

set macro ciscosmartports

To set the global Cisco SmartPorts template, use the **set macro ciscosmartports** command.

set macro ciscosmartports

Syntax Description This command has no keywords or arguments

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines When you enter the **set macro ciscosmartports** global macro command, the following configuration is displayed:

```
set macro ciscosmartports
-----
set udld enable
set errdisable-timeout enable udld
set errdisable-timeout enable duplex-mismatch
set errdisable-timeout enable channel-misconfig
set errdisable-timeout enable bpdu-guard
set errdisable-timeout interval 60
set cdp enable
set cdp version v2
set spantree mode rapid-pvst+
set spantree macreduction enable
set spantree portfast bpdu-guard enable
set spantree global-default loop-guard enable
set qos autoqos
```

Examples This example shows how to enable the Cisco SmartPorts global macro:

```
Console> (enable) set macro ciscosmartports
Console> (enable)
```

Related Commands [set port macro](#)

set mac utilization load-interval

To set the MAC utilization load interval, use the **set mac utilization load-interval** command.

set mac utilization load-interval

Syntax Description This command has no keywords or arguments

Defaults The default is 300 seconds.

Command Types Switch command.

Command Modes Enabled.

Examples This example shows how to set the MAC utilization load interval:

```
Console> (enable) set mac utilization load-interval  
Set the mac utilization load interval(30 or 300 seconds)
```

```
Console> (enable) set mac utilization load-interval 30  
Load interval set to 30 seconds.
```

Related Commands [show mac](#)
[clear mac utilization](#)

set mls agingtime

To specify the MLS aging time of shortcuts to an MLS entry in the Catalyst 6500 series switches, use the **set mls agingtime** command.

```
set mls agingtime ip agingtime
```

```
set mls agingtime fast {fastagingtime} {pkt_threshold}
```

```
set mls agingtime long-duration {longagingtime}
```

Syntax Description		
ip		Specifies IP MLS.
<i>agingtime</i>		MLS aging time of shortcuts to an MLS entry; valid values are from 1 to 1920 seconds.
fast		Specifies the MLS aging time of shortcuts to an MLS entry that has no more than <i>pkt_threshold</i> packets switched within <i>fastagingtime</i> seconds after it is created.
<i>fastagingtime</i>		MLS aging time of shortcuts to an MLS entry; valid values are from 0 to 128 seconds.
<i>pkt_threshold</i>		Packet threshold value; valid values are from 0 to 127 packets.
long-duration		Sets the aging time for active flows.
<i>longagingtime</i>		MLS aging time of shortcuts to an MLS entry; valid values are 0 (to disable) and 8 to 1920 seconds.

Defaults

- The default IP *agingtime* is 16 seconds.
- The default *fastagingtime* is 0, no fast aging.
- The default *pkt_threshold* is 0.
- The default *longagingtime* is 320.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use the **ip** keyword, you are specifying a shortcut for IP MLS.

If you enter **0** for the *fastagingtime* value, fast aging is disabled.

If you do not specify *fastagingtime* or *pkt_threshold*, the default value is used.

If you enter any of the **set mls** commands on a Catalyst 6500 series switch without MLS, this warning message displays:

```
MLS not supported on feature card.
```

The *fastagingtime* value can be configured in the range of 0 to 128 seconds.

The default *pkt_threshold* value is 0. If you do not configure *fastagingtime* exactly the same for these values, it adjusts to the closest value. A typical value for *fastagingtime* and *pkt_threshold* is 32 seconds and 0 packet, respectively. (It means no packet switched within 32 seconds after the entry was created.)

The *agingtime* value applies to an MLS entry that has no more than *pkt_threshold* packets switched within *fastagingtime* seconds after it is created. A typical example is the MLS entry destined to or sourced from a DNS or TFTP server. This entry may never be used again once it is created. For example, only one request goes to a server and one reply returns from the server, and then the connection is closed.

The **agingtime fast** option is used to purge entries associated with very short flows, such as DNS and TFTP.

Keep the number of MLS entries in the MLS cache below 32,000. If the number of MLS entries exceed 32,000, some flows (less than 1 percent) are sent to the router.

To keep the number of MLS cache entries below 32,000, decrease the aging time up to 8 seconds. If your switch has a lot of short flows used by only a few packets, then you can use fast aging.

If cache entries continue to exceed 32,000, decrease the normal aging time in 64-second increments from the 256-second default.

You can force an active flow to age out by entering the **set mls agingtime long-duration** command. You can specify the aging time of the active flow in the range of 64 to 1920 seconds in increments of 64.

Examples

These example shows how to set the aging time:

```
Console> (enable) set mls agingtime 512  
IP Multilayer switching aging time set to 512 seconds.  
Console> (enable)
```

This example shows how to set the fast aging time:

```
Console> (enable) set mls agingtime fast 32 0  
Multilayer switching fast aging time set to 32 seconds for entries with no more than 0  
packet switched.  
Console> (enable)
```

This example shows how to set the aging time for active flows:

```
Console> (enable) set mls agingtime long-duration 128  
Multilayer switching agingtime set to 128 seconds for long duration flows  
Console> (enable)
```

Related Commands

[clear mls statistics entry](#)
[show mls](#)

set mls bridged-flow-statistics

To enable or disable statistics for bridged flows for specified VLANs, use the **set mls bridged-flow-statistics** command.

```
set mls bridged-flow-statistics {enable | disable} {vlanlist}
```

Syntax Description	enable	enable
	enable	Enables statistics for bridged flows.
	disable	Disables statistics for bridged flows.
	<i>vlanlist</i>	Number of the VLAN or VLANs; valid values are 1 to 4094. See the “Usage Guidelines” section for more information.

Defaults By default, bridged-flow statistics is disabled on all VLANs.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines You can enter one or multiple VLANs. The following examples are valid VLAN lists: 1; 1,2,3; 1-3,7. Bridged flows are exported through NDE when bridged flow statistics is enabled.

Examples This example shows how to enable bridged-flow statistics on the specified VLANs:

```
Console> (enable) set mls bridged-flow-statistics enable 1-21
Netflow statistics is enabled for bridged packets on vlan(s) 1-21.
Console> (enable)
```

Related Commands

- [show mls nde](#)
- [show mls entry](#)
- [show mls statistics](#)

set mls cef load-balance

To include or exclude Layer 4 ports in a load-balancing hash, use the **set mls cef load-balance** command.

```
set mls cef load-balance {full | source-destination-ip}
```

Syntax Description	full	Bases the hash on Layer 4 ports and source and destination IP addresses.
	source-destination-ip	Bases the hash on source and destination IP addresses.

Defaults By default, the load-balancing hash is based on source and destination IP addresses.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines When multiple paths are available to reach a destination, the new hash is used to choose the path to be used for forwarding.

Examples This example shows how to base the hash on Layer 4 ports and source and destination IP addresses:

```
Console> (enable) set mls cef load-balance full
Console> (enable)
```

This example shows how to base the hash on source and destination IP addresses:

```
Console> (enable) set mls cef load-balance source-destination-ip
Console> (enable)
```

Related Commands [show mls](#)

set mls cef maximum-routes

To set the maximum number of routes that can be programmed in the FIB TCAM for a protocol, use the **set mls cef maximum-routes** command.

```
set mls cef maximum-routes {ip | ip-multicast} routes
```

Syntax Description

ip	Specifies IP MLS.
ip-multicast	Specifies IP multicasting MLS.
<i>routes</i>	Number of routes that can be programmed in the FIB TCAM.

Defaults

The *routes* argument is 0, which means that the system-determined bootup default is used:

- IP version 4 unicast—192,000.
- IP version 4 multicast—32,000.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is only available on the Supervisor Engine 720.

Routes that exceed the specified number of routes are not installed in the hardware. Packets that take those routes are switched by MSFC. The *routes* argument is a unit of 1,000 entries. Setting the *routes* argument to 0 returns the system to a system-determined default value.

When no protocols are set, an initial default value is assigned for each protocol. When at least one protocol is set, the default value for other unassigned protocols might change as the system tries to assign the remaining space to the unassigned protocols.

This command has the following characteristics:

- Changing the setting takes effect only after rebooting the active supervisor engine. The change does not take effect after a switchover.
- The setting on the standby supervisor engine is synchronized with the active supervisor engine. If the standby supervisor is inserted, both the bootup setting and new setting, if existing, on the active supervisor engine are synchronized with the standby supervisor engine. The standby supervisor engine uses the bootup setting to configure the FIB TCAM. The standby supervisor engine might need to be reset if its original bootup setting is different from the bootup setting of the active supervisor engine. An informational message (FIB_MAXROUTES_RESET) is printed on the active supervisor engine console if this situation occurs.
- To maximize the TCAM utilization, we recommend that you set the maximum routes for IP unicast as a multiple of 16,000 and set the maximum routes for IP multicast as a multiple of 8,000. The internal allocation scheme uses 16,000 as the allocation unit for unicast and 8,000 as the allocation unit for multicast. For example, if IP unicast is set to 1,000, 16,000 entries are reserved, but only 1,000 is allowed.

- When the maximum routes is exceeded or the allocated TCAM space for a protocol is full, a system message (FIB_ALLOC_TCAM_FULL) displays. Note that because of the internal software allocation scheme, the allocated TCAM space might be full before the maximum routes is exceeded.

**Note**

The sum of the number of maximum routes for all protocols cannot exceed 256,000.

**Note**

If the *routes* values for all protocols are set to 0, the bootup default is used. When you set the *routes* value for one protocol to a non-zero value, the default value for the other protocol changes to the remaining size.

Examples

This example shows how to set the maximum number of routes for IP unicast:

```
Console> (enable) set mls cef maximum-routes ip 220  
Configuration change will take effect after next reboot.  
Console> (enable)
```

Related Commands

[show mls cef maximum-routes](#)

set mls cef per-prefix-statistics

To set MLS CEF per-prefix statistics mode, use the **set mls cef per-prefix statistics** command.

```
set mls cef per-prefix statistics {enable | disable}
```

Syntax Description

enable	Enables per-prefix statistics for all FIB entries
disable	Disables per-prefix statistics for all FIB entries.

Defaults

MLS CEF per-prefix statistics mode is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When the **set mls cef per-prefix-statistics** command is enabled, the switch makes a best effort to allocate adjacencies with statistics for each prefix. Statistics for a prefix are computed by adding up the packet/byte counts of all the adjacencies that are associated with the prefix. Because only half of the adjacency table entries have statistics, all prefixes might not be associated with adjacencies that have statistics.

Examples

This example shows how to enable per-prefix statistics for all FIB entries:

```
Console> (enable) set mls cef per-prefix-stats enable
Per prefix stats is enabled
Console> (enable)
```

This example shows how to disable per-prefix statistics for all FIB entries:

```
Console> (enable) set mls cef per-prefix-stats disable
Per prefix stats is disabled
Console> (enable)
```

Related Commands

[show mls](#)

set mls exclude protocol

To exclude an MLS protocol port on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC, use the **set mls exclude protocol** command. To exclude protocols from statistics gathering on switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2), use the **set mls exclude protocol** command.

```
set mls exclude protocol {tcp | udp | both} {port_number | port_name}
```

Syntax Description	
tcp udp both	Specifies a TCP, UDP port, or that the port be applied to both TCP and UDP traffic.
<i>port_number</i>	Number of the protocol port; valid values are from 1 to 65535.
<i>port_name</i>	Name of the port; valid values are dns , ftp , smtp , telnet , x , www .

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines If you enter any of the **set mls** commands on a Catalyst 6500 series switch without MLS, this warning message is displayed:

```
MLS not supported on feature card.
```

You can add a maximum of four protocol ports to the exclude table.

MLS exclusion is supported in full flow mode only.

If you enter **x** for the port name, this specifies the Layer 4 port used by the X-windows application.

Examples This example shows how to exclude TCP packets on protocol port 6017:

```
Console> (enable) set mls exclude protocol tcp 6017
TCP packets with protocol port 6017 will be switched by RP.
Console> (enable)
```

This example shows how to exclude UDP packets on protocol port 6017:

```
Console> (enable) set mls exclude protocol udp 6017
TCP and UDP packets with protocol port 6017 will be switched by RP.
Console> (enable)
```

Related Commands [show mls](#)

set mls flow

To specify the minimum flow mask used for MLS, use the **set mls flow** command. This command is needed to collect statistics for the supervisor engine.

set mls flow {destination | destination-source | full | null}



Caution

Use this command carefully. This command *purges all existing shortcuts* and affects the number of active shortcuts. This command can increase the cache usage and increase the load on the router.



Caution

Be extremely careful if you enter this command on a switch that already has a large number of shortcuts (greater than 16,000).



Caution

Do not place this command in scripts that are frequently executed—changing the MLS flow mask purges all MLS cache entries.

Syntax Description

destination	Sets the minimum flow mask to destination flow.
destination-source	Sets the minimum flow mask to source flow.
full	Sets the minimum flow mask to an extended access list.
null	Clears the flow mask.

Defaults

In software release 8.5(1) and subsequent releases, **null** is the default action.

Before software release 8.5(1), if there are no access lists on any MLS-RP, the flow mask is set to **destination** flow.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command specifies the minimum MLS flow mask. Depending on the MLS-RP configuration, the actual flow mask used might be more specific than the specified minimum flow mask. For example, if you configure the minimum flow mask to **destination-source**, but an MLS-RP interface is configured with IP extended access lists, the actual flow mask used will be **full**.

If you configure a more specific flow mask (for example, **destination-source** or **full**), the number of active flow entries increases. To limit the number of active flow entries, you might need to decrease the MLS aging time.

This command is intended to be used for gathering very detailed statistics at the protocol port level—for example, when NetFlow data is exported to an RMON2 probe.

In software release 8.5(1) and subsequent releases, multiple flow masks are supported on the Supervisor Engine 720. Various RP features, such as NAT in the hardware, are also supported. Because of flow mask resolution requirements in NDE and NAT, if the NDE flow mask has been configured and you need to use NAT, the NDE flow mask must be cleared. To clear the flow mask, use the **null** keyword.

When the flow mask is set to **null** and no feature is driving a more specific flow mask, all the netflows will match the same null flow. The counters for that flow are incremented each time another flow hits it. When the flow mask is set to **null** and you enter the **show mls stat entry** command, the command output will show information about this null flow.

If NDE is enabled when the **null** option is configured, NDE will not export any flows.

If you upgrade the software from software release 8.4 to release 8.5, the NVRAM configuration is preserved. You will not encounter issues during an upgrade from previous images to 8.5(1) or subsequent releases if the switch configuration mode is set to binary. In text configuration mode, if you had entered the **destination** keyword, then you must set the flow mask again after upgrade.

Examples

These examples show how to specify that only expired flows to subnet 171.69.194.0 are exported:

```
Console> (enable) set mls flow destination
Configured flow mask is set to destination flow.
Console> (enable)

Console> (enable) set mls flow destination-source
Configured flow mask is set to destination-source flow.
Console> (enable)

Console> (enable) set mls flow full
Configured flow mask is set to full flow.
Console> (enable)
```

Related Commands

[show config mode](#)
[show mls](#)
[show mls flowmask](#)

set mls nde

To configure the NetFlow Data Export (NDE) feature in the Catalyst 6500 series switches to allow command-exporting statistics to be sent to the preconfigured collector, use the **set mls nde** command.

```
set mls nde {enable | disable}
```

```
set mls nde {collector_ip | collector_name} {udp_port_num}
```

```
set mls nde version {1 | 5 | 7 | 8}
```

```
set mls nde flow [exclude | include] [destination ip_addr_spec] [source ip_addr_spec]
[protocol protocol] [src-port src_port] [dst-port dst_port]
```

```
set mls nde {destination-ifindex | source-ifindex} {enable | disable}
```

Syntax Description

enable	Enables NDE.
disable	Disables NDE.
<i>collector_ip</i>	IP address of the collector if DNS is enabled.
<i>collector_name</i>	Name of the collector if DNS is enabled.
<i>udp_port_num</i>	Number of the UDP port to receive the exported statistics.
version	Specifies the version of the NDE; valid versions are 1 , 5 , 7 , and 8 .
1 5 7 8	Version of the NDE feature.
flow	Adds filtering to NDE.
exclude	(Optional) Allows exporting of all flows except the flows matching the given filter.
include	(Optional) Allows exporting of all flows matching the given filter.
destination	(Optional) Specifies the destination IP address.
<i>ip_addr_spec</i>	(Optional) Full IP address or a subnet address in these formats: <i>ip_addr</i> , <i>ip_addr/netmask</i> , or <i>ip_addr/maskbit</i> .
source	(Optional) Specifies the source IP address.
protocol	(Optional) Specifies the protocol type.
<i>protocol</i>	(Optional) Protocol type; valid values can be a number from 0 to 255 or ip , ipinip , icmp , igmp , tcp , or udp . 0 indicates “do not care.”
src-port <i>src_port</i>	(Optional) Specifies the number of the TCP/UDP source port (decimal). Used with dst-port to specify the port pair if the protocol is tcp or udp . 0 indicates “do not care.”
dst-port <i>dst_port</i>	(Optional) Specifies the number of the TCP/UDP destination port (decimal). Used with src-port to specify the port pair if the protocol is tcp or udp . 0 indicates “do not care.”
destination-ifindex	Specifies destination ifIndex support.
source-ifindex	Specifies source ifIndex support.
enable	Enables ifIndex support.
disable	Disables ifIndex support.

Defaults The defaults are Netflow Data Export version 7, and all expired flows are exported until the filter is specified explicitly. Destination ifIndex support and source ifIndex support are enabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines If you enter any **set mls nde** commands on a Catalyst 6500 series switch without MLS, this warning message is displayed:

```
mls not supported on feature card.
```

When you try to enable NDE and there are previously configured filtered flows on the switch, this warning message is displayed:

```
Console> (enable) set mls nde enable
Netflow export configured for port 80 on host 172.20.25.101
Netflow export enabled.
Warning!! There is a potential statistics mismatch due to existing excluded
protocols.
```

When you try to add a filter to exclude some protocol packets and NDE is currently enabled, this warning message is displayed:

```
Console> (enable) set mls nde flow exclude protocol tcp 80
Netflow tables will not create entries for TCP packets with protocol port 80.
Warning!! There's a potential statistics mismatch due to enabled NDE.
```

Before you use the **set mls nde** command for the first time, you must configure the host to collect MLS statistics. The host name and UDP port number are saved in NVRAM, so you do not need to specify them. If you specify a host name and UDP port, values in NVRAM overwrite the old values. Collector values in NVRAM do not clear when NDE is disabled because this command configures the collector but does not enable NDE automatically.

The **set mls nde enable** command enables NDE, exporting statistics to the preconfigured collector.

If the *protocol* is not **tcp** or **udp**, set the **dst-port** *dst_port* and **src-port** *src_port* values to 0; otherwise, no flows are displayed.

If you try to enable NDE without first specifying a collector, you see this display:

```
Console> (enable) set mls nde enable
Please set host name and UDP port number with 'set mls nde <collector_name | collector_ip>
<udp_port_number>'.
Console> (enable)
```

The **set mls nde flow** command adds filtering to the NDE. Expired flows matching the specified criteria are exported. These values are stored in NVRAM and do not clear when NDE is disabled. If any option is not specified in this command, it is treated as a wildcard. The NDE filter in NVRAM does not clear when NDE is disabled.

In software releases before 8.3(1), only one filter can be active at a time. If you do not enter the **exclude** or **include** keyword, the filter is assumed to be an inclusion filter.

In software release 8.3(1) and later releases, the dual destination feature allows NetFlow export data to be sent to two destinations simultaneously. With this enhancement, you can set up two unique collectors. The same NetFlow data is exported to both the destinations. However, the count of the packets to the two collectors may differ depending on the time the two destinations were created. The count of the packets sent to the individual collectors is maintained separately. Apart from the count, the other NetFlow parameters for both the destinations are the same.

NDE cannot be enabled unless a collector is set up. Both the primary and secondary destinations should be set up before enabling NDE. The secondary destination IP address and port number cannot be equal to the primary destination IP address and port number.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the short subnet address format. The trailing decimal number 00 in an IP address YY.YY.YY.00 specifies the boundary for an IP subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 172.22.36.00/255.255.255.0), and 173.24.00.00 indicates a 16-bit subnet address (subnet mask 173.24.00.00/255.255.0.0). However, this format can identify only a subnet address of 8, 16, or 24 bits.
- *ip_addr/subnet_mask*—This is the long subnet address format. For example, 172.22.252.00/255.255.252.00 indicates a 22-bit subnet address. This format can specify a subnet address of any bit number. To provide more flexibility, the *ip_addr* is a full host address, such as 172.22.253.1/255.255.252.00.
- *ip_addr/maskbits*—This is the simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The *ip_addr* is a full host address, such as 193.22.253.1/22, which has the same subnet address as the *ip_subnet_addr*.

When you use the **set mls nde** {*collector_ip* | *collector_name*} {*udp_port_num*} command, the host name and UDP port number are saved in NVRAM and need not be specified again. If you specify a host name and UDP port, the new values overwrite the values in NVRAM. Collector values in NVRAM do not clear when you disable NDE.

If NDE is enabled when you set the MLS flow mask to null by entering the **set mls flow null** command, NDE will not export any flows.

Examples

This example shows how to set the NDE version to 5:

```
Console> (enable) set mls nde version 5
Multilayer switching netflow data export version set to 5
Console> (enable)
```

This example shows how to specify that only expired flows to a specific subnet are exported:

```
Console> (enable) set mls nde flow include destination 171.69.194.140/24
NDE destination filter set to 171.69.194.0/24
Console> (enable)
```

This example shows how to specify that only expired flows to a specific host are exported:

```
Console> (enable) set mls nde flow include destination 171.69.194.140
NDE destination filter set to 171.69.194.140/32.
Console> (enable)
```

This example shows how to specify that only expired flows from a specific subnet to a specific host are exported:

```
Console> (enable) set mls nde flow include destination 171.69.194.140/24 source
171.69.173.5/24
```

```
NDE destination filter set to 171.69.194.0/24, source filter set to 171.69.173.0/24
Console> (enable)
```

This example shows how to specify that only flows from a specific port are exported:

```
Console> (enable) set mls nde flow include dst_port 23
NDE source port filter set to 23.
Console> (enable)
```

This example shows how to specify that only expired flows from a specific host that are of a specified protocol are exported:

```
Console> (enable) set mls nde flow include source 171.69.194.140 protocol 51
NDE destination filter set to 171.69.194.140/32, protocol set to 51.
Console> (enable)
```

This example shows how to specify that all expired flows except those from a specific host to a specific destination port are exported:

```
Console> (enable) set mls nde flow exclude source 171.69.194.140 dst_port 23
NDE destination filter set to 171.69.194.140/32, source port filter set to 23.
Flows matching the filter will be excluded.
Console> (enable)
```

This example shows how to disable destination ifIndex support:

```
Console> (enable) set mls nde destination-ifindex disable
destination-index export has been disabled.
Console> (enable)
```

This example shows how to disable source ifIndex support:

```
Console> (enable) set mls nde source-ifindex disable
source-index export has been disabled.
Console> (enable)
```

This example shows how to specify an NDE collector when no other collectors have been configured:

```
Console> (enable) set mls nde 10.6.1.10 7772
Number of collectors configured is 1
Netflow export configured for port 7772 on host 10.6.1.10
Netflow export is not enabled. Please enable it now.
Console> (enable)
```

This example shows how to specify an NDE collector when one collector has already been configured:

```
Console> (enable) set mls nde 10.6.1.10 7775
Number of collectors configured is 2
Netflow export configured for port 7775 on host 10.6.1.10
Netflow export is not enabled. Please enable it now.
Console> (enable)
```

This example shows the message that displays if a collector with the same IP address and port already exists:

```
Console> (enable) set mls nde 10.6.1.10 7772
Collector Exists with same IP address and port Number
Failed to set Netflow Data Export
Console> (enable)
```

This example shows the message that displays when two collectors have already been configured:

```
Console> (enable) set mls nde 10.6.1.10 7777
Collector Not set up
A maximum of 2 collectors allowed
Please clear an exiting Collector first
```

```
Failed to set Netflow Data Collector.  
Console> (enable)
```

Related Commands

[clear mls nde flow](#)
[show mls](#)
[show mls nde](#)

set mls netflow-entry-create

To specify the VLANs on which you can enable or disable the creation of NetFlow entries, use the **set mls netflow-entry-create** command.

```
set mls netflow-entry-create {enable | disable} vlan_list
```

Syntax Description		
enable		Specifies that NetFlow entry creation can be enabled on the specified VLANs.
disable		Specifies that NetFlow entry creation cannot be enabled on the specified VLANs.
<i>vlan_list</i>		VLAN numbers; valid values are from 1 to 4094.

Defaults The creation of NetFlow entries is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The status of the creation of NetFlow entries on specific VLANs (whether this feature is enabled or disabled) is displayed as part of the **show mls** command output. The VLANs that have entry creation enabled are displayed as part of the VLANs that have the bridged flow statistics feature enabled.

NetFlow entries on the specified VLANs are not created until you enter the **set mls netflow-per-interface enable** command.

Related Commands [set mls netflow-per-interface](#)
[show mls](#)

set mls netflow-per-interface

To enable or disable the creation of NetFlow entries on a per-VLAN basis, use the **set mls netflow-per-interface** command.

```
set mls netflow-per-interface {enable | disable}
```

Syntax Description

enable	Enables the creation of NetFlow entries on a per-VLAN basis.
disable	Disables the creation of NetFlow entries on a per-VLAN basis.

Defaults

The creation of NetFlow entries is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Entering the **set mls netflow-per-interface disable** command results in the creation of NetFlow entries for all VLANs.

If you enable this feature, NetFlow entries are created both for VLANs on which bridged-flow statistics is enabled and for VLANs on which NetFlow entry creation is enabled. Enabling this feature on specific VLANs causes bridged-flow statistics to be enabled automatically.

For example, if you enable Layer 3 per-VLAN entry creation on VLANs 100 and 200 and at the same time you want to enable bridged-flow statistics on VLANs 150 and 250, NetFlow entry creation and bridged-flow statistics are both enabled on all four VLANs. To collect only bridged-flow statistics for VLAN 150 and 250, you must disable the per-VLAN entry creation feature.

Use the [set mls netflow-entry-create](#) command to specify the VLANs for which NetFlow entry creation can be enabled or disabled.

Related Commands

[set mls netflow-entry-create](#)
[show mls](#)

set mls rate

To set the rate at which index-directed packets are sent to the MSFC, use the **set mls rate** command.

```
set mls rate kpps
```

Syntax Description	<i>kpps</i>	MLS rate in thousands of packets per second; valid values are from 0 to 700. See the “Usage Guidelines” section for more information.
---------------------------	-------------	---------------------------------------------------------------------------------------------------------------------------------------

Defaults	The <i>kpps</i> argument is 0.
-----------------	--------------------------------

Command Types	Switch command.
----------------------	-----------------

Command Modes	Privileged.
----------------------	-------------

Usage Guidelines	You disable MLS rate limiting when you set the <i>kpps</i> argument to 0. When you disable MLS rate limiting, the switch bridges packets to the MSFC; packets are not index-directed.
-------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Examples	This example shows how to set MLS rate limiting to 100 kpps:
-----------------	--------------------------------------------------------------

```
Console> (enable) set mls rate 100  
MLS rate limiting set to 100 Kpps  
Console> (enable)
```

This example shows how to disable MLS rate limiting:

```
Console> (enable) set mls rate 0  
MLS rate limiting disabled  
Console> (enable)
```

Related Commands	show mls
-------------------------	--------------------------

set mls statistics protocol

To add protocols to the protocols statistics list, use the **set mls statistics protocol** command.

```
set mls statistics protocol protocol src_port
```

Syntax Description	<i>protocol</i>	Name or number of the protocol; valid values are from 1 to 255, ip , ipinip , icmp , igmp , tcp , and udp .
	<i>src_port</i>	Number or type of the source port; valid values are from 1 to 65535, dns , ftp , smtp , telnet , x , and www .

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines If you enter any **set mls** commands on a Catalyst 6500 series switch without MLS, this warning message is displayed:

```
MLS not supported on feature card.
```

You can configure a maximum of 64 ports using the **set mls statistics protocol** command.

If you enter **x** for the source port, this specifies the Layer 4 port used by the X-windows application.

Examples This example shows how to set protocols for statistic collection:

```
Console> (enable) set mls statistics protocol 17 1934
Protocol 17 port 1934 is added to protocol statistics list.
Console> (enable)
```

Related Commands [clear mls statistics entry](#)
[show mls statistics](#)

set mls verify

To enable or disable checksum or packet checking based on packet length, use the **set mls verify** command.

```
set mls verify checksum {enable | disable}
```

```
set mls verify length ip inconsistent {enable | disable}
```

Syntax Description	checksum	Specifies IP checksum.
	enable	Enables IP checksum.
	disable	Disables IP checksum.
	length	Specifies checking IP packets based on packet length.
	ip	Specifies IP packet.
	inconsistent	Specifies checking inconsistent packet length. See the “Usage Guidelines” section for more information.
	enable	Enables checking IP packets based on packet length.
	disable	Disables checking IP packets based on packet length.

Defaults

IP checksum is enabled.

Checking IP packets based on inconsistent packet length is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set mls verify** command is available on Supervisor Engine 2 (WS-X6K-SUP2-2GE).

If you enable IP checksum or packet checking based on packet length, the Layer 3 ASIC drops Layer 3 error packets that it encounters. If you disable this feature, the packets are not dropped.



Note We recommend that you do not disable IP checksum or packet checking based on packet length unless you have a specific need to pass nonstandard packets.

Checking for inconsistent packet length means that the switch checks for an inconsistency between the physical length of the packet and the length coded in the packet.

Examples

This example shows how to enable IP checksum:

```
Console> (enable) set mls verify checksum enable
Ip checksum verification enabled
Console> (enable)
```

This example shows how to enable checking inconsistent IP packet length:

```
Console> (enable) set mls verify length ip inconsistent enable  
Ip inconsistant length verification enabled  
Console> (enable)
```

Related Commands [show mls verify](#)

set module

To enable or disable a module, use the **set module** command.

set module enable | disable *mod*

Syntax Description	enable	Enables a module.
	disable	Disables a module.
	<i>mod</i>	Number of the module.

Defaults The default is all modules are enabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines Avoid disabling a module when you are connected through a Telnet session; if you disable your session, you will disconnect your Telnet session.

If there are no other network connections to a Catalyst 6500 series switch (for example, on another module), you have to reenable the module from the console.

You can specify a series of modules by entering a comma between each module number (for example, 2,3,5). You can specify a range of modules by entering a dash between module numbers (for example, 2-5).

The **set module disable** command does not cut off the power to a module, it only disables the module. To turn off power to a module, refer to the **set module power** command.

If an individual port on a module was previously disabled, enabling the module does not enable the disabled port.

Examples This example shows how to enable module 2:

```
Console> (enable) set module enable 2
Module 2 enabled.
Console> (enable)
```

This example shows how to disable module 3 when connected through the console port:

```
Console> (enable) set module disable 3
Module 3 disabled.
Console> (enable)
```

This example shows how to disable module 2 when connected through a Telnet session:

```
Console> (enable) set module disable 2  
This command may disconnect your telnet session.  
Do you want to continue (y/n) [n]? y  
Module 2 disabled.  
Console> (enable)
```

Related Commands [show module](#)

set module autoshut

To enable or disable automatic module shutdown, use the **set module autoshut** command.

```
set module autoshut { enable | disable } mod
```

Syntax Description	enable	Disables automatic module shutdown.
	disable	Enables automatic module shutdown.
	<i>mod</i>	Module number.

Defaults Automatic module shutdown is disabled. If enabled, the defaults are as follows:

- The frequency is three times.
- The period is 2 minutes.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines You can shut down a module manually using the **set module disable** or the **set module power down** commands.

After the module shuts down, you must reenable the module manually.

This command is supported on Ethernet modules only.

Each time a module shuts down by automatic module shutdown, the following SYSLOG message is sent to the configured logging destination:

```
%SYS-5-MOD_AUTOSHUT: Module 2 shutdown automatically, reset 4 times in last 5 minutes
due to inband failure
```

Each time a module exceeds the reset frequency but occurs over a period greater than the configured period, the following SYSLOG message is sent to the configured logging destination:

```
%%SYS-4-MOD_AUTOSHUT_SLOW:Module 1 reset frequency exceeded threshold but over 46
mins. Hence NOT powering down module
```

Examples This example shows how to enable automatic module shutdown on a module:

```
Console> (enable) set module autoshut enable 2
Console> (enable)
```

This example shows how to disable automatic module shutdown on a module:

```
Console> (enable) set module autoshut disable 2
Console> (enable)
```

Related Commands

[clear autoshut](#)
[set autoshut](#)
[show autoshut](#)

set module name

To set the name for a module, use the **set module name** command.

```
set module name mod [mod_name]
```

Syntax Description	<i>mod</i>	Number of the module.
	<i>mod_name</i>	(Optional) Name created for the module.

Defaults The default is no module names are configured for any modules.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines If no module name is specified, any previously specified name is cleared.
Use the **set module name** command to set the module for the MSM. Additional **set module** commands are not supported by the MSM.

Examples This example shows how to set the name for module 1 to Supervisor:

```
Console> (enable) set module name 1 Supervisor  
Module name set.  
Console> (enable)
```

Related Commands [show module](#)

set module power

To turn the power on or off to a module, use the **set module power** command.

```
set module power {up | down} mod [pm_option]
```

Syntax Description		
up	Turns on the power to a module.	
down	Turns off the power to a module.	
<i>mod</i>	Number of the module.	
<i>pm_option</i>	(Optional) Power management bit; valid values are 0 to 15.	

Defaults

The default is power is on to a module.

The power management bit is set to 0.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set module power up** command allows you to check if adequate power is available in the system to turn the power on. If not enough power is available, the module status changes from power-down to power-deny, and this message is displayed:

```
Module 4 could not be powered up due to insufficient power.
```

The *pm_option* argument allows you to set the power management bit for the module on which disaster recovery is needed. Setting the power management bit triggers the downloading of the image from supervisor engine flash memory to the Communication Media Module (CMM) every time the CMM is reset. For more information about disaster recovery and power management bit values on different supervisor engines, see the “Disaster Recovery for CMM Software Upgrades” section of the *Catalyst 6500 Series and Cisco 7600 Series CMM Installation and Configuration Note*. This note is located here:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_14107.htm

Examples

This example shows how to power up module 4:

```
Console> (enable) set module power up 4
Module 4 powered up.
Console> (enable)
```

This example shows how to power down module 4:

```
Console> (enable) set module power down 4
Module 4 powered down.
Console> (enable)
```

Related Commands

[set poll](#)
[show environment](#)

set module shutdown

To shut down the NAM and Intrusion Detection System Module (IDS), use the **set module shutdown** command.

```
set module shutdown {all | mod}
```

Syntax Description

all	Shuts down NAM and IDSs.
<i>mod</i>	Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use the **set module shutdown** command, the configuration is not saved in NVRAM. The next time when the module boots up, it will come online. You can either reinsert or reset the module to bring it online.

If there are no other network connections to a Catalyst 6500 series switch (for example, on another module), you have to reenable the module from the console.

You can specify a series of modules by entering a comma between each module number (for example, 2,3,5).

Examples

This example shows how to shutdown the NAM or IDS:

```
Console> (enable) set module shutdown 2
Console> (enable)
```

set msfcautostate

To enable or disable the line protocol state determination of the Multilayer Switch Feature Cards (MSFCs) due to port state changes, use the **set msfcautostate** command.

```
set msfcautostate {enable | disable}
```

```
set msfcautostate {exclude | track} mod/ports
```

```
set msfcautostate track {enable | disable} vlan_list
```

Syntax Description

enable	Activates the line protocol state determination.
disable	Deactivates the line protocol state determination.
exclude	Excludes ports from autostate.
track	Tracks ports for autostate.
<i>mod/ports</i>	Module number and port numbers.
enable	Enables autostate tracking on a VLAN or VLANs.
disable	Disable autostate tracking on a VLAN or VLANs.
<i>vlan_list</i>	VLAN numbers; valid values are from 1 to 4094.

Defaults

The default is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This feature is used to accurately reflect the Layer 3 interface status based on the underlying Layer 2 interface status so that routing and other protocols converge faster. Faster protocol convergence prevents traffic from being discarded without notice.

When you enable the MSFC auto state feature, VLAN interfaces on the MSFC are active only when there is at least one other active interface in the spanning tree forwarding state on the Catalyst 6500 series switch. This interface could be a physical end-user port, a trunk connection for which the VLAN is active, or even another MSFC with an equivalent VLAN interface.

If you enable and then disable or disable and then enable the **set msfcautostate** command, you might have to use the **shutdown** and **no shutdown** commands to disable and then restart the VLAN and WAN interfaces on the MSFC.

If your FXS module ports are in an auxiliary VLAN and there are no switching module ports active in the VLAN, the FXS module will not initialize because the MSFC auto state feature shuts down all MSFC interfaces and subinterfaces. We recommend that you add a physical Ethernet port to the VLAN.

**Caution**

You should not disable the MSFC auto state feature because the Layer 3 interface status might not accurately reflect the Layer 2 interface status. If you disable this feature, traffic might be discarded without notice even though other valid traffic paths might exist.

Autostate exclude mode allows you to specify the ports to exclude from autostate. In normal autostate mode, Layer 3 interfaces remain up if at least one port in the VLAN remains up. If there are appliances like load balancers or firewall servers that are connected to ports in the VLAN, you can configure these ports to be excluded from the autostate feature to make sure that the forwarding SVI does not go down if these ports become inactive.

Autostate exclude mode affects all VLANs to which the port belongs and is supported on Ethernet, Fast Ethernet, and Gigabit Ethernet ports only.

You can use autostate track mode to track key VLAN or port connections to the MSFC. When you configure the autostate track mode, the SVI stays up if any tracked connections remain up in the VLAN. Track mode requires that you define a global tracked VLAN group. The VLANs in this group will be tracked by MSFC autostate whether or not you define a member port to be tracked.

When you configure a VLAN and ports to be tracked by autostate, tracked SVIs remain down until at least one tracked Ethernet port in the VLAN moves to the Spanning Tree Protocol (STP) forwarding state. Conversely, tracked SVIs remain up if at least one tracked Ethernet port stays in the STP forwarding state.

Autostate track mode is supported on Ethernet, Fast Ethernet, and Gigabit Ethernet ports only.

**Note**

You cannot configure both autostate exclude mode and autostate track mode on the same port.

Examples

This example shows how to disable the line protocol state determination of the MSFC:

```
Console> (enable) set msfcautostate disable
Console> (enable)
```

This example shows how to exclude a port from MSFC autostate:

```
Console> (enable) set msfcautostate exclude 3/1
Port 3/1 configured as excluded port
Console> (enable)
```

This example shows how to configure autostate to track ports 1-5 on module 3:

```
Console> (enable) set msfcautostate track 3/1-5
Port 3/1-5 configured as tracked port
Console> (enable)
```

This example shows how to configure autostate to track VLANs 20, 21, 22, and 28:

```
Console> (enable) set msfcautostate track enable 20-22,28
Vlans 20-22,28 added to MSFC autostate track vlan group
Console> (enable)
```

Related Commands

[clear msfcautostate](#)
[show msfcautostate](#)

set msmautostate

To enable or disable the line protocol state determination of the MSMs due to port state changes, use the **set msmautostate** command.

```
set msmautostate {enable | disable}
```

Syntax Description	enable	Deactivates the line protocol state determination.
	enable	Activates the line protocol state determination.

Defaults The default configuration has line protocol state determination disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This feature is useful for discontinuing the advertisement of routing paths when access to them is severed (either through fault or administrative disabling).

When you enable **msmautostate**, VLAN interfaces on the MSM are active only when there is at least one other active interface within the Catalyst 6500 series switch. This could be a physical end-user port, a trunk connection for which the VLAN is active, or even another MSM with an equivalent VLAN interface.

If you disable **msmautostate**, you might have to use the **shutdown** and **no shutdown** commands to disable and then restart the VLAN interface to bring the MSM back up.

Examples This example shows how to enable the line protocol state determination of the MSM:

```
Console> (enable) set msmautostate enable
MSM port auto state enabled.
Console> (enable)
```

This example shows how to disable the line protocol state determination of the MSM:

```
Console> (enable) set msmautostate disable
MSM port auto state disabled.
Console> (enable)
```

Related Commands [show msmautostate](#)

set multicast ratelimit

To configure multicast rate limiting, use the **set multicast ratelimit** command.

```
set multicast ratelimit { enable | disable }
```

```
set multicast ratelimit rate rate
```

Syntax Description

enable	Enables multicast rate limiting.
disable	Disables multicast rate limiting.
rate <i>rate</i>	Specifies the rate limit in packets per second (pps); valid values are from 0 to 10000.

Defaults

Multicast rate limiting is disabled.
The default rate is 0 pps.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Because the default rate is 0, multicast rate limiting is still operationally disabled even after entering the **set multicast ratelimit enable** command. You must enter a non-zero rate to enable it.

Examples

This example shows how to enable multicast rate limiting:

```
Console> (enable) set multicast ratelimit enable
Enabling Multicast Ratelimiting
Set a non-zero threshold rate to operationally enable multicast ratelimiting
Console> (enable)
```

This example shows how to set the rate limit in pps:

```
Console> (enable) set multicast ratelimit rate 300
Multicast ratelimit watermark rate is set to 300 pps
Console> (enable)
```

This example shows how to disable multicast rate limiting:

```
Console> (enable) set multicast ratelimit disable
Multicast Ratelimiting already disabled
Console> (enable)
```

Related Commands

[show multicast ratelimit-info](#)

set multicast router

To configure a port manually as a multicast router port, use the **set multicast router** command.

set multicast router *mod/port*

Syntax Description	<i>mod/port</i> Number of the module and port on the module.
Defaults	The default is no ports are configured as multicast router ports.
Command Types	Switch command.
Command Modes	Privileged.
Usage Guidelines	When you enable IGMP snooping, the ports to which a multicast-capable router is attached are identified automatically. The set multicast router command allows you to configure multicast router ports statically.
Examples	This example shows how to configure a multicast router port: Console> (enable) set multicast router 3/1 Port 3/1 added to multicast router port list. Console> (enable)
Related Commands	clear multicast router set igmp show multicast group count show multicast router

set mvrp

To enable or disable MVRP on an entire switch, use this command.

```
set mvrp { enable | disable }
```

Syntax Description	enable	Disables MVRP on an entire switch.
	enable	Enables MVRP on an entire switch.

Defaults MVRP is disabled globally.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to enable MVRP:

```
Console(enable) set mvrp enable
MVRP enabled
console(enable)
```

This example shows how to disable MVRP:

```
Console(disable) set mvrp disable
MVRP disabled
console(enable)
```

Usage Guidelines MVRP may be operational on a port only if MVRP is administratively enabled both globally and at the port level. Only when MVRP is operational on a port, MVRP PDUs can be transmitted out on the port (which must be a forwarding trunk) and other MVRP-related operations can be effective on the port.

set mvrp dynamic-VLAN creation

To configure dynamic-VLAN-creation on the switch through MVRP use the **set mvrp dynamic-vlan-creation** command. Dynamic-VLAN-creation will be enabled, if VTP mode is transparent/off.

```
set mvrp dynamic-vlan-creation {enable | disable}
```

Syntax Description	enable	Disables dynamic-VLAN-creation through MVRP.
	disable	Enables dynamic-VLAN-creation through MVRP.

Defaults MVRP dynamic-VLAN-creation is disabled.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to enable dynamic-VLAN-creation through MVRP:

```
console(enable) set mvrp dynamic-vlan-creation enable
MVRP dynamic vlan creation can not be enabled in VTP server/client mode
console(enable)
console(enable) set vtp mode transparent
Changing VTP mode for all features
VTP domain cisco modified
console(enable)
console(enable) set mvrp dynamic-vlan-creation enable
MVRP dynamic vlan creation is enabled
console(enable)
```

set ntp broadcastclient

To enable or disable NTP in broadcast-client mode, use the **set ntp broadcastclient** command.

set ntp broadcastclient {enable | disable}

Syntax Description	enable	Disables NTP in broadcast-client mode.
	enable	Enables NTP in broadcast-client mode.

Defaults The default is broadcast-client mode is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The broadcast-client mode assumes that a broadcast server, such as a router, sends time-of-day information regularly to a Catalyst 6500 series switch.

Examples This example shows how to enable an NTP broadcast client:

```
Console> (enable) set ntp broadcastclient enable
NTP Broadcast Client mode enabled.
Console> (enable)
```

This example shows how to disable an NTP broadcast client:

```
Console> (enable) set ntp broadcastclient disable
NTP Broadcast Client mode disabled.
Console> (enable)
```

Related Commands [show ntp](#)

set ntp broadcastdelay

To configure a time-adjustment factor so the Catalyst 6500 series switch can receive broadcast packets, use the **set ntp broadcastdelay** command.

```
set ntp broadcastdelay microseconds
```

Syntax Description	<i>microseconds</i> Estimated round-trip time, in microseconds, for NTP broadcasts; valid values are from 1 to 999999.
Defaults	The default is the NTP broadcast delay is set to 3000 milliseconds.
Command Types	Switch command.
Command Modes	Privileged.
Examples	This example shows how to set the NTP broadcast delay to 4000 milliseconds: <pre>Console> (enable) set ntp broadcastdelay 4000 NTP broadcast delay set to 4000 microseconds. Console> (enable)</pre>
Related Commands	show ntp

set ntp client

To enable or disable a Catalyst 6500 series switch as an NTP client, use the **set ntp client** command.

```
set ntp client { enable | disable }
```

Syntax Description

enable	Enables a Catalyst 6500 series switch as an NTP client.
disable	Disables a Catalyst 6500 series switch as an NTP client.

Defaults

The default is NTP client mode is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure NTP in either broadcast-client mode or client mode. The broadcast-client mode assumes that a broadcast server, such as a router, sends time-of-day information regularly to a Catalyst 6500 series switch. The client mode assumes that the client (a Catalyst 6500 series switch) regularly sends time-of-day requests to the NTP server.

Examples

This example shows how to enable NTP client mode:

```
Console> (enable) set ntp client enable
NTP client mode enabled.
Console> (enable)
```

Related Commands

[show ntp](#)

set ntp server

To specify the NTP server address and configure an NTP server authentication key, use the **set ntp server** command.

```
set ntp server ip_addr [key public_keynum]
```

Syntax Description

<i>ip_addr</i>	IP address of the NTP server.
key <i>public_keynum</i>	(Optional) Specifies the key number; valid values are 1 to 4292945295.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The client mode assumes that the client (a Catalyst 6500 series switch) sends time-of-day requests regularly to the NTP server. A maximum of ten servers per client is allowed.

Examples

This example shows how to configure an NTP server:

```
Console> (enable) set ntp server 172.20.22.191  
NTP server 172.20.22.191 added.  
Console> (enable)
```

Related Commands

[clear ntp server](#)
[show ntp](#)

set ntp summertime

To set the clock ahead one hour during daylight saving time, use the **set ntp summertime** command.

```
set ntp summertime {enable | disable} [zone]
```

```
set ntp summertime recurring [{week} {day} {month} {hh:mm} {week | day | month | hh:mm}
[offset]]
```

```
set ntp summertime date {month} {date} {year} {hh:mm} {month | date | year | hh:mm} [offset]
```

Syntax Description

enable	Causes the system to set the clock ahead one hour during daylight saving time.
disable	Prevents the system from setting the clock ahead one hour during daylight saving time.
<i>zone</i>	(Optional) Time zone used by the set summertime command.
recurring	Specifies the summertime dates that recur every year.
<i>week</i>	(Optional) Week of the month (first, second, third, fourth, last , 1...5).
<i>day</i>	(Optional) Day of the week (Sunday, Monday, Tuesday , and so forth).
<i>month</i>	Month of the year (January, February, March , and so forth).
<i>hh:mm</i>	Hours and minutes.
<i>offset</i>	(Optional) Amount of offset in minutes (1 to 1440 minutes).
date	Specifies summertime dates for specific non-recurring dates.
<i>date</i>	Day of the month (1 to 31).
<i>year</i>	Number of the year (1993 to 2035).

Defaults

By default, the **set ntp summertime** command is disabled. Once enabled, the default for *offset* is 60 minutes, following U.S. standards.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

After you enter the **clear config** command, the dates and times are set to default.

Unless you configure it otherwise, this command advances the clock one hour at 2:00 a.m. on the first Sunday in April and moves back the clock one hour at 2:00 a.m. on the last Sunday in October.

Examples

This example shows how to cause the system to set the clock ahead one hour during daylight saving time:

```
Console> (enable) set ntp summertime enable PDT
Summertime is enabled and set to "PDT".
Console> (enable)
```

This example shows how to prevent the system from setting the clock ahead one hour during daylight saving time:

```
Console> (enable) set ntp summertime disable
Summertime disabled.
Console> (enable)
```

This example shows how to set daylight saving time to the zonename AUS and repeat every year, starting from the third Monday of February at noon and ending at the second Saturday of August at 3:00 p.m. with an offset of 30 minutes:

```
Console> (enable) set ntp summertime AUS recurring 3 Mon Feb 12:00 2 Saturday Aug 15:00 30
Summer time is disabled and set to 'AUS' with offset 30 minutes.
  start: 12:00:00 Sun Feb 13 2000
  end:   14:00:00 Sat Aug 26 2000
  Recurring, starting at 12:00:00 on Sunday of the third week of February and ending
  on Saturday of the fourth week of August.
Console> (enable)
```

This example shows how to set the daylight saving time to start on January 29, 1999 at 2:00 a.m. and end on August 19, 2004 at 3:00 p.m. with an offset of 30 minutes:

```
Console> (enable) set ntp summertime date jan 29 1999 02:00 aug 19 2004 15:00 30
Summertime is disabled and set to ''
Start : Fri Jan 29 1999, 02:00:00
End   : Thu Aug 19 2004, 15:00:00
Offset: 30 minutes
Recurring: no
Console> (enable)
```

This example shows how to set recurring to reset default to US summertime:

```
Console> (enable) set ntp summertime recurring 3 mon feb 4 thurs oct 8:00 500
Command authorization none.
Summertime is enabled and set to ''
Start : Mon Feb 21 2000, 03:00:00
End   : Fri Oct 20 2000, 08:00:00
Offset: 500 minutes (8 hours 20 minutes)
Recurring: yes, starting at 03:00am of third Monday of February and ending on 08:00am of
fourth Thursday of October.
Console> (enable)
```

Related Commands [show ntp](#)

set ntp timezone

To configure the time offset from Greenwich Mean Time, use the **set ntp timezone** command.

```
set ntp timezone [zone_name] [hours [minutes]]
```

Syntax Description	
<i>zone_name</i>	(Optional) Name of the time zone.
<i>hours</i>	(Optional) Time offset (hours) from Greenwich Mean Time; valid values are from -12 to 12 hours.
<i>minutes</i>	(Optional) Time offset (minutes) from Greenwich Mean Time; valid values are 0 to 59 minutes.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The **set ntp timezone** command is effective only when NTP is running. If you set the time explicitly and NTP is disengaged, the **set ntp timezone** command has no effect. If you have enabled NTP and have not entered the **set timezone** command, the Catalyst 6500 series switch displays UTC by default.

Examples This example shows how to set the time zone to Pacific Standard Time with an offset of minus 8 hours from UTC:

```
Console> (enable) set ntp timezone PST -8
Timezone set to "PST", offset from UTC is -8 hours.
Console> (enable)
```

Related Commands [clear ntp timezone](#)
[show ntp](#)

set packet-capture

To specify the source module and port for Mini Protocol Analyzer packet capturing and to start or stop packet capturing, use the **set packet-capture** command.

```
set packet-capture mod/port
```

```
set packet-capture {start | stop}
```

Syntax Description		
<i>mod</i>		Number of the module.
<i>port</i>		Number of the port on the module.
start		Starts packet capturing.
stop		Stops packet capturing.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The **set packet-capture *mod/port*** command is stored in NVRAM and becomes effective when the **set packet-capture start** command is entered and SPAN is running. The **packet-capture start** command will not work if a *mod/port* argument has not been entered. Only one **set packet-capture *mod/port*** command is in effect at any one time. A new command will cancel an old one.

Examples This example shows how to specify a port on a module for packet capturing:

```
Console> (enable) set packet-capture 1/1
Capturing port set to 1/1.
Console> (enable)
```

This example shows how to start packet capturing on a port:

```
Console> (enable) set packet-capture start
Packet capturing can result in protocol packets(STP, UDLD, PAGP, etc.)
getting dropped resulting in network instability. Also, it can affect
system performance or inband connectivity as sc0/sc1 interface packets
can be dropped without warning
Do you want to continue(y/n) [n]? y
Successfully started the packet capture task.
Console> (enable)
```

This example shows the message that is displayed when you attempt to start packet capturing without specifying a source port for packet capturing:

```
Console> (enable) set packet-capture start  
Failed to start packet capturing as the source port has not been specified.  
Console> (enable)
```

Related Commands

- [clear packet-capture](#)
- [set packet-capture direction](#)
- [set packet-capture dump-file](#)
- [set packet-capture filter](#)
- [set packet-capture limit](#)
- [set packet-capture snap-length](#)
- [show packet-capture](#)

set packet-capture direction

To specify the direction of traffic to be captured for the Mini Protocol Analyzer, use the **set packet-capture direction** command.

```
set packet-capture direction {rx | tx | both}
```

Syntax Description	rx	Captures packets in the receive (rx) direction.
	tx	Captures packets in the transmit (tx) direction
	both	Captures packets in both the receive (rx) and transmit (tx) directions.

Defaults The default setting is receive (rx) only.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines Depending on the direction specified, rate limiters will be used to perform this task. If the required number of rate limiters are not available, the packet-capture process will not work. For example, if you attempt to capture bidirectional traffic using the **set packet-capture start both** command, you must make sure that there are at least two hardware rate limiters available. Only one rate-limiter is required for unidirectional packet capture.

Examples This example shows how to set packet capture in the receive direction:

```
Console> (enable) set packet-capture direction rx
Successfully updated the packet-capture direction.
Console> (enable)
```

This example shows how to set packet capture in the transmit direction:

```
Console> (enable) set packet-capture direction tx
Successfully updated the packet-capture direction.
Console> (enable)
```

This example shows how to set packet capture in both directions:

```
Console> (enable) set packet-capture direction both
Successfully updated the packet-capture direction.
Console> (enable)
```

Related Commands

- [clear packet-capture](#)
- [set packet-capture dump-file](#)
- [set packet-capture filter](#)

set packet-capture limit
set packet-capture snap-length
show packet-capture

set packet-capture filter

To configure Mini Protocol Analyzer packet-capturing filters, use the **set packet-capture filter** command.

```
set packet-capture filter {source | destination} mac mac-address
```

```
set packet-capture filter {source | destination} ip ip-address [ipmask]
```

Syntax Description

source	Sets a source MAC address or IP address as the packet-capturing filter.
destination	Sets a destination MAC address or IP address as the packet-capturing filter.
mac mac-address	MAC address.
ip ip-address	IP address.
ipmask (optional)	IP subnet mask.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The packets can be captured based on either the source or the destination MAC or IP address. The MAC address will be in the format **aa-bb-cc-dd-ee-ff**.

The packets can be captured based on either the source or the destination MAC or IP address. The IP address will be in the format **a.b.c.d**.

Examples

This example shows how to set a packet-capturing filter based on a destination MAC address:

```
Console> (enable) set packet-capture filter destination mac 10-10-10-10-10-10
Successfully added the filter string.
Console> (enable)
```

This example shows how to set a packet-capturing filter based on a destination IP address:

```
Console> (enable) set packet-capture filter destination ip 10.12.12.12
Successfully added the filter string.
Console> (enable)
```

Related Commands

[clear packet-capture](#)
[set packet-capture](#)
[set packet-capture direction](#)
[set packet-capture dump-file](#)
[set packet-capture limit](#)
[set packet-capture snap-length](#)
[show packet-capture](#)

set packet-capture limit

To specify the number of packets to be captured before the Mini Protocol Analyzer stops, use the **set packet-capture limit** command.

set packet-capture limit *num_packets*

Syntax Description	<i>num_packets</i>	Number of packets to capture before the Mini Protocol Analyzer stops; valid values are from 0 to 32000.
---------------------------	--------------------	---------------------------------------------------------------------------------------------------------

Defaults	The default is that the Mini Protocol Analyzer keeps running until all the space on the flash device is filled.
-----------------	-----------------------------------------------------------------------------------------------------------------

Command Types	Switch command.
----------------------	-----------------

Command Modes	Normal.
----------------------	---------

Usage Guidelines	If you enter 0 for the <i>num_packets</i> argument, packet capturing continues until the flash device is filled. To specify the flash device, use the set packet-capture dump-file command.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Examples	This example shows how to set the packet-capture limit:
-----------------	---------------------------------------------------------

```
Console> (enable) set packet-capture limit 32
Packet capture number set to 32.
Console> (enable)
```

Related Commands	<ul style="list-style-type: none"> clear packet-capture set packet-capture set packet-capture direction set packet-capture dump-file set packet-capture filter set packet-capture snap-length show packet-capture
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

set packet-capture snap-length

To specify the length in bytes of packets that are captured for the Mini Protocol Analyzer feature, use the **set packet-capture snap-length** command.

```
set packet-capture snap-length pkt_snap_len
```

Syntax Description	<i>pkt_snap_len</i> Length of captured packets; valid values are from 0 to 10258.
Defaults	The <i>pkt_snap_len</i> argument is 0.
Command Types	Switch command.
Command Modes	Normal.
Usage Guidelines	Captured packets are truncated to snap-length bytes of data. If you enter 0 for the <i>pkt_snap_len</i> argument, full packets are captured.
Examples	This example shows how to specify packet length: Console> (enable) set packet-capture snap-length 78 Packets captured will be truncated to 78 bytes. Console> (enable)
Related Commands	clear packet-capture set packet-capture set packet-capture direction set packet-capture dump-file set packet-capture filter set packet-capture limit show packet-capture

set password

To change the login password on the CLI, use the **set password** command.

set password

Syntax Description This command has no arguments or keywords.

Defaults The default is no password is configured.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines Passwords are case sensitive and may be from 0 to 19 characters in length, including spaces. The command prompts you for the old password. If the password you enter is valid, you are prompted to enter a new password and to verify the new password. A zero-length password is allowed by pressing **Return**.

Examples This example shows how to set an initial password:

```
Console> (enable) set password
Enter old password: <old_password>
Enter new password: <new_password>
Retype new password: <new_password>
Password changed.
Console> (enable)
```

set pbf

To enable policy-based forwarding (PBF) and to set a MAC address for the PFC2, use the **set pbf** command.

```
set pbf [mac mac_address]
```

Syntax Description

mac mac_address (Optional) Specifies MAC address for the PFC2.

Defaults

You can use the default MAC address, or you can specify a MAC address. See the “Usage Guidelines” section for more information.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must set a MAC address for the PFC2. We recommend that you use the default MAC address provided by the MAC PROM. When you specify your own MAC address using the **set pbf mac** command, if the MAC address is a duplicate of a MAC address already in use, packets might be dropped.

PBF is not supported with an operating (booted) MSFC2 in the Catalyst 6500 series switch that is being used for PBF. If an MSFC2 is present but not booted, you can configure PBF.

PBF may require some configuration on attached hosts. When a router is not present in the network, ARP table entries have to be statically added on each host participating in PBF. Refer to the “Configuring Policy-Based Forwarding” section of Chapter 16, “Configuring Access Control,” in the *Catalyst 6500 Series Software Configuration Guide* for detailed information on configuring hosts.



Note

PBF does not work with 802.1Q tunnel traffic. PBF is supported on Layer 3 IP unicast traffic, but it is not applicable to Layer 2 traffic. At the intermediate (PBF) switch, all 802.1Q tunnel traffic appears as Layer 2 traffic.

Examples

This example shows how to set the default MAC address for the PFC2:

```
Console> (enable) set pbf
Console> (enable) Operation successful.
Console> (enable)
```

This example shows how to set a specific MAC address for the PFC2:

```
Console> (enable) set pbf mac 00-01-64-61-39-c2
Console> (enable) Operation successful.
Console> (enable)
```

■ set pbf

Related Commands

[clear packet-capture](#)
[show pbf](#)

set pbf arp-inspection

To add an ARP-inspection ACE to the ACL for a client list or a gateway, use the **set pbf arp-inspection** command.

```
set pbf arp-inspection list_name
```

Syntax Description

list_name Client list or gateway list.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to add an ARP-inspection ACE to the ACL for a client list:

```
Console> (enable) set pbf arp-inspection c11  
.ccl1 editbuffer modified. Use 'commit' command to apply changes.  
Console> (enable) ACL commit in progress.
```

```
ACL '.ccl1' successfully committed.  
Console> (enable)
```

Related Commands

[clear pbf arp-inspection](#)
[show pbf arp-inspection](#)

set pbf client

To add new hosts to a PBF client list, use the **set pbf client** command.

```
set pbf client client_list ip_addr mac_addr vlan
```

Syntax Description	Parameter	Description
	<i>client_list</i>	Client list name.
	<i>ip_addr</i>	IP address.
	<i>mac_addr</i>	MAC address.
	<i>vlan</i>	VLAN number.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines Use this command with the **set pbf gw** command and the **set pbf-map** command to simplify the process of setting and committing the security ACLs and adjacency information. The **set pbf-map** command creates the security ACLs and adjacency information based on your input, commits them to the hardware, and maps them to VLANs. As part of creating the necessary VACLs to redirect traffic from one VLAN to another, the ARP packets are redirected to the software, and the supervisor engine generates ARP replies for the gateway and client requests.

PBF clients and PBF gateways must be on different VLANs. No clients or gateways can have the same IP address. The maximum number of entries is 1024.

The client name and gateway name must be no more than 12 characters.

If you create a PBF map between two VLANs that already have VACLs attached, the PBF ACLs overwrite the previous configuration. The opposite is also true. If you map a new VACL to VLANs with PBF ACLs that were created by using the **set pbf-map** command, the new VACL overwrites the previous configuration.



Note

The number of PBF-client groups that can be mapped to a single PBF gateway is dependent on the number of ACLs that are already configured. For example, if the number of supported ACLs is 250 and you already have 20 ACLs defined, you can have 229 client groups mapped to a gateway.

For more information about using the **set pbf client**, **set pbf gw**, and **set pbf-map** commands, refer to the “Configuring Policy-Based Forwarding” section of Chapter 16, “Configuring Access Control,” in the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows how to add a new host to a client list:

```
Console> (enable) set pbf client c11 21.1.1.1 00-00-00-00-40-01 101  
Commit operation successful.  
Console> (enable)
```

Related Commands

- clear pbf client**
- clear pbf gw**
- clear pbf-map**
- set pbf gw**
- set pbf-map**
- show pbf client**
- show pbf gw**
- show pbf-map**

set pbf gw

To add a PBF gateway to handle connections between VLANs, use the **set pbf gw** command.

```
set pbf gw gw_name ip_addr ip_mask mac_addr vlan
```

Syntax Description		
	<i>gw_name</i>	Gateway name.
	<i>ip_addr</i>	IP address.
	<i>ip_mask</i>	IP mask.
	<i>mac_addr</i>	MAC address.
	<i>vlan</i>	VLAN number.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines Use this command with the **set pbf gw** command and the **set pbf-map** command to simplify the process of setting and committing the security ACLs and adjacency information. The **set pbf-map** command creates the security ACLs and adjacency information based on your input, commits them to the hardware, and maps them to VLANs. As part of creating the necessary VACLs to redirect traffic from one VLAN to another, the ARP packets are redirected to the software, and the supervisor engine generates ARP replies for the gateway and client requests.

PBF clients and PBF gateways must be on different VLANs. No clients or gateways can have the same IP address. The maximum number of entries is 1024.

The client name and gateway name must be no more than 12 characters.

If you create a PBF map between two VLANs that already have VACLs attached, the PBF ACLs overwrite the previous configuration. The opposite is also true. If you map a new VACL to VLANs with PBF ACLs that were created by using the **set pbf-map** command, the new VACL overwrites the previous configuration.



Note

The number of PBF-client groups that can be mapped to a single PBF gateway is dependent on the number of ACLs that are already configured. For example, if the number of supported ACLs is 250 and you already have 20 ACLs defined, you can have 229 client groups mapped to a gateway.

For more information about using the **set pbf client**, **set pbf gw**, and **set pbf-map** commands, refer to the “Configuring Policy-Based Forwarding” section of Chapter 16, “Configuring Access Control,” in the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows how to add a PBF gateway to handle connections between VLANs:

```
Console> (enable) set pbf gw gw1 21.0.0.128 255.0.0.0 00-a0-c9-81-e1-13 102  
Commit operation successful.  
Console> (enable)
```

Related Commands

[clear pbf client](#)
[clear pbf gw](#)
[clear pbf-map](#)
[set pbf client](#)
[set pbf-map](#)
[show pbf client](#)
[show pbf gw](#)
[show pbf-map](#)

set pbf-map

To create security ACLs and to set adjacency information or to map a list of hosts to a gateway, use the **set pbf-map** command.

```
set pbf-map {ip_addr_1} {mac_addr_1} {vlan_1} {ip_addr_2} {mac_addr_2} {vlan_2}
```

```
set pbf-map {client_list} {gw_name}
```

Syntax Description

<i>ip_addr_1</i>	IP address of host 1.
<i>mac_addr_1</i>	MAC address of host 1.
<i>vlan_1</i>	Number of the first VLAN.
<i>ip_addr_2</i>	IP address of host 2.
<i>mac_addr_2</i>	MAC address of host 2.
<i>vlan_2</i>	Number of the second VLAN.
<i>client_list</i>	Client list name.
<i>gw_name</i>	Gateway name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set pbf-map** command does not change existing commands or NVRAM.

The **set pbf-map** command creates security ACLs and adjacency information based on your input, and then automatically commits the ACLs. This command simplifies the configuration of policy-based forwarding.

An example of the simplified syntax is **set pbf-map 1.1.1.1 0-0-0-0-0-1 11 2.2.2.2 0-0-0-0-0-2 12**.

The above example is equivalent to all of the following PBF commands, which were released prior to 7.4:

```
set security acl adjacency PBF_MAP_ADJ_0 11 0-0-0-0-0-1
set security acl adjacency PBF_MAP_ADJ_1 12 0-0-0-0-0-2
commit security acl adjacency
set security acl ip PBF_MAP_ACL_11 redirect PBF_MAP_ADJ_1 ip host 1.1.1.1 host 2.2.2.2
set security acl ip PBF_MAP_ACL_12 redirect PBF_MAP_ADJ_0 ip host 2.2.2.2 host 1.1.1.1
```

If the **permit ip any any** ACE is missing, the following two entries are added:

```
set security acl ip PBF_MAP_ACL_11 permit ip any any
set security acl ip PBF_MAP_ACL_12 permit ip any any
commit security acl ip PBF_MAP_ACL_11
```

```

commit security acl ip PBF_MAP_ACL_12
set security acl map PBF_MAP_ACL_11 11
set security acl map PBF_MAP_ACL_12 12

```

Each entry in the ACL that is added by the **set pbf-map** command is inserted before the default **permit ip any any** ACE.

If you want to add entries other than redirect ACEs to the adjacency table, use the **set security acl ip PBF_MAP_ACL_(VLAN_ID)** command.

Once the map is created between the client and gateway lists by entering the **set pbf-map {client_list} {gw_name}** command, no more mapping can be added for these two lists. Subsequent clients and gateways can be added.

For more information about using the **set pbf client**, **set pbf gw**, and **set pbf-map** commands, refer to the “Enhancements to PBF Configuration” section of Chapter 16, “Configuring Access Control,” in the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows how to specify a PBF_MAP_ACL:

```

Console> (enable) set pbf-map 1.1.1.1 0-0-0-0-0-1 11 2.2.2.2 0-0-0-0-0-2 22

Commit operation successful.
Commit operation successful.

ACL 'PBF_MAP_ACL_11' successfully committed.
Console> (enable)
ACL PBF_MAP_ACL_11 successfully mapped to VLAN 11.
Console> (enable)
ACL 'PBF_MAP_ACL_22' successfully committed.
Console> (enable)
ACL PBF_MAP_ACL_22 successfully mapped to VLAN 22.
Console> (enable) Operation successful.
Console> (enable)

```

This example show how to map a list of hosts to a gateway:

```

Console> (enable) set pbf-map c11 gw1
.ccl1 editbuffer modified. Use 'commit' command to apply changes.
.ggw1 editbuffer modified. Use 'commit' command to apply changes.
.cc11 editbuffer modified. Use 'commit' command to apply changes.
.ggw1 editbuffer modified. Use 'commit' command to apply changes.
.cc11 editbuffer modified. Use 'commit' command to apply changes.
.ggw1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) ACL commit in progress.
Console> (enable) ACL commit in progress.

ACL '.ccl1' successfully committed.
Console> (enable)
ACL '.ggw1' successfully committed.
Console> (enable) Mapping in progress.
Please configure VLAN 101.

ACL .ccl1 successfully mapped to VLAN 101.
Console> (enable) Mapping in progress.
Please configure VLAN 102.

ACL .ggw1 successfully mapped to VLAN 102.
Console> (enable)

```

Related Commands

`clear pbf client`
`clear pbf gw`
`clear pbf-map`
`set pbf client`
`set pbf gw`
`show pbf client`
`show pbf gw`
`show pbf-map`

set pbf vlan

To create policy-based forward (PBF) Layer 2 CAM entries on a VLAN, use the **set pbf vlan** command.

```
set pbf vlan vlan
```

Syntax Description

vlan VLAN number.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines



Note

Specifying the PBF MAC address on a VLAN is only required on the Supervisor Engine 720 with PFC3.

This command creates PBF Layer 2 CAM entries on the VLANs that you specify. Packets matching these entries are classified as Layer 3 packets. The Layer 2 entries are created only if the PBF MAC address is set using the **set pbf mac** command before entering the **set pbf vlan** command.

Using the **clear pbf** command does not clear the VLANs enabled for PBF. The **clear pbf** command does clear the Layer 2 table entries associated with the VLANs (because the MAC address is no longer valid). You must explicitly clear the PBF-enabled VLANs to remove them from NVRAM by entering the **clear pbf vlan *vlan_list*** command.

You can specify a range of VLANs in the CLI.

Examples

This example shows how to specify the PBF MAC address on VLANs 11 and 12:

```
Console> (enable) set pbf vlan 11-12
Console> (enable) PBF enabled on vlan(s) 11-12.
Operation successful.
Console> (enable)
```

In this example, the message “Operation successful” indicates that the PBF MAC address was saved in NVRAM.

Related Commands

[clear pbf vlan](#)
[set pbf](#)
[show pbf](#)

set policy

To configure an authentication policy group and name, use the **set policy** command.

```
set policy group group_name ip-address ip_addr [ip_mask]
```

```
set policy name policy_name group group_name
```

```
set policy name policy_name url-redirect url-redirect-string
```

Syntax Description

group <i>group_name</i>	Sets policy-based group memberships.
ip-address <i>ip_addr</i>	Specifies an IP address to be added to the policy group.
<i>ip_mask</i>	(Optional) IP mask.
name <i>policy_name</i>	Specifies the policy name.
url-redirect <i>url-redirect-string</i>	Maps a URL to a policy name. The <i>url-redirect-string</i> argument can be a maximum of 255 characters.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set policy group** *group_name* **ip-address** *ip_addr* command allows you to add an IP address to an existing policy group. This command fails if the group name is not already present in the group database.

You can add a policy group to a policy template by entering the **set policy name** *policy_name* **group** *group-name* command. If a policy template does not exist, the switch creates it. Similarly, if the policy group name does not exist, the switch creates it.

Examples

This example shows how to add an IP address to an existing policy group:

```
Console> (enable) set policy group grp1 ip-address 100.1.1.1 255.255.255.255
Added IP 100.1.1.1/255.255.255.255 to policy group grp1.
Console> (enable)
```

This example shows how to add a policy group to the policy template:

```
Console> (enable) set policy name pol1 group grp1
Added group grp1 to policy template pol1.
Console> (enable)
```

This example shows how to map a URL to a policy name:

```
Console> (enable) set policy name exception_policy url-redirect http://cisco.com  
Url Redirect http://cisco.com mapped successfully to policy name exception_policy  
Console> (enable)
```

Related Commands

[clear policy](#)
[show policy](#)

set poll

To enable or disable system polling, use the **set poll** command.

```
set poll {enable | disable}
```

Syntax Description

enable	Enables system polling.
disable	Disables system polling.

Defaults

System polling is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set poll** command is part of a recovery procedure that you can follow if the Communication Media Module (CMM) software image fails to load properly. For more information about this procedure, see the “Disaster Recovery for CMM Software Upgrades” section of the *Catalyst 6500 Series and Cisco 7600 Series CMM Installation and Configuration Note*. This note is located here:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_14107.htm

The **set poll disable** command disables the periodic polling of modules by the supervisor engine over the Ethernet Out-of-Band Channel (EOBC) link.



Note

Be careful when using the **set poll disable** command. If a failure occurs on the control plane with Serial Communication Protocol (SCP) communication and periodic polling of modules is disabled, the failure will not be immediately detected.



Note

If system polling is disabled, communication failures between the supervisor engine and the modules are not detected.

Examples

This example shows how to disable system polling:

```
Console> (enable) set poll disable
System polling disabled.
Console> (enable)
```

Related Commands

[set module power](#)
[show poll](#)

set port arp-inspection

To set Address Recognition Protocol (ARP) inspection thresholds and the ARP trust feature on a per-port basis, use the **set port arp-inspection** command.

```
set port arp-inspection mod/port drop-threshold rate shutdown-threshold rate
```

```
set port arp-inspection mod/port trust {enable | disable}
```

Syntax Description	
<i>mod/port</i>	Number of the module and the port or ports on the module.
drop-threshold	Indicates the drop threshold.
<i>rate</i>	Number of packets per second; valid values are from 0 to 1000 pps.
shutdown-threshold	Indicates the shutdown threshold.
trust	Specifies the ARP trust feature.
enable	Enables the trust feature on a port or ports. See the “Usage Guidelines” section for more information.
disable	Disables the trust feature on a port or ports.

Defaults
Both threshold rates are 0 packets per second.
The trust feature is disabled.

Command Types
Switch command

Command Modes
Privileged.

Usage Guidelines
If the number of packets exceeds the drop-threshold rate, the excess packets are dropped. The excess packets are still counted toward the shutdown-threshold rate. If the number of packets exceeds the shutdown-threshold rate, the port is shut down.
When the threshold rates are both at 0 packets per second, per-port rate limiting is not on.
The **set port arp-inspection** *mod/port* **trust** {**enable** | **disable**} command enables or disables the ARP inspection trust feature. The ARP packets from trusted ports are forwarded without inspection. Untrusted packets are intercepted and subject to matching both dynamic DHCP snooping and static ARP inspection rules.
Do not enable Dynamic ARP Inspection (DAI) on VLANs that have ports with static IP addresses unless the ports are trusted.

Examples

This example shows how to set the drop-threshold to 500 and the shutdown-threshold to 1000 for port 2/1:

```
Console> (enable) set port arp-inspection 2/1 drop-threshold 500 shutdown-threshold 1000  
Drop Threshold=500, Shutdown Threshold=1000 set on port 2/1.  
Console> (enable)
```

This example shows how to enable the ARP inspection trust feature on port 2 of module 2:

```
Console> (enable) set port arp-inspection 2/2 trust enable  
Port(s) 2/2 state set to trusted for ARP Inspection.  
Console> (enable)
```

This example shows how to disable the ARP inspection trust feature on port 2 of module 2:

```
Console> (enable) set port arp-inspection 2/2 trust disable  
Port 2/2 state set to untrusted for ARP Inspection.  
Console> (enable)
```

Related Commands

[set security acl arp-inspection](#)
[show port arp-inspection](#)

set port auto-mdix

To enable or disable the automatic Media-Dependent Interface Crossover (MDIX) function, use the **set port auto-mdix** feature.

```
set port auto-mdix mod/port {enable | disable}
```

Syntax Description

<i>mod/port</i>	Module number and port number.
enable	Enables automatic MDIX function.
disable	Disables automatic MDIX function.

Defaults

The automatic MDIX function is enabled on all WS-X6748-GE-TX ports.

The automatic MDIX function is disabled on the Supervisor Engine 720. See the “Usage Guidelines” section for more information.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Auto-MDI/MDIX has always been enabled on the following modules:

- WS-X6548-RJ-45, WS-X6548-RJ-21, WS-X6148-GE-TX, WS-X6548-GE-TX
Auto-MDI/MDIX works in 10-, 100-, and 1000-Mbps modes with autonegotiated and fixed speeds.
- WS-X6516-GE-TX
Auto-MDI/MDIX works with the speed set to auto/1000 Mbps, but not with the speed set to 10 Mbps or 100 Mbps.
- WS-X6316-GE-TX

With software release 8.2(1), auto-MDIX is also enabled on the following modules:

- WS-X6748-GE-TX, Supervisor Engine 720 port 2 (RJ-45)
Auto-MDI/MDIX works with the speed set to auto/1000, but not with the speed set to 10 Mbps or 100 Mbps
- WS-X6148X2-RJ-45, WS-X6148X2-45AF
Auto-MDI/MDIX works with the speed set to auto, but not with the speed set to 10 Mbps or 100 Mbps.



Note

Auto-MDI/MDIX is not supported on any other 10/100-Mbps Ethernet modules or GBIC, SFP, and XENPAK ports.

Examples

This example shows how to enable the automatic MDIX function on port 4/1:

```
Console> (enable) set port 4/1 auto-mdix  
Console> (enable)
```

Related Commands

[show port auto-mdix](#)