IPv6 Commands

ipv6 flow monitor

This command activates a previously created flow monitor by assigning it to the interface to analyze incoming or outgoing traffic.

To activate a previously created flow monitor, use the **ipv6 flow monitor** command. To de-activate a flow monitor, use the **no** form of the command.

ipv6 flow monitor *ipv6-monitor-name* [**sampler** *ipv6-sampler-name*] {**input** | **output**}
no ipv6 flow monitor *ipv6-monitor-name* [**sampler** *ipv6-sampler-name*] {**input** | **output**}

Syntax Description

ipv6-monitor-name	Activates a previously created flow monitor by assigning it to the interface to analyze incoming or outgoing traffic.
sampler *ipv6-sampler-name*	Applies the flow monitor sampler.
input	Applies the flow monitor on input traffic.
output	Applies the flow monitor on output traffic.

Command Default

IPv6 flow monitor is not activated until it is assigned to an interface.

Command Modes

Interface Configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You cannot attach a NetFlow monitor to a port channel interface. If both service module interfaces are part of an EtherChannel, you should attach the monitor to both physical interfaces.

This example shows how to apply a flow monitor to an interface:

```
Device(config)# interface gigabitethernet 1/1/2
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-2 output
Device(config-if)# end
```

ipv6 traffic-filter

This command enables IPv6 traffic filter.

To enable the filtering of IPv6 traffic on an interface, use the **ipv6 traffic-filter** command. To disable the filtering of IPv6 traffic on an interface, use the **no** form of the command.

Use the **ipv6 traffic-filter** interface configuration command on the switch stack or on a standalone switch to filter IPv6 traffic on an interface. The type and direction of traffic that you can filter depends on the feature set running on the switch stack. Use the **no** form of this command to disable the filtering of IPv6 traffic on an interface.

ipv6 traffic-filter [**web**] *acl-name*
no ipv6 traffic-filter [**web**]

Syntax Description

web	(Optional) Specifies an IPv6 access name for the WLAN Web ACL.
acl-name	Specifies an IPv6 access name.

Command Default

Filtering of IPv6 traffic on an interface is not configured.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6 {default | vlan}** global configuration command and reload the switch.

You can use the **ipv6 traffic-filter** command on physical interfaces (Layer 2 or Layer 3 ports), Layer 3 port channels, or switch virtual interfaces (SVIs).

You can apply an ACL to outbound or inbound traffic on Layer 3 interfaces (port ACLs), or to inbound traffic on Layer 2 interfaces (router ACLs).

If **any** port ACL (IPv4, IPv6, or MAC) is applied to an interface, that port ACL is used to filter packets, and any router ACLs attached to the SVI of the port VLAN are ignored.

This example shows how to filter IPv6 traffic on an interface:

```
Device(config-wlan)# ipv6 traffic-filter TestDocTrafficFilter
```

show wireless ipv6 statistics

This command is used to display the IPv6 packet counter statistics.

To view IPv6 packet counter statistics, use the **show wireless ipv6 statistics** command.

show wireless ipv6 statistics

Command Default

None.

Command Modes

User EXEC.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following example shows the summary of the IPv6 packet counter statistics:

```
Device# show wireless ipv6 statistics
NS Forwarding to wireless clients               : Enabled

RS count                                        : 0
RA count                                        : 0
NS count                                        : 0
NA count                                        : 0
Other NDP packet count                          : 0
-----------------------------------------------------
Non-IPv6 packets count                          : 0
Non-IPv6 Multicast Destination MAC packet count : 0
Invalid length packets count                    : 0
Null packets count                              : 0
Invalid Source MAC packets count                : 0
-----------------------------------------------------
TCP packets count                               : 0
UDP packets count                               : 0
Fragmented packets count                        : 0
No next header packets count                    : 0
Other type packets count                        : 0
-----------------------------------------------------
Total packets count                             : 0
-----------------------------------------------------
Blocked RA packets count                        : 0
Blocked NS packets count                        : 0
```