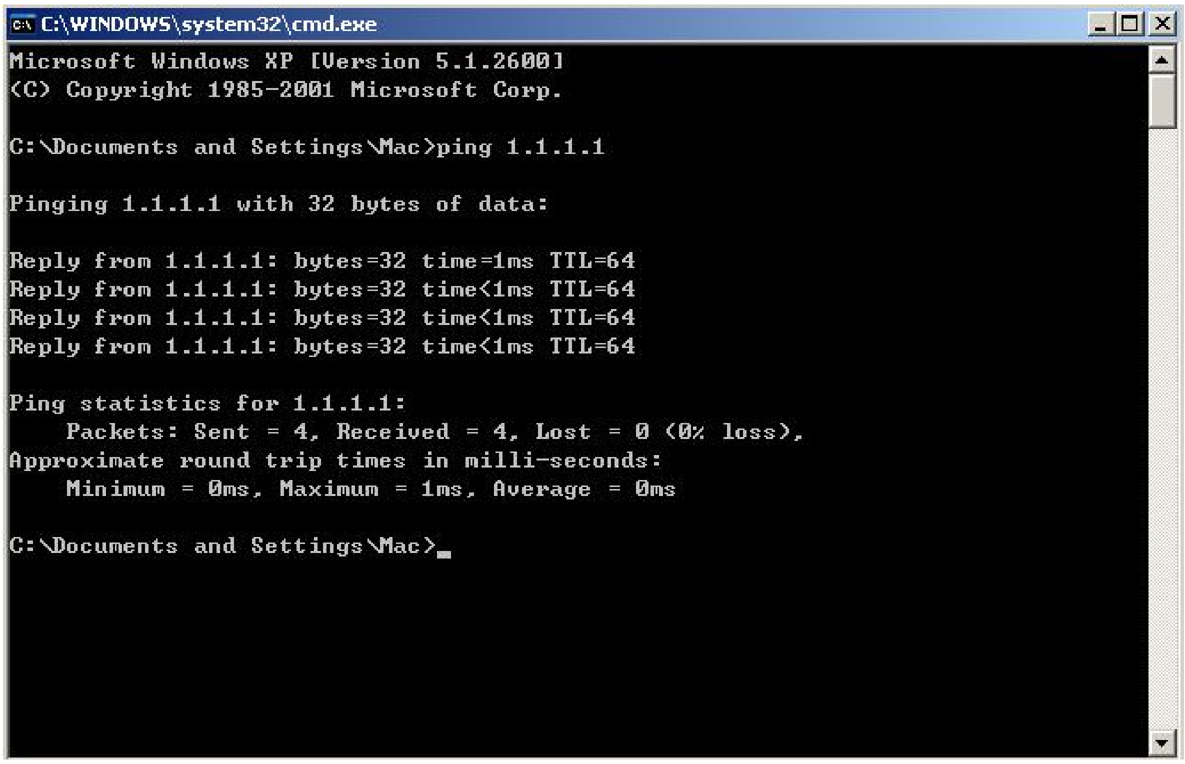


Figure 12-3 Ping test

Step 3 Open the WinRADIUS software on server.

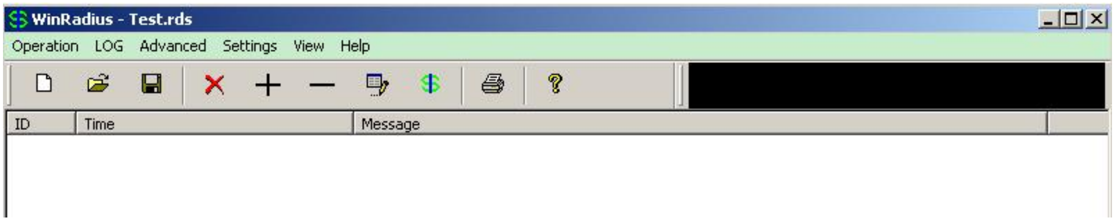


Figure 12-4 Open software on server

Step 4 Set System include Nas key and authorization port, show as Figure 12-5.

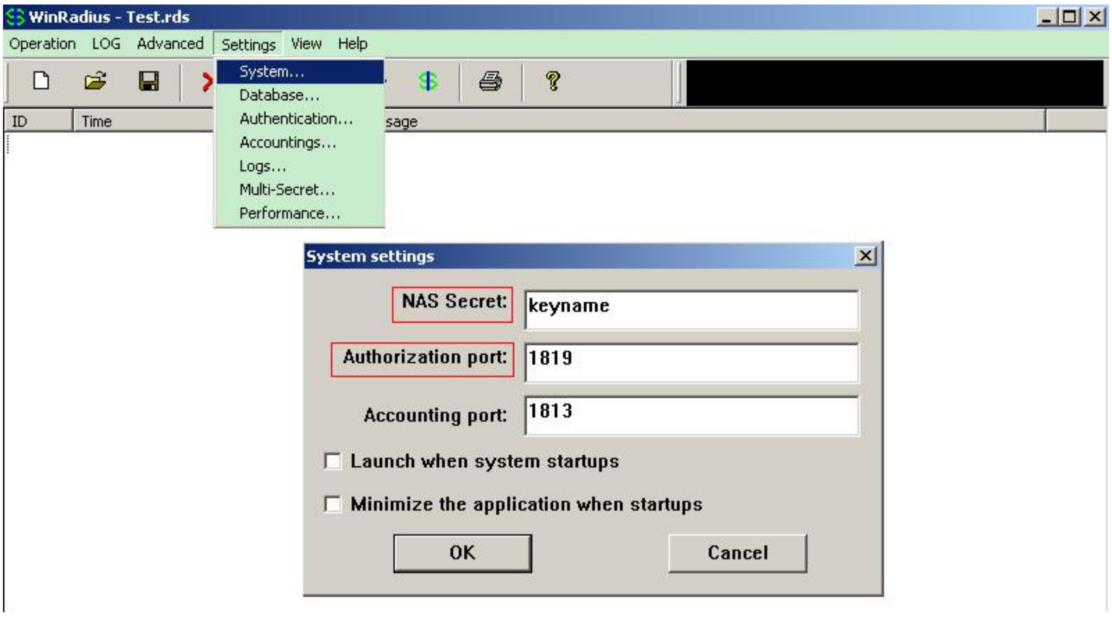


Figure 12-5 Set system

Step 5 Add username and password, show as Figure 12-6.

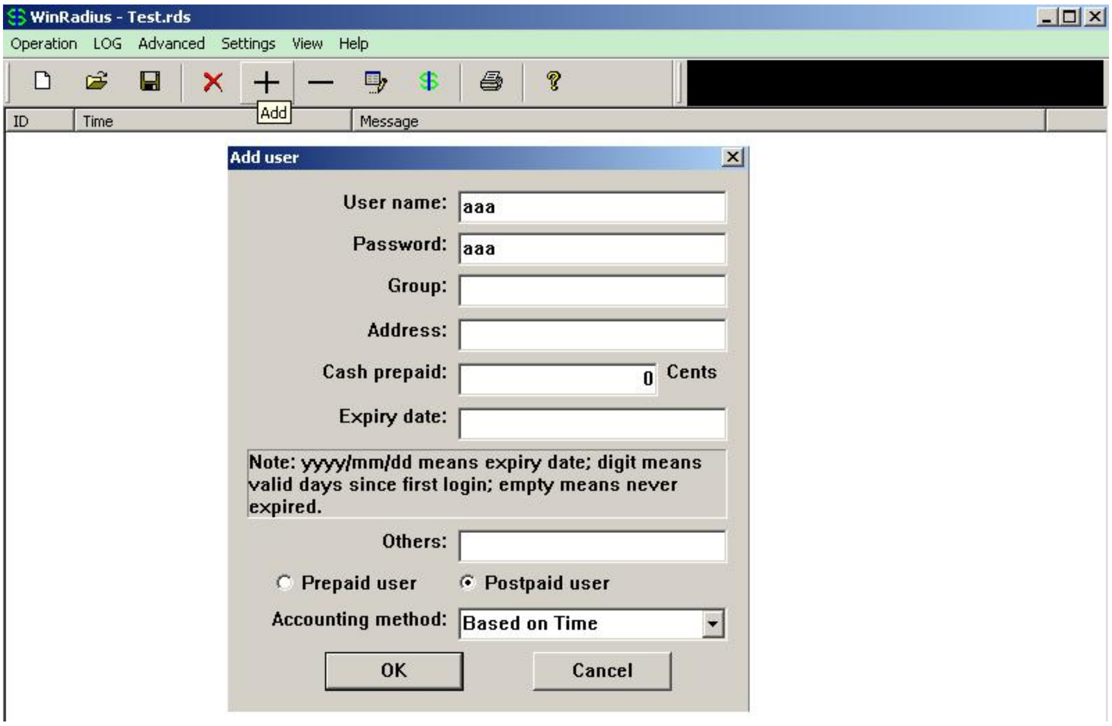


Figure 12-6 Add user

Step 6 Use Ping command for test on PC, show as Figure 12-7.

```
C:\Documents and Settings\mac>ping 10.10.29.215

Pinging 10.10.29.215 with 32 bytes of data:

Reply from 10.10.29.215: bytes=32 time<1ms TTL=63
Reply from 10.10.29.215: bytes=32 time<1ms TTL=63
Reply from 10.10.29.215: bytes=32 time<1ms TTL=63
Reply from 10.10.29.215: bytes=32 time<1ms TTL=63

Ping statistics for 10.10.29.215:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 12-7 Ping test

12.4 Validation

You can use command show authentication status in switch.

Switch#show aaa status

```
aaa stats:
     Authentication enable
```

You can use command show keys in switch.

Switch#show aaa method-lists authentication

```
authen queue=AAA_ML_AUTHEN_LOGIN
    Name = default  state = ALIVE :   local
Name = radius-login  state = ALIVE :   radius  local
```

12.5 Display Results

Telnet output

Figure 12-8 Telnet test

NOTE

Don't forget to turn RADIUS authentication feature on.
Make sure the cables is linked correctly
You can use command to check log messages if Switch can't do RADIUS authentication:
Switch# show logging buffer

13 Configuring Tacacs+

13.1 Overview

Authentication verifies users before they are allowed access to the network and network services. System can use AAA authentication methods and Non-AAA authentication methods. TACACS+ Authentication is one of AAA authentication methods. TACACS+ is a distributed client/server system that secures networks against unauthorized access. TACACS+ is widely used protocol in network environments. It is commonly used for embedded network devices such as routers, modem servers, switches, etc. TACACS+ clients run on support routers and switches. Clients send authentication requests to a central TACACS+ server, which contains all user authentication and network service access information.

13.2 Topology

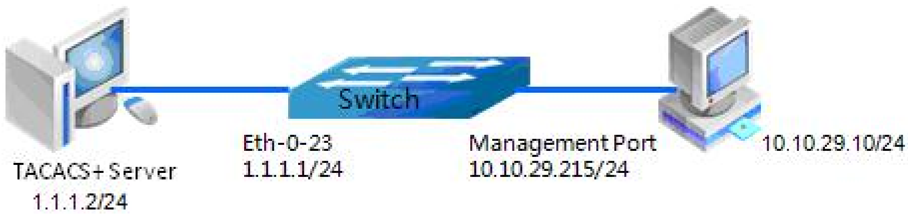


Figure 13-1 TACACS+ authentication application

Figure 13-1 is the networking topology for TACACS+ authentication functions. We need one Switch and two computers for this test.

One computer as TACACS+ server, it ip address of the eth0 interface is 1.1.1.2/24.

Switch has TACACS+ authentication function. The ip address of interface eth-0-23 is 1.1.1.1/24. The management ip address of switch is 10.10.29.215, management port(only in-band management port) is connected the PC for test login, PC's ip address is 10.10.29.10

13.3 Configuration Steps

The following example shows how to configure TACACS+ as the security protocol for login authentication.

Switch# configure terminal	Enter the Configure mode
Switch(config)# aaa new-model	Enable AAA on switch
Switch(config)# aaa authentication login tac-login tacacs-plus local	Configuration authentication login method list. "tac-login" is the login
Switch(config)# aaa authorization exec default tacacs-plus	Configuration authorization method list.
Switch(config)# aaa accounting exec default start-stop tacacs-plus	Configuration accounting exec method list.
Switch(config)# aaa accounting commands default tacacs-plus	Configuration accounting commands method list.
Switch(config)# tacacs-server host 1.1.1.2 port 123 key keyname	Configuration TACACS+ server parameter
Switch(config)# interface eth-0-23	Enter the interface mode
Switch(config-if)# no switchport	Change the port to L3 port
Switch(config-if)# ip address 1.1.1.1/24	Set ip address
Switch(config-if)# quit	Exit the Interface Configure mode
Switch(config)# line vty 0 7	enter line configuration mode
Switch(config-line)# login authentication tac-login Switch(config-line)# privilege level 4 Switch(config-line)# no line-password	configuration line authentication

13.4 Configuration TACACS+ Server

Download TACACS+ server code, DEVEL.201105261843.tar.bz2.

Build the TACACS+ server.

Add username and password in configure file.

```
#!../obj.linux-2.6.9-89.29.1.elsmp-x86_64/tac_plus
id = spawnd {
        listen = { port = 49 }
        spawn = {
                instances min = 1
                instances max = 10
        }
        background = no
}
        user = aaa {
                password = clear bbb
                member = guest
        }
```

Run TACACS+ server.

[disciple: ~]$ ./tac_plus ./tac_plus.cfg.in -d 1

Use Ping command for test on PC

```
C:\Documents and Settings\mac>ping 10.10.29.215

Pinging 10.10.29.215 with 32 bytes of data:

Reply from 10.10.29.215: bytes=32 time<1ms TTL=63
Reply from 10.10.29.215: bytes=32 time<1ms TTL=63
Reply from 10.10.29.215: bytes=32 time<1ms TTL=63
Reply from 10.10.29.215: bytes=32 time<1ms TTL=63

Ping statistics for 10.10.29.215:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 13-2 Ping result

13.5 Validation

You can use command show authentication status in switch.

Switch# show aaa status

```
aaa stats:
     Authentication enable
```

You can use command show keys in switch.

Switch#show aaa method-lists authentication

```
authen queue=AAA_ML_AUTHEN_LOGIN
    Name = default  state = ALIVE :   local
Name = tac-login  state = ALIVE :   tacacs-plus local
```

13.6 Display Results

Telnet output

Figure 13-3 Telnet result

14 Configuring Port Isolate

14.1 Overview

Port-isolation a security feature which is used to prevent from direct l2/l3 communication among a set of ports.

It can provide a safer and more flexible network solutions by isolating the ports which in the same VLAN.

Generally, it’s used as an access device for user isolation.

14.2 Topology

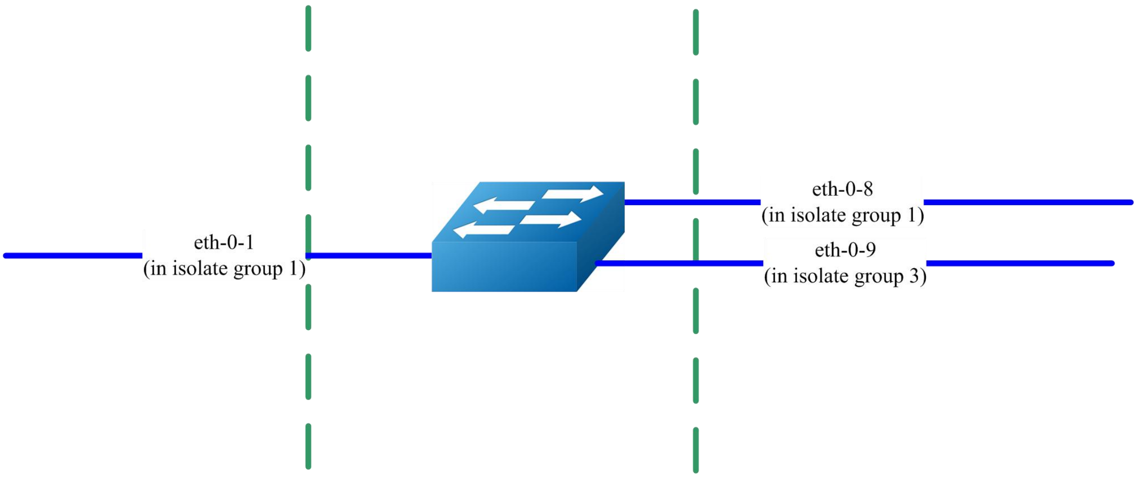


Figure 14-1 Basic topology for port-isolate

Port 1 and port 8 are in the same isolate group 1, they are isolated. So port1 can not communicate with port 8.

Port 9 is in a different isolate group 3, so port 9 can communicate with port 1 and port 8.

14.3 Configuration

Switch's configuration is as follow.

Switch# configure terminal	Enter the Configure mode.
Switch(config)# port-isolate mode l2	Configure the port-isolate mode (User can also use command "port-isolate mode all" to isolate both bridged and routed packets).
Switch(config-if)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode.
Switch(config-if)# port-isolate group 1	Configure interface to join isolate group 1
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode.
Switch(config)# interface eth-0-8	Specify the interface (eth-0-8) to be configured and enter the Interface mode.
Switch(config-if)# port-isolate group 1	Configure interface to join isolate group 1
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode.
Switch(config)# interface eth-0-9	Specify the interface (eth-0-9) to be configured and enter the Interface mode.
Switch(config-if)# port-isolate group 3	Configure interface to join isolate group 3
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode.
Switch(config)# end	Return to the EXEC mode
Switch# show port-isolate	Display the port-isolate configuration

15 Configuring Private-vlan

15.1 Overview

Private-vlan a security feature which is used to prevent from direct l2 communication among a set of ports in a vlan.

It can provide a safer and more flexible network solutions by isolating the ports which in the same VLAN.

15.2 Topology

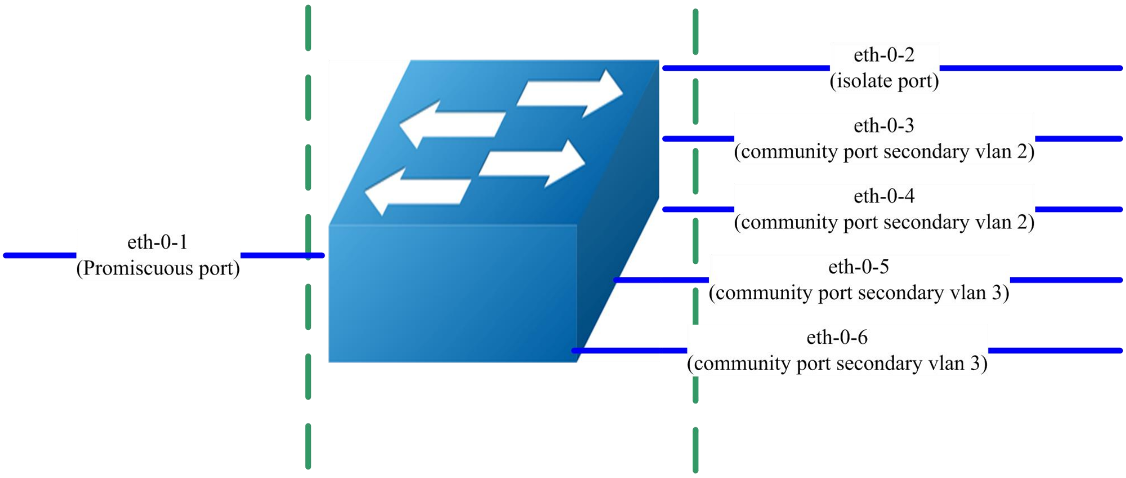


Figure 15-1 Basic topology for private vlan

All ports are in a same primary vlan.

Port 1 is promiscuous port; it can communicate with all other ports.

Port 2 is isolate port; it cannot communicate with all other ports except for the promiscuous port (port 1).

Port 3 and port 4 are community ports in secondary vlan 2; they can communicate with each other. They cannot communicate with all other ports except for the promiscuous port.

Port 5 and port6 are community ports in secondary vlan 3; they can communicate with each other. They cannot communicate with all other ports except for the promiscuous port.

15.3 Configuration

Switch's configuration is as follow.

Switch# configure terminal	Enter the Configure mode.
Switch (config)# vlan database	Enter the Vlan mode
Switch (config-vlan)# vlan 2	Create vlan 2
Switch (config-vlan)# quit	Quit Vlan mode
Switch (config)# interface eth-0-1	Enter interface mode
Switch (config-if)# switchport mode private-vlan promiscuous	Set private vlan mode as promiscuous
Switch (config-if)# switchport private-vlan 2	Set primary vlan as vlan 2
Switch (config-if)# quit	Quit interface mode
Switch (config)# interface eth-0-2	Enter interface mode
Switch (config-if)# switchport mode private-vlan host	Set private vlan mode as host
Switch (config-if)# switchport private-vlan 2 isolate	Set primary vlan as vlan 2, set private vlan mode as isolate
Switch (config-if)# quit	Quit interface mode
Switch (config)# interface eth-0-3	Enter interface mode
Switch (config-if)# switchport mode private-vlan host	Set private vlan mode as host
Switch (config-if)# switchport private-vlan 2 community-vlan 2	Set primary vlan as vlan 2, set private vlan mode as community, set secondary vlan as 2
Switch (config-if)# quit	Quit interface mode
Switch (config)# interface eth-0-4	Enter interface mode
Switch (config-if)# switchport mode private-vlan host	Set private vlan mode as host
Switch (config-if)# switchport private-vlan 2 community-vlan 2	Set primary vlan as vlan 2, set private vlan mode as community, set secondary vlan as 2
Switch (config-if)# quit	Quit interface mode
Switch (config)# interface eth-0-5	Enter interface mode

Switch (config-if)# switchport mode private-vlan host	Set private vlan mode as host
Switch (config-if)# switchport private-vlan 2 community-vlan 3	Set primary vlan as vlan 2, set private vlan mode as community, set secondary vlan as 3
Switch (config-if)# quit	Quit interface mode
Switch (config)# interface eth-0-6	Enter interface mode
Switch (config-if)# switchport mode private-vlan host	Set private vlan mode as host
Switch (config-if)# switchport private-vlan 2 community-vlan 3	Set primary vlan as vlan 2, set private vlan mode as community, set secondary vlan as 3
Switch (config-if)# quit	Quit interface mode

15.4 Validation

The result of show private-vlan is as follows.

switch # show private-vlan

Primary Secondary Type Ports

```
--------------------------------------------------------------------------------
2         N/A       promiscuous    eth-0-1
2         N/A       isloate        eth-0-2
2         2         community      eth-0-3    eth-0-4
2         3         community      eth-0-5    eth-0-6
```

16 Configuring DDOS

16.1 Overview

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. The term is generally used with regards to computer networks, but is not limited to this field, for example, it is also used in reference to CPU resource management.

DDoS prevent is a feature which can protect our switch from follow kinds of denial-of-service attack and intercept the attack packets.

ICMP flood - attackers overwhelms the victim with ICMP packets.

Smurf attack - attackers flood a target system via spoofed broadcast ping messages.

SYN flood - attackers send a succession of SYN requests to a target’s system.

UDP flood - attackers send a large number of UDP packets to random ports on a remote host.

Fraggle attack - attackers send a large number of UDP echo traffic to IP broadcast addresses, all fake source address.

16.2 Topology

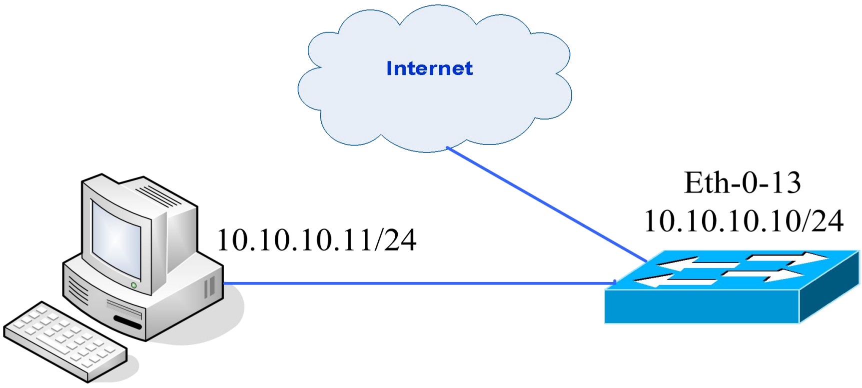


Figure 16-1 DDos prevent topology

16.3 Configuration

Switch's configuration is as follow.

Configuring resist ICMP flood attack

Switch# configure terminal	Enter the Configure mode
Switch(config)# ip icmp intercept maxcount 100	Enable ICMP flood intercept and set the max received ICMP packet rate 100 packets pre second
Switch(config)# end	Return to the EXEC mode
Switch# show ip-intercept config	Display the DDoS prevent configuration

Configuring resist UDP flood attack

Switch# configure terminal	Enter the Configure mode
Switch(config)# ip udp intercept maxcount 100	Enable UDP flood intercept and set the max received UDP packet rate 100 packets pre second
Switch(config)# end	Return to the EXEC mode
Switch# show ip-intercept config	Display the DDoS prevent configuration

Configuring resist Smurf attack

Switch# configure terminal	Enter the Configure mode

Switch(config)# ip smurf intercept	Enable Smurf attack intercept
Switch(config)# end	Return to the EXEC mode
Switch# show ip-intercept config	Display the DDoS prevent configuration

Configuring resist SYN flood attack

Switch# configure terminal	Enter the Configure mode
Switch(config)# ip tcp intercept maxcount 100	Enable SYN flood intercept and set the max received SYN packet rate 100 packets pre second
Switch(config)# end	Return to the EXEC mode
Switch# show ip-intercept config	Display the DDoS prevent configuration

Configuring resist Fraggle attack

Switch# configure terminal	Enter the Configure mode
Switch(config)# ip fraggle intercept	Enable Fraggle attack intercept
Switch(config)# end	Return to the EXEC mode
Switch# show ip-intercept config	Display the DDoS prevent configuration

Configuring resist Small-packet attack

Switch# configure terminal	Enter the Configure mode
Switch(config)# ip small-packet intercept maxlength 32	Enable Small-packet attack intercept and set the received packet length is be more than or equal to 32
Switch(config)# end	Return to the EXEC mode
Switch# show ip-intercept config	Display the DDoS prevent configuration

Configuring packet same IP intercept

Switch# configure terminal	Enter the Configure mode
Switch(config)# ip ipeq intercept	Enable packet source IP equals destination IP intercept
Switch(config)# end	Return to the EXEC mode

Switch# show ip-intercept config	Display the DDoS prevent configuration

Configuring packet same MAC intercept

Switch# configure terminal	Enter the Configure mode
Switch(config)# ip maceq intercept	Enable packet source MAC equals destination MAC intercept
Switch(config)# end	Return to the EXEC mode
Switch# show ip-intercept config	Display the DDoS prevent configuration

16.4 Validation

Switch# show ip-intercept config

```
Current DDoS Prevent configuration:
============================================================
ICMP Flood Intercept              :Enable  Maxcount:100
UDP Flood Intercept               :Enable  Maxcount:100
SYN Flood Intercept               :Enable  Maxcount:100
Small-packet Attack Intercept     :Enable  Packet Length:32
Sumrf Attack Intercept            :Enable
Fraggle Attack Intercept          :Disable
MAC Equal Intercept               :Enable
IP Equal Intercept                :Enable
```

Switch# show ip-intercept statistics

```
Current DDoS Prevent statistics:
============================================================
Resist Small-packet Attack packets number    :  65
Resist ICMP Flood packets number             :  0
Resist Smurf Attack packets number           :  0
Resist SYN Flood packets number              :  0
Resist UDP Flood packets number              :  0
```

17 Configuring Key Chain

17.1 Overview

Keychain is a common method of authentication to configure shared secrets on all the entities, which exchange secrets such as keys before establishing trust with each other. Routing protocols and network applications often use this authentication to enhance security while communicating with peers.

The keychain by itself has no relevance; therefore, it must be used by an application that needs to communicate by using the keys (for authentication) with its peers. The keychain provides a secure mechanism to handle the keys and rollover based on the lifetime.

If you are using keys as the security method, you must specify the lifetime for the keys and change the keys on a regular basis when they expire. To maintain stability, each party must be able to store and use more than one key for an application at the same time. A keychain is a sequence of keys that are collectively managed for authenticating the same peer, peer group, or both. Keychain groups a sequence of keys together under a keychain and associates each key in the keychain with a lifetime.

17.2 Configurations

Configure the keychain

Switch# configure terminal	Enter the Configure mode
Switch(config)# key chain test	Create a keychain named test and enter Keychain Configure mode
Switch(config-keychain)# key 1	Configure a key with ID 1 and enter Key Configure mode

Switch(config-keychain-key)# key-string ##test_keystring_1##	Configure key string
Switch(config-keychain-key)# accept-lifetime 0:0:1 1 jan 2012 infinite	Specifies the set time period during which an authentication key on a keychain is valid to be accept
Switch(config-keychain)# key 2	Configure a key with ID 2 and enter Key Configure mode
Switch(config-keychain-key)# key-string ##test_keystring_2##	Configure key string
Switch(config-keychain-key)# send-lifetime 0:0:1 2 jan 2012 infinite	Specifies the set time period during which an authentication key on a keychain is valid to be sent

17.3 Validation

To display the keychain configuration, use the command **show key chain** in the privileged EXEC mode.

Switch# show key chain

```
key chain test:
    key 1 -- text "key-string ##test_keystring_1##"
      accept-lifetime <00:00:01 Jan 01 2012> - <infinite>
      send-lifetime <always valid> - <always valid> [valid now]
    key 2 -- text "key-string ##test_keystring_2##"
      accept-lifetime <always valid> - <always valid> [valid now]
      send-lifetime <00:00:01 Jan 02 2012> - <infinite>
```

18 Configuring Port-Block

18.1 Overview

By default, the switch floods packets with unknown destination MAC addresses out of all ports. If unknown unicast and multicast traffic is forwarded to a protected port, there could be security issues. To prevent unknown unicast or multicast traffic from being forwarded from one port to another, you can block a port (protected or nonprotected) from flooding unknown unicast or multicast packets to otherports.

18.2 Configurations

Configure the port-block

Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# port-block unknown-unicast	Configure port-block
Switch(config-if)# end	Exit the Configure mode
Switch# show port-block interface eth-0-1	Show port-block configuration

18.3 Validation

To display the port-block configuration, use the command **show port-block** in the privileged EXEC mode.

```
Switch # show port-block interface eth-0-1
 Known unicast blocked: Enabled
 Known multicast blocked: Disabled
 Unknown unicast blocked: Disabled
 Unknown multicast blocked: Disabled
 Broadcast blocked: Disabled
```