F Commands

factory reset

To remove all the identifiable customer information on Cisco NX-OS devices in conditions of productremoval due to Return Merchandise Authorization (RMA), or upgrade or replacement, or system end-of- life you can use the factory-reset command to securely erase all information.

✎

Note   There is no form of this command, once deleted you cannot regain the deleted information.

factory-reset   fex-id | <all>

Command History

fex id	Securely erase fex as per identifier number. The range is 100-199.
all	Securely erase all the fex.
factory-reset	Securely erase data on the switch.

Command History

Release	Modification
7.3(11)N1(1)	This command was introduced.

Usage Guidelines   Youuse this command to erase customer information.

This command does not require a license.

✎

Note   If fex is attached to the switch, to erase the customer data on the connected fex perform below operation before performing a factory reset on the switch:

- To erase customer data on a single fex - factory reset fex <fex-id>

- To erase customer data on all fex - factory reset all

Examples   This example shows the factory-reset of a switch:

```
switch(config)# factory-reset
!!!! WARNING !!!!

The factory reset operation will erase ALL persistent storage on the specified module.
This includes configuration, all log data, and the full contents of flash and SSDs.
Special steps are taken in an effort to render data non-recoverable. Please, proceed with
caution and understanding that this operation cannot be undone and will leave the system
in a fresh-from-factory state.

!!!! WARNING !!!!
Continue? (y/n) [n] y
```

```
A device reload is required for the reset operation to proceed.
Please, wait...
WARNING: This command will reboot the system
2006 Apr 24 06:23:17 switch %$ VDC-1 %$ %PFMA-2-PFM_SYSTEM_RESET: Manual system restart
from Command Line Interface
[ 972.939186] Shutdown Ports..
[ 972.947864] writing reset reason 9,
Secure erase requested! Please, do not power off module!
```

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.

Command Default   Disabled

Command Modes   Global configuration mode

Command History

Release	Modification
7.0(0)N1(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 ptp

To enable the PTP feature, use the feature ptp command. To unconfigure the PTP feature, use the no form of this command.

feature ptp
no feature ptp

Syntax Description

There are no arguments or keywords for this command.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to enable PTP on the device:

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

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the device.
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 priority 1 value to use when advertising this clock.
ptp priority2	Configures the priority 1 value to use when advertising this clock.
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.

fex-group

To create a Fabric Extender (FEX) group, use the fex-group command. To delete a FEX group., use the no form of this command.

fex-group name
no fex-group name

Syntax Description

| name | Specifies the name of the FEX group. |

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
7.3(0)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to create a FEX group "fg1":

```
switch# fex-group fg1
```

This example shows how to delete a FEX group "fg1":

```
switch# no fex-group fg1
```

Related Commands

Command	Description
configure maintenance profile	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
show run mmode	Displays the currently running maintenance profile configuration on a switch.
show system mode	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
system mode maintenance on-reload reset-reason	Boots the switch into maintenance mode automatically in the event of a specified system crash.
system mode maintenance shutdown	Shuts down all protocols and interfaces except the management interface (by using the shutdown command and not the default isolate command).
system mode maintenance timeout	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

filter access-group

To apply an access group to an Encapsulated Remote Switched Port Analyzer (ERSPAN) or Switched Port Analyzer (SPAN) 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. |

Command Default   None

Command Modes   SPAN session configuration mode (config-monitor)

ERSPAN source session configuration mode (config-erspan-src)

Command History

Release	Modification
7.0(0)N1(1)	This command was introduced.

Usage Guidelines   ACL filtering allows you to filter SPAN and ERSPAN traffic so that you can reduce bandwidth congestion. An ACL is a list of permissions associated to any entity in the system; in the context of a monitoring session, an ACL is a list of rules which results in the spanning of traffic that matches the ACL criteria, saving bandwidth for more meaningful data. The filter applies to all sources in the session.

Note   If the ACL has rules with a log option configured, the log option is ignored but the rule is implemented.

Examples   This example shows how to enable an ACL filter for a SPAN session:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# filter access-group acl_span_ses_3
```

This example shows how to enable an ACL filter for a ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 4 type erspan-source
switch(config-erspan-src)# filter access-group acl_erspan_ses_3
```

Related Commands

Command	Description
monitor session	Creates a new SPAN or ERSPAN session.

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.

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

Command Modes   Global configuration mode

Command History

Release	Modification
7.0(0)N1(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 ipv4collection-type | netflow-original} —Specifies a flow record to use as follows:

    - record-name—Name of a record.
    - netflow ipv4collection-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
feature netflow	Enables the NetFlow feature.

flow monitor (interface)

To enable a Flexible NetFlow flow monitor for traffic that the router is receiving or forwarding, use the flow monitor (interface) command. To disable a Flexible NetFlow flow monitor, use the no form of this command.

ip | ipv6 flow monitor monitor-name input sampler sampler-name
no ip | ipv6 flow monitor monitor-name input sampler sampler-name

Syntax Description

ip	Configures IP Flexible NetFlow flow monitoring.
ipv6	Configures IPv6 Flexible NetFlow flow monitoring.
monitor-name	Name of a flow monitor that you previously configured.
input	Monitors traffic that the routers are receiving on the interface.
sampler	Specifies the name of a flow sampler for the flow monitor.
sampler-name	Flow sampler for this flow monitor using the name of a sampler that you previously configured.

Command Default   Disabled

Command Modes   Interface configuration (config-if)

VLAN feature configuration (config-vlan-config)

Command History

Release	Modification
7.0(0)N1(1)	This command was introduced.

Usage Guidelines   You must have already created a flow monitor by using the flow monitor command before you can apply the flow monitor to an interface with the ip flow monitor or ipv6 flow monitor command to enable traffic monitoring with Flexible NetFlow.

You must have already created a sampler by using the sampler command before you can enable a flow sampler for this flow monitor with the ip flow monitor or ipv6 flow monitor command.

When adding a sampler to a flow monitor, only packets that are selected by the named sampler are entered into the cache to form flows. Each use of a sampler results in separate statistics being stored for that usage.

You cannot add a sampler to a flow monitor after the flow monitor has been enabled on an interface. You must remove the flow monitor from the interface before you enable the same flow monitor with a sampler. See the "Examples" section for more information.

Note   The statistics for each flow needs to be scaled to give the expected true usage. For example, if you are using a 1 in 16 sampler, you must multiply the packet and byte counters by 16.

This command does not require a license.

Examples

This example shows how to enable an IPv6 flow monitor for monitoring input traffic on a VLAN:

```
switch(config)# vlan  configuration 2
switch(config-vlan-config)# ip flow monitor FLOW-MONITOR-1 input sampler vlan-sampler
```

Note VLAN configuration mode enables you to configure VLANs independently of their creation, which is required for VTP client support.

- Egress NetFlow on VLAN is not supported

This example shows how to enable a flow monitor for monitoring input traffic:

```
switch(config)# interface ethernet1/1
switch(config-if)# ip flow monitor FLOW-MONITOR-1 input sampler sampler-1
```

This example shows how to enable two different flow monitors on two different interfaces for monitoring input traffic:

```
switch(config)# interface ethernet1/1
switch(config-if)# ip flow monitor FLOW-MONITOR-1 input sampler sampler-2
switch(config)# interface ethernet1/2
switch(config-if)# ip flow monitor FLOW-MONITOR-2 input sampler sampler-3
```

This example shows how to enable a flow monitor for monitoring input traffic with a sampler to limit the input packets that are sampled:

```
switch(config)# interface ethernet1/1
switch(config-if)# ip flow monitor FLOW-MONITOR-1 input sampler SAMPLER-1
```

This example shows how to remove the flow monitor and sampler from an IPv6 interface:

```
switch(config)# interface Ethernet
1/1
switch(config-if)# no ipv6 flow monitor FLOW-MONITOR-1 input sampler SAMPLER-1
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.
flow monitor	Creates a flow monitor.
flow record	Creates a flow record.
sampler	Creates a flow sampler.

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.

Command Default

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

Command Modes

Global configuration mode

Command History

Release	Modification
7.0(0)N1(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
flow monitor	Creates a flow monitor.

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 [seconds]
no flow timeout [seconds]

Syntax Description

| seconds | Flow timeout value in seconds. The range is from 5 to 60 seconds. |

Command Default

The default settings is 15 seconds.

Command Modes

Global configuration mode

Command History

Release	Modification
7.0(0)N1(1)	This command was introduced.

Usage Guidelines

Cisco NX-OS exports data to the remote collector, using UDP frames, whenever a timeout occurs. By default, the flow timeout value is set to 15 seconds.

This command does not require a license.

Examples

This example shows how to specify the flow timeout in seconds:

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

Related Commands

Command	Description
flow record	Creates a flow exporter.
flow monitor	Creates a flow monitor.