Management Plane Protection

First Published: February 27, 2006
Last Updated: February 27, 2006

The Management Plane Protection (MPP) feature in Cisco IOS software provides the capability to restrict the interfaces on which network management packets are allowed to enter a device. The MPP feature allows a network operator to designate one or more router interfaces as management interfaces. Device management traffic is permitted to enter a device only through these management interfaces. After MPP is enabled, no interfaces except designated management interfaces will accept network management traffic destined to the device.

Restricting management packets to designated interfaces provides greater control over management of a device, providing more security for that device. Other benefits include improved performance for data packets on nonmanagement interfaces, support for network scalability, need for fewer access control lists (ACLs) to restrict access to a device, and management packet floods on switching and routing interfaces are prevented from reaching the CPU.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Management Plane Protection" section on page 11.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Management Plane Protection

- IP Cisco Express Forwarding must be enabled before a management interface can be configured.

Restrictions for Management Plane Protection

- Out-of-band management interfaces (also called dedicated management interfaces) are not supported. An out-of-band management interface is a dedicated Cisco IOS physical or logical interface that processes management traffic only.
- Loopback and virtual interfaces not associated to physical interfaces are not supported.
- Fallback and standby management interfaces are not supported.
- Hardware-switched and distributed platforms are not supported.
- Secure Copy (SCP) is supported under the Secure Shell (SSH) Protocol and not directly configurable in the command-line interface (CLI).
- Uninformed management stations lose access to the router through nondesignated management interfaces when the Management Plane Protection feature is enabled.

Information About Management Plane Protection

Before you enable the Management Plane Protection feature, you should understand the following concepts:

In-Band Management Interface

An in-band management interface is a Cisco IOS physical or logical interface that processes management as well as data-forwarding packets. Loopback interfaces commonly are used as the primary port for network management packets. External applications communicating with a networking device direct network management requests to the loopback port. An in-band management interface is also called a shared management interface.

Control Plane Protection Overview

A control plane is a collection of processes that run at the process level on a route processor and collectively provide high-level control for most Cisco IOS software functions. All traffic directly or indirectly destined to a router is handled by the control plane.

Control Plane Policing (CoPP) is a Cisco IOS control-plane feature that offers rate limiting of all control-plane traffic. CoPP allows you to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets. This QoS filter helps to protect the control plane of Cisco IOS routers and switches against denial-of-service (DoS) attacks and helps to maintain packet forwarding and protocol states during an attack or during heavy traffic loads.

Control Plane Protection is a framework that encompasses all policing and protection features in the control plane. The Control Plane Protection feature extends the policing functionality of the CoPP feature by allowing finer policing granularity. Control Plane Protection also includes a traffic classifier, which intercepts control-plane traffic and classifies it in control-plane categories. Management Plane Protection operates within the Control Plane Protection infrastructure.

For more information about the Control Plane Policing feature in Cisco IOS software, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/gtrtlimt.htm.

For more information about the Control Plane Protection feature in Cisco IOS software, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t4/htcpp.htm.

Management Plane

The management plane is the logical path of all traffic related to the management of a routing platform. One of three planes in a communication architecture that is structured in layers and planes, the management plane performs management functions for a network and coordinates functions among all the planes (management, control, data). The management plane also is used to manage a device through its connection to the network.

Examples of protocols processed in the management plane are Simple Network Management Protocol (SNMP), Telnet, HTTP, Secure HTTP (HTTPS), and SSH. These management protocols are used for monitoring and for CLI access. Restricting access to devices to internal sources (trusted networks) is critical.

Management Plane Protection Feature

The MPP feature in Cisco IOS software provides the capability to restrict the interfaces on which network management packets are allowed to enter a device. The MPP feature allows a network operator to designate one or more router interfaces as management interfaces. Device management traffic is permitted to enter a device through these management interfaces. After MPP is enabled, no interfaces except designated management interfaces will accept network management traffic destined to the device. Restricting management packets to designated interfaces provides greater control over management of a device.

The MPP feature is disabled by default. When you enable the feature, you must designate one or more interfaces as management interfaces and configure the management protocols that will be allowed on those interfaces. The feature does not provide a default management interface. Using a single CLI

command, you can configure, modify, or delete a management interface.When you configure a management interface, no interfaces except that management interface will accept network management packets destined to the device. When the last configured interface is deleted, the feature turns itself off.

Following are the management protocols that the MPP feature supports. These management protocols are also the only protocols affected when MPP is enabled.

- Blocks Extensible Exchange Protocol (BEEP)
- FTP
- HTTP
- HTTPS
- SSH, v1 and v2
- SNMP, all versions
- Telnet
- TFTP

Cisco IOS features enabled on management interfaces remain available when the MPP feature is enabled. Nonmanagement packets such as routing and Address Resolution Protocol (ARP) messages for in-band management interfaces are not affected.

This feature generates a syslog for the following events:

- When the feature is enabled or disabled
- When a management interface fails.

  For example, a failure will occur when the management interface cannot successfully receive or process packets destined for the control plane for reasons other than resource exhaustion.

Benefits of the Management Plane Protection Feature

Implementing the MPP feature provides the following benefits:

- Greater access control for managing a device than allowing management protocols on all interfaces
- Improved performance for data packets on nonmanagement interfaces
- Support for network scalability
- Simplifies the task of using per-interface ACLs to restrict management access to the device
- Fewer ACLs needed to restrict access to the device
- Management packet floods on switching and routing interfaces are prevented from reaching the CPU

How to Configure a Device for Management Plane Protection

This section contains the following task:

- Configuring a Device for Management Plane Protection, page 5

Configuring a Device for Management Plane Protection

Perform this task to configure a device that you have just added to your network or a device already operating in your network. This task shows how to configure MPP where SSH and SNMP are allowed to access the router only through the FastEthernet 0/0 interface.

Prerequisites

- IP Cisco Express Forwarding must be enabled before a management interface can be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **control-plane host**
4. **management-interface** *interface* **allow** *protocols*
5. **Ctrl z**
6. **show management-interface** [*interface* | **protocol** *protocol-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**control-plane host** **Example:** `Router(config)# control-plane host`	Enters control-plane host configuration mode.
Step 4	**management-interface** *interface* **allow** *protocols* **Example:** `Router(config-cp-host)# management-interface FastEthernet 0/0 allow ssh snmp`	Configures an interface to be a management interface, which will accept management protocols, and specifies which management protocols are allowed. *interface*—Name of the interface that you are designating as a management interface. *protocols*—Management protocols you want to allow on the designated management interface. • BEEP • FTP • HTTP • HTTPS • SSH, v1 and v2 • SNMP, all versions • Telnet • TFTP
Step 5	**Ctrl z** **Example:** `Router(config-cp-host)# Ctrl z`	Returns to privileged EXEC mode.
Step 6	**show management-interface** [*interface* | **protocol** *protocol-name*] **Example:** `Router# show management-interface FastEthernet 0/0`	Displays information about the management interface such as type of interface, protocols enabled on the interface, and number of packets dropped and processed. *interface*—(Optional) Interface for which you want to view information. **protocol**—(Optional) Indicates that a protocol is specified. *protocol-name*—(Optional) Protocol for which you want to view information

Examples

The configuration in this example shows MPP configured to allow SSH and SNMP to access the router only through the FastEthernet 0/0 interface. This configuration results in all protocols in the remaining subset of supported management protocols to be dropped on all interfaces unless explicitly permitted. BEEP, FTP, HTTP, HTTPS, Telnet, and TFTP will not be permitted to access the router through any interfaces, including FastEthernet 0/0. Additionally, SNMP and SSH will be dropped on all interfaces except FastEthernet 0/0, where it is explicitly allowed.

To allow other supported management protocols to access the router, you must explicitly allow these protocols by adding them to the protocol list for the FastEthernet 0/0 interface or enabling additional management interfaces and protocols.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# control-plane host
Router(config-cp-host)# management-interface FastEthernet 0/0 allow ssh snmp
Router(config-cp-host)#
.Aug  2 15:25:32.846: %CP-5-FEATURE: Management-Interface feature enabled on Control plane
host path
Router(config-cp-host)#
```

The following is output from the **show management-interface** command issued after configuring MPP in the previous example. The **show management-interface** command is useful for verifying your configuration.

```
Router# show management-interface

Management interface FastEthernet0/0
        Protocol        Packets processed
             ssh                0
            snmp                0

Router#
```

Configuration Examples for Management Plane Protection

This section provides the following configuration example:

- Configuring Management Plane Protection on Gigabit Ethernet Interfaces: Example, page 7

Configuring Management Plane Protection on Gigabit Ethernet Interfaces: Example

The following example shows how to configure MPP where only SSH, SNMP, and HTTP are allowed to access the router through the Gigabit Ethernet 0/3 interface and only HTTP is allowed to access the router through the Gigabit Ethernet 0/2 interface.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# control-plane host
Router(config-cp-host)# management-interface GigabitEthernet 0/3 allow http ssh snmp
Router(config-cp-host)#
.Aug  2 17:00:24.511: %CP-5-FEATURE: Management-Interface feature enabled on Control plane
host path
Router(config-cp-host)# management-interface GigabitEthernet 0/2 allow http
Router(config-cp-host)#
```

The following is output from the **show management-interface** command issued after configuring MPP in the previous example. The **show management-interface** command is useful for verifying your configuration.

```
Router# show management-interface
Management interface GigabitEthernet0/2
        Protocol        Packets processed
            http                0

Management interface GigabitEthernet0/3
        Protocol        Packets processed
            http                0
             ssh                0
            snmp                0
```

Additional References

The following sections provide references related to Management Plane Protection.

Related Documents

Related Topic	Document Title
Network management	*Cisco IOS Network Management Configuration Guide*, Release 12.4
Network security	*Cisco IOS Security Configuration Guide*, Release 12.4
Control Plane Policing	http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/gtrtlimt.htm
Control Plane Protection	http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t4/htcpp.htm

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3871	Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure

Technical Assistance

Description	Link
The Cisco Technical Support and Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features

- **management-interface allow**
- **show management-interface**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.
For information about all Cisco IOS commands, see the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or the Master Command List.

Feature Information for Management Plane Protection

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Management Plane Protection

Feature Name	Releases	Feature Information
Management Plane Protection	12.4(6)T	Provides the capability to restrict the interfaces on which network management packets are allowed to enter a device.