



Implementing Management Plane Protection

The Management Plane Protection (MPP) feature in Cisco IOS XR 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 may enter a device only through these management interfaces. After MPP is enabled, no interfaces except designated management interfaces 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.

This module describes how to implement management plane protection on Cisco 8000 Series Routers.

- [Prerequisites for Implementing Management Plane Protection, on page 1](#)
- [Restrictions for Implementing Management Plane Protection, on page 1](#)
- [Information About Implementing Management Plane Protection, on page 2](#)
- [How to Configure a Device for Management Plane Protection, on page 4](#)
- [Configuration Examples for Implementing Management Plane Protection, on page 5](#)
- [Additional References, on page 7](#)

Prerequisites for Implementing Management Plane Protection

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Restrictions for Implementing Management Plane Protection

- Currently, MPP does not keep track of denied or dropped protocol requests.
- MPP configuration does not enable the protocol services. MPP is responsible only for making the services available on different interfaces. The protocols are enabled explicitly.
- Management requests that are received on inband interfaces are not necessarily acknowledged there.
- Route Processor (RP) interfaces are by default designated as out-of-band interfaces, and can be configured under MPP.

- The changes made for the MPP configuration do not affect the active sessions that are established before the changes.
- Currently, MPP controls only the incoming management requests for protocols, such as TFTP, Telnet, Simple Network Management Protocol (SNMP), Secure Shell (SSH), and HTTP.
- MPP does not support MIB.
- In an MPLS L3VPN, when MPP has a VRF interface attached, it applies the VRF filter on an incoming interface through LPTS. When an incoming packet from the core interface has a different VRF, then MPP does not allow it.



Note When configuring a device for MPP for an inband interface the **interface all** configuration does not apply specific VRF filter and allows traffic for all source and destination interfaces.

Information About Implementing Management Plane Protection

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

Inband Management Interface

An *inband management interface* is a Cisco IOS XR software physical or logical interface that processes management packets, as well as data-forwarding packets. An inband management interface is also called a *shared management interface*.

Out-of-Band Management Interface

Out-of-band refers to an interface that allows only management protocol traffic to be forwarded or processed. An *out-of-band management interface* is defined by the network operator to specifically receive network management traffic. The advantage is that forwarding (or customer) traffic cannot interfere with the management of the router, which significantly reduces the possibility of denial-of-service attacks.

Out-of-band interfaces forward traffic only between out-of-band interfaces or terminate management packets that are destined to the router. In addition, the out-of-band interfaces can participate in dynamic routing protocols. The service provider connects to the router's out-of-band interfaces and builds an independent overlay management network, with all the routing and policy tools that the router can provide.

Peer-Filtering on Interfaces

The peer-filtering option allows management traffic from specific peers, or a range of peers, to be configured.

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 XR software functions. All traffic directly or indirectly destined

to a router is handled by the control plane. Management Plane Protection operates within the Control Plane Infrastructure.

Management Plane

The *management plane* is the logical path of all traffic that is 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, and data). In addition, the management plane 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 command-line interface (CLI) access. Restricting access to devices to internal sources (trusted networks) is critical.

Management Plane Protection Feature

The MPP protection feature, as well as all the management protocols under MPP, are disabled by default. When you configure an interface as either out-of-band or inband, it automatically enables MPP. Consequently, this enablement extends to all the protocols under MPP.

If MPP is disabled and a protocol is activated, all interfaces can pass traffic.

When MPP is enabled with an activated protocol, the only default management interfaces allowing management traffic are the route processor (RP) and standby route processor (SRP) Ethernet interfaces. You must manually configure any other interface for which you want to enable MPP as a management interface, using the MPP CLI that follows. Afterwards, only the default management interfaces and those you have previously configured as MPP interfaces will accept network management packets destined for the device. All other interfaces drop such packets.



Note Logical interfaces (or any other interfaces not present on the data plane) filter packets based on the ingress physical interface.

After configuration, you can modify or delete a management interface.

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

- SSH, v1 and v2
- SNMP, all versions
- Telnet
- TFTP
- HTTP
- HTTPS

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 non-management interfaces.
- Support for network scalability.
- Simplifies the task of using per-interface access control lists (ACLs) to restrict management access to the device.
- Fewer ACLs are needed to restrict access to the device.
- Prevention of packet floods on switching and routing interfaces from reaching the CPU.

How to Configure a Device for Management Plane Protection

This section contains the following tasks:

Configuring a Device for Management Plane Protection for an Inband Interface

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 as an inband interface in which Telnet is allowed to access the router only through a specific interface.

Perform the following additional tasks to configure an inband MPP interface in non-default VRF.

- Configure the interface under the non-default inband VRF.
- Configure the global inband VRF.
- In the case of Telnet, configure the Telnet VRF server for the inband VRF.

```
Router#configure terminal
Router(config)#control-plane
Router(config-ctrl)#management-plane
Router(config-mpp)#inband
Router(config-mpp-inband)#interface fourHundredGigE 0/0/0/0
Router(config-mpp-inband-if)#allow telnet peer
Router(config-telnet-peer)#address ipv4 10.1.0.0/16
Router(config-telnet-peer)#commit
```

- FourHundredGigE 0/0/0/0 is configured as an inband interface. Use the **interface all** command form to configure all interfaces as inband interfaces.
- Telnet protocol is configured on the inband interface. To enable all protocols, use the **allow all** command form.

Running Configuration

The following is a sample output of **show mgmt-plane** command for the inband interface fourHundredGigE 0/0/0/0.

```
Router#show mgmt-plane inband interface fourHundredGigE 0/0/0/0

interface - fourHundredGigE 0/0/0/0
  telnet configured -
    peer v4 allowed - 10.1.0.0/16
```

Configuring a Device for Management Plane Protection for an Out-of-band Interface

Perform the following tasks to configure an out-of-band MPP interface.

- Configure the interface under the out-of-band VRF.
- Configure the global out-of-band VRF.
- For a specific protocol, configure the protocol VRF server for the out-of-band VRF.

```
Router#configure terminal
Router(config)#control-plane
Router(config-ctrl)#management-plane
Router(config-mpp)#out-of-band
Router(config-mpp-outband)#vrf target
Router(config-mpp-outband)#interface fourHundredGigE 0/0/0/3
Router(config-mpp-outband-if)#allow tftp peer
Router(config-tftp-peer)#address ipv6 33::33
Router(config-tftp-peer)#commit
```

- FourHundredGigE 0/0/0/3 is configured as an out-of-band interface, for the VRF **target**. Use the **interface all** command form to configure all interfaces as out-of-band interfaces.
- TFTP protocol is configured on the out-of-band interface. To enable all protocols, use the **allow all** command form.

Running Configuration

The following is a sample output of the **show mgmt-plane out-of-band vrf** command.

```
Router#show mgmt-plane out-of-band vrf

Management Plane Protection -
  out-of-band VRF - target
```

Configuration Examples for Implementing Management Plane Protection

This section provides the following configuration example:

Configuring Management Plane Protection: Example

The following example shows a detailed example of how to configure inband and out-of-band interfaces under MPP:

```

configure
control-plane
management-plane
inband
interface all
allow SSH
!
interface fourHundredGigE 0/0/0/0
allow all
allow SSH
allow Telnet peer
address ipv4 10.1.0.0/16
!
!
interface fourHundredGigE 0/0/0/0
allow Telnet peer
address ipv4 10.1.0.0/16
!
!
!
out-of-band
vrf target
interface fourHundredGigE 0/0/0/3
allow TFTP peer
address ipv6 33::33
!
!
!
!
show mgmt-plane

Management Plane Protection

inband interfaces
-----

interface - fourHundredGigE 0/0/0/0
ssh configured -
    All peers allowed
telnet configured -
    peer v4 allowed - 10.1.0.0/16
all configured -
    All peers allowed
interface - fourHundredGigE 0/0/0/0
telnet configured -
    peer v4 allowed - 10.1.0.0/16

interface - all
all configured -
    All peers allowed

outband interfaces
-----
interface - fourHundredGigE 0/0/0/3

```

```

tftp configured -
    peer v6 allowed - 33::33

show mgmt-plane out-of-band vrf

Management Plane Protection -
    out-of-band VRF - target

```

Additional References

The following sections provide references related to implementing management plane protection.

Related Documents

Related Topic	Document Title
MPP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Management Plane Protection Commands on System Security Command Reference for Cisco 8000 Series Routers.</i>

Standards

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

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support 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

