Implementing Management Plane Protection

The Management Plane Protection (MPP) feature 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.

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.

Afterwards, only the default management interfaces and those you have previously configured as MPP interfaces accept network management packets destined for the device. All other interfaces drop such packets. Logical interfaces (or any other interfaces not present on the data plane) filter packets based on the ingress physical interface.

Implementing Management Plane Protection

The Management Plane Protection (MPP) feature 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.

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.

Afterwards, only the default management interfaces and those you have previously configured as MPP interfaces accept network management packets destined for the device. All other interfaces drop such packets. Logical interfaces (or any other interfaces not present on the data plane) filter packets based on the ingress physical interface.

Benefits of Management Plane Protection

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.

Restrictions for Implementing Management Plane Protection

The following restrictions are listed for implementing Management Plane Protection (MPP):

- Currently, MPP does not keep track of the 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.
- Both Route Processor (RP) and distributed route processor (DRP) Ethernet interfaces are by default 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), XML , HTTP and Netconf.
- MPP does not support MIB.

Configure Device for Management Plane Protection for Inband Interface

An *inband management interface* is a 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*. 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.

SUMMARY STEPS

1. **configure**
2. control-plane
3. management-plane
4. inband
5. **interface** {*type instance* | **all**}
6. **allow** {*protocol* | **all**} [**peer**]
7. **address ipv4** {*peer-ip-address* | *peer ip-address/length*}
8. Use the **commit** or **end** command.
9. **show mgmt-plane** [**inband** | **out-of-band**] [**interface** {*type instance*}]

DETAILED STEPS

Step 1 **configure**

Example:

```
RP/0/RP0/CPU0:router# configure
```

Enters global configuration mode.

Step 2 control-plane

Example:

```
RP/0/RP0/CPU0:router(config)# control-plane
RP/0/RP0/CPU0:router(config-ctrl)#
```

Enters control plane configuration mode.

Step 3 management-plane

Example:

```
RP/0/RP0/CPU0:router(config-ctrl)# management-plane
RP/0/RP0/CPU0:router(config-mpp)#
```

Configures management plane protection to allow and disallow protocols and enters management plane protection configuration mode.

Step 4 inband

Example:

```
RP/0/RP0/CPU0:router(config-mpp)# inband
RP/0/RP0/CPU0:router(config-mpp-inband)#
```

Configures an inband interface and enters management plane protection inband configuration mode.

Step 5 **interface** {*type instance* | **all**}

Example:

```
RP/0/RP0/CPU0:router(config-mpp-inband)# interface HundredGigE 0/6/0/1
RP/0/RP0/CPU0:router(config-mpp-inband-Gi0_6_0_1)#
```

Configures a specific inband interface, or all inband interfaces. Use the **interface** command to enter management plane protection inband interface configuration mode.

- Use the **all** keyword to configure all interfaces.

Step 6 **allow** {*protocol* | **all**} [**peer**]

Example:

```
RP/0/RP0/CPU0:router(config-mpp-inband-Gi0_6_0_1)# allow Telnet peer
RP/0/RP0/CPU0:router(config-telnet-peer)#
```

Configures an interface as an inband interface for a specified protocol or all protocols.

- Use the *protocol* argument to allow management protocols on the designated management interface.
  - HTTP or HTTPS
  - SNMP (also versions)
  - Secure Shell (v1 and v2)
  - TFTP
  - Telnet
  - Netconf
  - XML
- Use the **all** keyword to configure the interface to allow all the management traffic that is specified in the list of protocols.
- (Optional) Use the **peer** keyword to configure the peer address on the interface.

Step 7 **address ipv4** {*peer-ip-address* | *peer ip-address/length*}

Example:

```
RP/0/RP0/CPU0:router(config-telnet-peer)# address ipv4 10.1.0.0/16
```

Configures the peer IPv4 address in which management traffic is allowed on the interface.

- Use the *peer-ip-address* argument to configure the peer IPv4 address in which management traffic is allowed on the interface.
- Use the *peer ip-address/length* argument to configure the prefix of the peer IPv4 address.

Step 8 Use the **commit** or **end** command.

commit —Saves the configuration changes and remains within the configuration session.

end —Prompts user to take one of these actions:

- **Yes** — Saves configuration changes and exits the configuration session.
- **No** —Exits the configuration session without committing the configuration changes.
- **Cancel** —Remains in the configuration session, without committing the configuration changes.

Step 9 **show mgmt-plane** [**inband** | **out-of-band**] [**interface** {*type instance*}]

Example:

```
RP/0/RP0/CPU0:router# show mgmt-plane inband interface HundredGigE 0/6/0/1
```

Displays information about the management plane, such as type of interface and protocols enabled on the interface.

- (Optional) Use the **inband** keyword to display the inband management interface configurations that are the interfaces that process management packets as well as data-forwarding packets.
- (Optional) Use the **out-of-band** keyword to display the out-of-band interface configurations.
- (Optional) Use the **interface** keyword to display the details for a specific interface.

Configure Device for Management Plane Protection for Out-of-band 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.

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.
- In the case of Telnet, configure the Telnet VRF server for the out-of-band VRF.

SUMMARY STEPS

1. **configure**
2. control-plane
3. management-plane
4. out-of-band
5. **vrf** *vrf-name*

6. **interface** {*type instance* | **all**}
7. **allow** {*protocol* | **all**} [**peer**]
8. **address ipv6** {*peer-ip-address* | *peer ip-address/length*}
9. Use the **commit** or **end** command.
10. **show mgmt-plane** [**inband** | **out-of-band**] [**interface** {*type instance*} | **vrf**]

DETAILED STEPS

Step 1 **configure**

Example:

```
RP/0/RP0/CPU0:router# configure
```

Enters global configuration mode.

Step 2 control-plane

Example:

```
RP/0/RP0/CPU0:router(config)# control-plane
RP/0/RP0/CPU0:router(config-ctrl)#
```

Enters control plane configuration mode.

Step 3 management-plane

Example:

```
RP/0/RP0/CPU0:router(config-ctrl)# management-plane
RP/0/RP0/CPU0:router(config-mpp)#
```

Configures management plane protection to allow and disallow protocols and enters management plane protection configuration mode.

Step 4 out-of-band

Example:

```
RP/0/RP0/CPU0:router(config-mpp)# out-of-band
RP/0/RP0/CPU0:router(config-mpp-outband)#
```

Configures out-of-band interfaces or protocols and enters management plane protection out-of-band configuration mode.

Step 5 **vrf** *vrf-name*

Example:

```
RP/0/RP0/CPU0:router(config-mpp-outband)# vrf target
```

Configures a Virtual Private Network (VPN) routing and forwarding (VRF) reference of an out-of-band interface.

- Use the *vrf-name* argument to assign a name to a VRF.

Step 6 **interface** {*type instance* | **all**}

Example:

```
RP/0/RP0/CPU0:router(config-mpp-outband)# interface HundredGigE 0/6/0/2
RP/0/RP0/CPU0:router(config-mpp-outband-if)#
```

Configures a specific out-of-band interface, or all out-of-band interfaces, as an out-of-band interface. Use the **interface** command to enter management plane protection out-of-band configuration mode.

- Use the **all** keyword to configure all interfaces.

Step 7 **allow** {*protocol* | **all**} [**peer**]

Example:

```
RP/0/RP0/CPU0:router(config-mpp-outband-if)# allow TFTP peer
RP/0/RP0/CPU0:router(config-tftp-peer)#
```

Configures an interface as an out-of-band interface for a specified protocol or all protocols.

- Use the *protocol* argument to allow management protocols on the designated management interface.
  - HTTP or HTTPS
  - SNMP (also versions)
  - Secure Shell (v1 and v2)
  - TFTP
  - Telnet
  - Netconf
- Use the **all** keyword to configure the interface to allow all the management traffic that is specified in the list of protocols.
- (Optional) Use the **peer** keyword to configure the peer address on the interface.

Step 8 **address ipv6** {*peer-ip-address* | *peer ip-address/length*}

Example:

```
RP/0/RP0/CPU0:router(config-tftp-peer)# address ipv6 33::33
```

Configures the peer IPv6 address in which management traffic is allowed on the interface.

- Use the *peer-ip-address* argument to configure the peer IPv6 address in which management traffic is allowed on the interface.
- Use the *peer ip-address/length* argument to configure the prefix of the peer IPv6 address.

Step 9 Use the **commit** or **end** command.

commit —Saves the configuration changes and remains within the configuration session.

end —Prompts user to take one of these actions:

- **Yes** — Saves configuration changes and exits the configuration session.
- **No** —Exits the configuration session without committing the configuration changes.
- **Cancel** —Remains in the configuration session, without committing the configuration changes.

Step 10 **show mgmt-plane** [**inband** | **out-of-band**] [**interface** {*type instance*} | **vrf**]

Example:

```
RP/0/RP0/CPU0:router# show mgmt-plane out-of-band interface HundredGigE 0/6/0/2
```

Displays information about the management plane, such as type of interface and protocols enabled on the interface.

- (Optional) Use the **inband** keyword to display the inband management interface configurations that are the interfaces that process management packets as well as data-forwarding packets.
- (Optional) Use the **out-of-band** keyword to display the out-of-band interface configurations.
- (Optional) Use the **interface** keyword to display the details for a specific interface.
- (Optional) Use the **vrf** keyword to display the Virtual Private Network (VPN) routing and forwarding reference of an out-of-band interface.

Example

The following example shows how to configure inband and out-of-band interfaces for a specific IP address under MPP:

```
configure
 control-plane
  management-plane
   inband
    interface all
     allow SSH
     !
    interface HundredGigE 0/6/0/0
     allow all
     allow SSH
     allow Telnet peer
      address ipv4 10.1.0.0/16
    !
```

```
   !
    interface HundredGigE 0/6/0/1
     allow Telnet peer
      address ipv4 10.1.0.0/16
     !
    !
   !
   out-of-band
    vrf my_out_of_band
    interface HundredGigE 0/6/0/2
     allow TFTP peer
      address ipv6 33::33
     !
    !
   !
  !
 !

show mgmt-plane

Management Plane Protection

inband interfaces
----------------------

interface - HundredGigE0_6_0_0
        ssh configured -
                All peers allowed
        telnet configured -
                peer v4 allowed - 10.1.0.0/16
        all configured -
                All peers allowed
interface - HundredGigE0_6_0_1
        telnet configured -
                peer v4 allowed - 10.1.0.0/16

interface - all
        all configured -
                All peers allowed

outband interfaces
----------------------
interface - HundredGigE0_6_0_2
        tftp configured -
                peer v6 allowed - 33::33

show mgmt-plane out-of-band vrf

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

MPP Parity for Management Ethernet Interface

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
MPP Parity for Management Ethernet Interface	Release 7.5.1	This release brings in parity between inband interfaces and management Ethernet interfaces with respect to the default behavior for network management traffic permissions. The feature provides a default configuration option to block the management traffic on management Ethernet interfaces when MPP is enabled. This feature thus enhances router-level security and provides more granularity in controlling management access to the router. In earlier releases, all management traffic was allowed, by default, on the management Ethernet interfaces, even with MPP enabled. This feature is supported on routers that have the Cisco NC57 line cards installed and operating in the native mode. This feature introduces the **enable-inband-behaviour** command.

The MPP feature on Cisco IOS XR Software allows you to select a set of line card data interfaces (also known as inband interfaces) or specific source hosts or networks that are reachable over inband interfaces, or management Ethernet interfaces, for the network management traffic. MPP configuration on the inband interfaces allows you to selectively permit management traffic through them. When MPP is enabled, by default, the management traffic is blocked on all inband interfaces. However, by default, the management traffic is not blocked on management Ethernet interfaces. Thus, until Cisco IOS XR Software Release 7.5.1, there was a difference in the default behavior between the inband interfaces and management Ethernet interfaces with respect to allowing or blocking the management traffic.

To enhance security over management Ethernet interfaces, Cisco IOS XR Software enhances the existing MPP functionality by providing the same level of management plane protection for management Ethernet interfaces as the already-available level for inband interfaces. By enabling this MPP parity or inband MPP behavior, by default, the router blocks the management traffic on all management Ethernet interfaces, when MPP feature is enabled. This blocking is unlike in earlier cases where the management traffic was allowed on all management Ethernet interfaces irrespective of the fact that MPP was enabled. Thus, the new functionality brings in parity, between the inband interfaces and management Ethernet interfaces, in the default behavior for permitting the network management traffic.

MPP Scenarios for Inband and Management Ethernet Interface

This table compares the pattern of traffic restriction on inband and management Ethernet interfaces when MPP parity for management Ethernet interface is enabled with various MPP configurations.

Table 2: MPP Scenarios for Inband and Management Ethernet Interfaces

MPP Configuration	Permission for Network Management Traffic (on inband interface)	Permission for Network Management Traffic (on management Ethernet interface)
Not configured	Allows all network management traffic	Allows all network management traffic
MPP is configured to enable a given management protocol on an inband interface. (For details, see Configure Device for Management Plane Protection for Inband Interface, on page 2.)	Allows the traffic of the specified management protocol only on that interface; blocks it on other inband interfaces, unless configured otherwise.	Blocks the traffic of the specified management protocol, and the traffic of other management protocols on all management Ethernet interfaces, unless configured otherwise.
MPP is configured to enable a given management protocol on management Ethernet interface. (For details, see Configure Device for Management Plane Protection for Out-of-band Interface, on page 5 and How to Enable Inband MPP Behavior for Management Ethernet Interface, on page 11.)	Blocks the traffic of the specified management protocol as well as other management protocols on all inband interfaces, unless configured otherwise.	Allows only the traffic of the specified management protocol on that management Ethernet interface; blocks the traffic of all other management protocols, unless configured otherwise.

How to Enable Inband MPP Behavior for Management Ethernet Interface

By default, MPP parity or inband MPP behavior for management Ethernet interface is disabled. To enable the feature, use the **enable-inband-behaviour** command in out-of-band configuration mode (under control-plane->management-plane configuration mode).

Prerequisites and Guidelines to Enable or Disable Inband MPP Behavior for Management Ethernet Interface

- Inband MPP behavior for management Ethernet interface takes effect only with MPP configuration in place.

For details on configuring MPP, see Configure Device for Management Plane Protection for Inband Interface, on page 2 and Configure Device for Management Plane Protection for Out-of-band Interface, on page 5.

- If MPP configuration is already present, the router rejects the configuration to enable or disable inband MPP behavior for management Ethernet interface. As a result, we recommend that you enable this feature before configuring MPP. Similarly, disable the feature only after removing the existing MPP configuration.

  The recommended order of tasks to enable inband MPP behavior for management Ethernet interface is:

  1. Enable inband MPP behavior for management Ethernet interface.
  2. Enable the management protocols.
  3. Configure the MPP feature.

  The recommended order of tasks to disable inband MPP behavior for management Ethernet interface is:

  1. Remove all MPP configurations.
  2. Disable inband MPP behavior for management Ethernet interface.
  3. Reconfigure MPP configurations, if required.

Configuration Example for Enabling Inband MPP Behavior for Management Ethernet Interface

```
Router#configure
Router(config)#control-plane
Router(config-ctrl)#management-plane
Router(config-mpp)#out-of-band
Router(config-mpp-outband)#enable-inband-behaviour
Router(config-mpp-outband)#commit
```

Running Configuration

```
Router#show run control-plane
control-plane
 management-plane
  out-of-band
   enable-inband-behavior
  !
 !
!
```

MPP Feature Behavior for Management Ethernet Interface

This table provides a comparison of various scenarios where inband MPP behavior for management Ethernet interface feature is enabled and disabled.

See the *Verification* section for sample configurations and feature behavior in these scenarios.

Table 3: MPP Feature Behavior for Management Ethernet Interface

Scenarios	Behavior with Inband MPP Behavior for Management Ethernet Interface Disabled	Behavior with Inband MPP Behavior for Management Ethernet Interface Enabled
At router boot up (without MPP configuration)	Allows all management protocols (that are enabled) on both inband and management Ethernet interfaces.	Allows all management protocols (that are enabled) on both inband and management Ethernet interfaces.
With MPP for inband configured (for a given management protocol)	• Allows the traffic of the specified management protocol only on that inband interface, and on all management Ethernet interfaces; blocks it on all other inband interfaces, unless configured otherwise. • Blocks the traffic of all other management protocols on all inband interfaces, unless configured otherwise, whereas, allows them on all management interfaces.	• Allows the traffic of the specified management protocol only on that inband interface; blocks it on all other inband interfaces, and on management Ethernet interfaces. • Blocks the traffic of all other management protocols on all inband interfaces, unless configured otherwise.
With MPP for out-of-band configured (for a given management protocol on the default VRF, and on management interfaces on that default VRF)	• Allows the traffic of that specified protocol on all management Ethernet interfaces; blocks it on all inband interfaces, unless configured otherwise. • Allows the traffic of all other management protocols also on all management Ethernet interfaces.	• Allows the traffic of the specified management protocol only on management Ethernet interfaces; blocks it on all inband interfaces, unless configured otherwise. • Blocks the traffic of all other management protocols on all management Ethernet interfaces, and on all inband interfaces, unless configured otherwise.

Verification

- **Scenario 1: Router boot up**
  - **Without enabling inband MPP behavior for management Ethernet interface:**

    When router boots up, it allows all enabled management protocols on both inband and management Ethernet interfaces. Consider an example where the management protocols SSH, telnet, and SNMP are enabled.

    The **show** commands include port numbers 22, 23 and 161, which are assigned for SSH, telnet and SNMP respectively.

The LPTS entries for SSH are as follows:

```
Router#show  lpts bindings brief | inc any,22
Tue May 11 12:02:44.914 IST
0/RP0/CPU0 TPA_ LR IPV4 TCP    default   any          any,22 any
0/RP0/CPU0 TPA_ LR IPV6 TCP    default   any          any,22 any
0/RP0/CPU0 TPA_ LR IPV4 TCP    vrf1      any          any,22 any
0/RP0/CPU0 TPA_ LR IPV6 TCP    vrf1      any          any,22 any
```

The LPTS entries for telnet are as follows:

```
Router#show  lpts bindings brief | inc any,23

Tue May 11 12:02:55.802 IST
0/RP0/CPU0 TCP  LR IPV4 TCP    default   any          any,23 any
0/RP0/CPU0 TCP  LR IPV4 TCP    port_fwd  any          any,23 any
```

The LPTS entries for SNMP are as follows:

```
Router#show  lpts bindings brief | inc any,161

Tue May 11 12:02:59.575 IST
0/RP0/CPU0 UDP  LR IPV4 UDP    default                          any any,161 any
0/RP0/CPU0 UDP  LR IPV6 UDP    default                          any any,161 any
0/RP0/CPU0 UDP  LR IPV6 UDP    test                             any any,161 any
0/RP0/CPU0 UDP  LR IPV4 UDP    test                             any any,161 any
0/RP0/CPU0 UDP  LR IPV4 UDP    vrf1                             any any,161 any
0/RP0/CPU0 UDP  LR IPV6 UDP    vrf1                             any any,161 any
0/RP0/CPU0 UDP  LR IPV6 UDP    port_fwd                         any any,161 any
0/RP0/CPU0 UDP  LR IPV4 UDP    port_fwd                         any any,161 any
0/RP0/CPU0 UDP  LR IPV6 UDP    8W7TFFUHSBDQ9NIRCA7083S27NC6XVZ0 any any,161 any
0/RP0/CPU0 UDP  LR IPV4 UDP    8W7TFFUHSBDQ9NIRCA7083S27NC6XVZ0 any any,161 any
```

The **show** command outputs show that the router allows all enabled management protocols on all management Ethernet interfaces.

- **With inband MPP behavior for management Ethernet interface enabled:**

  In this scenario, there is no change to the LPTS entry programming because the feature is not yet enabled and MPP is not configured. As a result, the behavior remains the same: router allows all enabled management protocols on both inband and management Ethernet interfaces.

- **Scenario 2: With MPP for inband configured**
  - **Without enabling inband MPP behavior for management Ethernet interface:**

    Consider an example where you have configured MPP to enable one of the management protocols, say SSH, on an inband interface.

```
Router#show run control-plane
Tue May 11 12:06:44.378 IST
control-plane
 management-plane
  inband
   interface HundredGigE0/1/0/28
    allow SSH peer
     address ipv4 192.0.2.0
    !
   !
```

The router allows SSH only on that inband interface and the management interface on both RPs.

The LPTS entries for SSH are as follows:

```
Router#show  lpts bindings brief | inc any,22
Tue May 11 12:03:30.967 IST
0/RP0/CPU0 TPA_ LR IPV4 TCP    default   Mg0/RP0/CPU0/0 any,22 any
0/RP0/CPU0 TPA_ LR IPV4 TCP    default   Mg0/RP1/CPU0/0 any,22 any
0/RP0/CPU0 TPA_ LR IPV4 TCP    default   Hu0/1/0/28     any,22 192.0.2.0
0/RP0/CPU0 TPA_ LR IPV6 TCP    default   Mg0/RP0/CPU0/0 any,22 any
0/RP0/CPU0 TPA_ LR IPV6 TCP    default   Mg0/RP1/CPU0/0 any,22 any
```

The router blocks the other management protocols (such as telnet, SNMP, and so on) on all inband interfaces (unless configured otherwise). However, it allows them on management interface on both RPs, as shown in the following outputs.

The LPTS entries for telnet are as follows:

```
Router#show  lpts bindings brief | inc any,23

Tue May 11 12:03:51.483 IST
0/RP0/CPU0 TCP  LR IPV4 TCP    default   Mg0/RP0/CPU0/0 any,23 any
0/RP0/CPU0 TCP  LR IPV4 TCP    default   Mg0/RP1/CPU0/0 any,23 any
```

The LPTS entries for SNMP are as follows:

```
Router#show  lpts bindings brief | inc any,161
0/RP0/CPU0 UDP  LR IPV4 UDP    default   Mg0/RP0/CPU0/0 any,161 any
0/RP0/CPU0 UDP  LR IPV4 UDP    default   Mg0/RP1/CPU0/0 any,161 any
0/RP0/CPU0 UDP  LR IPV6 UDP    default   Mg0/RP0/CPU0/0 any,161 any
0/RP0/CPU0 UDP  LR IPV6 UDP    default   Mg0/RP1/CPU0/0 any,161 any
```

- **With inband MPP behavior for management Ethernet interface enabled:**

  Here, the feature is enabled before MPP configuration.

```
Router#show run control-plane
Wed Jul 14 12:27:50.054 UTC
control-plane
 management-plane
  inband
   interface HundredGigE0/1/0/28
    allow SSH peer
     address ipv4 192.0.2.0
    !
   !
  !
  out-of-band
   enable-inband-behavior
  !
!
!
```

When you configure MPP to allow SSH on an inband interface (say, Hu0/1/0/28), the router allows SSH on only that inband interface. It blocks other management protocols (such as telnet, SNMP, and so on) on all inband interfaces (unless configured otherwise) and on management Ethernet interfaces, as shown in the following output.

The LPTS entries for SSH are:

```
Router#show  lpts bindings brief | inc any,22
Wed Jul 14 12:30:35.881 UTC
0/RP0/CPU0 TCP  LR IPV4 TCP    default   Hu0/1/0/28   any,22 192.0.2.0
```

The LPTS entries for telnet are:

```
Router#show  lpts bindings brief | inc any,23
Wed Jul 14 12:30:38.464 UTC
```

The LPTS entries for SNMP are:

```
Router#show  lpts bindings brief | inc any,161
Wed Jul 14 12:30:43.697 UTC
```

- **Scenario 3: With MPP for out-of-band configured**
  - **Without enabling inband MPP behavior for management Ethernet interface:**

    Consider an example where you have configured MPP for out-of-band for a given management protocol, say SSH, on the default VRF and on management interfaces on that default VRF.

```
Router#show run control-plane
Wed Jul 14 12:13:18.459 UTC
control-plane
 management-plane
  out-of-band
   interface MgmtEth0/RP0/CPU0/0
    allow SSH
   !
  !
 !
!
```

The router allows SSH on all management interfaces on both RPs.

The LPTS entries for SSH are:

```
Router#show  lpts bindings brief | inc any,22
Wed Jul 14 12:13:22.062 UTC
0/RP0/CPU0 TCP  LR IPV6 TCP    default   Mg0/RP0/CPU0/0 any,22 any
0/RP0/CPU0 TCP  LR IPV4 TCP    default   Mg0/RP0/CPU0/0 any,22 any
0/RP0/CPU0 TCP  LR IPV6 TCP    default   Mg0/RP1/CPU0/0 any,22 any
0/RP0/CPU0 TCP  LR IPV4 TCP    default   Mg0/RP1/CPU0/0 any,22 any
```

The router also allows the other management protocols (such as telnet, SNMP, and so on) on all management interfaces on both RPs, as shown in the following outputs.

The LPTS entries for telnet are:

```
Router#show  lpts bindings brief | inc any,23
Wed Jul 14 12:13:25.152 UTC
0/RP0/CPU0 TCP  LR IPV4 TCP    default   Mg0/RP0/CPU0/0 any,23 any
0/RP0/CPU0 TCP  LR IPV4 TCP    default   Mg0/RP1/CPU0/0 any,23 any
```

The LPTS entries for SNMP are:

```
Router#show  lpts bindings brief | inc any,161
Wed Jul 14 12:13:28.284 UTC
```

```
0/RP0/CPU0 UDP  LR IPV4 UDP    default   Mg0/RP0/CPU0/0 any,162 any
0/RP0/CPU0 UDP  LR IPV4 UDP    default   Mg0/RP1/CPU0/0 any,162 any
0/RP0/CPU0 UDP  LR IPV6 UDP    default   Mg0/RP0/CPU0/0 any,161 any
0/RP0/CPU0 UDP  LR IPV6 UDP    default   Mg0/RP1/CPU0/0 any,161 any
0/RP0/CPU0 UDP  LR IPV4 UDP    default   Mg0/RP0/CPU0/0 any,161 any
0/RP0/CPU0 UDP  LR IPV4 UDP    default   Mg0/RP1/CPU0/0 any,161 any
0/RP0/CPU0 UDP  LR IPV6 UDP    default   Mg0/RP0/CPU0/0 any,162 any
0/RP0/CPU0 UDP  LR IPV6 UDP    default   Mg0/RP1/CPU0/0 any,162 any
```

- **With inband MPP behavior for management Ethernet interface enabled:**

  Here, the feature is enabled before MPP configuration.

  When you configure MPP to allow SSH on only out-of-band interface (say, on management Ethernet interface), the router allows SSH only on management Ethernet interfaces. It blocks other management protocols (such as telnet, SNMP, and so on) on all inband interfaces (unless configured otherwise) and on management Ethernet interfaces, as shown in the following outputs.

  The LPTS entries for SSH are:

```
Router#show  lpts bindings brief | inc any,22
Tue July 13 12:13:00.180 IST
0/RP0/CPU0 TCP  LR IPV6 TCP    default   Mg0/RP0/CPU0/0 any,22 any
0/RP0/CPU0 TCP  LR IPV4 TCP    default   Mg0/RP0/CPU0/0 any,22 any
```

  The LPTS entries for telnet are:

```
Router#show  lpts bindings brief | inc any,23
Tue July 13 12:14:00.130 IST
```

  The LPTS entries for SNMP are:

```
Router#show  lpts bindings brief | inc any,161
Tue July 13 12:14:10.360 IST
```

Associated Command

- **enable-inband-behaviour**

Information About Implementing Management Plane Protection

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

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

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 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), SSH, XML and Netconf. 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.