F Commands

This chapter describes the Cisco NX-OS system management commands that begin with the letter F.

feature icam

To enable the Intelligent CAM (iCAM) feature, use the **feature icam** command. To disable the iCAM feature, use the **no** form of this command.

feature icam

no feature icam

Syntax Description

This command has no arguments or keywords.

Command Default

The iCAM feature is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco NX-OS Release 8.0(1)	This command was introduced.

Usage Guidelines

This feature requires the ENHANCED_LAYER2_PKG license.

Examples

This example shows how to enable the iCAM feature:

```
switch# configure terminal
switch(config)# feature icam
```

This example shows how to disable the iCAM feature:

```
switch# configure terminal
switch(config)# no feature icam
```

Related Commands

Command	Description
icam monitor entries	Enables monitoring on the TCAM entries.
icam monitor interval	Configures the iCAM monitor interval and the number of intervals in an iCAM monitor history.
icam monitor resource	Enables iCAM monitoring on TCAM resources.
show icam entries acl	Displays traffic analytics of the ACL TCAM, which includes RACL, VACL, QoS, PBR, WCCP, CoPP, and so on.
show icam entries multicast	Displays traffic analytics of multicast entries.

Command	Description
show icam prediction entries acl	Displays machine-learning predictive analytics of TCAM entries.
show icam prediction entries multicast	Displays machine-learning predictive analytics of multicast entries.
show icam prediction resource	Displays machine-learning predictive analytics of TCAM resource utilization.
show icam resource	Displays TCAM resource utilization.

feature lldp

To enable the Link Layer Discovery Protocol (LLDP) feature globally, use the **feature lldp** command. To disable the LLDP feature, use the **no** form of this command.

feature lldp

no feature lldp

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode (config)

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
5.0(1)	This command was introduced.

Usage Guidelines

In order for LLDP to discover servers connected to your device, the servers must be running openLLDP software.

LLDP must be enabled on the device before you can enable or disable it on any interfaces.

Note LLDP is supported only on physical interfaces. LLDP timers and type, length, and value (TLV) descriptions cannot be configured using Cisco DCNM.

LLDP can discover up to one device per port. LLDP can discover up to one server per port. LLDP can discover only Linux servers that are connected to your device. LLDP can discover Linux servers, if they are not using a converged network adapter (CNA); however, LLDP cannot discover other types of servers.

Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the **switchto vdc** command.

This command does not require a license.

Examples

This example shows how to enable the LLDP feature globally:

```
switch(config)# feature lldp
switch(config)
```

This example shows how to disable the LLDP feature:

```
switch(config)# no feature lldp
switch(config)#2010 Jan 11 01:50:33 switch %FEATURE-MGR-2-FM_AUTOCKPT_IN_PROGRESS:
AutoCheckpoint system-fm-lldp's creation in progress...
2010 Jan 21 01:50:34 switch %FEATURE-MGR-2-FM_AUTOCKPT_SUCCEEDED: AutoCheckpoint
  created successfully
switch(config)#
```

Related Commands

Command	Description
show running-config lldp	Displays the global LLDP configuration.

feature netflow

To globally enable the NetFlow feature, use the **feature netflow** command. To disable NetFlow, use the **no** form of this command.

feature netflow

no feature netflow

Syntax Description

This command does not have any arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable NetFlow on a Cisco NX-OS device:

```
switch(config)# configure terminal
switch(config)# feature netflow
switch(config)#
```

This example shows how to disable NetFlow on a Cisco NX-OS device:

```
switch(config)# no feature netflow
switch(config)#
```

Related Commands

Command	Description
flow record	Creates a flow record and enters flow record configuration mode.
show flow record	Displays information about NetFlow flow records.

feature ntp

To enable the Network Time Protocol (NTP) on a virtual device context (VDC), use the **feature ntp** command. To disable NTP on a VDC, use the **no** form of this command.

feature ntp

no feature ntp

Syntax Description

This command does not have any arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the **switchto vdc** command.

This command does not require a license.

Examples

This example shows how to enable NTP on a VDC:

```
switch# configure terminal
switch(config)# feature ntp
```

This example shows how to disable NTP on a VDC:

```
switch# configure terminal
switch(config)# no feature ntp
```

Related Commands

Command	Description
ntp master	Configures the device to act as an authoritative NTP server.
ntp enable	Enables the NTP feature on a VDC.

feature ptp

To enable the Precision Time Protocol (PTP) feature on the current virtual device context (VDC), use the **feature ptp** command. To disable the PTP feature, use the **no** form of this command.

feature ptp

no feature ptp

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable the PTP feature on the current VDC:

```
switch# configure terminal
switch(config)# feature ptp
switch(config)#
```

This example shows how to disable the PTP feature on the current VDC:

```
switch(config)# no feature ptp
2011 Jul  5 06:11:07 switch %FEATURE-MGR-2-FM_AUTOCKPT_IN_PROGRESS: AutoCheckpoi
nt system-fm-ptp's creation in progress...
2011 Jul  5 06:11:07 switch %FEATURE-MGR-2-FM_AUTOCKPT_SUCCEEDED: AutoCheckpoint
  created successfully
switch(config)#
```

Related Commands

Command	Description
ptp source	Configures the source IP address for all PTP packets.
ptp domain	Configures the domain number to use for this clock.
ptp priority1	Configures the priority1 value to use when advertising this clock.

Command	Description
ptp priority2	Configures the priority2 value to use when advertising this clock.
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.

feature scheduler

To enable the scheduling of maintenance jobs, use the **feature scheduler** command. To disable the scheduler, use the **no** form of this command.

feature scheduler

no feature scheduler

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modified
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the scheduler feature before you can configure a maintenance job.

Maintenance jobs can be scheduled for one-time-only or at periodic intervals. Maintenance jobs include quality of service policy changes, data and configuration backup, and so on.

This command does not require a license.

Examples

This example shows how to enable the scheduler:

```
switch# config t
switch(config)# feature scheduler
switch(config)#
```

This example shows how to disable the scheduler:

```
switch# config t
switch(config)# no feature scheduler
switch(config)#
```

Related Commands

Command	Description
scheduler	Creates and schedules maintenance jobs.
show scheduler	Displays scheduler information.

filesys delete

To delete a specific file in the /var/tmp directory, use the filesys delete command.

filesys delete /var/tmp/*file-name*

Syntax Description

file-name	The complete filename.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

network-operator

vdc-operator

Command History

Release	Modified
4.2(4)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to delete a specific file from the /var/tmp directory:

```
switch# filesys delete /var/tmp/abc.log
Please Wait.File is being deleted.
Successfully deleted the file.
switch#
```

filter (ERSPAN)

To configure the filters for an Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **filter** command. To remove the filters, use the **no** form of this command.

filter [**access-group** *acl-filter*] [**vlan** *vlan-range*] [**bpdu** [**true** | **false**]] [**cos** *cos-value*] [**dest-mac** *dest-mac*] [**eth-type** *eth-value*] [**flow-hash** *flow-value*] [**pc-lane** *port-number*] [**src_mac** *mac-address*] [**trace-route** [**true** | **false**]]

no filter [**access-group** *acl-filter*] [**vlan** *vlan-range*] [**bpdu** [**true** | **false**]] [**cos** *cos-value*] [**dest-mac** *dest-mac*] [**eth-type** *eth-value*] [**flow-hash** *flow-value*] [**pc-lane** *port-number*] [**src_mac** *mac-address*] [**trace-route** [**true** | **false**]]

Syntax Description

access-group *acl-filter*	(Optional) Specifies a filter based on an access control group.
vlan *vlan-range*	(Optional) Specifies a filter based on a VLAN range.
bpdu	(Optional) Specifies a filter based on the bridge protocol data unit (BPDU) class of packets.
true	(Optional) Specifies that a filter based on the bridge protocol data unit (BPDU) class of packets is used.
false	(Optional) Specifies a filter based on non-BPDU class of packets.
cos *cos-value*	(Optional) Specifies a filter based on the class of service (CoS) in the dotlq header.
dest-mac *dest-mac*	(Optional) Specifies a filter based on a destination MAC address.
eth-type *eth-value*	(Optional) Specifies a filter based on the Ethernet type.
flow-hash *flow-value*	(Optional) Specifies a filter based on the result bundle hash (RBH) value.
pc-lane *port-number*	(Optional) Specifies a filter based on a member of the port channel.
src_mac *mac-address*	(Optional) Specifies a filter based on a source MAC address.
trace-route	(Optional) Specifies a filter based on trace-route packets.
true	(Optional) Specifies a that a filter based on trace-route packets is used.
false	(Optional) Specifies a filter based on non trace-route packets.

Defaults

None

Command Modes

config-erspan-src mode

SupportedUserRoles

network-admin
VDC-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

You can configure filters for ingress or egress ERSPAN traffic based on a set of rules. A simple filter has only one rule, and multiple fields or conditions can be added to this rule. The packets are spanned only if all conditions are met.

Port channel member lane is not supported on F1 Series modules.

F2 and F2e Series modules do not support egress SPAN filtering for destination MAC addresses and source MAC addresses.

This command does not require a license.

Examples

This example shows how to configure filters for an ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 3 type erspan-source
switch(config-erspan-src)# filter vlan 3-5
switch(config-erspan-src)# filter trace-route true
```

Related Commands

Command	Description
filter (SPAN)	Configures the filters for a SPAN session.

filter (SPAN)

To configure the filters for an Ethernet Switched Port Analyzer (SPAN) session, use the **filter** command. To remove the filters, use the **no** form of this command.

filter [**vlan** *vlan-range*] [**bpdu** [**true** | **false**]] [**cos** *cos-value*] [**dest-mac** *dest-mac*] [**eth-type** *eth-value*] [**flow-hash** *flow-value*] [**pc-lane** *port-number*] [**src_mac** *mac-address*] [**trace-route** [**true** | **false**]]

no filter [**vlan** *vlan-range]* [**bpdu** [**true** | **false**]] [**cos** *cos-value*] [**dest-mac** *dest-mac*] [**eth-type** *eth-value*] [**flow-hash** *flow-value*] [**pc-lane** *port-number*] [**src_mac** *mac-address*] [**trace-route** [**true** | **false**]]

Syntax Description

vlan *vlan-range*	(Optional) Specifies a filter based on a VLAN range.
bpdu	(Optional) Specifies a filter based on the bridge protocol data unit (BPDU) class of packets.
true	(Optional) Specifies that a filter based on the bridge protocol data unit (BPDU) class of packets is used.
false	(Optional) Specifies a filter based on non-BPDU class of packets.
cos *cos-value*	(Optional) Specifies a filter based on the class of service (CoS) in the dotlq header.
dest-mac *dest-mac*	(Optional) Specifies a filter based on a destination MAC address.
eth-type *eth-value*	(Optional) Specifies a filter based on the Ethernet type.
flow-hash *flow-value*	(Optional) Specifies a filter based on the result bundle hash (RBH) value.
pc-lane *port-number*	(Optional) Specifies a filter based on a member of the port channel.
src_mac *mac-address*	(Optional) Specifies a filter based on a source MAC address.
trace-route	(Optional) Specifies a filter based on trace-route packets.
true	(Optional) Specifies a that a filter based on trace-route packets is used.
false	(Optional) Specifies a filter based on non trace-route packets.

Defaults

None

Command Modes

Config-monitor configuration mode (config-monitor)

SupportedUserRoles

network-admin
VDC-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

You can configure filters for ingress or egress SPAN traffic based on a set of rules. A simple filter has only one rule, and multiple fields or conditions can be added to this rule. The packets are spanned only if all conditions are met.

Port channel member lane is not supported on F1 Series modules.

F2 and F2e Series modules do not support egress SPAN filtering for destination MAC addresses and source MAC addresses.

This command does not require a license.

Examples

This example shows how to configure filters for an SPAN session:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# filter vlan 3-5
switch(config-monitor)# filter trace-route true
```

Related Commands

Command	Description
filter (ERSPAN)	Configures the filters for an ERSPAN session.
show monitor session	Displays information about a SPAN or ERSPAN session.

filter access-group

To apply an access group to an Encapsulated Remote Switched Port Analyzer (ERSPAN) source session, use the **filter access-group** command. To remove an access group, use the **no** form of this command.

filter access-group *acl_filter*

no filter access-group *acl_filter*

Syntax Description

acl_filter	Access control list (ACL) name. An ACL associates the access list with the SPAN session.

Defaults

None

Command Modes

config-monitor-erspan-src

SupportedUserRoles

network-admin
VDC-admin

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

Only the permit to deny actions are allowed for Encapsulated Remote Switched Port Analyzer (ERSPAN) access control list (ACL) filters.

For information about ACL-related commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

This command does not require a license.

Examples

This example shows how to apply an access group to an ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 3 type erspan-source
switch(config-monitor-erspan-src)# filter vlan 3-5, 7
switch(config-monitor-erspan-src)# filter access-group ACL1
```

This example shows how to disassociate an access group to an ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 3 type erspan-source
switch(config-monitor-erspan-src)# filter vlan 3-5, 7
switch(config-monitor-erspan-src)# no filter access-group ACL1
```

Related Commands

Command	Description
filter vlan	Applies a VLAN filter to a session.

filter frame-type arp

To configure the Address Resolution Protocol (ARP) frame type filter for the Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **filter frame-type arp** command. To remove the filter from the session, enter the **no** form of this command.

filter frame-type arp [**arp-rarp** [**arp** | **rarp**] [**req-resp** [**req** | **rsp**]] [**sender-ip** *ip-address*] [**target-ip** *ip-address*]]

no filter frame-type arp [**arp-rarp** [**arp** | **rarp**] [**req-resp** [**req** | **rsp**]] [**sender-ip** *ip-address*] [**target-ip** *ip-address*]]

Syntax Description

arp-rarp	(Optional) Specifies an ARP or Reverse Address Resolution Protocol (RARP) frame type filter.
arp	(Optional) Specifies an ARP frame type filter.
rarp	(Optional) Specifies an RARP frame type filter.
req-resp	(Optional) Specifies a filter based on a request or response.
req	(Optional) Specifies a filter based on a request.
resp	(Optional) Specifies a filter based on a response.
sender-ip *ip-address*	(Optional) Specifies a filter based on a sender IP address.
target-ip *ip-address*	(Optional) Specifies a filter based on a target IP address.

Defaults

None

Command Modes

config-erspan-src mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the ARP frame type filter for the ERSPAN session:

```
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# filter frame-type arp arp-rarp arp
```

Related Commands

Command	Description
filter (ERSPAN)	Configures the filters for an ERSPAN session.
filter frame-type eth	Configures the Ethernet frame type filter for the SPAN or ERSPAN session.
filter frame-type fcoe	Configures the FCoE frame type filter for the SPAN or ERSPAN session.
filter frame-type ipv4	Configures the IPv4 frame type filter for the SPAN or ERSPAN session.
filter frame-type ipv6	Configures the IPv6 frame type filter for the SPAN or ERSPAN session.
monitor session	Places you in the monitor configuration mode for configuring a SPAN or ERSPAN session.

filter frame-type eth

To configure the Ethernet frame type filter for the Ethernet Switched Port Analyzer (SPAN) or Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **filter frame-type eth** command. To remove the Ethernet frame type filter, use the **no** form of this command.

filter frame-type eth

no filter frame-type eth

Syntax Description

This command has no arguments or keywords.

Command Modes

config-monitor mode (for a SPAN session)

config-erspan-src mode (for an ERSPAN session)

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the Ethernet frame type filter for a SPAN session:

```
switch(config)# monitor session 1
switch(config-monitor)# filter frame-type eth
```

This example shows how to configure the Ethernet frame type filter for an ERSPAN session:

```
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# filter frame-type eth
```

Related Commands

Command	Description
filter (ERSPAN)	Configures the filters for an ERSPAN session.
filter (SPAN)	Configures the filters for a SPAN session.
filter frame-type arp	Configures the ARP frame type filter for the ERSPAN session.
filter frame-type fcoe	Configures the FCoE frame type filter for the SPAN or ERSPAN session.
filter frame-type ipv4	Configures the IPv4 frame type filter for the SPAN or ERSPAN session.

Command	Description
filter frame-type ipv6	Configures the IPv6 frame type filter for the SPAN or ERSPAN session.
monitor session	Places you in the monitor configuration mode for configuring a SPAN or ERSPAN session.

filter frame-type fcoe

To configure the Fibre Channel over Ethernet (FCoE) frame type filter for the Ethernet Switched Port Analyzer (SPAN) or Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **filter frame-type fcoe** command. To remove the FCoE frame type filter, use the **no** form of this command.

filter frame-type fcoe [[**fc-sid** *FC-source-ID*] [**fc-did** *FC-dest-ID*] [**fcoe-type** *fcoe-value*] [**r-ctl** *r-ctl-value*] [**sof** *sof-value*] [**cmd-code** *cmd-value*]]

no filter frame-type fcoe [[**fc-sid** *FC-source-ID*] [**fc-did** *FC-dest-ID*] [**fcoe-type** *fcoe-value*] [**r-ctl** *r-ctl-value*] [**sof** *sof-value*] [**cmd-code** *cmd-value*]]

Syntax Description

fc-sid *FC-source-ID*	(Optional) Specifies a filter based on an FC source ID.
fc-did *FC-dest-ID*	(Optional) Specifies a filter based on an FC destination ID.
fcoe-type *fcoe-value*	(Optional) Specifies a filter based on an FCoE type.
r-ctl *r-ctl-value*	(Optional) Specifies a filter based on the routing control flags (R CTL) value.
sof *sof-value*	(Optional) Specifies a filter based on the start of frame (SOF) packets.
cmd-code *cmd-value*	(Optional) Specifies a filter based on a command code.

Defaults

None

Command Modes

config-monitor mode (for a SPAN session)

config-erspan-src mode (for an ERSPAN session)

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

F1 Series modules do not support FCoE source IDs and FCoE destination IDs.

This command does not require a license.

Examples

This example shows how to configure the FCoE frame type filter for a SPAN session:

```
switch(config)# monitor session 1
switch(config-monitor)# filter frame-type fcoe
```

This example shows how to configure the FCoE frame type filter for an ERSPAN session:

```
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# filter frame-type fcoe fc-did 2
```

Related Commands

Command	Description
filter (ERSPAN)	Configures the filters for an ERSPAN session.
filter (SPAN)	Configures the filters for a SPAN session.
filter frame-type arp	Configures the ARP frame type filter for the ERSPAN session.
filter frame-type eth	Configures the FCoE frame type filter for the SPAN or ERSPAN session.
filter frame-type ipv4	Configures the IPv4 frame type filter for the SPAN or ERSPAN session.
filter frame-type ipv6	Configures the IPv6 frame type filter for the SPAN or ERSPAN session.
monitor session	Places you in the monitor configuration mode for configuring a SPAN or ERSPAN session.

filter frame-type ipv4

To configure the IPv4 frame type filter for the Ethernet Switched Port Analyzer (SPAN) or Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **filter frame-type ipv4** command. To remove the Ethernet frame type filter, use the **no** form of this command.

filter frame-type ipv4 [[**src-ip** *src-ip*] [**dest-ip** *dest-ip*] [**tos** *tos-value*] [**l4-protocol** *l4-value*]]

no filter frame-type ipv4 [[**src-ip** *src-ip*] [**dest-ip** *dest-ip*] [**tos** *tos-value*] [**l4-protocol** *l4-value*]]

Syntax Description

src-ip *src-ip*	(Optional) Specifies a filter based on an IPv4 source IP address.
dest-ip *dest-ip*	(Optional) Specifies a filter based on an IPv4 destination IP address.
tos *tos-value*	(Optional) Specifies a filter based on the type of service (ToS) in the IP header.
l4-protocol *l4-value*	(Optional) Specifies a filter based on a Layer 4 protocol number set in the protocol field of the IP header.

Defaults

None

Command Modes

config-monitor mode (for a SPAN session)

config-erspan-src mode (for an ERSPAN session)

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the IPv4 frame type filter for a SPAN session:

```
switch(config)# monitor session 1
switch(config-monitor)# filter frame-type ipv4 l4-protocol 3
```

This example shows how to configure the IPv4 frame type filter for an ERSPAN session:

```
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# filter frame-type ipv4 l4-protocol 3
```

Related Commands

Command	Description
monitor session	Places you in the monitor configuration mode for configuring a SPAN or ERSPAN session.
filter (ERSPAN)	Configures the filters for an ERSPAN session.
filter (SPAN)	Configures the filters for a SPAN session.
filter frame-type arp	Configures the ARP frame type filter for the ERSPAN session.
filter frame-type eth	Configures the FCoE frame type filter for the SPAN or ERSPAN session.
filter frame-type fcoe	Configures the FCoE frame type filter for the SPAN or ERSPAN session.
filter frame-type ipv6	Configures the IPv6 frame type filter for the SPAN or ERSPAN session

filter frame-type ipv6

To configure the IPv6 frame type filter for the Ethernet Switched Port Analyzer (SPAN) or Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **filter frame-type ipv6** command. To remove the IPv6 frame type filter, use the **no** form of this command.

filter frame-type ipv6 [**src-ip** *src-ip*] [**dest-ip** *dest-ip*] [**tos** *tos-value*] [**l4-protocol** *l4-value*]

no filter frame-type ipv6 [**src-ip** *src-ip*] [**dest-ip** *dest-ip*] [**tos** *tos-value*] [**l4-protocol** *l4-value*]

Syntax Description

src-ip *src-ip*	(Optional) Specifies a filter based on an IPv6 source IP address.
dest-ip *dest-ip*	(Optional) Specifies a filter based on an IPv6 destination IP address.
tos *tos-value*	(Optional) Specifies a filter based on the type of service (ToS) in the IP header.
l4-protocol *l4-value*	(Optional) Specifies a filter based on a Layer 4 protocol number set in the protocol field of the IP header.

Defaults

None

Command Modes

config-monitor mode (for a SPAN session)

config-erspan-src mode (for an ERSPAN session)

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

F1 Series modules have limited support for rule-based SPAN. They do not support IPv6 source IP and IPv6 destination IP filters. They support only IPv4 and IPv6 ToS filters with values from 0 to 3.

F2 and F2e Series modules have limited support for rule-based SPAN. They do not support wildcards in the IPv6 source IP filter and IPv6 destination IP filter.

This command does not require a license.

Examples

This example shows how to configure the IPv6 frame type filter for a SPAN session:

```
switch(config)# monitor session 1
switch(config-monitor)# filter frame-type ipv6 src-ip 10.0.0.1
```

This example shows how to configure the IPv6 frame type filter for an ERSPAN session:

```
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# filter frame-type ipv6 src-ip 10.0.0.1
```

Related Commands

Command	Description
monitor session	Places you in the monitor configuration mode for configuring a SPAN or ERSPAN session.
filter (ERSPAN)	Configures the filters for an ERSPAN session.
filter (SPAN)	Configures the filters for a SPAN session.
filter frame-type arp	Configures the ARP frame type filter for the ERSPAN session.
filter frame-type eth	Configures the FCoE frame type filter for the SPAN or ERSPAN session.
filter frame-type fcoe	Configures the FCoE frame type filter for the SPAN or ERSPAN session.
filter frame-type ipv4	Configures the IPv4 frame type filter for the SPAN or ERSPAN session

filter vlan

To apply a VLAN access map to one or more VLANs, use the **filter vlan** command. To remove a VLAN access map, use the **no** form of this command.

filter vlan *vlan_mrange* [**include-untagged**]

no filter vlan *vlan_mrange* [**include-untagged**]

Syntax Description

vlan_mrange	Name of the VLAN access map that you want to create or configure. The range is from 1 to 3967 and from 4048 to 4093.
include-untagged	(Optional) Specifies untagged frames on a port with Layer 3 subinterfaces.

Defaults

None

Command Modes

Config-monitor configuration (config-monitor)

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to apply a VLAN access map to one or more VLANs:

```
switch(config)# monitor session 1
switch(config-monitor)# filter vlan 5-10 include-untagged
switch(config-monitor)#
```

This example shows how to remove the VLAN access map:

```
switch(config-monitor)# no filter vlan 5-10 include-untagged
switch(config-monitor)#
```

Related Commands

Command	Description
filter vlan include-untagged	Applies a VLAN access map to one or more VLANs and includes untagged frames on a port with Layer 3 subinterfaces.

filter vlan include-untagged

To apply a VLAN access map to one or more VLANs and include untagged frames on a port with Layer 3 subinterfaces, use the **filter vlan include-untagged** command. To remove a VLAN access map to one or more VLANs with untagged frames on a port with Layer 3 subinterfaces, use the **no** form of this command.

filter vlan include-untagged

no filter vlan include-untagged

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Config-monitor configuration (config-monitor)

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to apply a VLAN access map to one or more VLANs and include untagged frames on a port with Layer 3 subinterfaces:

```
switch(config)# monitor session 1
switch(config-monitor)# filter vlan 1-20 include-untagged
switch(config-monitor)#
```

This example shows how to remove a VLAN access map to one or more VLANs with untagged frames on a port with Layer 3 subinterfaces:

```
switch(config-monitor)# no filter vlan 1-20 include-untagged
switch(config-monitor)#
```

Related Commands

Command	Description
filter vlan	Applies a VLAN access map to one or more VLANs.

flow exporter

To create a Flexible NetFlow flow exporter or to modify an existing Flexible NetFlow flow exporter, use the **flow exporter** command. To remove a Flexible NetFlow flow exporter, use the **no** form of this command.

flow exporter *exporter-name*

no flow exporter *exporter-name*

Syntax Description

exporter-name	Name of the flow exporter that is created or modified.

Defaults

Flow exporters are not present in the configuration until you create them.

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors.

Once you enter the flow export configuration mode, the prompt changes to the following:

```
switch(config-flow-exporter)#
```

Within the flow export configuration mode, the following keywords and arguments are available to configure the flow exporters:

- **description** *description*—Provides a description for this flow exporter; you can use a maximum of 63 characters.
- **destination** {*ip-addr* | *ipv6-addr*} [**use-vrf** *label-name*]—Specifies the destination address for the collector. Enter the optional **use-vrf** *label-name* to specify a VRF. Use the following format when entering the destination address:
  - *ip-addr—A.B.C.D*
  - *ipv6-addr—A:B::C:D*

- **dscp** *value*—Specifies the differentiated services code point (DSCP) value. The range is from 0 to 63.
- **exit**—Exits from the current configuration mode.
- **no**—Negates a command or sets its defaults.
- **source** *interface*—Specifies the source interface for this destination. The valid values for *interface* are as follows:
  - **ethernet** *mod/port*—Specifies the Ethernet IEEE 802.3z interface module and port number. The ranges for the module and port number depend on the chassis used.
  - **loopback** *virtual-num*—Specifies the virtual interface number. The range is from 0 to 1023.
  - **mgmt** *num*—Specifies the management interface number. The range is from 0 to 10.
- **transport udp** *dest-port*—Specifies the transport UDP destination port. The range is from 0 to 65535.
- **version** {**5** | **9**}—Specifies the export version 5 or the version 9 and enters the export version configuration mode. See the **version** command for additional information.

This command does not require a license.

Examples

This example shows how to create a flow exporter named FLOW-EXPORTER-1, enter flow exporter configuration mode, and configure the flow exporter:

```
switch(config)# flow exporter FLOW-EXPORTER-1
switch(config-flow-exporter)# description located in Pahrump, NV
switch(config-flow-exporter)# destination A.B.C.D
switch(config-flow-monitor)# dscp 32
switch(config-flow-monitor)# source ethernet 3/2
switch(config-flow-monitor)# transport udp 59
switch(config-flow-monitor)# version 5
```

Related Commands

Command	Description
clear flow exporter	Clears the flow monitor.
show flow exporter	Displays flow monitor status and statistics.

flow monitor

To create a Flexible NetFlow flow monitor or to modify an existing Flexible NetFlow flow monitor and enter flow monitor configuration mode, use the **flow monitor** command. To remove a Flexible NetFlow flow monitor, use the **no** form of this command.

flow monitor *monitor-name*

no flow monitor *monitor-name*

Syntax Description

monitor-name	Name of the flow monitor that is created or modified.

Defaults

Flow monitors are not present in the configuration until you create them.

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Flow monitors are the Flexible NetFlow component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a record that you add to the flow monitor after you create the flow monitor and a cache that is automatically created at the time that the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in record that is configured for the flow monitor and stored in the flow monitor cache.

Once you enter the flow monitor configuration mode, the prompt changes to the following:

```
switch(config-flow-monitor)#
```

Within the flow monitor configuration mode, the following keywords and arguments are available to configure the flow monitor:

- **description** *description*—Provides a description for this flow monitor; you use a maximum of 63 characters.
- **exit**—Exits from the current configuration mode.
- **exporter** *name*—Specifies the name of an exporter to export records.
- **no**—Negates a command or sets its defaults.
- **record** {*record-name* | **netflow ipv4** *collection-type* | **netflow-original**}—Specifies a flow record to use as follows:

  - *record-name*—Name of a record.
  - **netflow ipv4** *collection-type*—Specifies the traditional IPv4 NetFlow collection schemes as follows:

    original-input—Specifies the traditional IPv4 input NetFlow.

    original-output—Specifies the traditional IPv4 output NetFlow.

    protocol-port—Specifies the protocol and ports aggregation scheme.
  - **netflow-original**—Specifies the traditional IPv4 input NetFlow with origin autonomous systems.

The **netflow-original** and **original-input** keywords are the same and are equivalent to the following commands:

- **match ipv4 source address**
- **match ipv4 destination address**
- **match ip tos**
- **match ip protocol**
- **match transport source-port**
- **match transport destination-port**
- **match interface input**
- **collect counter bytes**
- **collect counter packet**
- **collect timestamp sys-uptime first**
- **collect timestamp sys-uptime last**
- **collect interface output**
- **collect transport tcp flags**
- **collect routing next-hop address ipv4**
- **collect routing source as**
- **collect routing destination as**

The **original-output** keywords are the same as the **original-input** keywords except for the following:

- **match interface output** (instead of **match interface** input)
- **collect interface input** (instead of **collect interface** output)

This command does not require a license.

Examples

This example shows how to create and configure a flow monitor named FLOW-MONITOR-1:

```
switch(config)# flow monitor FLOW-MONITOR-1
switch(config-flow-monitor)# description monitor location las vegas, NV
switch(config-flow-monitor)# exporter exporter-name1
switch(config-flow-monitor)# record test-record
switch(config-flow-monitor)# netflow ipv4 original-input
```

Related Commands

Command	Description
clear flow monitor	Clears the flow monitor.
show flow sw-monitor	Displays flow monitor status and statistics.

flow record

To create a Flexible NetFlow flow record or to modify an existing Flexible NetFlow flow record and enter flow record configuration mode, use the **flow record** command. To remove a Flexible NetFlow flow record, use the **no** form of this command.

flow record *record-name*

no flow record *record-name*

Syntax Description

record-name	Name of the flow record that is created or modified.

Defaults

Flow records are not present in the configuration until you create them.

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Flexible NetFlow uses key and nonkey fields just as original NetFlow does to create and populate flows in a cache. In Flexible NetFlow, a combination of key and nonkey fields is called a record. Original NetFlow and Flexible NetFlow both use the values in key fields in IP datagrams, such as the IP source or destination address and the source or destination transport protocol port, as the criteria for determining when a new flow must be created in the cache while network traffic is being monitored. A flow is defined as a stream of packets between a given source and a given destination. New flows are created whenever NetFlow analyzes a packet that has a unique value in one of the key fields.

Once you enter the flow record configuration mode, the prompt changes to the following:

```
switch(config-flow-record)#
```

Within the flow record configuration mode, the following keywords and arguments are available to configure the flow record:

- **collect**—Specifies a nonkey field. See the **collect** command for additional information.
- **description** *description*—Provides a description for this flow record; you use a maximum of 63 characters.
- **exit**—Exits from the current configuration mode.
- **match**—Specifies a key field. See the **match** command for additional information.
- **no**—Negates a command or sets its defaults.

Cisco NX-OS enables the following match fields by default when you create a flow record:

- **match interface input**
- **match interface output**
- **match flow direction**

This command does not require a license.

Examples

This example shows how to create a flow record and enter flow record configuration mode:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)#
```

Related Commands

Command	Description
clear flow monitor	Clears the flow monitor.
flow monitor	Creates a flow monitor.
show flow sw-monitor	Displays flow monitor status and statistics.

flow timeout

To create a Flexible NetFlow flow timeout or to modify an existing Flexible NetFlow flow timeout, use the **flow timeout** command. To remove a Flexible NetFlow flow timeout, use the **no** form of this command.

flow timeout {**active** *seconds* | **aggressive threshold** *percentage* | **fast** *seconds* **threshold** *packets* | **inactive** *seconds* | **session** | *seconds*}

no flow timeout {**active** *seconds* | **aggressive threshold** *percentage* | **fast** *seconds* **threshold** *packets* | **inactive** *seconds* | **session** | *seconds*}

Syntax Description

active *seconds*	Specifies the active or long timeout in seconds. The range is from 60 to 4092. The default is 1800.
aggressive threshold *percentage*	Specifies the percentage of the NetFlow table content. The range is from 50 to 99.
fast *seconds*	Specifies the fast aging timeout in seconds. The range is from 32 to 512. The default is not supported.
threshold *packets*	Specifies the packet threshold for a flow timeout in packets. The range is from 1 to 4000. The default is not supported.
inactive *seconds*	Specifies the inactive or normal timeout in seconds. The range is from 15 to 4092. The default is 15.
session	Enables TCP session aging.
seconds	Flush timeout value in seconds for F2 Series modules. The range is from 5 to 60 seconds.

Defaults

The default settings are as follows:

- Active timeout—1800 seconds
- Aggressive aging timeout—Disabled
- Fast timeout—Disabled
- Inactive timeout—15 seconds
- Session aging timeout—Disabled
- Flush cache timeout – 15 seconds (enabled only on F2)

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
6.1(2)	Added the *seconds* argument for the syntax description and also the note.
4.0(1)	This command was introduced.

Usage Guidelines

The active timeout is the amount of time to wait before sending flow information about an active session. The flow is not removed from the cache after this timeout; however, the packet count, byte count, and timestamps are reset.

The aggressive timeout only affects hardware caches and is used when flows are being received faster than expected. If flows are being received faster than the threshold, they are aged out of the cache.

The fast timeout specifies when an inactive flow should be aged out.

The inactive timeout is used for Transmission Control Protocol (TCP) sessions that receive no more data from the sender (FIN) followed by an acknowledgment field is significant (ACK) or a reset (RST) packet being received. The inactive timeout indicates the session is over and the flow can be aged out.

Note Only the flow timeout seconds command is supported for F2 Series modules. All of the other NetFlow timeout commands are supported for M Series modules only.

This command does not require a license.

Examples

This example shows how to specify the active or long timeout value in seconds for the F1 and M1 Series modules:

```
switch(config)# flow timeout active 45
switch(config)#
```

This example shows how to specify the percentage of the NetFlow table content:

```
switch(config)# flow timeout aggressive threshold 45
switch(config)#
```

This example shows how to specify the fast aging timeout in seconds:

```
switch(config)# flow timeout fast 30 threshold 20
switch(config)#
```

This example shows how to specify the inactive or normal timeout in seconds:

```
switch(config)# flow timeout inactive 45
switch(config)#
```

This example shows how to specify the flush cache timeout in seconds for F2 Series module:

```
switch(config)# flow timeout 45
switch(config)#
```

Related Commands

Command	Description
flow record	Creates a flow exporter.
clear flow monitor	Clears the flow monitor.

Command	Description
flow monitor	Creates a flow monitor.
show flow sw-monitor	Displays flow monitor status and statistics.