



CHAPTER 15

Configuring IDSM-2

This chapter contains procedures that are specific to 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 the following sections:

- [Configuration Sequence, page 15-1](#)
- [Verifying IDSM-2 Installation, page 15-2](#)
- [Configuring the Catalyst 6500 Series Switch for Command and Control Access to IDSM-2, page 15-4](#)
- [Configuring the Catalyst Series 6500 Switch for IDSM-2 in Promiscuous Mode, page 15-7](#)
- [Configuring the Catalyst Series 6500 Switch for IDSM-2 in Inline Mode, page 15-16](#)
- [Administrative Tasks for IDSM-2, page 15-24](#)
- [Catalyst and Cisco IOS Software Commands, page 15-27](#)

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 15-4](#).
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. Initialize IDSM-2.
Run the **setup** command to initialize IDSM-2.
For the procedure, see [Initializing the Sensor, page 3-2](#).

4. Configure IDSM-2 to capture traffic for intrusion analysis.

For the procedures, see [Configuring the Catalyst Series 6500 Switch for IDSM-2 in Promiscuous Mode, page 15-7](#), and [Configuring the Catalyst Series 6500 Switch for IDSM-2 in Inline Mode, page 15-16](#). For the procedure for configuring IDSM-2 to run in promiscuous or inline mode, see [Chapter 5, “Configuring Interfaces.”](#) For information on the TCP reset interface, see [Using the TCP Reset Interface, page 15-7](#). For the procedure for configuring load balancing for IDSM-2 using Cisco IOS software, see [Configuring EtherChanneling, page 15-20](#).

5. Create the service account.

A service account is needed for password recovery and other special debug situations directed by TAC.

For the procedure, see [Creating the Service Account, page 4-13](#).



Caution

You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. However, you can use the service account to create a new password if the Administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

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 Blocking.”](#)

8. Perform miscellaneous tasks to keep IDSM-2 running smoothly.

For the procedures, see [Chapter 13, “Administrative Tasks for the Sensor,”](#) and [Administrative Tasks for IDSM-2, page 15-24](#).

9. Upgrade the IPS software with new signature updates and service packs.

For more information, see [Obtaining Cisco IPS Software, page 18-1](#).

10. Reimage the application partition and the maintenance partition when needed.

For the procedures, see [Installing the IDSM-2 System Image, page 17-25](#).

Verifying IDSM-2 Installation

Verify that the switch acknowledges IDSM-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:

```
cat6k> (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-IDSM2 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
cat6k> (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 15-24](#).

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 to IDSM-2, and contains the following topics:

- [Catalyst Software, page 15-4](#)
- [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:

```
cat6k> enable
```

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

```
cat6k> (enable) set vlan command_and_control_vlan_number
idsm2_slot_number/command_and_control_port_number
```

Example:

```
cat6k> (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:

```
cat6k> 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/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 10.89.149.126
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
cat6k> (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 if you have not yet done so.
For the procedure, see [Initializing the Sensor, page 3-2](#).

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. 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**

Prior to 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 15-7](#)
- [Configuring SPAN, page 15-8](#)
- [Configuring VACLs, page 15-11](#)
- [Configuring the mls ip ids Command, page 15-14](#)

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 15-8](#)
- [Cisco IOS Software, page 15-10](#)

Catalyst Software

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



Note

IDSM-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 IDSM-2, follow these steps:

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

```
cat6k> enable
```

Step 3 Enable SPAN to IDS-M-2:

- From a source port:

```

cat6k> (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

cat6k> (enable)

```



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

- From a VLAN:

```

cat6k> (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

cat6k> (enable)

```

Step 4 Show the SPAN sessions:

```

cat6k> (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
cat6k> (enable)

```

Step 5 To disable the SPAN session that is sending traffic to IDS-M-2:

```

cat6k> (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
cat6k> (enable)

```



Note For more information on SPAN, refer to the appropriate *Catalyst 6500 Series Switch Command Reference*.

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 IDSM-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 IDSM-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 (Optional) To disable the monitor session:

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

Step 6 (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 7 Exit configuration mode:

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

Step 8 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 appropriate *Catalyst 6500 Series Cisco IOS Command Reference*.

Configuring VACLs

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 VACLs, and contains the following topics:

- [Catalyst Software, page 15-12](#)
- [Cisco IOS Software, page 15-13](#)

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.

```
cat6k> enable
```

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

```
cat6k> (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 2/13
Successfully set 2/13 to capture ACL traffic.
```



Note For more information on trunk ports and ACLs, refer to the appropriate *Catalyst 6500 Series Switch Command Reference*.

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 IDS-M-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 IDS-M-2 to monitor all VLANs being routed. If you apply the VACL to a FlexWan2 port, you need to configure IDS-M-2 to monitor all VLANs.

Step 9 Enable the capture function on IDS-M-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
.
.
.
ip access-list extended MATCHALL
permit ip any any
router#
```

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

Catalyst Software

When you are running the Cisco IOS Firewall on the MSFC, you cannot use VACLs to capture traffic for IDSM-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. You will need to 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 will be 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:
`cat6k> 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.
`cat6k> enable`
- Step 9** On the supervisor engine, add the IDSM-2 monitoring port (port 7 or 8) to the VACL capture list:
`cat6k> (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 will be captured. Packets that are permitted by the ACL will be captured. Those denied by the ACL will not be 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 the IDSM-2 to operate in inline mode between two separate VLANs (one VLAN for each side of the IDM-2). To prepare the IDSM-2 for inline mode, you must configure the switch as well as the 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 promiscuous or inline mode, see [Chapter 5, “Configuring Interfaces.”](#)

This section contains the following topics:

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

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

For IPS 5.0(1) you can only configure one IDSM-2 for inline mode between two VLANs. This restriction has been removed for IPS 5.0(2).



Caution

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 will be trunking 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 mode, follow these steps:

Step 1 Log in to the console.

Step 2 Enter privileged mode.

```
cat6k> enable
```

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

```
cat6k (enable)> set vlan vlan_number slot_number/port_number
```

Example:

```
cat6k (enable)> set vlan 651 9/7
cat6k (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):

```
cat6k (enable)> clear trunk slot_number/port_number vlan_range
```

Example:

```
cat6k (enable)> clear trunk 9/7 1-650,652-4094
cat6k (enable)> clear trunk 9/8 1-651,653-4094
```

Step 5 Enable Bpdu spantree filtering on the IDSM-2 monitoring ports:

```
cat6k (enable)> set spantree bpdu-filter 6/7-8 enable
```



Note

For IPS 5.0(2), omit this step.

Cisco IOS Software

**Note**

Cisco IOS software 12.2(18)SXE with Supervisor Engine 720 supports only one IDSM-2 inline between two VLANs.

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

**Note**

Etherchannelling inline IDSM-2 is not yet supported in Cisco IOS.

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** Create two VLANs, one for each side of the inline IDSM-2:
- ```
router(config)# vlan vlan_number
router(config)# name vlan_name
router(config)# exit
router# exit
```
- Step 4** Configure an IOS access port for each interface on each inline VLAN, if you have not done so already:
- Enter global configuration mode:

```
router# configure terminal
```
 - Select the IOS interface to be configured:

```
router(config)# interface interface_name
```
 - Enter a description so you know what the interface is for:

```
router(config-if)# description description
```
 - Configure the interface as a layer 2 switchport:

```
router(config-if)# switchport
```
 - Configure the access mode VLAN:

```
router(config-if)# switchport access vlan vlan_number
```
 - Configure the interface/port to be an access port:

```
router(config-if)# switchport mode access
```
 - Exit global configuration mode:

```
router(config-if)# exit
router# exit
```
- Step 5** Configure one IDSM-2 data port to be on each of the two VLANs you created in Step 3.
- ```
router# configure terminal
router(config)# intrusion-detection module slot_number data-port data_port_number
access-vlan vlan_number
router(config)# exit
```

**Step 6** 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#
```

# Configuring EtherChanneling

This section describes how to configure EtherChanneling on IDSM-2 for Cisco IOS software. It contains the following topics:

- [Overview, page 15-20](#)
- [Enabling EtherChanneling, page 15-20](#)
- [Disabling EtherChanneling, page 15-22](#)
- [Verifying EtherChanneling, page 15-23](#)

## Overview

Supervisor Engines in the Catalyst 6500 series chassis recognize IDSM-2 devices that are running IPS 5.0 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. The EtherChannel feature allows up to eight IDSM-2 devices to participate in the load balancing on either port 7 or port 8.

**Note**

---

EtherChannel load balancing for IDSM-2 is only supported on Cisco IOS software. Instructions for configuring EtherChannel load balancing on IDSM-2 for Cisco Catalyst software will be provided when the Catalyst release to support it is available.

---

## Enabling EtherChanneling

**Note**

---

To configure EtherChannel load balancing on IDSM-2, you must install Cisco IOS 12.2(18)SXE and have Supervisor Engine 720. Cisco IOS only supports promiscuous IDSM-2 EtherChanneling 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. EtherChannel load balancing 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 EtherChannel load balancing, 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 EtherChanneling, refer to *Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.2SX*.

To configure EtherChannel load balancing on IDSM-2, follow these steps:

**Step 1** Configure each IDSM-2 for promiscuous operation.

For the procedure, see [Chapter 5, “Configuring Interfaces.”](#)



**Note** Make sure that all IDSM-2 VACL capture or SPAN or monitor configuration lines have been removed before configuring IDSM-2 EtherChanneling.

**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
```

**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
```

**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
```

**Step 8** For each IDSM-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
```

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 EtherChannel load balancing:

```
router(config)# port-channel load-balance [dst-ip | dst-mac | dst-port | mpls | src-dst-ip
| src-dst-mac | src-dst-port | src-ip | src-mac | src-port]
```

The following options apply:

- **dst-ip**—Destination IP address
- **dst-mac**—Destination MAC address
- **dst-port** —Destination TCP/UDP port
- **mpls**—Load balancing for MPLS packets
- **src-dst-ip**—Source and destination IP address
- **src-dst-mac**—Source and destination MAC address
- **src-dst-port**—Source and destination TCP/UDP port

- **src-ip**—Source IP address
- **src-mac**—Source MAC address
- **src-port**—Source TCP/UDP port

The default 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:

```
cat6k# 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
vian_list
```

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

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

**Step 13** Exit global configuration mode:

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

**Step 14** To save the changes:

```
router# write memory
```

---

## Disabling EtherChanneling

To disable IDS-M-2 EtherChanneling, 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 IDS-M-2 from the EtherChannel:

```
router(config)# no intrusion-detection module module_number data-port data_port_number
channel-group channel_number
```

**Step 4** To remove the whole EtherChannel:



**Note** The VACL capture commands for IDSM-2 will be left.

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

## Verifying EtherChanneling

To verify the IDSM-2 EtherChannel 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: -

cat6k#
```

**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 EtherChannel load balance 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
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 15-24](#)
- [Resetting IDSM-2, page 15-26](#)

## 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 15-24](#)
- [Cisco IOS Software, page 15-25](#)

## 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:

```
cat6k> enable
```

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

```
cat6k> (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.
cat6k> (enable)
```

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

**Step 4** Reset IDSM-2.

For the procedure, see [Resetting IDSM-2, page 15-26](#).

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 15-26](#).

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 15-26](#)
- [Cisco IOS Software, page 15-27](#)

### Catalyst Software

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

- 
- Step 1** Log in to the console.
- Step 2** Enter privileged mode:
- ```
cat6k> enable
```
- Step 3** Reset IDSM-2 to the application partition or the maintenance partition:
- ```
cat6k> (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.

---

The following example shows the output of the **reset** command:

```
cat6k> (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.
cat6k> (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 17-25](#).

---

## Cisco IOS Software



**Note** The reset process takes several minutes.

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

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

**Step 2** Reset IDSM-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), IDSM-2 uses the boot device variable.

This example shows the output of the **reset** command:

```
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 IDSM-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 the *Documentation Roadmap for Cisco Intrusion Prevention System* that shipped with your IDSM-2.

This section contains the following topics:

- [Catalyst Software, page 15-27](#)
- [Cisco IOS Software, page 15-29](#)

## Catalyst Software

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

- [Supported Supervisor Engine Commands, page 15-28](#)
- [Unsupported Supervisor Engine Commands, page 15-29](#)

## Supported Supervisor Engine Commands

IDSM-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 IDSM-2.
- **clear log** *module\_number*  
Deletes all entries in the error log for the specified IDSM-2.
- **session** *slot\_number*  
Logs in to the console of IDSM-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 IDSM-2.
- **set port name** *module\_number*  
Configures the name for the specified IDSM-2 port.
- **set span**  
Configures port 1 as a SPAN destination port. You cannot use port 1 on IDSM-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 IDSM-2.
- **show mac** *module\_number*  
Displays the MAC counters for the specified IDSM-2.
- **show module** *module\_number*  
With an IDSM-2 installed, displays “Intrusion Detection System Module” under Module-Type.
- **show port** *module\_number*  
Displays the port status for the specified IDSM-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 15-30](#)
- [Configuration Commands, page 15-31](#)

## 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 *slot\_number* reset**  
Resets IDSM-2 into the partition specified by the boot device variable; if the boot device variable has not been set, IDSM-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.
- **hw-module module *slot\_number* reset cf:1**  
Resets the module into the maintenance partition.
- **hw-module module *slot\_number* shutdown**  
Shuts down the module so that it can be safely removed from the chassis.
- **reload**  
Reloads the entire switch.
- **session slot *slot\_number* processor *processor\_number***  
Logs in to the console of IDSM-2 from the switch console.
- **show intrusion-detection module *module\_number* data-port *data\_port\_number* state**  
Displays the state of the specified IDSM-2 data port.
- **show intrusion-detection module *module\_number* data-port *data\_port\_number* traffic**  
Displays traffic statistics for IDSM-2 data port traffic.
- **show intrusion-detection module *module\_number* management-port state**  
Displays the state of the IDSM-2 management port.
- **show intrusion-detection module *module\_number* management-port traffic**  
Displays traffic statistics for the IDSM-2 management port.
- **show ip access-lists**  
Displays the current access lists.
- **show module**  
Displays the installed modules, versions, and states.
- **show running-config**  
Displays the configuration that is currently running.
- **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
  - **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/IDSM-2.
  - **intrusion-detection module module\_number management-port access-vlan access\_vlan\_number**  
Configures the access vlan for the IDSM-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 IDSM-2 data port.
  - **ip access-list extended word**  
Creates access lists for use in the VACL maps.
  - **monitor session session {destination {interface interface interface-number} [ , | -] {vlan vlan-id}}**  
Sets the destination for a SPAN session.
  - **monitor session session {source {interface interface interface-number} | {vlan vlan-id}} [ , | - | rx | tx | both]**  
Sets the sources for a SPAN session.
  - **no power enable module slot\_number**  
Shuts down IDSM-2 and removes power.
  - **power enable module slot\_number**  
Turns on the power for IDSM-2 if it is not already on.
  - **vlan access-map map\_name\_sequence**  
Creates the VACL maps.
  - **vlan filter map\_name vlan-list vlans**  
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 *vlan***  
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 submenu
  - **action forward capture**  
Designates that matched packets should be captured.
  - **match ip address [*1-199* | *1300-2699* | *acl\_name*]**  
Specifies filtering in the VACL.