



# CHAPTER 15

## Configuring IDSM-2



### Note

Catalyst 6500 Series Switch is used generically to refer to both the 6500 series switches and the 7600 series routers.

This chapter contains procedures that are specific to configuring IDSM-2. Once you set up IDSM-2 to receive traffic from the network, you can configure it for intrusion prevention. It contains the following sections:

- [Configuration Sequence, page 15-1](#)
- [Verifying IDSM-2 Installation, page 15-2](#)
- [Minimum Supported IDSM-2 Configurations, page 15-4](#)
- [Configuring the Catalyst 6500 Series Switch for Command and Control Access to IDSM-2, page 15-5](#)
- [IDSM-2 Sensing Modes, page 15-7](#)
- [Configuring the Catalyst Series 6500 Switch for IDSM-2 in Promiscuous Mode, page 15-8](#)
- [Configuring the Catalyst Series 6500 Switch for IDSM-2 in Inline Mode, page 15-19](#)
- [Configuring the Catalyst Series 6500 Switch for IDSM-2 for Inline VLAN Pair Mode, page 15-21](#)
- [Configuring EtherChannel Load Balancing, page 15-24](#)
- [Administrative Tasks for IDSM-2, page 15-38](#)
- [Catalyst and Cisco IOS Software Commands, page 15-41](#)

## Configuration Sequence

Perform the following tasks to configure IDSM-2:

1. Configure the Catalyst 6500 series switch for command and control access to IDSM-2.  
For the procedure, see [Configuring the Catalyst 6500 Series Switch for Command and Control Access to IDSM-2, page 15-5](#).
2. Log in to IDSM-2.  
For the procedure to session to the IDSM-2, see [Logging In to IDSM-2, page 2-4](#).

3. Configure the switch to send traffic to be monitored to IDS-M-2.
  - [Configuring the Catalyst Series 6500 Switch for IDS-M-2 in Promiscuous Mode, page 15-8](#)
  - [Configuring the Catalyst Series 6500 Switch for IDS-M-2 in Inline Mode, page 15-19](#)
  - [Configuring the Catalyst Series 6500 Switch for IDS-M-2 for Inline VLAN Pair Mode, page 15-21](#)
  - [Configuring EtherChannel Load Balancing, page 15-24](#)
4. Initialize IDS-M-2.
 

Run the **setup** command to initialize IDS-M-2. During setup, you can configure the interfaces of IDS-M-2. If you need to change the interface configuration, see [Chapter 5, “Configuring Interfaces.”](#)

For the procedure, see [Initializing the Sensor, page 3-2](#).
5. Create the service account.
 

For the procedure, see [Creating the Service Account, page 4-13](#).
6. Perform the other initial tasks, such as adding users, trusted hosts, and so forth.
 

For the procedures, see [Chapter 4, “Initial Configuration Tasks.”](#)
7. Configure intrusion prevention.
 

For the procedures, see [Chapter 6, “Configuring Event Action Rules,”](#) [Chapter 7, “Defining Signatures,”](#) and [Chapter 10, “Configuring Attack Response Controller for Blocking and Rate Limiting.”](#)
8. Perform miscellaneous tasks to keep IDS-M-2 running smoothly.
 

For the procedures, see [Chapter 13, “Administrative Tasks for the Sensor”](#) and [Administrative Tasks for IDS-M-2, page 15-38](#).
9. Upgrade the IPS software with new signature updates and service packs.
 

See [Chapter 18, “Obtaining Software”](#) for more information.
10. Reimage the application partition and the maintenance partition when needed.
 

For the procedures, see [Installing the IDS-M-2 System Image, page 17-27](#).

## Verifying IDS-M-2 Installation

Use the **show module** command to verify that the switch acknowledges IDS-M-2 and has brought it online.

To verify the installation, follow these steps:

**Step 1** Log in to the console.

**Step 2** For Catalyst software:

```
console> (enable) show module
```

Mod	Slot	Ports	Module-Type	Model	Sub	Status
1	1	2	1000BaseX Supervisor	WS-X6K-SUP1A-2GE	yes	ok
15	1	1	Multilayer Switch Feature	WS-F6K-MSFC	no	ok
2	2	48	10/100BaseTX Ethernet	WS-X6248-RJ-45	no	ok
3	3	48	10/100/1000BaseT Ethernet	WS-X6548-GE-TX	no	ok
4	4	16	1000BaseX Ethernet	WS-X6516A-GBIC	no	ok
6	6	8	Intrusion Detection Mod	WS-SVC-IDS-M2	yes	ok

```

Mod Module-Name          Serial-Num
-----
1          SAD041308AN
15         SAD04120BRB
2          SAD03475400
3          SAD073906RC
4          SAL0751QYN0
6          SAD062004LV

Mod MAC-Address(es)      Hw      Fw      Sw
-----
1  00-d0-c0-cc-0e-d2 to 00-d0-c0-cc-0e-d3 3.1      5.3.1      8.4(1)
   00-d0-c0-cc-0e-d0 to 00-d0-c0-cc-0e-d1
   00-30-71-34-10-00 to 00-30-71-34-13-ff
15 00-30-7b-91-77-b0 to 00-30-7b-91-77-ef 1.4      12.1(23)E2 12.1(23)E2
2  00-30-96-2b-c7-2c to 00-30-96-2b-c7-5b 1.1      4.2(0.24)V 8.4(1)
3  00-0d-29-f6-01-98 to 00-0d-29-f6-01-c7 5.0      7.2(1)      8.4(1)
4  00-0e-83-af-15-48 to 00-0e-83-af-15-57 1.0      7.2(1)      8.4(1)
6  00-e0-b0-ff-3b-80 to 00-e0-b0-ff-3b-87 0.102    7.2(0.67)  5.0(0.30)

Mod Sub-Type              Sub-Model          Sub-Serial  Sub-Hw  Sub-Sw
-----
1  L3 Switching Engine    WS-F6K-PFC        SAD041303G6 1.1
6  IDS 2 accelerator board WS-SVC-IDSUPG      .          2.0
console> (enable)

```

**Step 3** For Cisco IOS software:

```

router# show module
Mod Ports Card Type              Model              Serial No.
-----
1   48  48 port 10/100 mb RJ-45 ethernet  WS-X6248-RJ-45    SAD0401012S
2   48  48 port 10/100 mb RJ45          WS-X6348-RJ-45    SAL04483QBL
3   48  SFM-capable 48 port 10/100/1000mb RJ45 WS-X6548-GE-TX    SAD073906GH
6   16  SFM-capable 16 port 1000mb GBIC    WS-X6516A-GBIC    SAL0740MMYJ
7    2  Supervisor Engine 720 (Active)      WS-SUP720-3BXL    SAD08320L2T
9    1  1 port 10-Gigabit Ethernet Module  WS-X6502-10GE     SAD071903BT
10   3  Anomaly Detector Module            WS-SVC-ADM-1-K9    SAD084104JR
11   8  Intrusion Detection System          WS-SVC-IDSM2       SAD05380608
13   8  Intrusion Detection System          WS-SVC-IDSM-2      SAD072405D8

Mod MAC addresses      Hw      Fw      Sw      Status
-----
1  00d0.d328.e2ac to 00d0.d328.e2db 1.1      4.2(0.24)VAI 8.5(0.46)ROC Ok
2  0003.6c14.e1d0 to 0003.6c14.e1ff 1.4      5.4(2)      8.5(0.46)ROC Ok
3  000d.29f6.7a80 to 000d.29f6.7aaf 5.0      7.2(1)      8.5(0.46)ROC Ok
6  000d.ed23.1658 to 000d.ed23.1667 1.0      7.2(1)      8.5(0.46)ROC Ok
7  0011.21a1.1398 to 0011.21a1.139b 4.0      8.1(3)      12.2(PIKESPE Ok
9  000d.29c1.41bc to 000d.29c1.41bc 1.3      Unknown      Unknown      PwrDown
10 000b.fcf8.2ca8 to 000b.fcf8.2caf 0.101    7.2(1)      4.0(0.25)    Ok
11 00e0.b0ff.3340 to 00e0.b0ff.3347 0.102    7.2(0.67)    5.0(1)      Ok
13 0003.feab.c850 to 0003.feab.c857 4.0      7.2(1)      5.0(1)      Ok

Mod Sub-Module          Model              Serial          Hw      Status
-----
7  Policy Feature Card 3  WS-F6K-PFC3BXL   SAD083305A1     1.3     Ok
7  MSFC3 Daughterboard   WS-SUP720        SAD083206JX     2.1     Ok
11 IDS 2 accelerator board WS-SVC-IDSUPG      .          2.0     Ok
13 IDS 2 accelerator board WS-SVC-IDSUPG      0347331976     2.0     Ok

Mod Online Diag Status
-----
1  Pass

```

```

2 Pass
3 Pass
6 Pass
7 Pass
9 Unknown
10 Not Applicable
11 Pass
13 Pass
router#

```

**Note**

It is normal for the status to read `other` when IDSM-2 is first installed. After IDSM-2 completes the diagnostics routines and comes online, the status reads `ok`. Allow up to 5 minutes for IDSM-2 to come online.

For information on enabling a full memory test after verifying IDSM-2 installation, see [Enabling Full Memory Tests, page 15-38](#).

## Minimum Supported IDSM-2 Configurations

**Note**

The following matrix is not intended to recommend any particular version, but rather lists the earliest supported versions.

[Table 15-1](#) lists the minimum supported configurations for IDSM-2.

**Table 15-1** Minimum Catalyst 6500 Software Version for IDSM-2 Feature Support

Catalyst/IDSM-2 Feature	Catalyst Software				Cisco IOS Software			
	Sup1	Sup2	Sup32	Sup720	Sup1	Sup2	Sup32	Sup720
SPAN	7.5(1)	7.5(1)	8.4(1)	8.1(1)	12.1(19)E1	12.1(19)E1 12.2(18)SXF1	12.2(18)SXF1	12.2(14)SX1
VACL capture <sup>1</sup>	7.5(1)	7.5(1)	8.4(1)	8.1(1)	12.1(19)E1	12.1(19)E1 12.2(18)SXF1	12.2(18)SXF1	12.2(14)SX1
ECLB with VACL capture <sup>2</sup>	8.5(1)	8.5(1)	8.5(1)	8.5(1)	N/A	12.2(18)SXF4	12.2(18)SXF1	12.2(18)SXE1
Inline interface pairs	8.4(1)	8.4(1)	8.4(1)	8.4(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXE1
ECLB with inline interface pairs	8.5(1)	8.5(1)	8.5(1)	8.5(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4
Inline VLAN pairs	8.4(1)	8.4(1)	8.4(1)	8.4(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4
ECLB with inline VLAN pairs	8.5(1)	8.5(1)	8.5(1)	8.5(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4

1. Requires PFC2/3 or MSFC2/3.

2. Requires PFC2/3 or MSFC2/3.

# Configuring the Catalyst 6500 Series Switch for Command and Control Access to IDSM-2

You must configure the Catalyst 6500 series switch to have command and control access to IDSM-2. This section describes how to configure the switch to have command and control access, and contains the following topics:

- [Catalyst Software, page 15-5](#)
- [Cisco IOS Software, page 15-6](#)

## Catalyst Software

To configure the Catalyst 6500 series switch to have command and control access to IDSM-2, follow these steps:

**Step 1** Log in to the console.

**Step 2** Enter privileged mode:

```
console> enable
```

**Step 3** Put the command and control port into the correct VLAN:

```
console> (enable) set vlan command_and_control_vlan_number
idsm2_slot_number/command_and_control_port_number
```

Example:

```
console> (enable) set vlan 147 6/2
VLAN 147 modified.
VLAN 146 modified.
VLAN   Mod/Ports
-----
147    2/5,2/16-18
        6/2
```

The command and control port number is always 2.

**Step 4** Session to IDSM-2 and ping a network IP address:

```
console> session slot_number
idsm-2# ping network_ip_address
```

Example:

```
console> (enable) session 6
Trying IDS-6...
Connected to IDS-6.
Escape character is '^']'.
```

```
login: cisco
```

```
Password:
```

```
Last login: Thu Mar 3 09:40:53 from 127.0.0.11
```

```
***NOTICE***
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance

with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:  
<http://www.cisco.com/wwl/export/crypto/tool/stgrg.html>

If you require further assistance please contact us by sending email to  
[export@cisco.com](mailto:export@cisco.com).

\*\*\*LICENSE NOTICE\*\*\*

There is no license key installed on the system.

Please go to <http://www.cisco.com/go/license> to obtain a new license or install a license.

idsm-2# **ping 10.89.149.126**

PING 10.89.149.126 (10.89.149.126): 56 data bytes

64 bytes from 10.89.149.126: icmp\_seq=0 ttl=255 time=0.3 ms

64 bytes from 10.89.149.126: icmp\_seq=1 ttl=255 time=0.3 ms

64 bytes from 10.89.149.126: icmp\_seq=2 ttl=255 time=0.3 ms

64 bytes from 10.89.149.126: icmp\_seq=3 ttl=255 time=0.3 ms

--- 10.89.149.126 ping statistics ---

4 packets transmitted, 4 packets received, 0% packet loss

round-trip min/avg/max = 0.3/0.3/0.3 ms

idsm-2# **exit**

console> (enable)

**Step 5** Initialize IDSM-2.

For the procedure, see [Initializing the Sensor, page 3-2](#).

**Step 6** Ping the default router of IDSM-2.

**Step 7** Verify the management station can ping, SSH or Telnet, and web browse to IDSM-2.

## Cisco IOS Software

To configure the Catalyst 6500 series switch to have command and control access to IDSM-2, follow these steps:

**Step 1** Log in to the console.

**Step 2** Enter global configuration mode:

```
router# configure terminal
```

**Step 3** Put the command and control port into the correct VLAN:

```
router (config)# intrusion-detection module module_number management-port access-vlan  
vlan_number
```

Example:

```
router (config)# intrusion-detection module 11 management-port access-vlan 146
```

**Step 4** Verify that you have connectivity by sessioning in to IDSM-2 and pinging a network IP address:

```
router# session slot module_number processor 1  
idsm-2# ping network_ip_address
```

Example:

```
router# session slot 11 processor 1
```

```

The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open

login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
idsm-2# ping 10.89.149.254
PING 10.89.149.254 (10.89.149.254): 56 data bytes
64 bytes from 10.89.149.254: icmp_seq=0 ttl=255 time=0.2 ms
64 bytes from 10.89.149.254: icmp_seq=1 ttl=255 time=0.2 ms
64 bytes from 10.89.149.254: icmp_seq=2 ttl=255 time=0.2 ms
64 bytes from 10.89.149.254: icmp_seq=3 ttl=255 time=0.2 ms
--- 10.89.149.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.2 ms
idsm-2# exit
[Connection to 127.0.0.91 closed by foreign host]
router#

```

#### Step 5 Initialize IDSM-2.

For the procedure, see [Initializing the Sensor, page 3-2](#).

## IDSM-2 Sensing Modes

IDSM-2 supports three sensing modes:

- Promiscuous mode—When IDSM-2 was introduced, promiscuous mode was the only sensing mode supported on IDSM-2 and it is the default sensing mode for both data ports. For more information on promiscuous mode on the sensor, see [Promiscuous Mode, page 5-14](#).

In promiscuous mode, IDSM-2 passively monitors network traffic copied to its data ports by the Catalyst switch. The data ports operate as 802.1q trunks and you can configure the two data ports to trunk the same or different VLANs. The Catalyst switch uses either SPAN or VACL capture to copy specific traffic to the data ports. You can send the same or different traffic to the two data ports. Because IDSM-2 is passive in this mode, it cannot drop packets to block a network intrusion attempt, but you can configure it to send TCP resets to both sides of the network connection to try to break the connection. For more information on TCP reset, see [TCP Reset Interfaces, page 5-6](#). For the procedure for configuring SPAN, see [Configuring SPAN, page 15-9](#). For the procedure for configuring VACL capture, see [Configuring VACL Capture, page 15-13](#).

**Note**

Because the Catalyst switch does not forward traffic received from a capture destination port, IDSM-2 cannot send TCP resets over the data ports to try to block an intrusion. Therefore, a separate reset port available only in promiscuous mode is reserved for this purpose.

- **Inline mode**—Beginning with IPS 5.0(1), you can configure IDSM-2 to be an active network device in inline interface pair mode. The two data ports operate together to bridge two VLANs through IDSM-2. You configure each data port as an access port and assign a different VLAN to each data port. IDSM-2 bridges the two VLANs by forwarding traffic between the two data ports. It inspects the traffic it receives on each data port and can either forward the packets to the other data port or drop the packet if it detects intrusion. For more information on inline mode for sensors, see [Inline Interface Mode, page 5-15](#). You must configure the switch for inline mode (for more information see [Configuring the Catalyst Series 6500 Switch for IDSM-2 in Inline Mode, page 15-19](#)), and then create the inline interface pairs on IDSM-2 (for more information, see [Configuring Inline Interface Pairs, page 5-15](#)).
- **Inline VLAN pair mode**—Beginning with IPS 5.1(1), you can configure IDSM-2 in inline VLAN pair mode. IDSM-2 performs VLAN bridging between pairs of VLANs within the same data port operating as an 802.1q trunk. IDSM-2 inspects the traffic it receives on each VLAN in a VLAN pair and can either forward the packets on the other VLAN in the pair (on the same data port on which the packet was received) or drop the packet if an intrusion is detected. You can configure IDSM-2 to simultaneously bridge up to 255 VLAN pairs on each data port. IDSM-2 replaces the VLAN ID field in the 802.1q header of each packet with the ID of the VLAN on which the packet is forwarded. It drops any packets received on VLANs that are not assigned to an inline VLAN pair. For more information on inline VLAN pair mode, see [Inline VLAN Pair Mode, page 5-17](#). For the procedure for configuring IDSM-2 inline VLAN pair mode, see [Configuring the Catalyst Series 6500 Switch for IDSM-2 for Inline VLAN Pair Mode, page 15-21](#).

**Note**

You are responsible for coordinating the IPS and switch configuration to make sure each of the VLANs associated with an inline VLAN pair is also an allowed VLAN for the data port trunk.

You can mix sensing modes on IDSM-2, for example, you can configure one data port for promiscuous mode and the other data port for inline VLAN pair mode. But because IDSM-2 only has two data ports and inline mode requires the use of both data ports as a pair, you cannot mix inline mode with either of the other two modes.

## Configuring the Catalyst Series 6500 Switch for IDSM-2 in Promiscuous Mode

Traffic is captured for promiscuous analysis on IDSM-2 through SPAN or VACL capture (if you are running the Cisco IOS Firewall on the MSFC, you cannot use VACLs, but you can use the **mls ip ids** command). Port 1 (GigabitEthernet0/1) is used as the TCP reset port, port 2 (GigabitEthernet0/2) is the command and control port, and ports 7 and 8 (GigabitEthernet0/7 and GigabitEthernet0/8) are the monitoring ports. You can configure both monitoring ports to be either SPAN destination ports or VACL capture ports.



**Caution**

If you configure both ports as monitoring ports, make sure that they are configured to monitor different traffic.

**Caution**

You should not configure an IDSM-2 data port as both a SPAN destination port and a VACL capture port, because IDSM-2 will not receive traffic. This dual configuration (SPAN and VACL) causes problems on the switch and traffic is not sent properly.

**Note**

Before Catalyst Software 8.4(3), IDSM-2 data ports defaulted to trunking all VLANs. In Catalyst Software 8.4(3) and later, IDSM-2 data ports default to trunking no VLANs. Make sure that the IDSM-2 ports are trunking the proper VLANs, especially if you upgrading from pre-8.4(3) to 8.4(3) or later.

This section contains the following topics:

- [Using the TCP Reset Interface, page 15-9](#)
- [Configuring SPAN, page 15-9](#)
- [Configuring VACL Capture, page 15-13](#)
- [Configuring the mls ip ids Command, page 15-17](#)

## Using the TCP Reset Interface

The IDSM-2 has a TCP reset interface—port 1. The IDSM-2 has a specific TCP reset interface because it cannot send TCP resets on its sensing ports.

If you have reset problems with the IDSM-2, try the following:

- If the sensing ports are access ports (a single VLAN), you need to configure the reset port to be in the same VLAN.
- If the sensing ports are dot1q trunk ports (multi-VLAN), the sensing ports and reset port all must have the same native VLAN, and the reset port must trunk all the VLANs being trunked by both the sensing ports.

## Configuring SPAN

IDSM-2 can analyze Ethernet VLAN traffic from Ethernet or Fast Ethernet SPAN source ports, or you can specify an Ethernet VLAN as the SPAN source.

This section describes how to configure SPAN, and contains the following topics:

- [Catalyst Software, page 15-10](#)
- [Cisco IOS Software, page 15-11](#)

## Catalyst Software

Use the **set span** command in privileged mode to enable SPAN to IDS-M-2.



### Note

IDS-M-2 port numbers are 7 or 8 only.

The following options apply:

- **disable**—Disables port monitoring.
- *module/port*—Source module and port numbers.
- *vlan*—Source VLAN numbers.
- *module/port*—Destination module and port numbers.
- **both**—Both receiving and transmitting traffic.
- **filter**—Applies filter to VLAN.
- **inpkts**—Enables/disables destination port incoming packets.
- **learning**—Enables/disables MAC address learning.
- **multicast**—Enables/disables multicast traffic.
- **rx**—Receiving traffic.
- **session**— Session number for SPAN session.
- **tx** —Transmitting traffic.

To enable SPAN on IDS-M-2, follow these steps:

**Step 1** Log in to the console.

**Step 2** Enter privileged mode:

```
console> enable
```

**Step 3** Enable SPAN to IDS-M-2:

- From a source port:

```
console> (enable) set span 3/3 13/7
Destination      : Port 13/7
Admin Source     : Port 3/3
Oper Source      : Port 3/3
Direction        : transmit/receive
Incoming Packets : disabled
Learning         : enabled
Multicast        : enabled
Filter           : -

Session Number   : 1

console> (enable)
```



### Note

Use the **filter** keyword to monitor traffic on specific VLANs on source trunk ports.

- From a VLAN:

```
console> (enable) set span 650 13/7 rx
```

```

Destination : Port 13/7
Admin Source : VLAN 650
Oper Source : Port 11/1,13/1
Direction : receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -

Session Number : 1

console> (enable)

```

**Step 4** Show the SPAN sessions:

```

console> (enable) show span

Destination      : Port 13/7
Admin Source     : VLAN 650
Oper Source      : Port 11/1,13/1
Direction       : receive
Incoming Packets : disabled
Learning        : enabled
Multicast       : enabled
Filter          : -

Session Number   : 1

Total local span sessions: 1
console> (enable)

```

**Step 5** To disable the SPAN session that is sending traffic to IDSM-2:

```

console> (enable) set span disable session 1
This command will disable your span session.
Do you want to continue (y/n) [n]? y
Disabled Port 13/7 to monitor receive traffic of VLAN 650
console> (enable)

```

**Note**

For more information on SPAN, refer to the Cisco Catalyst 6500 series switches configuration guides found at this URL:  
[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html)

## Cisco IOS Software

Use the **monitor session** command in global configuration mode to enable SPAN on IDSM-2.

**Note**

Use 1 or 2 for IDSM-2 data port numbers.

The following options apply:

- **interface**—SPAN source interface
- **remote**—SPAN source Remote

- **vlan**— SPAN source VLAN
- **GigabitEthernet**— GigabitEthernet IEEE 802.3z
- **Port-channel**— Ethernet Channel of interfaces
- **,**— Specify another range of interfaces
- **--**— Specify a range of interfaces
- **both**— Monitor received and transmitted traffic
- **rx**— Monitor received traffic only
- **tx**— Monitor transmitted traffic only
- **intrusion-detection-module**— SPAN destination intrusion detection module
- **destination**— SPAN destination interface or VLAN
- **filter**— SPAN filter VLAN
- **source**— SPAN source interface, VLAN
- **type**— Type of monitor session

To enable SPAN on IDS-2, follow these steps:

**Step 1** Log in to the console.

**Step 2** Enter global configuration mode:

```
router# configure terminal
```

**Step 3** Set the source interfaces for the monitor session:

```
router(config)# monitor session (session_number) source interface interface/port_number
[, | - | rx | tx | both]
```

Example:

```
router(config)# monitor session 1 source interface GigabitEthernet2/23 both
```

**Step 4** Enable an IDS-2 data port as a SPAN destination:

```
router(config)# monitor session (session_number) destination intrusion-detection-module
module_number data-port data_port_number
```

Example:

```
router(config)# monitor session 1 destination intrusion-detection-module 9 data-port 1
```

**Step 5** Make sure autostate is included for the data port:

```
router(config)# intrusion-detection-module module_number data-port data_port_number
autostate include
```

Example:

```
router(config)# intrusion-detection-module 9 data-port 1 autostate include
```

This allows the switch virtual interface to stay up if the data port is the only port in the VLAN. The default is **no include**.

**Step 6** (Optional) Enable PortFast for the data port:

```
router(config)# intrusion-detection-module module_number data-port data_port_number
portfast enable
```

Example:

```
router(config)# intrusion-detection-module 9 data-port 1 portfast enable
```

The default is disabled.

**Step 7** (Optional) To disable the monitor session:

```
router(config)# no monitor session session_number
```

**Step 8** (Optional) To filter the SPAN session so that only certain VLANs are seen from switch port trunks:

```
router(config)# monitor session (session_number) {filter vlan {vlan_ID} [, | - ]}
```

Example:

```
router(config)# monitor session 1 filter vlan 146
```

**Step 9** Exit configuration mode:

```
router(config)# exit
```

**Step 10** To show current monitor sessions:

```
router# show monitor session session_number
```

Example:

```
router# show monitor session 1
Session 1
-----
Type                : Local Session
Source Ports        :
    Both             : Gi2/23
Destination Ports   : intrusion-detection-module 9 data-port 1
```



**Note**

For more information on SPAN, refer to the Cisco Catalyst 6500 series switches configuration guides found at this URL:  
[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html)

## Configuring VACL Capture

You can set VACLs to capture traffic for IPS from a single VLAN or from multiple VLANs or from FLeXWAN2 ports on the 7600 router when using Cisco IOS software.

This section describes how to configure VACL capture, and contains the following topics:

- [Catalyst Software, page 15-14](#)
- [Cisco IOS Software, page 15-15](#)

## Catalyst Software



### Note

Port 1 is set as the TCP reset port. Ports 7 and 8 are the sensing ports and can be configured as security ACL capture ports. By default, in Catalyst Software 8.4(1) and earlier releases, ports 7 and 8 are configured as trunk ports and trunk all VLANs on which a security ACL has been applied with the capture feature. If you want to monitor traffic from specific VLANs only, you need to clear the VLANs that you do not want to monitor so that they are not trunked to ports 7 and 8.

Use the **set security acl** command to configure security ACL capture ports.

The following options apply:

- **ACL**—Sets security ACL features
  - **capture-port**—Sets ports for ACL capture
  - **cram**—Sets security ACL cram
  - **ip**—Sets IP security ACL features
  - **ipx**—Sets IPX security ACL features
  - **mac**—Sets MAC security ACL features
  - **map**—Sets security ACL to VLAN mapping
- **permit**—Specifies packets to forward
- **deny**—Specifies packets to reject
- **redirect**—Specifies packets to redirect to ports
- **before**—Inserts ACE before a specified ace in editbuffer
- **capture**—Makes a copy of this flow in capture ports
- **modify**—Modifies a specified ACE in editbuffer

To configure VACLs to capture IPS traffic on VLANs, follow these steps:

**Step 1** Log in to the console.

**Step 2** Enter privileged mode.

```
console> enable
```

**Step 3** Create the VACL to capture traffic. Specify what traffic is permitted, denied, and captured:

```
console> (enable) set security acl ip acl_name permit ip [permit (...) | deny (...)]
capture
```



### Note

Only permitted traffic can be captured. If you want to permit traffic but not capture it, do not use the **capture** keyword

Example:

```
console> (enable) set security acl ip CAPTUREALL permit ip any any capture
CAPTUREALL editbuffer modified. Use 'commit' command to apply changes.
```

**Step 4** Commit the VACL:

```
console> (enable) commit security acl CAPTUREALL
```

ACL commit in progress.

Committing the VACL writes the VACL and associated ACEs to NVRAM.

**Step 5** Map the VACL to the VLANs:

```
console> (enable) set security acl map acl_name vlan_number
```

Example:

```
console> (enable) set security acl map CAPTUREALL 650
Mapping in progress.
```

ACL CAPTUREALL successfully mapped to VLAN 650.

**Step 6** Configure IDSM-2 ports (port 7 or 8) to be capture ports:

```
console> (enable) set security acl capture module_number/port_number
```

Example:

```
console> (enable) set security acl capture 2/7
Successfully set 2/7 to capture ACL traffic.
```



**Note**

For more information on trunk ports and ACLs, refer to the Cisco Catalyst 6500 series switches configuration guides found at this URL:

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html)

## Cisco IOS Software

Use the following commands to configure VACLs to capture IPS traffic on VLANs.

The following options apply:

- **ip-access-list**—Named access list
  - **extended**—Extended Access List
  - **hardware**—Enable Hardware Fragment Handling
  - **log-update**—Control access list log updates
  - **logging**—Control access list logging
  - **resequence**—Resequence Access List
  - **standard**—Standard Access List

To configure VACLs to capture IPS traffic on VLANs, follow these steps:

**Step 1** Log in to the console.

**Step 2** Enter global configuration mode:

```
router# configure terminal
```

**Step 3** Define the ACL:

```
router(config)# ip access-list [standard | extended] acl_name
```

Example:

```
router(config)# ip access-list standard CAPTUREALL
router(config-std-nacl)# exit
```

**Step 4** Define the VLAN access map:

```
router(config)# vlan access-map map_name [0-65535]
```

**Step 5** Configure a match clause in a VLAN access map sequence:

```
router(config-access-map)# match [ip address {1-199 | 1300-2699 | acl_name}]
```

**Step 6** Configure an action clause in the VLAN access map sequence to accompany the preceding match clause:

```
router(config-access-map)# action forward capture
```

**Step 7** Apply the VLAN access-map to the specified VLANs:

```
router(config)# vlan filter map_name vlan-list vlan_list
```

**Step 8** Configure the IDSM-2 data ports to capture the captured-flagged traffic:

```
router(config)# intrusion-detection module module_number data-port data_port_number
capture allowed-vlan capture_vlans
```



**Note** When the switch is routing traffic, you should configure IDSM-2 to monitor all VLANs being routed. If you apply the VACL to a FlexWan2 port, you need to configure IDSM-2 to monitor all VLANs.

**Step 9** Enable the capture function on IDSM-2:

```
router(config)# intrusion-detection module module_number data-port data_port_number
capture
```

This example shows the output from the **show run** command:

```
router# show run
intrusion-detection module 4 data-port 1 capture allowed-vlan 450,1002-1005
intrusion-detection module 4 data-port 1 capture
.
.
.
vlan access-map CAPTUREALL 10
match ip address MATCHALL
action forward capture
.
.
vlan filter CAPTUREALL vlan-list 450,1002-1005
.
ip access-list extended MATCHALL
permit ip any any
router#
```

**Step 10** Make sure autostate is included for the data port:

```
router(config)# intrusion-detection-module module_number data-port data_port_number
autostate include
```

Example:

```
router(config)# intrusion-detection-module 4 data-port 1 autostate include
```



This allows the switch virtual interface to stay up if the data port is the only port in the VLAN. The default is **no include**.

**Step 11** (Optional) Enable PortFast for the data port:

```
router(config)# intrusion-detection-module module_number data-port data_port_number
portfast enable
```

Example:

```
router(config)# intrusion-detection-module 4 data-port 1 portfast enable
```

The default is disabled.



**Note**

For more information on autostate and PortFast, refer to the Cisco Catalyst 6500 series switches configuration guides found at this URL:

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html)

## Configuring the mls ip ids Command

This section describes how to use the **mls ip ids** command to capture IPS traffic, and contains the following topics:

- [Catalyst Software, page 15-17](#)
- [Cisco IOS Software, page 15-18](#)

### Catalyst Software

When you are running the Cisco IOS Firewall on the MSFC, you cannot use VACLs to capture traffic for IDS-M-2, because you cannot apply VACLs to a VLAN in which you have applied an IP inspect rule for the Cisco IOS Firewall. However, you can use the **mls ip ids** command to designate which packets are captured. Packets that are permitted by the ACL are captured. Those denied by the ACL are not captured. The **permit/deny** parameter does not affect whether a packet is forwarded to destination ports. Packets coming into that router interface are checked against the IPS ACL to determine if they should be captured. The **mls ip ids** command is applied as part of the MSFC configuration instead of the supervisor configuration. The **mls ip ids** command only captures incoming traffic. Use the **mls ip ids** command on both the client-side router interface and server-side router interface, so that both directions of the connection are captured.

To use the **mls ip ids** command to capture IPS traffic, follow these steps:

**Step 1** Log in to the MSFC.

**Step 2** Enter privileged mode:

```
console> enable
```

**Step 3** Enter configuration mode:

```
router# configure terminal
```

**Step 4** Configure an ACL to designate which packets will be captured:

```
router(config)# ip access-list extended word
```

**Step 5** Select the interface that carries the packets to be captured:

```
router(config)# interface interface_name
```

**Step 6** Apply the ACL created in Step 4 to the interface selected in Step 5:

```
router(config-if)# mls ip ids word
```

**Step 7** Log in to the supervisor engine.

**Step 8** Enter privileged mode.

```
console> enable
```

**Step 9** On the supervisor engine, add the IDSM-2 monitoring port (port 7 or 8) to the VACL capture list:

```
console> (enable) set security acl capture module_number/port_number
```



#### Caution

For IDSM-2 to capture all packets marked by the **mls ip ids** command, port 7 or 8 of IDSM-2 must be a member of all VLANs to which those packets are routed.

## Cisco IOS Software

When you are using ports as router interfaces rather than switch ports, there is no VLAN on which to apply a VACL.

You can use the **mls ip ids** command to designate which packets are captured. Packets that are permitted by the ACL are captured. Those denied by the ACL are not captured. The **permit/deny** parameter does not affect whether a packet is forwarded to destination ports. Packets coming into that router interface are checked against the IPS ACL to determine if they should be captured.

To use the **mls ip ids** command to capture IDS traffic, follow these steps:

**Step 1** Log in to the console.

**Step 2** Enter global configuration mode:

```
router# configure terminal
```

**Step 3** Configure an ACL to designate which packets will be captured:

```
router(config)# ip access-list extended word
```

**Step 4** Select the interface that carries the packets to be captured:

```
router(config)# interface interface_name
```

**Step 5** Specify the capture VLANs:

```
router(config)# intrusion-detection module module_number data-port data_port_number
capture allowed-vlan capture_vlans
```

Example:

```
router(config)# intrusion-detection module 4 data-port 1 capture allowed-vlan 165
```

**Step 6** Apply the ACL created in Step 4 to the interface selected in Step 5:

```
router(config-if)# mls ip ids word
```



**Caution**

For IDSM-2 to capture all packets marked by the **mls ip ids** command, data port 1 or data port 2 of IDSM-2 must be a member of all VLANs to which those packets are routed.

## Configuring the Catalyst Series 6500 Switch for IDSM-2 in Inline Mode

You can use IDM or the CLI to configure IDSM-2 to operate in inline mode between two separate VLANs (one VLAN for each side of IDSM-2). To prepare IDSM-2 for inline mode, you must configure the switch as well as IDSM-2. Configure the switch first, then configure the IDSM-2 interfaces for inline mode. For the procedure for configuring IDSM-2 to run in inline mode, see [Configuring Inline Interface Pairs, page 5-15](#).

This section contains the following topics:

- [Catalyst Software, page 15-19](#)
- [Cisco IOS Software, page 15-20](#)

### Catalyst Software

You configure IDSM-2 monitoring ports as trunk ports for inline operation for Catalyst software 8.4(1) or later with Supervisor Engine 1a, Supervisor Engine 2, Supervisor Engine 32, or Supervisor Engine 720. Because the native VLAN is the same as the sole VLAN being trunked, the traffic is not 802.1q encapsulated.



**Caution**

Before Catalyst software 8.4.(3), the default configuration for IDSM-2 ports 7 and 8 is to trunk all VLANs 1 to 4094. If you clear the IDSM-2 configuration (**clear configuration module\_number**), IDSM-2 trunks all VLANs. If the IDSM-2 interfaces are configured for inline, spanning tree loops will likely be created and a storm will occur. A storm is numerous packets looping and never reaching their destination.

To configure the monitoring ports on IDSM-2 for inline operation, follow these steps:

**Step 1** Log in to the console.

**Step 2** Enter privileged mode.

```
console> enable
```

**Step 3** Set the native VLAN for each IDSM-2 monitoring port:

```
console (enable)> set vlan vlan_number slot_number/port_number
```

Example:

```
console (enable)> set vlan 651 9/7
console (enable)> set vlan 652 9/8
```

- Step 4** Clear all VLANs from each IDSM-2 monitoring port except for the native VLAN on each port (651 for port 7 and 652 on port 8):

```
console (enable)> clear trunk slot_number/port_number vlan_range
```

Example:

```
console (enable)> clear trunk 9/7 1-650,652-4094
console (enable)> clear trunk 9/8 1-651,653-4094
```

- Step 5** Use the IPS CLI or IDM to pair the interfaces from Step 3 on IDSM-2. For more information, see [Configuring Inline Interface Pairs, page 5-15](#).

## Cisco IOS Software

Configure the IDSM-2 monitoring ports as access ports for inline operation.

To configure inline VLANs, follow these steps:

- Step 1** Log in to the console.

- Step 2** Enter global configuration mode:

```
router# configure terminal
```

- Step 3** Select the VLANs the IDSM-2 will link.

- Step 4** Configure each IDSM-2 data port to be on a single VLAN.

```
router(config)# intrusion-detection module slot_number data-port {1 | 2} access-vlan
vlan_number
router(config)# exit
```

Example:

```
router(config)# intrusion-detection module 13 data-port 1 access-vlan 661
router(config)# intrusion-detection module 13 data-port 2 access-vlan 662
router(config)# exit
```

- Step 5** Verify the configuration:



**Note** In these examples, the IDSM-2 in slot 13 is inline between VLANs 661 and 662. The IDSM-2 data port 1 is on VLAN 661 and data port 2 is on VLAN 662.

- a. Verify the IDSM-2 intrusion detection settings:

```
router# show run | include intrusion-detection
intrusion-detection module 13 management-port access-vlan 147
intrusion-detection module 13 data-port 1 access-vlan 661
intrusion-detection module 13 data-port 2 access-vlan 662
router#
```

- b. Verify that the IDSM-2 data port 1 is an access port on VLAN 661:

```
router# show intrusion-detection module slot_number data-port data_port_number state
```

Example:

```
router# show intrusion-detection module 13 data-port 1 state
Intrusion-detection module 13 data-port 1:
```

```
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q Operational Trunking Encapsulation:
native Negotiation of Trunking: Off Access Mode VLAN: 661 (inline-vlan-1) Trunking
Native Mode VLAN: 1 (default) Trunking VLANs Enabled: NONE Pruning VLANs Enabled:
2-1001 Vlans allowed on trunk:661 Vlans allowed and active in management domain: 661
Vlans in spanning tree forwarding state and not pruned: 661
Administrative Capture Mode: Disabled
Administrative Capture Allowed-vlans: <empty>
```

- c. Verify the VLAN number:

```
router# show vlan id vlan-number
```

Example:

```
router# show vlan id 661
VLAN Name                Status    Ports
-----
661  ward-attack3           active    Gi3/2, Gi13/d1

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp    BrdgMode Trans1 Trans2
-----
661  enet    100661    1500    -      -      -      -      -      0      0

Remote SPAN VLAN
-----
Disabled

Primary Secondary Type      Ports
-----
router#
```

**Step 6** Use the IPS CLI or IDM to pair the interfaces from Step 4 on IDSM-2. For more information, see [Configuring Inline VLAN Pairs, page 5-18](#).

## Configuring the Catalyst Series 6500 Switch for IDSM-2 for Inline VLAN Pair Mode

You can use IDM or the CLI to configure IDSM-2 to operate in inline VLAN pair mode. To prepare IDSM-2 for inline VLAN pair mode, you must configure the switch as well as IDSM-2. Configure the switch first, then configure the IDSM-2 interfaces for inline VLAN pair mode. For the procedure for configuring IDSM-2 to run in inline VLAN pair mode, see [Configuring Inline VLAN Pairs, page 5-18](#).

This section contains the following topics:

- [Catalyst Software, page 15-22](#)
- [Cisco IOS Software, page 15-23](#)

## Catalyst Software

You configure IDSM-2 monitoring ports as trunk ports for inline VLAN pair mode for Catalyst software 8.4(1) or later with Supervisor Engine 1a, Supervisor Engine 2, Supervisor Engine 32, or Supervisor Engine 720.

To configure the monitoring ports on IDSM-2 for inline vlan pair mode, follow these steps:

---

**Step 1** Log in to the console.

**Step 2** Enter privileged mode.

```
console> enable
```

**Step 3** Clear all VLANs from the IDSM-2 monitoring port:

```
console (enable)> clear trunk slot_number/port_number 1-4094
```

Example:

```
console (enable)> clear trunk 9/7 1-4094
```



---

**Note** Before Catalyst software 8.4.(3), the value for the VLAN range when clearing VLANs from the IDSM-2 monitoring port was 1-1005, 1024-4094. In later versions you can clear the entire VLAN range, 1-4094.

---

**Step 4** Configure the IDSM-2 monitoring port to trunk the VLANs to be paired:

```
console (enable)> set trunk slot_number/port_number vlans_to_be_paired
```

Example:

```
console (enable)> set trunk 9/7 651,652
```

**Step 5** Set the native VLAN for the IDSM-2 monitoring port to a value other than the paired VLANs used in Step 4:

```
console (enable)> set vlan vlan-number slot_number/port_number
```

Example:

```
console (enable)> set vlan 1 9/7
```

The default native VLAN is VLAN 1.

**Step 6** Repeat Step 4 for other VLANs to be paired on the IDSM-2 monitoring port.

**Step 7** To configure the other monitoring port, repeat Steps 3 through 6.

**Step 8** Use the IPS CLI or IDM to pair the VLANs from Step 4 on IDSM-2. For more information, see [Configuring Inline VLAN Pairs, page 5-18](#).

---

## Cisco IOS Software

Configure the IDSM-2 monitoring ports as trunk ports for inline VLAN pair operation.

To configure inline VLAN pairs, follow these steps:

**Step 1** Log in to the console.

**Step 2** Enter global configuration mode:

```
router# configure terminal
```

**Step 3** Configure one IDSM-2 data port to trunk the VLANs to be paired:

```
router(config)# intrusion-detection module slot_number data-port data_port_number trunk  
allowed-vlan vlans_to_be_paired  
router(config)# exit
```

Example:

```
router(config)# intrusion-detection module 13 data-port 1 trunk allowed-vlan 661,662  
router(config)# exit
```

**Step 4** Verify the configuration:



**Note** In these examples, data port 1 of IDSM-2 in slot 13 is trunking VLANs 661 and 662.

a. Verify the IDSM-2 intrusion detection settings:

```
router# show run | include intrusion-detection  
intrusion-detection module 13 management-port access-vlan 147  
intrusion-detection module 13 data-port 1 trunk allowed-vlan 661,662  
router#
```

b. Verify that the IDSM-2 data port is trunking the proper VLANs:

```
router# show intrusion-detection module slot_number data-port data_port_number state
```

Example:

```
router# show intrusion-detection module 13 data-port 1 state  
Intrusion-detection module 13 data-port 1:
```

```
Switchport: Enabled  
Administrative Mode: trunk  
Operational Mode: trunk  
Administrative Trunking Encapsulation: dot1q  
Operational Trunking Encapsulation: dot1q  
Negotiation of Trunking: Off  
Access Mode VLAN: 1 (default)  
Trunking Native Mode VLAN: 1 (default)  
Trunking VLANs Enabled: 661,662  
Pruning VLANs Enabled: 2-1001  
Vlans allowed on trunk: 661-662  
Vlans allowed and active in management domain: none  
Vlans in spanning tree forwarding state and not pruned:  
    none  
Administrative Capture Mode: Disabled
```

```
Administrative Capture Allowed-vlans: empty
Autostate mode: excluded
Portfast mode: default

router#
```

- Step 5** Use the IPS CLI or IDM to pair the VLANs from Step 3 on IDSM-2. For more information, see [Configuring Inline VLAN Pairs, page 5-18](#).
- 

## Configuring EtherChannel Load Balancing

This section describes how to configure ECLB on IDSM-2. It contains the following topics:

- [Overview, page 15-24](#)
- [EtherChannel and the Three Sensing Modes, page 15-24](#)
- [Enabling ECLB, page 15-25](#)
- [Disabling ECLB, page 15-34](#)
- [Verifying ECLB, page 15-36](#)

### Overview

Supervisor Engines in the Catalyst 6500 series chassis recognize IDSM-2 devices that are running IPS 5.x and greater as EtherChannel devices. This lets you install up to eight IDSM-2 devices in the same chassis.

The IDSM-2 in the Catalyst 6500 series switch has eight internal ports. Only four of these ports are used. Port 1 is a TCP/IP reset port. Port 2 is the command and control port. Ports 7 and 8 are the sensing ports for Catalyst software and data ports 1 and 2 for Cisco IOS software. The other ports are not used.

The backplane is 1000 Mbps, which is why IDSM-2 shows 1000 Mbps even though it can only handle about 600 Mbps of performance. ECLB allows up to eight IDSM-2 devices to participate in the load balancing on either port 7 or port 8.

### EtherChannel and the Three Sensing Modes

EtherChannel provides load balancing and failover between multiple IDSM-2s in all three sensing modes. IDSM-2 does not participate in EtherChannel protocols, such as LACP or PAgP. Cisco IOS only allows load balancing using **src-dst-ip** algorithm so that all packets between a given pair of IP addresses are always mapped to the same channel. Catalyst software uses the **ip both** algorithm. This is necessary so IDSM-2 can correctly track the connections between two hosts.



#### Caution

You cannot mix IDSM-2 data ports with other port types in an EtherChannel group. You must configure all data ports in an EtherChannel group identically.

---



EtherChannel and IDSM-2 operate in the following way in the three sensing modes:

- EtherChannel and promiscuous mode—When IDSM-2 operates in promiscuous mode, the two data ports operate independently of each other. If you configure the switch so that a data port has two or more IDSM-2s in a group, the switch distributes traffic between the IDSM-2s. This balances the traffic between multiple IDSM-2s. You should rebalance the channel when a data port goes to the `errDisabled` state, or IDSM-2 is shut down, powered down, or reset.
- EtherChannel and inline mode—When you configure multiple IDSM-2s for inline mode, you can load balance the traffic between the IDSM-2s by putting data port 1 of each IDSM-2 into one channel group and data port 2 of each IDSM-2 into another channel group.

**Caution**

To make sure that the same traffic is assigned to the two data ports on each IDSM-2, you must assign the same EtherChannel index to both data ports on each of the IDSM-2s even though they are in different EtherChannel groups.

- EtherChannel and inline VLAN pair mode—When IDSM-2 is in inline on-a-stick mode, the two data ports operate independently of each other. The same restrictions apply as for promiscuous mode.

## Enabling ECLB

This section describes how to enable ECLB for Cisco IOS and Catalyst software. It contains the following sections:

- [Catalyst Software, page 15-25](#)
- [IOS Software, page 15-27](#)

### Catalyst Software

This section describes how to enable ECLB for the three sensing modes in Catalyst software. It contains the following topics:

- [ECLB in Promiscuous and VLAN Pair mode, page 15-25](#)
- [ECLB in Inline Mode, page 15-26](#)

#### ECLB in Promiscuous and VLAN Pair mode

For promiscuous mode and inline VLAN pair mode, add the single port (port 7 or port 8) from each IDSM-2 to an EtherChannel.

To configure the monitoring ports on IDSM-2 for ECLB in promiscuous or inline VLAN pair mode, follow these steps:

---

**Step 1** Log in to the console.

**Step 2** Enter privileged mode.

```
console> enable
```

**Step 3** Configure each IDSM-2 for promiscuous or inline VLAN pair mode.

Use the IPS CLI or IDM to pair the VLANs on IDSM-2. For more information, see [Configuring Inline VLAN Pairs, page 5-18](#).

**Step 4** Add the IDSM-2 monitoring ports to an EtherChannel

```
console (enable)> set port channel slot_number/port_number channel_number
```

Example:

```
console (enable)> set port channel 1/7,7/7 1
```

**Step 5** Set the distribution method:

```
console (enable)> set port channel all distribution ip both
Channel distribution is set to ip both.
console (enable)>
```

**Step 6** Enable ECLB:

```
console (enable)> set port channel slot_number/port_number mode on
```

Example:

```
console (enable)> set port channel 1/7,7/7 mode on
```

---

**ECLB in Inline Mode**

For inline mode, add the single port 7 from each IDSM-2 to an EtherChannel and port 8 from each IDSM-2 to a different EtherChannel.

To configure the monitoring ports on IDSM-2 for ECLB in inline mode, follow these steps:

**Step 1** Log in to the console.**Step 2** Enter privileged mode.

```
console> enable
```

**Step 3** Configure each IDSM-2 for inline mode.

Use the IPS CLI or IDM to pair the interfaces on IDSM-2. For more information, see [Configuring Inline Interface Pairs, page 5-15](#).

**Step 4** Add the IDSM-2 monitoring port 7s to an EtherChannel:

```
console (enable)> set port channel slot_number/7 channel_A_number
```

Example:

```
console (enable)> set port channel 1/7,7/7 1
```

**Step 5** Enable ECLB for that EtherChannel:

```
console (enable)> set port channel slot_number/7 mode on
```

Example:

```
console (enable)> set port channel 1/7,7/7 mode on
```

**Step 6** Add the IDSM-2 monitoring port 8s to another EtherChannel:

```
console (enable)> set port channel slot_number/8 channel_B_number
```

Example:

```
console (enable)> set port channel 1/8,7/8 2
```

**Step 7** Enable ECLB for that EtherChannel:

```
console (enable)> set port channel slot_number/8 mode on
```

Example:

```
console (enable)> set port channel 1/8,7/8 mode on
```

**Step 8** Set the distribution method:

```
console (enable)> set port channel all distribution ip both
Channel distribution is set to ip both.
console (enable)>
```

## IOS Software

**Note**

IOS 12.2(18)SXF4 or later is required for inline mode.

This section describes how to enable ECLB for the three sensing modes in Cisco IOS software. It contains the following topics:

- [Restoring Defaults, page 15-27](#)
- [ECLB in Promiscuous Mode, page 15-27](#)
- [ECLB in Inline Mode, page 15-30](#)

### Restoring Defaults

Use the **intrusion-detection module *module\_number* data-port {1 | 2} default** command to restore the defaults to the specified data port. This command restores the following defaults: allowed VLANs, autostate, portfast, cost, and priority settings. If the data port belongs to a port channel, this command has no effect. This command is useful for clearing the data port before you add it to a port channel group.

This command is equivalent to using all of the following commands:

- **no intrusion-detection module *module\_number* data-port {1 | 2} trunk allowed-vlan**
- **intrusion-detection module *module\_number* data-port {1 | 2} access vlan**
- **intrusion-detection module *module\_number* data-port {1 | 2} autostate include**
- **intrusion-detection module *module\_number* data-port {1 | 2} portfast**
- **intrusion-detection module *module\_number* data-port {1 | 2} spanning-tree cost**
- **intrusion-detection module *module\_number* data-port {1 | 2} spanning-tree priority**

### ECLB in Promiscuous Mode

**Note**

For Cisco IOS version and supervisor requirements for EtherChannel load balancing on IDSM-2, see [Table 15-1 on page 15-4](#).

**Note**

Cisco IOS supports promiscuous IDSM-2 EtherChannel using VACL capture (not SPAN or monitor).

An EtherChannel balances the traffic load across the links in an EtherChannel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel.

EtherChannel load balancing can use MAC addresses, IP addresses, or Layer 4 port numbers, which can be source or destination or both source and destination addresses or ports. The selected mode applies to all EtherChannels configured on the switch. ECLB can also use MPLS Layer 2 information.

Use the option that provides the balance criteria with the greatest variety in your configuration. For example, if the traffic on an EtherChannel is going only to a single MAC address and you use the destination MAC address as the basis of ECLB, the EtherChannel always chooses the same link in the EtherChannel; using source addresses or IP addresses might result in better load balancing.

For more information on EtherChannel, refer to *Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.2SX*.

To configure ECLB for promiscuous operation on IDS-M-2, follow these steps:

- Step 1** Configure each IDS-M-2 for promiscuous operation.

For the procedure, see [Configuring Promiscuous Mode, page 5-15](#).



**Note** Make sure that all IDS-M-2 VACL capture or SPAN or monitor configuration lines have been removed before configuring ECLB for IDS-M-2.

- Step 2** Log in to the console.

- Step 3** Enter global configuration mode:

```
router# configure terminal
```

- Step 4** Create the VACL:

```
router(config)# ip access-list extended vACL_name
```

Example:

```
router(config)# ip access-list extended idstest
```

- Step 5** Add any access control entries, for example, permit any any:

```
router(config-ext-nacl)# permit ip any any
```

- Step 6** Create at least one VLAN access map sequence:

```
router(config-ext-nacl)# vlan access-map vlan_access_map_name sequence_number
router(config-access-map)# match ip address vACL_name
router(config-access-map)# action forward capture
```

Example:

```
router(config)# vlan access-map idstestmap 10
router(config-access-map)# match ip address idstest
router(config-access-map)# action forward capture
```

- Step 7** Apply the VLAN access map to the VLAN(s):

```
router(config-access-map)# vlan filter vlan_access_map_name vlan-list vlan-list
```

Example:

```
router(config)# vlan filter idstestmap vlan-list 50-60
```

**Step 8** For each IDS/SM-2, add the desired data ports into the desired EtherChannel:

```
router(config)# intrusion-detection module module_number data-port data_port_number
channel-group channel_number
```

Example:

```
router(config)# intrusion-detection module 13 data-port 7 channel-group 3
router(config)# intrusion-detection module 12 data-port 7 channel-group 3
```

Each EtherChannel has a numbered port channel interface. You can configure a maximum of 64 port channel interfaces, numbered from 1 to 256.

**Step 9** Configure ECLB:

```
router(config)# port-channel load-balance src-dst-ip
```

The default and only load balancing algorithm supported for IDS/SM-2 is **src-dst-ip**, which means EtherChannel uses the combination of source and destination IP addresses for its distribution method.

**Step 10** Verify the load balancing:

```
router# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
    src-dst-ip

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
IPv4: Source XOR Destination IP address
IPv6: Source XOR Destination IP address
MPLS: Label or IP
```

**Step 11** Set the VLANs to be captured to the EtherChannel:

```
router(config)# intrusion-detection port-channel channel_number capture allowed-vlan
vlan_list
```

Example:

```
router(config)# intrusion-detection port-channel 3 capture allowed-vlan 10
```

**Step 12** Enable capture to the EtherChannel:

```
router(config)# intrusion-detection port-channel channel_number capture
```

Example:

```
router(config)# intrusion-detection port-channel 3 capture
```

**Step 13** Make sure autostate is included for the channel group:

```
router(config)# intrusion-detection port-channel channel_number autostate include
```

Example:

```
router(config)# intrusion-detection port-channel 3 autostate include
```

This allows the switch virtual interface to stay up if the data port is the only port in the VLAN. The default is **no include**.

**Step 14** (Optional) Enable PortFast for the channel group:

```
router(config)# intrusion-detection port-channel channel_number portfast enable
```

Example:

```
router(config)# intrusion-detection port-channel 3 portfast enable
```

The default is disabled.

**Step 15** Exit global configuration mode:

```
router(config)# exit
```

**Step 16** To save the changes:

```
router# write memory
```



**Note**

For more information on autostate and PortFast, refer to the Cisco Catalyst 6500 series switches configuration guides found at this URL:

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html)

## ECLB in Inline Mode



**Note**

Make sure that all IDS-M-2 VACL capture or SPAN or monitor configuration lines have been removed before configuring ECLB for IDS-M-2. You receive an error if you try to change the channel group to inline mode if you have capture enabled on any of the ports.

To configure ECLB for inline mode on IDS-M-2, follow these steps:

**Step 1** Log in to the console.

**Step 2** Enter global configuration mode:

```
router# configure terminal
```

**Step 3** For each IDS-M-2, add all data port 1s into an EtherChannel:

```
router(config)# intrusion-detection module module_number data-port 1 port-channel  
channel_number
```

Example:

```
router(config)# intrusion-detection module 1 data-port 1 port-channel 5
```

Each EtherChannel has a numbered port channel interface. You can configure a maximum of 64 port channel interfaces, numbered from 1 to 256. If the channel group and port channel have not been created, this command creates it with an empty allowed VLAN list. If the port channel exists, its allowed VLAN list, port fast, autostate, spanning tree cost, and priority settings are assigned to the data port.



**Note**

You receive an error if you try to add a data port to a channel group that contains other port types or if you try to add another port type to a port channel containing one or more data ports.

**Step 4** For each IDS-M-2, add all data port 2s into a different EtherChannel:

```
router(config)# intrusion-detection module module_number data-port 2 port-channel  
channel_number
```

Example:

```
router(config)# intrusion-detection module 1 data-port 2 port-channel 6
```

- Step 5** Set the sensing mode to access (inline) and set the access VLAN for the channel group that contains the data port 1s:

```
router(config)# intrusion-detection port-channel channel_number access-vlan vlan_id
```

Example:

```
router(config)# intrusion-detection port-channel 5 access-vlan 1050
```



**Note** You receive an error message if the port channel does not exist or if the port channel is already configured for trunk or capture mode. You must create the port channel or remove the port channel from trunk or capture mode.

- Step 6** Set the sensing mode to access (inline) and set the access VLAN for the channel group that contains the data port 2s:

```
router(config)# intrusion-detection port-channel channel_number access-vlan vlan_id
```

Example:

```
router(config)# intrusion-detection port-channel 6 access-vlan 10
```

- Step 7** Configure ECLB:

```
router(config)# port-channel load-balance src-dst-ip
```

The default is **src-dst-ip**, which means EtherChannel uses the combination of source and destination IP addresses for its distribution method.

Example:

```
router(config)# port-channel load-balance src-dst-ip
```

- Step 8** Verify ECLB:

```
router# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
src-dst-ip
```

```
EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
IPv4: Source XOR Destination IP address
IPv6: Source XOR Destination IP address
MPLS: Label or IP
```

- Step 9** For access (inline) mode, set autostate to **include** each channel group:

```
router(config)# intrusion-detection port-channel channel_number autostate include
```

Example:

```
router(config)# intrusion-detection port-channel 5 autostate include
```

The default is **no include**. This prevents the switch virtual interface from going down if the data port is up and in the VLAN.

- Step 10** (Optional) You can enable or disable PortFast for each channel group:

```
router(config)# intrusion-detection port-channel channel_number portfast enable
```

Example:

```
router(config)# intrusion-detection port-channel 5 portfast enable
```

The default is disabled.

- Step 11** (Optional) Set the spanning tree path cost for each of the two channel groups:

```
router(config)# intrusion-detection port-channel channel_number spanning-tree cost
port_cost
```

Example:

```
router(config)# intrusion-detection port-channel 5 spanning-tree cost 4
```

Both channel groups must be set to the same port cost to make sure that data port 1 and data port 2 of each IDSM-2 are in the same state (forwarding versus blocking).

- Step 12** (Optional) Set the spanning tree port priority for each of the two channel groups:

```
router(config)# intrusion-detection port-channel channel_number spanning-tree priority
priority
```

Example:

```
router(config)# intrusion-detection port-channel 5 spanning-tree priority 16
```

The possible port priority value is a multiple of 16 from 0 to 240. The default is 32.

- Step 13** Exit global configuration mode:

```
router(config)# exit
```

- Step 14** To save the changes:

```
router# write memory
```



**Note**

For more information on autostate, PortFast, spanning tree, and priority, refer to the Cisco Catalyst 6500 series switches configuration guides found at this URL:  
[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html)

## ECLB in Inline VLAN Pair Mode



**Note**

Make sure that all IDSM-2 VACL capture or SPAN or monitor configuration lines have been removed before configuring ECLB for IDSM-2. You receive an error if you try to change the channel group to inline VLAN pair mode if you have **capture** enabled on any of the ports.

To configure ECLB for inline VLAN pair mode on IDSM-2, follow these steps:

- Step 1** Log in to the console.

- Step 2** Enter global configuration mode:

```
router# configure terminal
```

- Step 3** Add the data port (either data port 1 or data port 2) from each IDSM-2 to the Etherchannel:

```
router(config)# intrusion-detection module module_number data-port [1:2] port-channel
channel_number
```



Example:

```
router(config)# intrusion-detection module 1 data-port 1 port-channel 5
```

Each EtherChannel has a numbered port channel interface. You can configure a maximum of 64 port channel interfaces, numbered from 1 to 256. If the channel group and port channel have not been created, this command creates it with an empty allowed VLAN list. If the port channel exists, its allowed VLAN list, port fast, autostate, spanning tree cost, and priority settings are assigned to the data port.



**Note** You receive an error if you try to add a data port to a channel group that contains other port types or if you try to add another port type to a port channel containing one or more data ports.

- Step 4** Set the sensing mode to trunk (inline VLAN pair) and set the allowed VLANs for the channel group that contains the data port 1s. Determine which VLANs are going to be paired (100 and 200, 101 and 201) and set the allowed VLAN list to include all VLANs in all the pairs:

```
router(config)# intrusion-detection port-channel channel_number trunk allowed-vlan
vlan_list
```

Example:

```
router(config)# intrusion-detection port-channel 5 trunk allowed-vlans 100,101,200,201
```



**Note** The allowed VLAN list on the switch must include all VLANs that are paired as inline VLAN pairs on IDS-M-2. Otherwise, traffic may be dropped.



**Note** You receive an error message if the port channel does not exist or if the port channel is already configured for trunk or capture mode. You must create the port channel or remove the port channel from trunk or capture mode.

- Step 5** Configure ECLB:

```
router(config)# port-channel load-balance src-dst-ip
```

The default is **src-dst-ip**, which means EtherChannel uses the combination of source and destination IP addresses for its distribution method.

Example:

```
router(config)# port-channel load-balance src-dst-ip
```

- Step 6** Verify ECLB:

```
router# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
src-dst-ip
```

```
EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
IPv4: Source XOR Destination IP address
IPv6: Source XOR Destination IP address
MPLS: Label or IP
```

- Step 7** For access (inline) mode, set autostate to **include** the channel group:

```
router(config)# intrusion-detection port-channel channel_number autostate include
```

Example:

```
router(config)# intrusion-detection port-channel 5 autostate include
```

The default is **no include**. This prevents the switch virtual interface from going down if the data port is up and in the VLAN.

**Step 8** (Optional) You can enable or disable PortFast for the channel group:

```
router(config)# intrusion-detection port-channel channel_number portfast enable
```

Example:

```
router(config)# intrusion-detection port-channel 5 portfast enable
```

The default is disabled.

**Step 9** (Optional) Set the spanning tree port cost for the channel group:

```
router(config)# intrusion-detection port-channel channel_number spanning-tree cost port_cost
```

Example:

```
router(config)# intrusion-detection port-channel 5 spanning-tree cost 4
```

**Step 10** (Optional) Set the spanning tree port priority for the channel group:

```
router(config)# intrusion-detection port-channel channel_number spanning-tree priority priority
```

Example:

```
router(config)# intrusion-detection port-channel 5 spanning-tree priority 16
```

The possible port priority value is a multiple of 16 from 0 to 240. The default is 32.

**Step 11** Exit global configuration mode:

```
router(config)# exit
```

**Step 12** To save the changes:

```
router# write memory
```

**Step 13** Use the IPS CLI or IDM to pair the VLANs from Step 4 on IDS-M-2. For more information, see [Configuring Inline VLAN Pairs, page 5-18](#).



**Note**

For more information on autostate, PortFast, spanning tree, and priority, refer to the Cisco Catalyst 6500 series switches configuration guides found at this URL:  
[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html)

## Disabling ECLB

This section explains how to disable ECLB, and contains the following topics:

- [Catalyst Software, page 15-35](#)
- [Cisco IOS Software, page 15-35](#)

## Catalyst Software

To disable ECLB, follow these steps:

- 
- Step 1** Log in to the console.
- Step 2** Enter privileged mode.
- ```
console> enable
```
- Step 3** Disable ECLB for promiscuous or inline VLAN pair mode:
- ```
console (enable)> set port channel slot_number/port_number mode off
```
- Example:
- ```
console (enable)> set port channel 1/7,7/7 mode off
```
- Step 4** Disable ECLB for inline mode:
- a.** Disable ECLB for one EtherChannel:
- ```
console (enable)> set port channel slot_number/7 mode off
```
- Example:
- ```
console (enable)> set port channel 1/7,7/7 mode off
```
- b.** Disable ECLB for the other EtherChannel:
- ```
console (enable)> set port channel slot_number/8 mode off
```
- Example:
- ```
console (enable)> set port channel 1/8,7/8 mode off
```
- 

## Cisco IOS Software

To disable ECLB for IDSM-2, follow these steps:

- 
- Step 1** Log in to the console.
- Step 2** Enter global configuration mode:
- ```
router# configure terminal
```
- Step 3** To remove a single IDSM-2 from the EtherChannel:
- ```
router(config)# no intrusion-detection module module_number data-port data_port_number
channel-group channel_number
```
- Example:
- ```
router(config)# no intrusion-detection module 1 data-port 1 channel-group 5
```
- Step 4** To remove the whole EtherChannel:
- ```
router(config)# no intrusion-detection module port-channel channel_number
```

Example:

```
router(config)# no intrusion-detection module port-channel 5
```



#### Note

The VACL capture commands for IDSM-2 are left.

## Verifying ECLB

This section explains how to verify your ECLB configuration, and contains the following topics:

- [Catalyst Software, page 15-36](#)
- [Cisco IOS Software, page 15-37](#)

## Catalyst Software

To verify the ECLB configuration, follow these steps:

**Step 1** Log in to the console.

**Step 2** Enter privileged mode.

```
console> enable
```

**Step 3** To see all EtherChannels:

```
console (enable)> show channel slot_number/port_number mode off
```

Example:

```
console> (enable) show channel
Channel Id    Ports
-----
1669         1/7,7/7
1698         2/1-6
console> (enable)
```



#### Note

In this output, an EtherChannel with ID 1669 is created to have two IDSM-2 data ports. Port 1/7 is for port 7 on the IDSM-2 in slot 1 while port 7/7 is for port 7 on the IDSM-2 in slot 7. Both IDSM-2s are configured for promiscuous operation. The switch load balances between each of the two IDSM-2 ports (one port on each IDSM-2).

**Step 4** To see specific EtherChannel status:

```
console (enable)> show channel hash channel_id source_ip_addr dest_ip_addr
```

Example:

```
console> (enable) show channel hash 1669 10.20.2.1 10.20.5.3
Selected channel port: 1/7
console> (enable)
```



**Note**

This output shows that traffic from 10.20.2.1 to 10.20.5.3 will be sent to port 1/7 (port 7 for the IDS/IPS in slot 1).

## Cisco IOS Software

To verify the IDS/IPS ECLB configuration, follow these steps:

**Step 1** Log in to the console.

**Step 2** To see all EtherChannels:

```
router# show etherchannel
Channel-group listing:
-----

Group: 10
-----
Group state = L2
Ports: 0 Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol: -

router#
```

**Step 3** To see specific EtherChannel status:

```
router# show etherchannel 1 [summary | detail | port | port-channel | protocol]
```

Example:

```
router# show etherchannel 1 summary
Flags: D - down P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3 S - Layer2
       U - in use f - failed to allocate aggregator

       u - unsuitable for bundling
Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
-----+-----+-----+-----
router#
```

**Step 4** To see the ECLB setting:

```
router# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
src-dst-ip
mpls label-ip
```

```

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
    IPv4: Source XOR Destination IP address
    IPv6: Source XOR Destination IP address
MPLS: Label or IP
router#

```

**Step 5** To see IDSM-2 data port information:

```
router# show intrusion-detection module module_number data-port data_port_number state
```

Example:

```
router# show intrusion-detection module 11 data-port 2 state
Intrusion-detection module 11 data-port 2:
```

```

Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 662 (ward-victim3)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: NONE
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:none
Vlans allowed and active in management domain: none
Vlans in spanning tree forwarding state and not pruned:
    none
Administrative Capture Mode: Disabled
Administrative Capture Allowed-vlans: empty

```

---

## Administrative Tasks for IDSM-2

This section contains procedures that help you with administrative tasks for IDSM-2. It contains the following topics:

- [Enabling Full Memory Tests, page 15-38](#)
- [Resetting IDSM-2, page 15-40](#)

### Enabling Full Memory Tests

When IDSM-2 initially boots, by default it runs a partial memory test. You can enable a full memory test in Catalyst software and Cisco IOS software.

This section describes how to enable full memory tests, and contains the following topics:

- [Catalyst Software, page 15-39](#)
- [Cisco IOS Software, page 15-39](#)

## Catalyst Software

Use the **set boot device** *boot\_sequence module\_number* **mem-test-full** command to enable a full memory test. The full memory test takes about 12 minutes.

To enable a full memory test, follow these steps:

**Step 1** Log in to the console.

**Step 2** Enter privileged mode:

```
console> enable
```

**Step 3** Enable the full memory test:

```
console> (enable) set boot dev cf:1 3 mem-test-full
Device BOOT variable = cf:1
Memory-test set to FULL
Warning: Device list is not verified but still set in the boot string.
console> (enable) set boot dev hdd:1 3 mem-test-full
Device BOOT variable = hdd:1
Memory-test set to FULL
Warning: Device list is not verified but still set in the boot string.
console> (enable)
```

The **set boot device** command can either contain **cf:1** or **hdd:1**.

**Step 4** Reset IDS-2.

For the procedure, see [Resetting IDS-2, page 15-40](#).

The full memory test runs.



**Note** A full memory test takes more time to complete than a partial memory test.

## Cisco IOS Software

Use the **hw-module module** *module\_number* **reset mem-test-full** command to enable a full memory test. The full memory test takes about 12 minutes.

To enable a full memory test, follow these steps:

**Step 1** Log in to the console.

**Step 2** Enable the full memory test:

```
router# hw-module module 9 reset mem-test-full
Device BOOT variable for reset = <empty>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]
% reset issued for module 9
router#
```

**Step 3** Reset IDSM-2.

For the procedure, see [Resetting IDSM-2, page 15-40](#).

The full memory test runs.



**Note** A full memory test takes more time to complete than a partial memory test.

## Resetting IDSM-2

If for some reason you cannot communicate with IDSM-2 through SSH, Telnet, or the switch **session** command, you must reset IDSM-2 from the switch console. The reset process requires several minutes.

This section contains the following topics:

- [Catalyst Software, page 15-40](#)
- [Cisco IOS Software, page 15-41](#)

## Catalyst Software

To reset IDSM-2 from the CLI, follow these steps:

**Step 1** Log in to the console.

**Step 2** Enter privileged mode:

```
console> enable
```

**Step 3** Reset IDSM-2 to the application partition or the maintenance partition:

```
console> (enable) reset module_number [hdd:1 | cf:1]
```



**Note** If you do not specify either the application partition (hdd:1 the default) or the maintenance partition (cf:1), IDSM-2 uses the boot device variable.

Example:

```
console> (enable) reset 3
2003 Feb 01 00:18:23 %SYS-5-MOD_RESET: Module 3 reset from console//
Resetting module 3... This may take several minutes.
2003 Feb 01 00:20:03 %SYS-5-MOD_OK: Module 3 is online.
console> (enable)
```



### Caution

If IDSM-2 is removed from the switch chassis without first being shut down, or the chassis loses power, you may need to reset IDSM-2 more than once. If IDSM-2 fails to respond after three reset attempts, boot the maintenance partition, and perform the instructions for restoring the application partition. For the procedure, see [Installing the IDSM-2 System Image, page 17-27](#).



## Cisco IOS Software

Use the **hw-module module slot\_number reset [hdd:1 | cf:1]** command in EXEC mode to reset IDS-2. The reset process takes several minutes. IDS-2 boots into the boot partition you specify. If you do not specify the boot string, the default boot string is used.

To reset IDS-2 from the CLI, follow these steps:

**Step 1** Log in to the console.

**Step 2** Reset IDS-2:

```
router# hw-module module module-number reset [hdd:1 | cf:1]
```



**Note** If you do not specify either the application partition (**hdd:1** the default) or the maintenance partition (**cf:1**), IDS-2 uses the boot device variable.

Example:

```
router# hw-module module 8 reset
Device BOOT variable for reset =
Warning: Device list is not verified.
Proceed with reload of module? [confirm]
% reset issued for module 8
router#
```

## Catalyst and Cisco IOS Software Commands

This section lists the Catalyst and Cisco IOS software commands that pertain to IDS-2.



**Note**

For more detailed information on Catalyst and Cisco IOS software commands, refer to the command references found on Cisco.com. For instructions on how to locate these documents, refer to [Documentation Roadmap for Cisco Intrusion Prevention System 5.1](#).

This section contains the following topics:

- [Catalyst Software, page 15-41](#)
- [Cisco IOS Software, page 15-43](#)

## Catalyst Software

This section lists supported and unsupported Catalyst Software Commands. It contains the following topics:

- [Supported Supervisor Engine Commands, page 15-42](#)
- [Unsupported Supervisor Engine Commands, page 15-43](#)

## Supported Supervisor Engine Commands

IDS-M-2 also supports the following supervisor engine CLI commands, which are described in more detail in the Catalyst 6500 Series Command References.

- **clear config** *module\_number*  
Clears the configuration on the supervisor engine that is associated with the specified IDS-M-2.
- **clear log** *module\_number*  
Deletes all entries in the error log for the specified IDS-M-2.
- **session** *slot\_number*  
Logs in to the console of IDS-M-2 from the switch console.
- **set module** commands (all other **set module** commands return an error message):
  - **set module name** *module\_number*  
Sets the name of the module.
  - **set module power** *module\_number* [**up** | **down**]  
Enables or disables power to the specified IDS-M-2.
- **set port name** *module\_number*  
Configures the name for the specified IDS-M-2 port.
- **set span**  
Configures port 1 as a SPAN destination port. You cannot use port 1 on IDS-M-2 as a SPAN source port.
- **set trunk**  
Configures trunk ports.
- **set vlan**  
Configures VLAN capture ports.
- **show config**  
Displays the supervisor engine NVRAM configurations.
- **show log**  
Displays the error logs for the specified IDS-M-2.
- **show mac** *module\_number*  
Displays the MAC counters for the specified IDS-M-2.
- **show module** *module\_number*  
With an IDS-M-2 installed, displays Intrusion Detection System Module under Module-Type.
- **show port** *module\_number*  
Displays the port status for the specified IDS-M-2.
- **show port capabilities** [*module* | *module\_number*]  
Displays the capabilities of the module and ports.
- **show test**  
Displays the errors reported from the diagnostic tests for both the SPAN port (port 1) and the management port (port 2) and the BIOS and CMOS boot results.

## Unsupported Supervisor Engine Commands

The following supervisor engine CLI commands are not supported by IDSM-2:

- **set module** [enable | disable] *module\_number*
- **set port broadcast**
- **set port channel**
- **set port cops**
- **set port disable**
- **set port enable**
- **set port flowcontrol**
- **set port gmrp**
- **set port gvrp**
- **set port host**
- **set port inlinepower**
- **set port jumbo**
- **set port membership**
- **set port negotiation**
- **set port protocol**
- **set port qos**
- **set port rsvp**
- **set port security**
- **set port speed**
- **set port trap**
- **set protocolfilter**
- **set rgmp**
- **set snmp**
- **set spantree**
- **set udd**
- **set vtp**

## Cisco IOS Software

This section lists the Cisco IOS software commands that IDSM-2 supports. These commands are grouped according to mode.

This section contains the following topics:

- [EXEC Commands, page 15-44](#)
- [Configuration Commands, page 15-45](#)

## EXEC Commands

The following commands are all performed in EXEC mode:

- **clock read-calendar**  
Updates the clock time to the calendar time.
- **clock set** *time date*  
Sets the current time and date.
- **clock update-calendar**  
Updates the calendar time to the clock time.
- **hw-module module** *module\_number* **reset** [**cf:1** | **hdd:1**]  
Resets IDS-M-2 into the partition specified by the boot device variable; if the boot device variable has not been set, IDS-M-2 is reset to the application partition by default. Use the command **show boot device module** *module\_number* to view the current setting of the boot device variable. **cf:1** is the maintenance partition. **hdd:1** is the application partition.
- **hw-module module** *module\_number* **shutdown**  
Shuts down IDS-M-2 so that it can be safely removed from the chassis.
- **reload**  
Reloads the entire switch.
- **session slot** *module\_number* **processor** *processor\_number*  
Logs in to the console of IDS-M-2 from the switch console.
- **show boot device module** *module\_number*  
Displays the current boot string for the specified module.
- **show diagnostic result module** *module\_number*  
Displays the results of the online diagnostics that were performed when IDS-M-2 was last booted up.
- **show interface port-channel** *channel\_number*  
Displays the status of the port channel.
- **show intrusion-detection module** *module\_number* **data-port** {**1** | **2**} {**state** | **traffic**}  
Displays the state or traffic statistics of the specified IDS-M-2 data port.
- **show intrusion-detection module** *module\_number* **management-port** {**state** | **traffic**}  
Displays the state or traffic statistics of the IDS-M-2 management port.
- **show ip access-lists**  
Displays the current access lists.
- **show module** [*module\_number* | **all** | **version**]  
Displays the installed modules, versions, and states.
- **show monitor session** *session\_number*  
Displays the SPAN source and destination for the specified session.
- **show running-config**  
Displays the configuration that is currently running.

- **show spanning-tree active**  
Displays spanning tree state information for active interfaces only.
- **show spanning-tree detail**  
Displays detailed spanning tree state information.
- **show spanning-tree summary [totals]**  
Displays the high level state of spanning tree. Does not show interface specific information.
- **show spanning-tree vlan *vlan\_number***  
Displays spanning tree state information for the specified VLAN. Includes list of ports on which those VLANs are forwarded or blocked.
- **show startup-config**  
Displays the saved configuration.
- **show vlan access-map**  
Displays all current VLAN access maps.

## Configuration Commands

The following configuration commands are all performed in either global configuration mode, interface configuration mode, or VACL configuration submode:

- Global configuration mode
  - **boot device module *number\_number* {cf:1 | hdd:1}**  
Sets the default boot device for the specified module. **cf:1** boots to the MP and **hdd:1** boots to the AP. The **no** option clears the boot string, which sets the default boot device to the AP.
  - **clock calendar valid**  
Sets the current calendar time as the switch time on bootup.
  - **clock summer-time *zone* recurring**  
Sets the switch to use the summertime settings.
  - **clock timezone *zone* *offset***  
Sets the timezone for the switch/IDS-M-2.
  - **fabric switching-mode force busmode**  
Lets service modules that do not support packet recirculation, be forced into communicating through the chassis shared bus instead of the switched fabric. This forces the supervisor to handle the packet recirculation centrally and lets the service module communicate properly on VLANs meeting the conditions stated above. Other fabric enabled modules that are not affected by this problem continue to communicate through the switch fabric even if this command is enabled.
  - **[no] intrusion-detection module *module\_number* data-port {1 | 2} access vlan *vlan\_id***  
Sets the data port to access (inline) mode and sets the access VLAN for the data port for the specified module.

- **[no] intrusion-detection module *module\_number* data-port {1 | 2} autostate include**  
Includes (or excludes) the specified data port in the autostate calculation. When included, the switch virtual interface associated with an MSFC or WLAN port remains up while the module's data port is enabled. When excluded, the switch virtual interface associated with the MSFC or WAN port goes down if the specified module's data port is the only active port in the VLAN. The default is **no include**.
- **[no] intrusion-detection module *module\_number* data-port {1 | 2} capture**  
Configures the specified data port as a capture destination port. You must also set the allowed VLAN list through the **intrusion-detection module *module\_number* data-port {1 | 2} capture** command before any packets are captured. The IDS-M-2 must be in promiscuous mode.
- **[no] intrusion-detection module *module\_number* data-port {1 | 2} capture allowed-vlan *vlan\_list***  
Sets the allowed VLANs on the specified data port for packet capture. You must also enable capture mode on the data port through the **intrusion-detection module *module\_number* data-port {1 | 2} capture** command before traffic is captured on the data port.
- **intrusion-detection module *module\_number* data-port {1 | 2} default**  
Restores the allowed VLANs, autostate, PortFast, port cost, and priority settings for the specified data port to the default values. This command is useful to remove any configuration from a data port before you add it to a channel group.
- **[no] intrusion-detection module *module\_number* data-port {1 | 2} port-channel *channel\_number***  
Adds the data port for the specified module to the channel group, which creates a port channel with the same numeric ID. If the channel group and port channel have not been created, this command creates it with an empty allowed VLAN list. The **no** option removes the data port from the channel group, restores the data port settings to their defaults, and deletes the port channel if it is empty.
- **[no] intrusion-detection module *module\_number* data-port {1 | 2} portfast enable | disable [trunk]**  
Enables or disables PortFast on the data port. When PortFast is enabled, traffic is forwarded by the switch to the IDS-M-2 data port while the spanning tree is being built. When disabled, traffic is inhibited until after the tree is built and the backplane port is in the forwarding state. The default is disabled. The trunk option enables or disables PortFast with the data port is configured as a trunk (in promiscuous or inline VLAN pairs mode).
- **[no] intrusion-detection module *module\_number* data-port {1 | 2} spanning-tree cost *path\_cost***  
Sets the spanning tree path cost for the data port on the specified module. The **no** option restores the spanning tree cost for the data port on the specified module to the default cost value.
- **[no] intrusion-detection module *module\_number* data-port {1 | 2} trunk allowed-vlan *vlan\_list***  
Sets the data port to trunking mode and sets the list of allowed VLANs on the data port for the specified module. The **no** option removes the data port from trunking mode and clears the list of allowed VLANs on the data port for the specified module.
- **intrusion-detection module *module\_number* management-port access-vlan *vlan\_number***  
Sets the access VLAN for the IDS-M-2 command and control port.

- **intrusion-detection module** *module\_number* **data-port** *data\_port\_number* **capture allowed-vlan** *allowed\_capture\_vlan(s)*  
Configures the VLAN(s) for VACL capture.
- **intrusion-detection module** *module\_number* **data-port** *data\_port\_number* **capture**  
Enables VACL capture for the specified IDS-M-2 data port.
- **[no] intrusion-detection port-channel** *channel\_number* **access vlan** *vlan\_id*  
Sets all data ports in the specified port channel to access mode and sets the access VLAN for the data ports. The **no** option clears the list of allowed VLANs on the data ports of all modules in the specified port channel.
- **[no] intrusion-detection port-channel** *channel\_number* **autostate include**  
Includes or excludes all data ports in the specified port channel from the autostate calculation. When included, the virtual switch interface associated with an MSFC or WLAN port remains up while the data port is enabled. When excluded, the virtual switch interface associated with the MSFC or WAN port goes down if the data port is the only active port in the VLAN. The data ports are excluded from the autostate calculations by default.
- **[no] intrusion-detection port-channel** *channel\_number* **capture**  
Configures all data ports in the channel group as capture ports. The **no** option disables the capture function on all data ports in the channel group.
- **[no] intrusion-detection port-channel** *channel\_number* **capture allowed-vlan** *vlan\_id*  
Sets the list of capture VLANs on the data ports of all modules in the specified port channel. This command does not set the channel group to capture mode. Use the **intrusion-detection port-channel** *channel\_number* **capture** command to set the channel group to capture mode. The **no** option clears the list of capture VLANs on the data ports of all modules in the specified port channel.
- **[no] intrusion-detection port-channel** *channel\_number* **portfast enable | disable [trunk]**  
Enables or disables PortFast on the data ports in the port channel. When PortFast is enabled, traffic is forwarded by the switch to the data port while the spanning tree is being built. When disabled, traffic is inhibited until after the tree is built and the backplane port is in the forwarding state. Use the **trunk** option to enable or disable PortFast when the data port is configured as a trunk (in promiscuous or inline VLAN pair mode). Do not use the **trunk** option when the data ports are configured as access ports (inline mode). PortFast and PortFast trunk are disabled by default.
- **[no] intrusion-detection port-channel** *channel\_number* **spanning-tree cost** *port\_cost*  
Sets the spanning tree port cost for the data port on the specified module. The **no** option restores the spanning tree port cost for the data port on the specified module to the default value.
- **[no] intrusion-detection port-channel** *channel\_number* **spanning-tree priority** *priority*  
Sets the spanning tree port priority for the data port on the specified module. The **no** option restores the spanning tree port priority for the data port on the specified module to the default value.
- **[no] intrusion-detection port-channel** *channel\_number* **trunk allowed-vlan** *vlan\_id*  
Sets the list of allowed VLANs on the data ports of all modules in the specified port channel. The **no** option clears the list of allowed VLANs on the data ports of all modules in the specified port channel.

- **ip access-list extended** *word*  
Creates access lists for use in the VACL maps.
- **[no] monitor session** *session\_number* **destination intrusion-detection module** *module\_number* **data-port** {1 | 2}  
Configures a SPAN destination port, which can be either a standard line card port or an IDS-M-2 data port.
- **[no] monitor session** *session\_number* {**source** {**interface** *interface\_number*} | {**vlan** *vlan\_id*}} [ , | - | **rx** | **tx** | **both**]  
Sets the sources for a SPAN session.
- **[no] power enable module** *module\_number*  
Powers IDS-M-2 off or on.
- **[no] spanning tree mode** {**pvtst** | **mst** | **rapid-pvtst**}  
Selects the spanning tree protocol (PVST+, MST, or Rapid-PVST+) to be used globally on the switch. The default is PVST. MST is not supported for IDS-M-2. The **no** option restores the spanning tree mode to the default.
- **vlan access-map** *map\_name\_sequence*  
Creates the VACL maps.
- **vlan filter** *map\_name* **vlan-list** *vlangs*  
Maps the VACL maps to VLANs.
- Interface configuration mode
  - **switchport**  
Sets the interface as a switch port.
  - **switchport access vlan** *vlan*  
Sets the access VLAN for the interface.
  - **switchport capture**  
Sets the interface as a capture port.
  - **switchport mode access**  
Sets the interface as an access port.
  - **switchport mode trunk**  
Sets the interface as a trunk port.
  - **switchport trunk allowed vlan** *vlangs*  
Sets the allowed VLANs for trunk.
  - **switchport trunk encapsulation dot1q**  
Sets dot1q as the encapsulation type.
  - **switchport trunk native vlan** *vlan*  
Sets the native VLAN for the trunk port.



- VACL configuration submode
  - **action forward capture**  
Designates that matched packets should be captured.
  - **match ip address** [*1-199* | *1300-2699* | *acl\_name*]  
Specifies filtering in the VACL.

