



CHAPTER 17

Cisco Routers

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 [Chapter 19, "Configuring Cisco Firewall Devices"](#), and [Chapter 2, "Configuring Network-based IDS and IPS 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.

This chapter contains the following topics:

- [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](#)
- [Add and Configure a Cisco Router in MARS, page 17-5](#)

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 [Selection of the Access Type, page 1-11](#).

Before you add a Cisco router to MARS, make sure that you have enabled SNMP, Telnet, SSH, or FTP access to the router. This topic contains guidance on configuring each supported access method.

This section contains the following topics:

- [Enable SNMP Administrative Access, page 17-2](#)
- [Enable Telnet Administrative Access, page 17-2](#)

- [Enable SSH Administrative Access, page 17-2](#)
- [Enable FTP-based Administrative Access, page 17-2](#)

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://www.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://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml

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 switch 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.

This section organizes the topics that describe how to configure these settings.

This section contains the following topics:

- [Enable Syslog Messages, page 17-3](#)
- [Enable SNMP RO Strings, page 17-3](#)
- [Enable NAC-specific Messages, page 17-4](#)
- [Enable SDEE for IOS IPS Software, page 17-5](#)

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, page 17-5](#) 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 topics that address the NAC configuration settings specific to each device type.

This section contains the following topics:

- [NAC on Cisco Routers, page 17-4](#)

NAC on 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 display 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, review the Network Admission Control feature document at the following URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_nac.html

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

Device Type:

→ *Device Name:

→ Access IP:

→ Reporting IP:

→ *Access Type:

 Login:

 Password:

 Enable Password:

 Config Path:

 File Name:

 SNMP RO Community:

→ Monitor Resource Usage:

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 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.

IOS IPS Information

Reporting IP: 192.168.20.1

User Name:

password:

Port:

143204

- Enter the username that has HTTPS access to this device in the User Name field.
- Enter the corresponding password in the Password field.
- 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.

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.

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 11 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 12 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](#).
