CHAPTER 4

Configuring Router and Switch Devices

Revised: November 10, 2007

This chapter describes how to bootstrap routers and switches and add those reporting devices and mitigation devices to MARS. It also describes how to configure NetFlow, NAC's EAP over UDP and 802.1x logging, and the Layer 2 (L2) mitigation features of switches.

Routers and switches provide MARS with data about traffic flows and the network topology, including address translations, endpoint devices, connected networks, and accepted and rejected sessions. Routers and switches also support modules that enable features common to specialty security appliances, such as firewalls and intrusion detection or prevention systems (IDS/IPS). This chapter does not describe how to enable the features on routers and switches that enable the modules or how to configure these modules for use by MARS. Such discussions are provided in Configuring Firewall Devices, page 5-1, and Configuring Network-based IDS and IPS Devices, page 7-1.

This chapter explains how to bootstrap and add the following router and switch devices to MARS:

Cisco Router Devices

To configure Cisco routers running Cisco IOS Software Release 12.2 and later to communicate with a MARS Appliance, you must perform three tasks:

Enable Administrative Access to Devices Running Cisco IOS 12.2 and Later

You must enable administrative access by the MARS Appliance to any Cisco routers or switches running Cisco IOS Software release 12.2 and later. The type of access that you must enable depends on whether modules are installed in your Cisco router or switch and the role of the device in your network. MARS

uses this administrative access to discover the device's configuration and, at times, to make changes to the device's running configuration. For information on selecting an administrative access method, see Selecting the Access Type, page 2-10.

Before you add a Cisco router to MARS, make sure that you have enabled SNMP, Telnet, SSH, or FTP access to the router. The following sections provide guidance on configuring each supported access method:

Enable SNMP Administrative Access

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

http://cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html

Enable Telnet Administrative Access

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

http://cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_example09186a0080204528.shtml

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:

http://cisco.com/en/US/docs/ios/12_1t/12_1t1/feature/guide/sshv1.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 router or switch. For information on copying the running configuration, refer to your device documentation or the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_tech_note09186a008020260d.shtml

Configure the Device Running Cisco IOS 12.2 and Later to Generate Required Data

Cisco routers and switches that are running Cisco IOS Software release 12.2 and later can be configured to provide different types of data to MARS:

- **Syslog messages.** The syslog messages provide information about activities on the network, including accepted and rejected sessions.
- **SNMP traffic.** SNMP RO community strings support the discovery of your network's topology.
- **NAC-specific data.** NAC logs events that are specific to its configuration, including Extensible Authentication Protocol (EAP) over UDP messages and 802.1x accounting messages.
- **Access lists or NAT statements.** You must enable SSH or Telnet access if the configuration on the Cisco router or swtich includes access lists or NAT statements.
- **Spanning tree messages** (Switch only). You must have STP (spanning tree protocol) configured correctly on the switches to enable L2 discovery and mitigation. STP provides MARS with access to the L2 MIB, which is required to identify L2 re-routes of traffic and to perform L2 mitigation. MARS also uses the MIB to identify trunks to other switches, which are used to populate VLAN information used in L2 path calculations. STP, which is enabled by default on Cisco Switches, should remain enabled, as it is required for L2 mitigation.

The following topics describe how to configure these settings:

- Enable Syslog Messages, page 4-3
- Enable SNMP RO Strings, page 4-3
- Enable NAC-specific Messages, page 4-4
- Enable L2 Discovery Messages, page 4-12
- Enable SDEE for IOS IPS Software, page 4-6

Enable Syslog Messages

To send syslog messages to the MARS Appliance from a device running Cisco IOS Software Release 12.2 and later, follow these steps:

Step 1 Log in to the Cisco IOS device with enabled password.

Step 2 Enter the commands:

```
Router(config)#logging source-interface <interface name>
Router(config)#logging trap <logging level desired>
Router(config)#logging <IP address of MARS Appliance>
```

Enable SNMP RO Strings

To enable SNMP RO strings for topology discovery on the Cisco IOS device, you must enable the SNMP server and define the RO community.

To configure the SNMP RO string settings, follow these steps:

Step 1 Enter configuration mode:

```
Router> enable
Password: <password>
Router#
```

Step 2 Enter the **configure terminal** command to enter configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Step 3 Set the SNMP read community string as follows:

```
Router(config)# snmp-server community <read community>  RO <ACL name if required>
```

Note This information is required to retrieve the MAC addresses and associated L2 information.

Step 4 Set the SNMP write community string as follows:

```
Router(config)# snmp-server community <write community> RW
```

The Add and Configure a Cisco Router in MARS procedure provides instructions for configuring the MARS Appliance to discover configuration and settings using these strings

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

This section contains the following two topics, which address the NAC configuration settings specific to each device type:

- Cisco Routers, page 4-4
- Cisco Switches, page 4-5

Cisco Routers

This command ensures that the IOS device sends the IP address of the host that is being NAC'd in its calling-station-id attribute in all RADIUS requests to the ACS.

To configure the NAC Phase I data on a Cisco router to work with MARS, you must allow EAP over UDP and allow an IP address in the AAA station-id field of the packets. (Cisco Secure ACS includes this detail in its logs. MARS presents this data in reports and queries that dispay the host IP addresses.) In addition, you must enable logging of these events, which are published as syslog messages.

To enable the NAC-specific data on a Cisco router, enter the following commands:

```
Router(config)#eou allow ip-station-id
Router(config)#eou logging
```

For more information on these commands and related commands, see the Network Admission Control feature document at the following URL:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_net_admssn_ctrl_ps6350_TSD_Products_Configuration_Guide_Chapter.html

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 becauise 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 e 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 15-5. Second, the switch must be configured to use a 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

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

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 toConfigure Cisco Secure ACS to Generate Logs, page 15-3.

Enable SDEE for IOS IPS Software

Before you enable SDEE, you must enable either Telnet or SSH as the access type for configuration discovery on a Cisco IOS device. You must also enable SDEE on the device that supports the IOS IPS software feature. SDEE is used to publish events to MARS about signatures that have fired.

To enable SDEE protocol on the Cisco IOS device that supports IOS IPS, follow these steps:

Step 1 Log in to the Cisco IOS device using the enable password.

Step 2 Enter the following commands to enable MARS to retrieve events from the IOS IPS software:

```
Router(config)#ip http secure-server
Router(config)#ip ips notify sdee
Router(config)#ip sdee subscriptions 3
Router(config)#ip sdee events 1000
Router(config)#no ip ips notify log
```

Note The “no ips notify log” causes the IOS IPS software to stop sending IPS events over syslog.

Add and Configure a Cisco Router in MARS

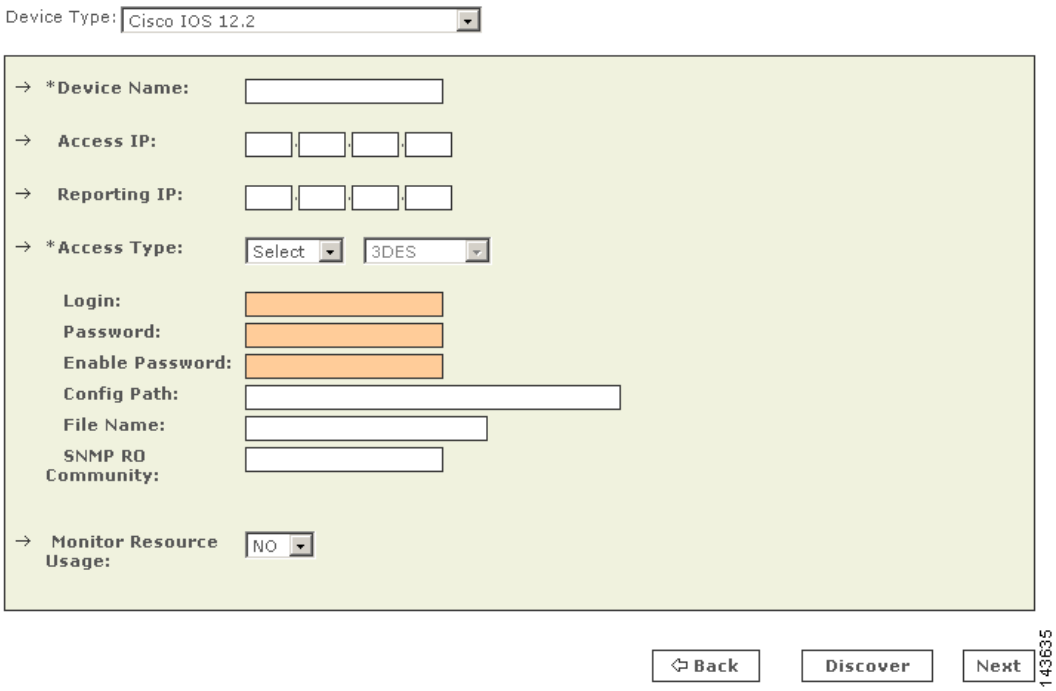
Cisco routers provide data about the network and its activities in the form of syslog messages and SNMP RO MIBs. In addition, MARS can discover settings, such as network address translations, attached networks, and active access rules, that improve the accuracy of false positive identification, attack path analysis, and L3 network discovery.

To add a Cisco router running Cisco IOS 12.2 and later, follow these steps:

Step 1 Select **Admin > System Setup > Security and Monitor Devices > Add**.

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**



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 2-8.

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 2-8.

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 2-11
- Configure Telnet Access for Devices in MARS, page 2-12
- Configure SSH Access for Devices in MARS, page 2-12
- Configure FTP Access for Devices in MARS, page 2-12

For more information on determining the access type, see Selecting the Access Type, page 2-10.

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.

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.

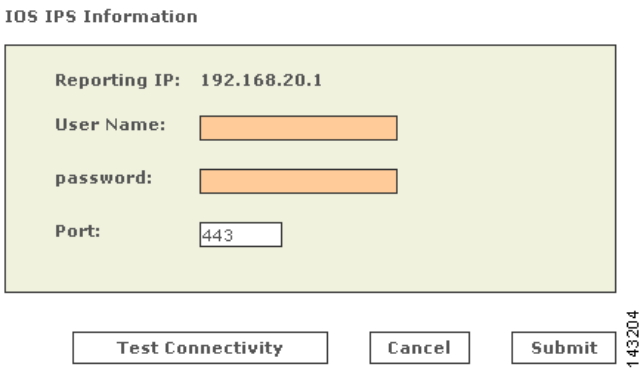
Step 8 (Optional) To enable MARS to monitor this device for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

Result: 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 2-42.

Step 9 (Optional) If this router has the IOS IPS feature and SDEE access enabled and you have configured the router to accept HTTPS connections from the MARS Appliance, click **Add IPS** to provide the username and password required to pull SDEE events.

Note IOS IPS does *not* refer to an IPS module. It refers to a software feature in the IOS software.

Result: The IOS IPS Information page appears.



a. Enter the username that has HTTPS access to this device in the User Name field.

b. Enter the corresponding password in the Password field.

c. In the Port field, verify the port used for SDEE communications with this device.

   MARS pulls data using SDEE over HTTPS. The default port number for HTTPS/SDEE is 443. This access allows MARS to retrieve XML files that contain the events generated by the IOS IPS feature.

   Result: MARS can query the router for SDEE events.

Step 10 (Optional) If you defined an access IP and selected and configured an access type, click **Discover** to determine the device settings, including the IOS IPS settings.

Result: 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 2-40.

Step 11 To add this device to the MARS database, click **Submit**.

Result: 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 12 Click **Activate**.

Result: 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 2-28.

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 4-1
- Configure the Device Running Cisco IOS 12.2 and Later to Generate Required Data, page 4-3

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

- Enable Communications Between Devices Running CatOS and MARS, page 4-9
- Configure the Device Running CatOS to Generate Required Data, page 4-11

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 4-13
- Adding Modules to a Cisco Switch, page 4-14

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 swtich. First, you must configure the MARS Appliance as an IP address that is permited 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/6.x/configuration/guide/ip_perm.html#wp1019819

Next, you must ensure that your switch is configured to enable the correct access method. The following sections provide guidance on configuring each supported access method:

- Enable SNMP Administrative Access, page 4-10
- Enable Telnet Administrative Access, page 4-10
- Enable SSH Administrative Access, page 4-10

- Enable FTP-based Administrative Access, page 4-10

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#wp1019913

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#wp1019893

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#wp1022739l

Configure the Device Running CatOS to Generate Required Data

You can configure the following message types:

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

For information on configuring these settings, refer to the following topics:

- Enable SNMP RO Strings on CatOS, page 4-11
- Enable NAC-specific Messages, page 4-4
- Enable L2 Discovery Messages, page 4-12
- Enable Syslog Messages on CatOS, page 4-11

Enable SNMP RO 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
```

Step 5 Exit configuration mode as follows:

```
switch> (enable) exit
```

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 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, see the section, **Spanning Tree Protocol** at the following URL:

http://www.cisco.com/en/US/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 2-8.

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 2-8.

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 2-11
- Configure Telnet Access for Devices in MARS, page 2-12
- Configure SSH Access for Devices in MARS, page 2-12
- Configure FTP Access for Devices in MARS, page 2-12

For more information on determining the access type, see Selecting the Access Type, page 2-10.

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.

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.

Result: 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 2-42.

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

Result: 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 2-40.

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

Result: 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**.

Result: 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 2-28.

After submitting, you can add modules. See Adding Modules to a Cisco Switch, page 4-14.

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 5-1.

For instructions on adding and configuring an intrusion detection or prevention services module (IDSM or IPSM), see Cisco IPS Modules, page 8-16.

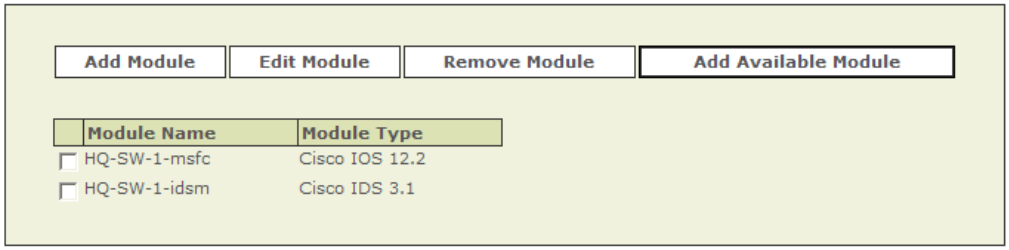
This section contains the following topics:

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.**



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 4-15
- Cisco Firewall Devices (PIX, ASA, and FWSM), page 5-1
- Cisco IPS Modules, page 8-16.

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

Result: 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**.

Result: 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 2-28.

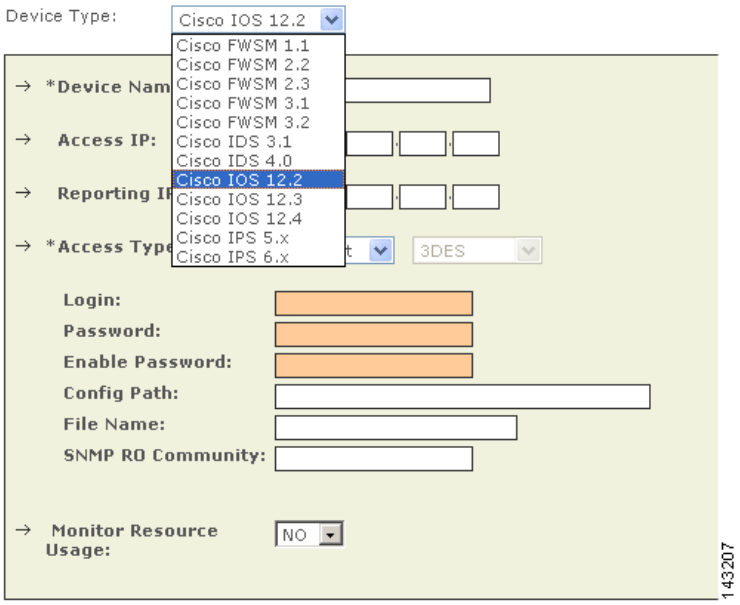
Add Cisco IOS Modules Manually

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**



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 2-8.

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 2-8.

Step 6 If you entered an address in the Access IP field, select **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 2-12
- Configure SSH Access for Devices in MARS, page 2-12
- Configure FTP Access for Devices in MARS, page 2-12

For more information on determining the access type, see Selecting the Access Type, page 2-10.

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.

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.

Result: 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 2-42.

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

Result: 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 2-40.

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

Result: 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.

Extreme ExtremeWare 6.x

MARS can use Extreme ExtremeWare switches to enforce L2 mitigation. To configure MARS to communicate with an ExtremeWare switch, you must configure the switch to publish SNMP notifications to the MARS Appliance. In addition, you must add and configure the switch in the web interface.

This section contains the following topics:

Configure ExtremeWare to Generate the Required Data

To bootstrap an ExtremeWare switch, you must configure two features. First, you must configure the switch to send syslog messages to the MARS Appliance. Next, you must configure the SNMP RO community for MARS to access available L2 information.

To prepare the ExtremeWare device to generate the data required by MARS, follow these steps:

Step 1 For syslog configuration, add this command:

```
configure syslog add <MARS's IP address> local7 debug
enable syslog
```

Step 2 For SNMP configuration add these commands:

```
enable snmp dot1dTpFdbTable
configure snmp delete community readonly all
configure snmp delete community readwrite all
configure snmp add community readonly encrypted <encrypted community string>
configure snmp add community readwrite encrypted <encrypted community string>
```

Add and Configure an ExtremeWare Switch in MARS

To add and configure an ExtremeWare switch in MARS, follow these steps:

Step 1 Select **Admin > System Setup > Security and Monitor Devices > Add**.

Step 2 Select **Extreme ExtremeWare 6.x** from the Device Type list.

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 2-8.

Step 5 Enter the IP address of the interface that publishes syslog messages, SNMP notifications, or both 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 2-8.

Step 6 If you entered an address in the Access IP field, select **SNMP** from the Access Type list.

For more information on understanding the access type, see Selecting the Access Type, page 2-10.

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.

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

Result: 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 9 Click **Activate**.

Result: 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.

Generic Router Device

You can add any L2 or L3 device to the MARS as long as SNMP is enabled on the device. A generic router refers to any L2 or L3 device that is not listed in the *Supported Devices and Software Versions for CS-MARS Local Controller 4.1*.

Add and Configure a Generic Router in MARS

To add and configure a generic router device in MARS, follow these steps:

Step 1 Select **Admin > System Setup > Security and Monitor Devices > Add**.

Step 2 Select **Generic Router version unknown** from the Device Type list.

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 2-8.

Step 5 Enter the IP address of the interface that publishes syslog messages, SNMP notifications, or both 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 2-8.

Step 6 If you entered an address in the Access IP field, select **SNMP** from the Access Type list.

For more information on understanding the access type, see Selecting the Access Type, page 2-10.

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.

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

Result: 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 9 Click **Activate**.

Result: 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.