Management Plane Protection Commands

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

Note All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

Note

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

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 5500 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*

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	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 address 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-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.
speer 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	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 or out-of-band 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 or management plane protection out-of-band interface configuration.

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: • HTTP(S) • NETCONF (version 1.1 protocol) • 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	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
```

allow local-port

To configure a local port and third-party application protocols for management plane protection (MPP) on an interface, use the **allow local-port** command in management plane protection TPA mode. To disallow a protocol on an interface, use the **no** form of this command.

allow local-port *port-number* **protocol** *protocol-number* **interface** *interface-name* **local-address** *IP local address* **remote-address** *IP remote address*

Syntax Description

local-port	Specifies local L4 port of an interface.
protocol	Specifies the L4 protocol to be configured on MPP.
Protocol number	Enter the protocol number corresponding to different protocols. You can choose a value from range 1 to 255. Following are some of the protocol numbers dedicated to different protocols: • gre - Generic Routing Encapsulation. (47) • udp - User Datagram Protocol, RFC 768. (17) • tcp - Transmission Control Protocol, RFC 793. (6) • pptp - Point-to-Point Tunneling Protocol. Entering the pptp protocol literal is equivalent to entering the gre protocol literal. (47) • pim - Protocol Independent Multicast. (103) • ospf - Open Shortest Path First routing protocol, RFC 1247. (89) • ipsec - IP Security. Entering the ipsec protocol literal is equivalent to entering the esp protocol literal. (50) • ipinip - IP-in-IP encapsulation. (4) • icmp6 - Internet Control Message Protocol for IPv6, RFC 2463. (58) • igmp - Internet Group Management Protocol, RFC 1112. (2) • igrp - Interior Gateway Routing Protocol. (9) **Note** In IOS XR release 6.5.2, protocol number is replaced by protocol names. The supported protocols are *tcp* and *udp*.
interface	Specify the MPP interface on which the protocol has to be configured.
local-address	Specify the local IP address of the host or client.
remote-address	Specify the remote IP address of the host or client.

Command Default

Not Applicable

Command Modes

Management plane protection TPA

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Example

```
Router(config)# control-plane
Router(config-ctrl)# management-plane
Router(config-mpp)# tpa vrf default address-family [ipv4 | ipv6]
Router(config-mpp-tpa-vrf-afi)# allow local-port 57600 protocol tcp interface mgmtEth
0/RP0/CPU0/0 local-address 10.1.1.1/32 remote-address 10.2.2.2/32
```

enable-inband-behaviour

To enable inband management plane protection (MPP) behavior for management Ethernet interface, use the **enable-inband-behaviour** command in out-of-band configuration mode (under control-plane->management-plane configuration mode). To disable the feature, use the **no** form of this command.

enable-inband-behaviour

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled, by default.

Command Modes

Out-of-band configuration

Command History

Release	Modification
Release 7.5.1	This command was introduced.

Usage Guidelines

This feature takes effect only with MPP configuration in place.

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

Task ID

Task ID	Operations
system	read, write

Examples

This example shows how to enable 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
```

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	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 or out-of-band interface, use the **interface** command in management plane protection inband configuration mode or management plane protection out-of-band 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 out-of-band configuration

Management plane protection inband configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **interface** command to enter management plane protection inband interface configuration mode or management plane protection out-of-band 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)#
```

The following example shows how to configure all out-of-band 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)# out-of-band
RP/0/RP0/CPU0:router(config-mpp-outband)# interface all
RP/0/RP0/CPU0:router(config-mpp-outband-all)#
```

out-of-band

To configure out-of-band interfaces or protocols and to enter management plane protection out-of-band configuration mode, use the **out-of-band** command in management plane protection configuration mode. To disable all configurations under management plane protection out-of-band configuration mode, use the **no** form of this command.

out-of-band
no out-of-band

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Management plane protection out-of-band configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **out-of-band** command to enter management plane protection out-of-band configuration mode.

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.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to enter management plane protection out-of-band configuration mode using the **out-of-band** 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)# out-of-band
RP/0/RP0/CPU0:router(config-mpp-outband)#
```

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** | **out-of-band**] [**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*.
out-of-band	(Optional) Displays the out-of-band interface configurations. Out-of-band interfaces are defined by the network operator to specifically receive network management traffic.
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.
vrf	(Optional) Displays the Virtual Private Network (VPN) routing and forwarding reference of an out-of-band interface.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **vrf** keyword is valid only for out-of-band VRF configurations.

Task ID

Task ID	Operations
system	read

Examples

The following sample output displays all the interfaces that are configured as inband or out-of-band interfaces under MPP:

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

```
Management Plane Protection

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

interface - HundredGigabitEthernet0_1_1_0
        ssh configured -
                All peers allowed
        telnet configured -
                peer v4 allowed - 10.1.0.0/16
        all configured -
                All peers allowed
interface - HundredGigabitEthernet0_1_1_0
        telnet configured -
                peer v4 allowed - 10.1.0.0/16

interface - all
        all configured -
                All peers allowed

outband interfaces
----------------------
interface - HundredGigabitEthernet0_1_1_0
        tftp configured -
                peer v6 allowed - 33::33
```

The following sample output displays the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an out-of-band interface:

```
RP/0/RP0/CPU0:router# show mgmt-plane out-of-band vrf

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

tpa (MPP)

To configure a third-party application protocol for Management Plane Protection (MPP), use the **tpa** command in management plane protection configuration mode. To disable all configurations related to the third-party application, use the **no** form of this command.

tpa vrf default address-family [ipv4 |ipv6]

Syntax Description

vrf	Configures a Virtual Private Network (VPN) routing and forwarding (VRF) reference.
address-family	Enables support for various address family configuration modes while configuring TPA.
ipv4	Specifies IP Version 4 address prefixes.
ipv6	Specifies IP Version 6 address prefixes.

Command Default

Not Applicable

Command Modes

Management plane protection configuration

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Usage Guidelines

Only default vrf is supported for TPA configuration.

Example

```
Router(config)# control-plane
Router(config-ctrl)# management-plane
Router(config-mpp)# tpa vrf default address-family [ipv4 | ipv6]
```

vrf (MPP)

To configure a Virtual Private Network (VPN) routing and forwarding (VRF) reference of an out-of-band interface, use the **vrf** command in management plane protection out-of-band configuration mode. To remove the VRF definition before the VRF name is used, use the **no** form of this command.

vrf *vrf-name*
no vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

The VRF concept must be used to configure interfaces as out-of-band. If no VRF is configured during an out-of-band configuration, the interface goes into a default VRF.

Command Modes

Management plane protection out-of-band configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If the VRF reference is not configured, the default name MPP_OUTBAND_VRF is used.

If there is an out-of-band configuration that is referring to a VRF and the VRF is deleted, all the MPP bindings are removed.

Task ID

Task ID	Operations
system	read

Examples

The following example shows how to configure the VRF:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# vrf my_out_of_band
RP/0/RP0/CPU0:router(config-vrf)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-vrf-af)# exit
RP/0/RP0/CPU0:router(config-vrf)# address-family ipv6 unicast
RP/0/RP0/CPU0:router(config-vrf-af)# commit
RP/0/RP0/CPU0:router(config-vrf-af)# end
RP/0/RP0/CPU0:router#
```

The following example shows how to configure the VRF definition 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)# out-of-band
RP/0/RP0/CPU0:router(config-mpp-outband)# vrf my_out_of_band
```