FS.COM

FiberstoreOS

IPv6 Service Configuration Guide

Contents

1 Configuring DHCPv6 Snooping

1.1 Overview

DHCPv6 snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCPv6 servers. The DHCPv6 snooping feature performs the following activities:

- Validate DHCPv6 messages received from untrusted sources and filters out invalid messages.
- Build and maintain the DHCPv6 snooping binding database, which contains information about untrusted hosts with leased IPv6 addresses.
- The DHCPv6 snooping feature is implemented in software basis. All DHCPv6 messages are intercepted in the chip and directed to the CPU for processing.

1.2 Topology

This figure is the networking topology for testing DHCPv6 snooping functions. We need two Linux boxes and one switch to construct the test bed.

- Computer A is used as a DHCPv6 server.
- Computer B is used as a DHCPv6 client.
- Switch A is used as a DHCPv6 Snooping box.

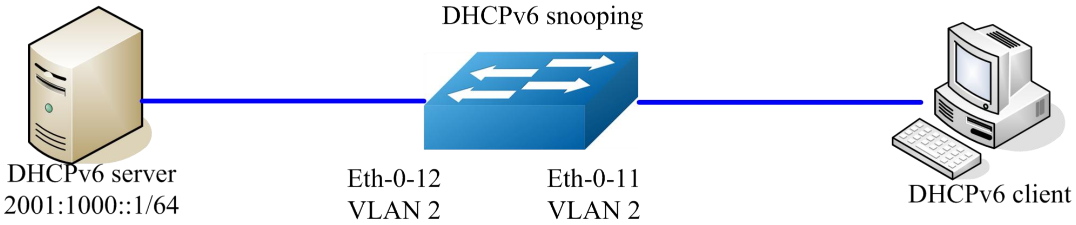


Figure 1-1 DHCPv6 Snooping Topology

1.3 Configuration

Configure 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 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 2	Add the port to vlan 2
Switch(config-if)# dhcpv6 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 2	Add the port to vlan 2
Switch(config-if)# no shutdown	Make sure the port is enabled
Switch(config-if)# exit	Exit the Interface Configure mode

Enable DHCPv6 snooping global feature

Switch(config)# service dhcpv6 enable	Enable dhcp services
Switch(config)# dhcpv6 snooping	Enable dhcp snooping feature
Switch(config)# dhcpv6 snooping vlan 2	Enable dhcp snooping feature on vlan 2

1.4 Validation

Step 2 Check the interface configuration.

Switch(config)# show running-config interface eth-0-12

```
!
interface eth-0-12
 switchport access vlan 2
 dhcpv6 snooping trust

!
```

Switch(config)# show running-config interface eth-0-11

```
!
interface eth-0-11
 switchport access vlan 2
!
```

Step 3 Check the dhcpv6 service status.

Switch# show services

```
Networking services configuration:
Service Name         Status
============================================================
dhcp                   disable
dhcpv6                 enable
```

Step 4 Print dhcpv6 snooping configuration to check current configuration.

Switch# show dhcpv6 snooping config

```
dhcpv6 snooping service: enabled
dhcpv6 snooping switch: enabled
dhcpv6 snooping vlan 2
```

Step 5 Show dhcpv6 snooping statistics.

Switch# show dhcpv6 snooping statistics

```
DHCPv6 snooping statistics:
============================================================
DHCPv6 packets                              21

Packets forwarded                        21
Packets invalid                           0
Packets dropped                           0
```

Step 6 Show dhcpv6 snooping binding information.

Switch# show dhcpv6 snooping binding all

```
DHCPv6 snooping binding table:
VLAN MAC Address    Lease(s)    Interface   IPv6 Address
============================================================
2    0016.76a1.7ed9 978         eth-0-11    2001:1000::2
```

2 Configuring ACLv6

2.1 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.

2.2 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.

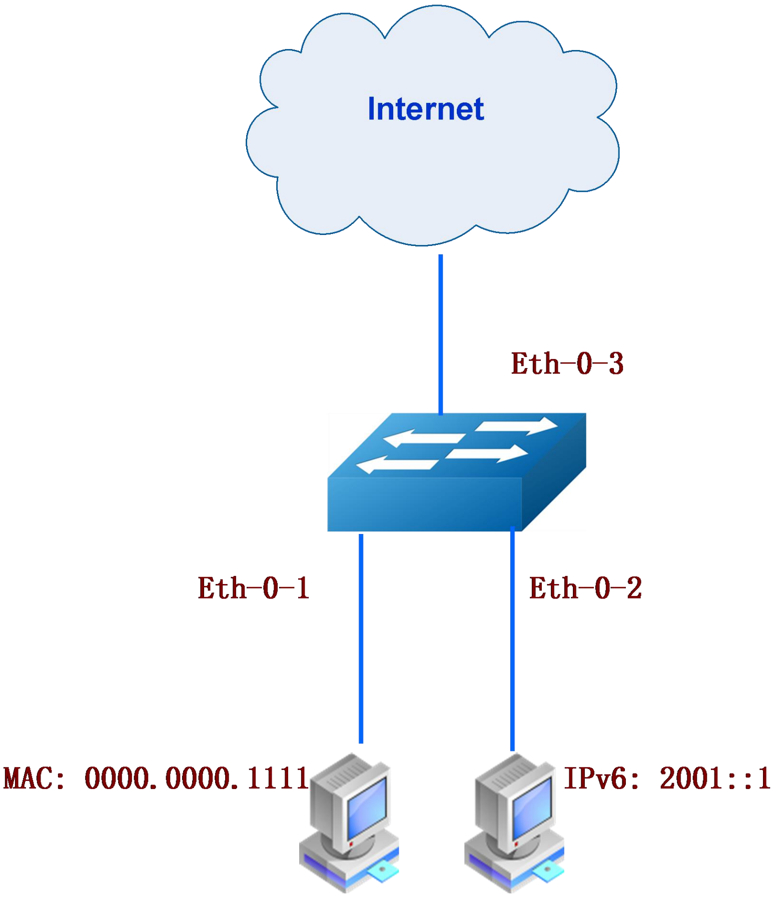
Time Range

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.

2.3 Limitation

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

2.4 Topology



2.5 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

2.6 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
!
```