FS.COM

FiberstoreOS

IPv6 Security Command Line Reference

Contents

1 DHCPv6 Snooping Commands

1.1 no dhcpv6 snooping bindings

Use the no dhcpv6 snooping bindings global configuration command on the switch to clear the dynamic DHCPv6 binding items.

Command Syntax

clear dhcpv6 snooping bindings learning (ipv6 *IP-ADDRESS* | **mac** *MAC-ADDRESS* | **vlan** *VLAN-ID*| **interface** *IFNAME* |)

ipv6 *IP-ADDRESS*	Clear the binding entry with the IPv6 address
mac *MAC-ADDRESS*	Clear the binding entry with the MAC address
vlan *VLAN-ID*	Clear the binding entry with the VLAN
interface *IFNAME*	Clear the binding entry with the Interface

Command Mode

Global Configuration

Default

No default is defined.

Usage

This command is used to clear dynamic DHCPv6 snooping binding item.

Examples

This example shows how to clear all DHCPv6 snooping binding items:

Switch# clear dhcpv6 snooping bindings learning

Related Commands

show dhcpv6 snooping binding

1.2 clear dhcpv6 snooping statistics

Use the clear dhcpv6 snooping statistics privileged EXEC command on the switch to clear the DHCPv6 snooping statistics counters.

Command Syntax

clear dhcpv6 snooping statistics

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

This command is used to clear DHCPv6 snooping statistics.

Examples

This example shows how to clear the DHCPv6 snooping statistics counters:

Switch# clear dhcpv6 snooping statistics

Related Commands

show dhcpv6 snooping statistics

1.3 dhcpv6 snooping

Use the dhcpv6 snooping global configuration command on the switch to globally enable DHCPv6 snooping. Use the no form of this command to return to the default setting.

Command Syntax

dhcpv6 snooping

no dhcpv6 snooping

Command Mode

Global Configuration

Default

DHCPv6 snooping is disabled.

Usage

For any DHCPv6 snooping configuration to take effect, you must globally enable DHCPv6 snooping. DHCPv6 snooping is not active until you enable snooping on a VLAN by using the dhcpv6 snooping vlan global configuration command.

Examples

This example shows how to enable DHCPv6 snooping:

Switch(config)# dhcpv6 snooping

You can verify your settings by entering the show dhcpv6 snooping config privileged EXEC command.

Related Commands

dhcpv6 snooping vlan

show dhcpv6 snooping config

1.4 dhcpv6 snooping binding

Use the dhcpv6 snooping binding global configuration command on the switch to configure the DHCPv6 snooping binding database and to add binding entries to the database.

Command Syntax

dhcpv6 snooping binding mac *MAC-ADDRESS* **vlan** *VLAN-ID* **ipv6** *IP-ADDRESS* **interface** *IFNAME* **expiry** *SECONDS*

no dhcpv6 snooping bindings (**ipv6** *IP-ADDRESS* | **mac** *MAC-ADDRESS* | **vlan** *VLAN-ID* | **interface** *IFNAME* |)

mac *MAC-ADDRESS*	Specify a MAC address
vlan *VLAN-ID*	Specify a VLAN number. The range is 1 to 4094

ipv6 *IP-ADDRESS*	Specify an IPv6 address
interface *IFNAME*	Specify an interface on which to add or delete a binding entry
expiry *SECONDS*	Specify the interval (in seconds) after which the binding entry is no longer valid. The range is 0 to 86400

Command Mode

Global Configuration

Default

No default database is defined.

Usage

Use this command when you are testing or debugging the switch.

In the DHCPv6 snooping binding database, each database entry, also referred to a binding, has an IP address, an associated MAC address, the lease time, the interface to which the binding applies, and the VLAN to which the interface belongs.

Use the show dhcpv6 snooping binding privileged EXEC command to display the configured bindings.

Examples

This example shows how to generate a DHCPv6 binding with an expiration time of 1000 seconds on a port in VLAN 1:

Switch(config)# dhcpv6 snooping binding mac 0001.000c.01ef vlan 1 ipv6 2001:1::1 interface eth-0-1 expiry 1000

Related Commands

show dhcpv6 snooping binding

1.5 dhcpv6 snooping database

Use the dhcpv6 snooping database global configuration command on the switch to configure the DHCPv6 snooping binding database agent. Use the no form of this command to reset the write-delay value.

Command Syntax

dhcpv6 snooping database auto-save interval *SECONDS*

interval *SECONDS*	Specify the interval (in seconds) that how long to save the binding database. The range is 15 to 1200

Command Mode

Global Configuration

Default

Default interval is 600 seconds.

Usage

The DHCPv6 snooping database is save as flash:/dhcpv6snooping.

Examples

The following is sample output from the dhcpv6 snooping database command:

Switch(config)# dhcpv6 snooping database auto-save interval 120

Related Commands

dhcpv6 snooping

dhcpv6 snooping binding

1.6 dhcpv6 snooping trust

Use the dhcpv6 snooping trust interface configuration command on the switch to configure a port as trusted for DHCPv6 snooping purposes. Use the no form of this command to return to the default setting.

Command Syntax

dhcpv6 snooping trust

no dhcpv6 snooping trust

Command Mode

Interface configuration

Default

DHCPv6 snooping trust is disabled.

Usage

Configure as trusted ports those that are connected to a DHCPv6 server or to other switches or routers. Configure as untrusted ports those that are connected to DHCPv6 clients.

Examples

This example shows how to enable DHCPv6 snooping trust on a port:

Switch(config-if)# dhcpv6 snooping trust

Related Commands

show dhcpv6 snooping trusted-sources

1.7 dhcpv6 snooping vlan

Use the dhcpv6 snooping vlan global configuration command on the switch to enable DHCPv6 snooping on a VLAN. Use the no form of this command to return to the default setting.

Command Syntax

dhcpv6 snooping vlan *VLAN-RANGE*

no dhcpv6 snooping vlan *VLAN-RANGE*

VLAN-RANGE	Specify a VLAN ID or a range of VLANs on which to enable DHCP snooping. The range is 1 to 4094

Command Mode

Global Configuration

Default

DHCPv6 snooping is disabled on all VLANs.

Usage

You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.

You must first globally enable DHCPv6 snooping before enabling DHCPv6 snooping on a VLAN.

Examples

This example shows how to enable DHCPv6 snooping on VLAN 10:

Switch(config)# dhcpv6 snooping vlan 10

Related Commands

show dhcpv6 snooping config

1.8 debug dhcpv6 snooping

Use this command to turn on the debug switches of dhcpv6 snooping module.

To restore the default, use the **no** form of this command

Command Syntax

debug dhcpv6 snooping (**events** | **error** | **dump** | **packet** | **all**)

no debug dhcpv6 snooping (**events** | **error** | **dump** | **packet** | **all**)

events	Snooping events
error	Error DHCPv6 message
packet	DHCPv6 message fields
dump	Dump message in hex format
all	Turn all debugging on

Command Mode

Privileged EXEC

Default

None

Usage

Use command “terminal monitor ” to make debug messages print on the VTY immediately.

Use command “show logging buffer” to check the debug messages in the logging buffer.

Examples

The following is sample to open dhcpv6 snooping debug switches:

Switch# debug dhcpv6 snooping all

Related Commands

terminal monitor

show logging buffer

1.9 show dhcpv6 snooping binding

Use the show dhcpv6 snooping binding privileged EXEC command to display the DHCPv6 snooping binding database and configuration information for all interfaces on a switch.

Command Syntax

show dhcpv6 snooping binding (（**all** | **manual** | **learning** ）**(ipv6** *IPv6-ADDRESS* | **mac** *MAC-ADDRESS* | **vlan** *VLAN-ID* | **interface** *IFNAME* |) **summary|)**

all	Display all entries
manual	Display static entries
learning	Display dynamic entries
mac *MAC-ADDRESS*	Specify MAC address
vlan *VLAN-ID*	Specify a VLAN number. The range is 1 to 4094
Ipv6 *IP-ADDRESS*	Specify an IPv6 address
interface *IFNAME*	Specify an interface on which to add or delete a binding entry
summary	Display summary information of DHCPv6 snooping bindings

Command Mode

Privileged EXEC

Default

None

Usage

If DHCPv6 snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.

Examples

The following is sample output from the show dhcpv6 snooping binding command:

Switch# show dhcpv6 snooping binding all

```
DHCPv6 snooping binding table:
VLAN MAC Address     Interface  Lease(s)    IPv6 Address
============================================================
1    0001.0001.0001 eth-0-2    static      1:1::1:1
```

Switch# show dhcpv6 snooping binding summary

```
Total 1 DHCPv6 snooping binding entries
    0 learning entry, 1 configured entry
```

Related Commands

dhcpv6 snooping binding

1.10 show dhcpv6 snooping config

Use the show dhcpv6 snooping privileged EXEC command to display the DHCPv6 snooping configuration.

Command Syntax

show dhcpv6 snooping config

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the configuration of DHCPv6 snooping.

Examples

The following is sample output from the show dhcpv6 snooping config command:

Switch# show dhcpv6 snooping config

```
dhcpv6 snooping service: enabled
dhcpv6 snooping switch: enabled
dhcpv6 snooping vlan 3
```

Related Commands

dhcpv6 snooping

dhcpv6 snooping vlan

1.11 show dhcpv6 snooping trusted-sources

Use the show dhcpv6 snooping trusted-sources privileged EXEC command to display the DHCPv6 snooping trusted interface.

Command Syntax

show dhcpv6 snooping trusted-sources

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the trusted interface of DHCPv6 snooping.

Examples

The following is sample output from the show dhcpv6 snooping trusted-sources command:

Switch# show dhcpv6 snooping trusted-source

```
List of DHCPv6 snooping trusted interface(s):
============================================================
eth-0-20
```

Related Commands

dhcpv6 snooping trust

1.12 show dhcpv6 snooping statistics

Use the show dhcpv6 snooping statistics privileged EXEC command to display DHCPv6 snooping statistics.

Command Syntax

show dhcpv6 snooping statistics

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the statistics of DHCPv6 snooping.

Examples

The following is sample output from the show dhcpv6 snooping statistics command:

Switch# show dhcpv6 snooping statistics

```
DHCPv6 snooping statistics:
============================================================
DHCPv6 packets                          137

Packets forwarded                       137
Packets invalid                         0
Packets dropped                         0
```

Related Commands

clear dhcpv6 snooping statistics

2 ACLv6 Commands

2.1 ipv6 access-list

Use this command to create IPv6 ACL and then enter IPv6 ACL in global configuration mode.

Command Syntax

ipv6 access-list *ACL-NAME*

no ipv6 access-list *ACL-NAME*

ACL-NAME	The name of the IPv6 ACL

Command Mode

Global Configuration

Default

None

Usage

If the system already has an IPv6 ACL with the same name, this command will enter the IPv6 ACL configuration mode. However, if the ACL name is used by other type of ACL, a prompt message will be shown.

When the name is not used by any ACL, this command is to create the IPv6 ACL firstly and then enter the IPv6 ACL configuration mode.

Examples

This example shows how to create an IPv6 ACL named list_ipv6_1 and then enter the IPv6 ACL configuration mode.

Switch(config)# ipv6 access-list list_ipv6_1

Switch(config-ipv6-acl)#

This example shows how to remove the IPv6 ACL named list_ipv6_1.

Switch(config)# no ipv6 access-list list_ipv6_1

Related Commands

match access-group

2.2 sequence-num

Use this command to remove a filter from IPv6 ACL.

Command Syntax

no sequence-num *SEQUENCE-NUM*

SEQUENCE-NUM	The sequence number of a IPv6 filter, the range is 1 to 2147483646

Command Mode

IPv6 ACL Configuration

Default

None

Usage

None

Examples

This example shows how to remove a filter with the sequence-num 10 from IPv6 ACL.

Switch(config-ipv6-acl)# no sequence-num 10

Related Commands

deny

deny tcp

deny udp

deny icmp

permit

permit tcp

permit udp

permit icmp

2.3 remark

Use this command to add remarks for the IPv6 ACL.

To remove remarks of the IPv6 ACL, use the no form of this command.

Command Syntax

remark *REMARK*

no remark

REMARK	The remarks of the IPv6 ACL

Command Mode

IPv6 ACL Configuration

Default

None

Usage

The remarks are up to 100 characters. The exceed parts will not be stored and will be truncated.

Examples

This example shows how to add a remark to describe the IPv6 ACL.

Switch(config-ipv6-acl)# remark remark of List for ipv6

This example shows how to remove the remark of the IPv6 ACL.

Switch(config-ipv6-acl)# no remark

Related Commands

ipv6 access-list

2.4 show access-list ipv6

Use this command to show the IPv6 ACL information.

Command Syntax

show access-list ipv6 (*ACL-NAME* |)

ACL-NAME	The name of the IPv6 ACL

Command Mode

Privileged EXEC

Default

None

Usage

If no ipv6 acl are specified, all ipv6 access-lists in the system should be shown.

Examples

This example shows how to show the IPv6 ACL information.

Switch# show access-list ipv6

```
ipv6 access-list list_ipv6_1
  10 deny any 2001::/48 any
  20 permit any any any
```

Related Commands

ipv6 access-list

2.5 deny

Use this command to discard ongoing IPv6 packets matching the IPv6 filter.

Command Syntax

(*SEQUENCE-NUM* |) **deny** (*PROTO-NUM* | **any**) (*SOURCE-PREFIX* | **any** | **host** *SOURCE*) (*DESTINATION-PREFIX* | **any** | **host** *DESTINATION*) (**routed-packet** |) (**time-range** *TIME-RANGE-NAME* |)

SEQUENCE-NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented. The range is 1 to 2147483646
PROTO-NUM	An IPv6 protocol number, the range is 0 to 255
any	Any IPv6 protocol
SOURCE-PREFIX	The source IPv6 prefix address
any	Any source host
host *SOURCE*	The source IPv6 address of a host
DESTINATION-PREFIX	The destination IPv6 prefix address
any	Any destination host
host *DESTINATION*	The destination IPv6 address of a host
routed-packet	Match routed packet
time-range *TIME-RANGE-NAME*	The time-range used by the IPv6 filter

Command Mode

IPv6 ACL configuration

Default

None

Usage

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the IPv6 ACL. For example, when the maximum existing sequence number is 100, the sequence number of subsequent created IPv6 filter is 110.

Examples

This example shows how to create a filter in IPv6 ACL to deny any IPv6 packets.

Switch(config-ipv6-acl)# 1 deny any any any

This example shows how to create a filter in IPv6 ACL to deny any routed packets.

Switch(config-ipv6-acl)# 2 deny any any any routed-packet

Related Commands

no sequence-num

2.6 deny tcp

Use this command to reject TCP packets matching the IPv6 filter.

Command Syntax

(*SEQUENCE-NUM* |) **deny tcp** (*SOURCE-PREFIX* | **any** | **host** *SOURCE*) (**src-port** *OPERATOR PORT* |) (*DESTINATION-PREFIX* | **any** | **host** *DESTINATION*) (**dst-port** *OPERATOR PORT* |) (**routed-packet** |) (**time-range** *TIME-RANGE-NAME* |)

SEQUENCE-NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented. the range is 1 to 2147483646
SOURCE-PREFIX	The source IPv6 prefix address
any	Any source host
host *SOURCE*	The source IPv6 address of a host
src-port *OPERATOR PORT*	Source port, the range is 0 to 65535, including eq (equal to)
DESTINATION-PREFIX	The destination IPv6 prefix address
any	Any destination host
host *DESTINATION*	The destination IPv6 address of a host
dst-port *OPERATOR PORT*	Destination port, the range is 0 to 65535, including eq (equal to)
routed-packet	Match routed packet
time-range *TIME-RANGE-NAME*	The time-range used by the IPv6 filter

Command Mode

IPv6 ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to deny any TCP packets.

Switch(config-ipv6-acl)# 1 deny tcp any any

This example shows how to create a filter in IPv6 ACL to deny the TCP packets with the source IPv6 address 2001::2020, source port 8080.

Switch(config-ipv6-acl)# 2 deny tcp host 2001::2020 src-port eq 8080 any

Related Commands

no sequence-num

2.7 deny udp

Use this command to reject UDP packets matching the IPv6 filter.

Command Syntax

(*SEQUENCE-NUM* |) **deny udp** (*SOURCE-PREFIX* | **any** | **host** *SOURCE*) (**src-port** *OPERATOR PORT* |) (*DESTINATION-PREFIX* | **any** | **host** *DESTINATION*) (**dst-port** *OPERATOR PORT* |) (**routed-packet** |) (**time-range** *TIME-RANGE-NAME* |)

Please reference to command “deny tcp” for the parameters.

Command Mode

IPv6 ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to deny any UDP packets.

Switch(config-ipv6-acl)# 1 deny udp any any

This example shows how to create a filter in IPv6 ACL to deny the UDP packets with the source IPv6 address 2001::2020, source port 8080.

Switch(config-ipv6-acl)# 2 deny udp host 2001::2020 src-port eq 8080 any

Related Commands

no sequence-num

2.8 deny icmp

Use this command to reject ICMP packets matching the IPv6 filter.

Command Syntax

(*SEQUENCE-NUM* |) **deny icmp** (*SOURCE-PREFIX* | **any** | **host** *SOURCE*) (*DESTINATION-PREFIX* | **any** | **host** *DESTINATION*) (**icmp-type** *TYPE-NUM* **(icmp-code** *CODE-NUM* |) |) (**routed-packet** |) (**time-range** *TIME-RANGE-NAME* |)

icmp-type *TYPE-NUM*	ICMP message type, the range is 0 to 255
icmp-code *CODE-NUM*	ICMP message code, the range is 0 to 255

Please reference to command “deny” for the parameters.

Command Mode

IPv6 ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to deny any ICMP packets.

Switch(config-ipv6-acl)# 1 deny icmp any any

This example shows how to create a filter in IPv6 ACL to deny the ICMP packets with the icmp-type 3 and icmp-code 3.

Switch(config-ipv6-acl)# 2 deny icmp any any icmp-type 3 icmp-code 3

Related Commands

no sequence-num

2.9 permit

Use this command to permit ongoing IPv6 packets matching the IPv6 filter.

Command Syntax

(*SEQUENCE-NUM* |) **permit** (*PROTO-NUM* | **any**) (*SOURCE-PREFIX* | **any** | **host** *SOURCE*) (*DESTINATION-PREFIX* | **any** | **host** *DESTINATION*) (**routed-packet** |) (**time-range** *TIME-RANGE-NAME* |)

SEQUENCE-NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented. The range is 1 to 2147483646
PROTO-NUM	An IPv6 protocol number, the range is 0 to 255
any	Any IPv6 protocol
SOURCE-PREFIX	The source IPv6 prefix address
any	Any source host
host *SOURCE*	The source IPv6 address of a host
DESTINATION-PREFIX	The destination IPv6 prefix address
any	Any destination host
host *DESTINATION*	The destination IPv6 address of a host
routed-packet	Match routed packet

time-range *TIME-RANGE-NAME*	The time-range used by the IPv6 filter

Command Mode

IPv6 ACL configuration

Default

None

Usage

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the IPv6 ACL. For example, when the maximum existing sequence number is 100, the sequence number of subsequent created IPv6 filter is 110.

Examples

This example shows how to create a filter in IPv6 ACL to permit any IPv6 packets.

Switch(config-ipv6-acl)# 1 permit any any any

This example shows how to create a filter in IPv6 ACL to permit any routed packets.

Switch(config-ipv6-acl)# 2 permit any any any routed-packet

Related Commands

no sequence-num

2.10 permit tcp

Use this command to permitTCP packets matching the IPv6 filter.

Command Syntax

(*SEQUENCE-NUM* |) **permit tcp** (*SOURCE-PREFIX* | **any** | **host** *SOURCE*) (**src-port** *OPERATOR PORT* |) (*DESTINATION-PREFIX* | **any** | **host** *DESTINATION*) (**dst-port** *OPERATOR PORT* |) (**routed-packet** |) (**time-range** *TIME-RANGE-NAME* |)

SEQUENCE-NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented. the range is 1 to 2147483646
SOURCE-PREFIX	The source IPv6 prefix address
any	Any source host
host *SOURCE*	The source IPv6 address of a host
src-port *OPERATOR PORT*	Source port, the range is 0 to 65535, including eq (equal to)
DESTINATION-PREFIX	The destination IPv6 prefix address
any	Any destination host
host *DESTINATION*	The destination IPv6 address of a host
dst-port *OPERATOR PORT*	Destination port, the range is 0 to 65535, including eq (equal to)
routed-packet	Match routed packet
time-range *TIME-RANGE-NAME*	The time-range used by the IPv6 filter

Command Mode

IPv6 ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to permit any TCP packets.

Switch(config-ipv6-acl)# 1 permit tcp any any

This example shows how to create a filter in IPv6 ACL to permit the TCP packets with the source IPv6 address 2001::2020, source port 8080.

Switch(config-ipv6-acl)# 2 permit tcp host 2001::2020 src-port eq 8080 any

Related Commands

no sequence-num

2.11 permit udp

Use this command to permit UDP packets matching the IPv6 filter.

Command Syntax

(*SEQUENCE-NUM* |) **permit udp** (*SOURCE-PREFIX* | **any** | **host** *SOURCE*) (**src-port** *OPERATOR PORT* |) (*DESTINATION-PREFIX* | **any** | **host** *DESTINATION*) (**dst-port** *OPERATOR PORT* |) (**routed-packet** |) (**time-range** *TIME-RANGE-NAME* |)

Please reference to command “permit tcp” for the parameters.

Command Mode

IPv6 ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to permit any UDP packets.

Switch(config-ipv6-acl)# 1 permit udp any any

This example shows how to create a filter in IPv6 ACL to permit the UDP packets with the source IPv6 address 2001::2020, source port 8080.

Switch(config-ipv6-acl)# 2 permit udp host 2001::2020 src-port eq 8080 any

Related Commands

no sequence-num

2.12 permit icmp

Use this command to reject ICMP packets matching the IPv6 filter.

Command Syntax

(*SEQUENCE-NUM* |) **permit icmp** (*SOURCE-PREFIX* | **any** | **host** *SOURCE*) (*DESTINATION-PREFIX* | **any** | **host** *DESTINATION*) (**icmp-type** *TYPE-NUM* **(icmp-code** *CODE-NUM* |) |) (**routed-packet** |) (**time-range** *TIME-RANGE-NAME* |)

icmp-type *TYPE-NUM*	ICMP message type, the range is 0 to 255
icmp-code *CODE-NUM*	ICMP message code, the range is 0 to 255

Please reference to command “permit” for the parameters.

Command Mode

IPv6 ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to permit any ICMP packets.

Switch(config-ipv6-acl)# 1 permit icmp any any

This example shows how to create a filter in IPv6 ACL to permit the ICMP packets with the icmp-type 3 and icmp-code 3.

Switch(config-ipv6-acl)# 2 permit icmp any any icmp-type 3 icmp-code 3

Related Commands

no sequence-num