Management Plane Protection Commands

This module describes the commands used to configure management plane protection (MPP).

For detailed information about keychain management concepts, configuration tasks, and examples, see the Implementing Management Plane Protection chapter in the *System Security Configuration Guide for Cisco NCS 5000 Series Routers*.

Note   Currently, only default VRF is supported. VPNv4, VPNv6 and VPN routing and forwarding (VRF) address families will be supported in a future release.

address ipv4 (MPP)

To configure the peer IPv4 or IPv6 address in which management traffic is allowed on the interface, use the **address ipv4**command in interface peer configuration mode. To remove the IP address that was previously configured on this interface, use the **no** form of this command.

address {**ipv4** | **ipv6**}
peer-ip-address
|*peer-ip-address* / *length*
no address {**ipv4** | **ipv6**}
peer-ip-address
| *peer-ip-address* / *length*
address ipv4 {*peer-ip-address* | *peer-ip-address* / *length*}
no address ipv4 {*peer-ip-address* | *peer-ip-address* / *length*}

Syntax Description	*peer-ip-address* (Required) Peer IPv4 or IPv6 address in which management traffic is allowed on the interface. This address can effectively be the source address of the management traffic that is coming in on the configured interface.

peer ip-address/length (Required) Prefix of the peer IP address and IPv4 address. or IPv6 format:

- IPv4—*A.B.C.D/length*

- IPv6—*X.X:X.X*

Command Default   If no specific peer is configured, all peers are allowed.

Command Modes   Interface peer configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines   No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
system	read, write

Examples   The following example shows how to configure the peer IPv4 address 10.1.0.0, with a prefix of 16 for traffic management:

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

```
RP/0/RP0/CPU0:router(config-mpp-inband)# interface all
RP/0/RP0/CPU0:router(config-mpp-inbandoutband-all)# allow all peer
RP/0/RP0/CPU0:router(config-telnettftp-peer)# address ipv4 10.1.0.0/16
```

address ipv6 (MPP)

To configure the peer IPv6 address in which management traffic is allowed on the interface, use the **address ipv6** command in interface peer configuration mode. To remove the IP address that was previously configured on this interface, use the **no** form of this command.

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

Syntax Description

peer-ip-address	Peer IPv6 address in which management traffic is allowed on the interface. This address can effectively be the source address of the management traffic that is coming in on the configured interface.
s*peer ip-address/length*	Prefix of the peer IPv6 address.

Command Default If no specific peer is configured, all peers are allowed.

Command Modes Interface peer configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
system	read, write

Examples The following example shows how to configure the peer IPv6 address 33::33 for management traffic:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# control-plane
RP/0/RP0/CPU0:router(config-ctrl)# management-plane
RP/0/RP0/CPU0:router(config-mpp)# inband
RP/0/RP0/CPU0:router(config-mpp-outband)# interface GigabitEthernet 0/1/1/2
RP/0/RP0/CPU0:router(config-mpp-outband-GigabitEthernet0_1_1_2)# allow TFTP peer
RP/0/RP0/CPU0:router(config-tftp-peer)# address ipv6 33::33
```

allow (MPP)

To configure an interface as an inband interface to allow all peer addresses for a specified protocol or all protocols, use the **allow** command in management plane protection inband interface configuration mode.

To disallow a protocol on an interface, use the **no** form of this command.

allow {*protocol* | **all**} [**peer**]
no allow {*protocol* | **all**} [**peer**]

Syntax Description	*protocol* Interface configured to allow peer-filtering for the following specified protocol's traffic:

        • Netconf
        • SNMP (also versions)
        • Secure Shell (v1 and v2)
        • TFTP
        • Telnet
        • XML

all	Configures the interface to allow peer-filtering for all the management traffic that is specified in the list of protocols.
peer	(Optional) Configures the peer address on the interface. Peer refers to the neighboring router interface in which traffic might arrive to the main router.

Command Default   By default, no management protocol is allowed on any interface except the management interfaces.

Command Modes   Management plane protection inband interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines   If you permit or allow a specific protocol to an interface, traffic is allowed only for that protocol, and all other management traffic is dropped.

The IOS XR XML API provides a programmatic interface to the router for use by external management applications. This interface provides a mechanism for router configuration and monitoring utilizing XML formatted request and response streams. As one of the management services, XML should be capable of applying MPP. To secure XML MPP data, XML keyword has been added to the command.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to configure all management protocols for all inband interfaces:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# control-plane
RP/0/RP0/CPU0:router(config-ctrl)# management-plane
RP/0/RP0/CPU0:router(config-mpp)# inband
RP/0/RP0/CPU0:router(config-mpp-inband)# interface all
RP/0/RP0/CPU0:router(config-mpp-inband-all)# allow all
```

The following example shows how to configure MPP support on an XML peer in-band interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# control-plane
RP/0/RP0/CPU0:router(config-ctrl)# management-plane
RP/0/RP0/CPU0:router(config-ctrl-mpp)# inband interface all allow xml peer address ipv4
172.10.10.1
```

control-plane

To enter the control plane configuration mode, use the **control-plane** command. To disable all the configurations under control plane mode, use the **no** form of this command.

control-plane
no control-plane

Syntax Description	This command has no keywords or arguments.
Command Default	None
Command Modes	XR Config mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines Use the **control-plane** command to enter control plane configuration mode.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to enter control plane configuration mode using the **control-plane** command:

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

inband

To configure an inband interface and to enter management plane protection inband configuration mode, use the **inband** command in management plane protection configuration mode. To disable all configurations under inband configuration mode, use the **no** form of this command.

inband
no inband

Syntax Description	This command has no keywords or arguments.
Command Default	None
Command Modes	Management plane protection inband configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines   Use the **inband** command to enter management plane protection inband configuration mode.

Task ID

Task ID	Operations
system	read, write

Examples   The following example shows how to enter management plane protection inband configuration mode using the **inband** command:

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

interface (MPP)

To configure a specific interface or all interfaces as an inband interface, use the **interface** command in management plane protection inband configuration mode.

To disable all the configurations under an interface mode, use the **no** form of this command.

interface {*type interface-path-id* | **all**}
no interface {*type interface-path-id* | **all**}

Syntax Description	*type*	Interface type. For more information, use the question mark (?) online help function.
	interface-path-id	Virtual interface instance. Number range varies depending on interface type.

	Note	Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (**?**) online help function.

	all	Configures all interfaces to allow for management traffic.

Command Default None

Command Modes Management plane protection inband configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines Use the **interface** command to enter management plane protection inband interface configuration mode.

For the *instance* argument, you cannot configure Management Ethernet interfaces as inband interfaces.

Task ID

Task ID	Operations
system	read, write

Examples The following example shows how to configure all inband interfaces for MPP:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# control-plane
RP/0/RP0/CPU0:router(config-ctrl)# management-plane
RP/0/RP0/CPU0:router(config-mpp)# inband
RP/0/RP0/CPU0:router(config-mpp-inband)# interface all
RP/0/RP0/CPU0:router(config-mpp-inband-all)#
```

management-plane

To configure management plane protection to allow and disallow protocols, use the **management-plane** command in control plane configuration mode. To disable all configurations under management-plane mode, use the **no** form of this command.

management-plane
no management-plane

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Control plane configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines Use the **management-plane** command to enter the management plane protection configuration mode.

Task ID

Task ID	Operations
system	read, write

Examples The following example shows how to enter management plane protection configuration mode using the **management-plane** command:

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

show mgmt-plane

To display information about the management plane such as type of interface and protocols enabled on the interface, use the **show mgmt-plane** command.

show mgmt-plane [{**inband**}] [{**interface** *type interface-path-id* | **vrf**}]

Syntax Description	inband	(Optional) Displays the inband management interface configurations that are the interfaces that process management packets as well as data-forwarding packets. An inband management interface is also called a *shared management interface*.
	interface	(Optional) Displays all the protocols that are allowed in the specified interface.
	type	Interface type. For more information, use the question mark (?) online help function.
	interface-path-id	Interface instance. Number range varies depending on interface type.
	Note	Use the **show interfaces** command to see a list of all interfaces currently configured on the router.
		For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default	None

Command Modes	XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Task ID

Task ID	Operations
system	read

Examples

The following sample output displays all the interfaces that are configured as inband under MPP:

```
RP/0/RP0/CPU0:router# show mgmt-plane

Management Plane Protection

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

interface - TenGigabitEthernet0_1_1_0
      ssh configured -
            All peers allowed
      telnet configured -
            peer v4 allowed - 10.1.0.0/16
```

```
                all configured -
                        All peers allowed
        interface - TenGigabitEthernet0_1_1_0
                telnet configured -
                        peer v4 allowed - 10.1.0.0/16
```