



CHAPTER 15

Cisco Switch Devices

You can manage Cisco switches that run either CatOS or Cisco IOS Software Release 12.2 or later. The configuration of the switch varies between these two operating system, as does the addition of the device in MARS. Adding a Cisco switch involves three steps:

1. Configure the switch to enable MARS to discover the its settings.
2. Configure the switch to generate the data required by MARS.
3. Add and configure the switch in MARS.
4. Add modules to the switch.

To prepare a Cisco switch running Cisco IOS Software Release 12.2 or later, refer to the following procedures:

- [Enable Administrative Access to Devices Running Cisco IOS 12.2 and Later, page 17-1](#)
- [Configure the Device Running Cisco IOS 12.2 and Later to Generate Required Data, page 17-2](#)

To prepare a Cisco switch running CatOS, refer to the following procedures:

- [Enable Communications Between Devices Running CatOS and MARS, page 15-1](#)
- [Configure the Device Running CatOS to Generate Required Data, page 15-3](#)

Adding a Cisco switch running to MARS has two distinct steps. First, you add the base module of the switch, providing administrative access to that device. Second, you add any modules that are running in the switch. For instructions on performing these two steps, refer to the following topics:

- [Add and Configure a Cisco Switch in MARS, page 15-6](#)
- [Adding Modules to a Cisco Switch, page 15-8](#)

Enable Communications Between Devices Running CatOS and MARS

Before you add a Cisco switch running CatOS to MARS, make sure that you have enabled SNMP, Telnet, SSH, or FTP access to the switch. First, you must configure the MARS Appliance as an IP address that is permitted to access the switch.

For information on permitting IP addresses and specifying the access type, see the following URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/ip_perm.html

Next, you must ensure that your switch is configured to enable the correct access method.

This section contains the following topics:

- [Enable SNMP Administrative Access, page 15-2](#)
- [Enable Telnet Administrative Access, page 15-2](#)
- [Enable SSH Administrative Access, page 15-2](#)
- [Enable FTP-based Administrative Access, page 15-2](#)

Enable SNMP Administrative Access

To enable configuration discovery using SNMP access to the Cisco switch, refer to your device documentation or the following URL:

IP Access

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/ip_perm.html

Configure SNMP

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/snmp.html>

Enable Telnet Administrative Access

To enable configuration discovery using Telnet access to the Cisco switch, refer to your device documentation or the following URL:

IP Access

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/ip_perm.html

Enable SSH Administrative Access

To enable configuration discovery using SSH access to the Cisco router or switch, refer to your device documentation or the following URL:

IP Access

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/ip_perm.html

Enable FTP-based Administrative Access

To enable configuration discovery using FTP access, you must place a copy the Cisco router's or switch's configuration file on an FTP server to which the MARS Appliance has access. This FTP server must have user authentication enabled.

**Note**

TFTP is not supported. You must use an FTP server.

You must copy the running configuration from the Cisco switch. For information on copying the running configuration, refer to your device documentation or the following URL:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/cli.html#wp10227391>

Configure the Device Running CatOS to Generate Required Data

You can configure the following message types:

- Syslog message
- SNMP RO or RW strings
- NAC messages (802.1x)
- L2 discover settings

This section contains the following topics:

- [Enable Syslog Messages on CatOS, page 15-3](#)
- [Enable SNMP RO/RW Strings on CatOS, page 15-4](#)
- [Enable NAC-specific Messages, page 17-4](#)
- [Enable L2 Discovery Messages, page 15-6](#)

Enable Syslog Messages on CatOS

To configure a Cisco switch running CatOS to send syslog information to MARS, follow these steps:

Step 1 To enable the syslog server on the switch, enter:

```
set logging server enable
```

Step 2 To identify the MARS Appliance as a destination for syslog messages, enter the following command:

```
set logging server <IP address of MARS Appliance>
```

Step 3 The remaining commands tell the switch what kinds of logging information to provide and at what level. The commands in the following example can be changed to suit your requirements.

```
set logging level cdp 7 default
set logging level mcast 7 default
set logging level dtp 7 default
set logging level dvlan 7 default
set logging level earl 7 default
set logging level fddi 7 default
set logging level ip 7 default
set logging level pruning 7 default
set logging level snmp 7 default
set logging level spantree 7 default
set logging level sys 7 default
set logging level tac 7 default
set logging level tcp 7 default
set logging level telnet 7 default
set logging level tftp 7 default
set logging level vtp 7 default
set logging level vmps 7 default
set logging level kernel 7 default
```

```

set logging level filesys 7 default
set logging level drip 7 default
set logging level pagp 7 default
set logging level mgmt 7 default
set logging level mls 7 default
set logging level protfilt 7 default
set logging level security 7 default
set logging server facility SYSLOG
set logging server severity 7
set logging buffer 250
set logging timestamp enable

```

Enable SNMP RO/RW Strings on CatOS

If the supervisor SNMP server is not configured, you must perform this procedure.

To configure the supervisor SNMP server and enabled SNMP traps on the Catalyst switch, follow these steps:

-
- Step 1** Enter configuration mode:
- ```

switch> enable
Enter password: <password>
switch> (enable)

```
- Step 2** Set the SNMP read community string as follows:
- ```

switch> (enable) set snmp community read-only <read community>

```
- Step 3** Set the SNMP write community string as follows:
- ```

switch> (enable) set snmp community read-write <write community>
switch> (enable) set snmp community read-write-all <write community>

```
- Step 4** To collect RMON Ethernet statistics, RMON data collection must be enabled in the CatOS agent (this is not required in Native IOS). To enable RMON collection, enter the following:
- ```

switch> (enable) set snmp rmon enable

switch> (enable) set snmp rmon enable

```
- Step 5** Exit configuration mode as follows:
- ```

switch> (enable) exit

```
- 

## Enable NAC-specific Messages

Cisco routers and switches that are running Cisco IOS Software release 12.2 and later or CatOS can enable network Admission Control (NAC) specific data. This data includes:

- **Client logs.** These logs relate the activities of the client software.
- **RADIUS server logs.** These logs relate the authorization communications between clients and the posture validation servers.

- **Network access device logs.** These logs relate connection attempts by clients and final authorizations provided by the AAA server enforcing the NAC policies.

For more information on the events that are logged as part of NAC, see the *Monitoring and Reporting Tool Integration into Network Admission Control* white paper at the following URL:

[http://www.cisco.com/en/US/netsol/ns617/networking\\_solutions\\_white\\_paper0900aecd801dee49.shtml](http://www.cisco.com/en/US/netsol/ns617/networking_solutions_white_paper0900aecd801dee49.shtml)

This section contains the topics that address the NAC configuration settings specific to each device type.

This section contains the following topics:

- [Enable NAC Support in Cisco Switches, page 15-5](#)

## Enable NAC Support in Cisco Switches

NAC Phase II enables Cisco switches to act as network access devices. To support this new feature, you must configure the Cisco switch to initiate 802.1x authentication when the link state changes from down to up and periodically if the port remains up but unauthenticated. NAC requires that hosts use 802.1x supplicants, or clients, to authenticate to the Cisco Secure ACS server before gaining access to network services. Enabling the 802.1x messages on your network helps you troubleshoot supplicant failures because connection attempts are logged, which you can analyze.

Configuring the Cisco switch to act as proxy between the Cisco Secure ACS server and the 802.1x supplicants is a multi-step process. First, the switch must be defined as a AAA client (RADIUS) in the Cisco Secure ACS server. For information on defining a AAA client, see [Define AAA Clients, page 26-6](#). Second, the switch must be configured to use a RADIUS server. Then, you must enable the following features on each interface installed in the switch:

- **802.1X port-based authentication.** The device requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the system by using the client's MAC address.
- **802.1x reauthentication.** The device re-authenticates the supplicants after the reauthentication timeout value is reached, which is 3600 seconds by default.
- **802.1x accounting.** The device logs authentication successes and failures, as well as link down events and users logging off. The switch publishes these audit records to the Cisco Secure ACS server for logging.
- **DHCP snooping.** The device filters DHCP requests, safeguarding against spoof attacks. This feature ensures that MARS receives reliable data and identifies the port number of the 802.1x supplicant.

The following URLs detail how to configure these features:

### Dot1x and Radius Sever

#### IOS Software:

[http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2\\_25\\_sec/configuration/guide/sw8021x.html](http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_sec/configuration/guide/sw8021x.html)

#### CatOS Software:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/8021x.html>

### DHCP Snooping

**IOS Software:**

[http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2\\_25\\_sec/configuration/guide/swdhcp82.html](http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_sec/configuration/guide/swdhcp82.html)

**CatOS Software:**

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/dhcp.html>

After you configure the switch to act as proxy and it is defined as a AAA client in Cisco Secure ACS, you must ensure that the authentication messages are sent to the MARS Appliance. For 802.1x accounting records, you must ensure that the audit records are written to the RADIUS log on the Cisco Secure ACS server. To configure these settings, refer to [Configure Cisco Secure ACS 4.x to Generate Logs, page 26-3](#) or [Configure Cisco Secure ACS 3.x to Generate Logs, page 26-4](#).

## Enable L2 Discovery Messages

To enable L2 discovery on your Cisco switches, you must enable the spanning tree protocol (STP) and provide the SNMP RO community string. All L 2 devices must support SNMP STP MIB (IETF RFC 1493). The discovered information includes interfaces, Layer 3 (L3) routes, L2 spanning trees, L2 forwarding tables, MAC addresses, and so on.

**Note**

STP is enabled by default on all Cisco switches. Therefore, unless you have altered this setting, no changes are necessary.

For more information on configuring STP, select **Spanning Tree Protocol** in the View Documents by Topics list at the following URL:

[http://www.cisco.com/en/US/partner/products/hw/switches/ps708/prod\\_configuration\\_examples\\_list.html](http://www.cisco.com/en/US/partner/products/hw/switches/ps708/prod_configuration_examples_list.html)

## Add and Configure a Cisco Switch in MARS

MARS monitors Cisco switches running either CatOS or Cisco IOS 12.2 and later.

To add the configuration information that MARS uses to monitor a Cisco switch running Cisco IOS 12.2 and later, follow these steps:

- 
- Step 1** Select **Admin > System Setup > Security and Monitor Devices > Add**.
- Step 2** Do one of the following:
- If the switch is running any version of CatOS, select **Cisco Switch-CatOS ANY** from the Device Type list.
  - If the switch is running Cisco IOS 12.2 or later, select one of the following options from the Device Type list:
    - **Cisco IOS 12.2**
    - **Cisco IOS 12.3**
    - **Cisco IOS 12.4**
- Step 3** Enter the name of the device in the Device Name field.

MARS maps this name to the reporting IP address. This name is used in topology maps, queries, and in the Security and Monitoring Device list. For devices that support the discovery operation, such as routers and firewalls, MARS renames this field's value to match the name discovered in the device configuration, which typically uses the *hostname.domain* format. For devices that cannot be discovered, such as Windows and Linux hosts and host applications, MARS uses the provided value.

**Step 4** (Optional) To enable MARS to discover settings from this device, enter the administrative IP address in the Access IP field.

To learn more about the access IP address, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#).

**Step 5** Enter the IP address of the interface that publishes syslog messages, SNMP notifications, NetFlow MIBs, or any combination of the three, in the Reporting IP field.

To learn more about the reporting IP address, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#).

**Step 6** If you entered an address in the Access IP field, select **SNMP**, **TELNET**, **SSH**, or **FTP** from the Access Type list, and continue with the procedure that matches your selection:

- [Configure SNMP Access for Devices in MARS, page 1-13](#)
- [Configure Telnet Access for Devices in MARS, page 1-13](#)
- [Configure SSH Access for Devices in MARS, page 1-13](#)
- [Configure FTP Access for Devices in MARS, page 1-14](#)

For more information on determining the access type, see [Selection of the Access Type, page 1-11](#).

**Step 7** (Optional) To enable MARS to retrieve MIB objects for this reporting device, enter the device's read-only community string in the SNMP RO Community field.



**Note** To perform mitigation, MARS uses the SNMP Set commands, which require SNMP RW access to a Cisco router or Cisco switch. If you define an SNMP RW string in the SNMP RO Community field, then you do not also need to define an SNMP RO string, as the RW community string enables SNMP Gets (RO) as well.

Before you can specify the SNMP RO string, you must define an access IP address. MARS uses the SNMP RO string to read MIBs related to a reporting device's CPU usage, network usage, and device anomaly data and to discover device and network settings.

**Step 8** (Optional) To enable MARS to monitor this device for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

MARS monitors the device for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports. For more information, see [Configuring Resource Usage Data, page 1-21](#).

**Step 9** (Optional) If you defined an access IP and selected and configured an access type, click **Discover** to determine the device settings

If the username and password are correct and the MARS Appliance is configured as an administrative host for the device, the "Discovery is done." dialog box appears when the discovery operation completes. Otherwise, an error message appears. After the initial pull, the MARS Appliance pulls based on the schedule that you define. For more information, see [Scheduling Topology Updates, page 1-18](#).

**Step 10** To add this device to the MARS database, click **Submit**.

The submit operation records the changes in the database tables. However, it does not load the changes into working memory of the MARS Appliance. The activate operation loads submitted changes into working memory.

**Step 11** Click **Activate**.

MARS begins to sessionize events generated by this device and evaluate those events using the defined inspection and drop rules. Any events published by the device to MARS before activation can be queried using the reporting IP address of the device as a match criterion. For more information on the activate action, see [Activate the Reporting and Mitigation Devices, page 1-15](#).

After submitting, you can add modules. See [Adding Modules to a Cisco Switch, page 15-8](#).

---

## Adding Modules to a Cisco Switch

In MARS, you can represent, discover, and monitor modules that are installed in Cisco switches. These modules perform special purpose security functions for the switch, such as firewall or intrusion detection and prevention. MARS recognizes the following switch modules and versions:

- Cisco FWSM 1.1, 2.2, 2.3, 3.1, and 3.2
- Cisco IDS 3.1 and 4.0
- Cisco IPS 5.x and 6.x
- Cisco IOS 12.2, 12.3, and 12.4

To add a module, you must first add the base module, which is the Cisco switch. After the base module is defined in the web interface, you can discover the modules that are installed in the switch (click **Add Available Module** ) or add them manually (click **Add Module** ).

For instructions on adding and configuring a firewall services module (FWSM), see [Cisco Firewall Devices \(PIX, ASA, and FWSM\), page 19-1](#).

For instructions on adding and configuring an intrusion detection or prevention services module (IDSM or IPSM), see [Chapter 9, “Cisco IPS Modules”](#).

This section contains the following topics:

- [Add Available Modules, page 15-8](#)
- [Add Cisco IOS Modules Manually, page 15-9](#)

## Add Available Modules

When you perform a discovery operation on a base module, MARS lists the discovered modules. From this list, you can select the modules to monitor using MARS.

To add available modules, follow these steps:

---

**Step 1** Click **Add Available Module**.

The screenshot shows a web interface for managing modules. At the top, there are four buttons: "Add Module", "Edit Module", "Remove Module", and "Add Available Module". Below these buttons is a table with two columns: "Module Name" and "Module Type". The table contains two rows of data, each with a checkbox in the first column:

| Module Name                           | Module Type    |
|---------------------------------------|----------------|
| <input type="checkbox"/> HQ-SW-1-msfc | Cisco IOS 12.2 |
| <input type="checkbox"/> HQ-SW-1-idsm | Cisco IDS 3.1  |

On the right side of the interface, the number "143216" is displayed vertically.

If modules are installed in the switch, a list of the modules appears.

**Step 2** Select a module from the Select list.

**Step 3** Click **Add**.

**Step 4** Repeat for other modules.

**Step 5** After you add the desired modules, verify the configuration information of each. For example, verify that the SNMP RO community string matches that defined for use by MARS. To verify these settings, select a module and click **Edit Module**.

Basic guidance for editing these settings can be found in the topics that discuss manually adding these modules. See the following topics for more information:

- [Add Cisco IOS Modules Manually, page 15-9](#)
- [Cisco Firewall Devices \(PIX, ASA, and FWSM\), page 19-1](#)
- [Chapter 9, “Cisco IPS Modules”](#).

**Step 6** To add these modules to the base module defined in the MARS database, click **Submit**.

The submit operation records the changes in the database tables. However, it does not load the changes into working memory of the MARS Appliance. The activate operation loads submitted changes into working memory.

**Step 7** Click **Activate**.

MARS begins to sessionize events generated by this device and the selected modules and evaluate those events using the defined inspection and drop rules. Any events published by the device or its modules to MARS before activation can be queried using the reporting IP address of the device or module as a match criterion. For more information on the activate action, see [Activate the Reporting and Mitigation Devices, page 1-15](#).

## Add Cisco IOS Modules Manually

To add a module manually, follow these steps:

**Step 1** Click **Add Module**.

**Step 2** Select one of the following options from the Device Type list:

- **Cisco IOS 12.2**
- **Cisco IOS 12.3**
- **Cisco IOS 12.4**

Device Type: Cisco IOS 12.2

\*Device Name: \_\_\_\_\_

Access IP: \_\_\_\_\_

Reporting IP: \_\_\_\_\_

\*Access Type: 3DES

Login: \_\_\_\_\_

Password: \_\_\_\_\_

Enable Password: \_\_\_\_\_

Config Path: \_\_\_\_\_

File Name: \_\_\_\_\_

SNMP RO Community: \_\_\_\_\_

Monitor Resource Usage: NO

143207

**Step 3** Enter the name of the module in the Device Name field.

MARS maps this name to the reporting IP address. This name is used in topology maps, queries, and in the Security and Monitoring Device list. For modules that support the discovery operation, such as router and firewall modules, MARS renames this field's value to match the name discovered in the device configuration, which typically uses the *hostname.domain* format.

**Step 4** (Optional) To enable MARS to discover settings from this device, enter the administrative IP address in the Access IP field.

To learn more about the access IP address, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#).

**Step 5** Enter the IP address of the interface that publishes syslog messages, SNMP notifications, NetFlow MIBs, or any combination of the three, in the Reporting IP field.

To learn more about the reporting IP address, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#).

**Step 6** If you entered an address in the Access IP field, select **SNMP**, **TELNET**, **SSH**, or **FTP** from the Access Type list, and continue with the procedure that matches your selection:

- [Configure Telnet Access for Devices in MARS, page 1-13](#)
- [Configure SSH Access for Devices in MARS, page 1-13](#)
- [Configure FTP Access for Devices in MARS, page 1-14](#)

For more information on determining the access type, see [Selection of the Access Type, page 1-11](#).

**Step 7** (Optional) To enable MARS to retrieve MIB objects for this reporting device, enter the device's read-only community string in the SNMP RO Community field.



**Note** To perform mitigation, MARS uses the SNMP Set commands, which require SNMP RW access to a Cisco router or Cisco switch. If you define an SNMP RW string in the SNMP RO Community field, then you do not also need to define an SNMP RO string, as the RW community string enables SNMP Gets (RO) as well.

Before you can specify the SNMP RO string, you must define an access IP address. MARS uses the SNMP RO string to read MIBs related to a reporting device's CPU usage, network usage, and device anomaly data and to discover device and network settings.

- Step 8** (Optional) To enable MARS to monitor this device for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

MARS monitors the module for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports. For more information, see [Configuring Resource Usage Data, page 1-21](#).

- Step 9** (Optional) If you defined an access IP and selected and configured an access type, click **Discover** to determine the module settings.

If the username and password are correct and the MARS Appliance is configured as an administrative host for the module, the "Discovery is done." dialog box appears when the discovery operation completes. Otherwise, an error message appears. After the initial pull, the MARS Appliance pulls based on the schedule that you define. For more information, see [Scheduling Topology Updates, page 1-18](#).

- Step 10** To add this module to the device in the MARS database, click **Submit**.

The submit operation records the changes in the database tables. However, it does not load the changes into working memory of the MARS Appliance. The activate operation loads submitted changes into working memory.

---

