T Commands

track

To configure the system to monitor the track-list object that contains all the virtual port-channel (vPC) links to the core and to the vPC peer link when you are using only a single module for all links, use the **track** command. To return to the default, use the **no** form of this command.

track track-object-id
no track track-object-id

Syntax Description

track-object-id	Track-list object that you already configured.

Command Default

No tracking

Command Modes

vpc configuration mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Beginning with Release 4.2, if you must configure all the vPC peer links and core-facing interfaces on a single N7K-M132XP-12 module, you should configure a track object and a track list that is associated with the Layer 3 link to the core and on all vPC peer links on both vPC peer devices. You can use this configuration to avoid dropping traffic if that particular module goes down because when all the tracked objects on the track list go down, the system does the following:

- Stops the vPC primary peer device sending peer-keepalive messages, which forces the vPC secondary peer device to take over.
- Brings down all the downstream vPCs on that vPC peer device, which forces all the traffic to be rerouted in the access switch to the other vPC peer device.

Once you configure this feature and if the module fails, the system automatically suspends all the vPC links on the primary vPC peer device and stops the peer-keepalive messages. This action forces the vPC secondary device to take over the primary role and all the vPC traffic to go to this new vPC primary device until the system stabilizes.

Create a track list that contains all the links to the core and all the vPC peer links as its object. Enable tracking for the specified vPC domain for this track list. Apply this same configuration to the other PC peer device.

This command does not require a license.

Examples

This example shows how to put the previously configured track-list object into the vPC domain on the vPC peer device:

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# track object 5
```

Related Commands

Command	Description
show vpc brief	Displays information about a vPC tracked object.
feature vpc	Enables vPCs on the device.

tunnel destination

To configure the destination endpoint for a tunnel, use the **tunnel destination** command. To remove the tunnel destination, use the **no** form of this command.

tunnel destination {**ip-address** | **host-name**}
no tunnel destination {**ip-address** | **host-name**}

Syntax Description

ip-address	IP address for the tunnel destination.
host-name	Hostname for the tunnel destination.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **tunnel destination** command to configure the destination address for an IP tunnel.

You should not have two tunnels using the same encapsulation mode with the same source and destination address.

This command requires the Enterprise license.

Examples

This example shows how to configure the tunnel destination:

```
switch(config-if)# tunnel destination 192.0.2.120
```

Related Commands

Command	Description
tunnel source	Sets the source of the IP tunnel.
interface tunnel	Creates the IP tunnel.
show interface tunnel	Displays information about the traffic about the specified tunnel interface.

tunnel mode

To configure the tunnel encapsulation mode for a tunnel, use the **tunnel mode** command. To restore the default value, use the **no** form of this command.

tunnel mode gre {**ip** | **ipv6**}
no tunnel mode gre {**ip** | **ipv6**}

Syntax Description

ip	Configures this tunnel encapsulation mode as IPv4.
ipv6	Configures this tunnel encapsulation mode as IPv6.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **tunnel mode** command to configure the tunnel encapsulation mode for a tunnel.

This command requires the Enterprise license.

Examples

This example shows how to configure the tunnel mode:

```
switch(config-if)# tunnel mode gre ip
```

Related Commands

Command	Description
tunnel destination	Sets the destination of the IP tunnel.
interface tunnel	Creates the IP tunnel.
show interface tunnel	Displays information about the traffic about the specified tunnel interface.

tunnel path-mtu-discovery

To enable Path MTU Discovery (PMTUD) on a tunnel interface, use the **tunnel path-mtu-discovery** command. To disable PMTUD on a tunnel interface, use the **no** form of this command.

tunnel path-mtu-discovery [{**age-timer** {**aging-mins** | **infinite**} | **min-mtu** **mtu-bytes**}]
no tunnel path-mtu-discovery [{**age-timer** {**aging-mins** | **infinite**} | **min-mtu** **mtu-bytes**}]

Syntax Description

age-timer	(Optional) Sets a timer to run for a specified interval, in minutes, after which the tunnel interface resets the maximum transmission unit (MTU) of the path to the default tunnel MTU minus 24 bytes for GRE tunnels or minus 20 bytes for IP-in-IP tunnels.
aging-mins	Number of minutes. The range is from 10 to 30. The default is 10.
infinite	Disables the age timer.
min-mtu *mtu-bytes*	(Optional) Specifies the minimum Path MTU across GRE tunnels. The range is from 92 to 65535 bytes. The default is 92.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

When PMTUD (RFC 1191) is enabled on a tunnel interface, the router performs PMTUD processing for the tunnel IP packets. The router always performs PMTUD processing on the original data IP packets that enter the tunnel. When PMTUD is enabled, no packet fragmentation occurs on the encapsulated packets that travel through the tunnel. Without packet fragmentation, there is a better throughput of TCP connections. PMTUD maximizes the use of available bandwidth in the network between the endpoints of a tunnel interface.

After PMTUD is enabled, the Don't Fragment (DF) bit of the IP packet header that is forwarded into the tunnel is copied to the IP header of the external IP packets. The external IP packet is the encapsulating IP packet. Adding the DF bit allows the PMTUD mechanism to work on the tunnel path of the tunnel. The tunnel endpoint listens for Internet Control Message Protocol (ICMP) unreachable too-big messages and modifies the IP MTU of the tunnel interface, if required.

When the aging timer is configured, the tunnel code resets the tunnel MTU after the aging timer expires. After the tunnel MTU is reset, a set of full-size packets with the DF bit set is required to trigger the tunnel PMTUD and lower the tunnel MTU. At least two packets are dropped each time that the tunnel MTU changes.

When PMTUD is disabled, the DF bit of an external (encapsulated) IP packet is set to zero even if the encapsulated packet has a DF bit set to one.

The **min-mtu keyword** sets a low limit through the MTU that can be learned through the PMTUD process. Any ICMP signal received that specifies an MTU less than the minimum MTU configured is ignored. You can use this feature to prevent a denial- of-service attack from any node that can send an ICMP message to the router that specifies a very small MTU.

Note PMTUD on a tunnel interface requires that the tunnel endpoint is able to receive ICMP messages generated by routers in the path of the tunnel. You should check that ICMP messages can be received before you use PMTUD over firewall connections.

This command requires the Enterprise license.

Examples

This example shows how to configure PMTUD:

```
switch(config-if)# tunnel path-mtu-discovery
```

Related Commands

Command	Description
tunnel destination	Sets the destination of the IP tunnel.
interface tunnel	Creates the IP tunnel.
show interface tunnel	Displays information about the traffic about the specified tunnel interface.

tunnel source

To configure the source endpoint for a tunnel, use the **tunnel source** command. To remove the tunnel source, use the **no** form of this command.

tunnel source {**ip-address** | **interface-type number**}
no tunnel source [{**ip-address** | **interface-type number**}]

Syntax Description

ip-address	IP address for the tunnel source.
interface-type number	Interface for the tunnel source.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **tunnel source** command to configure the source address for an IP tunnel.

You should not have two tunnels using the same encapsulation mode with the same source and destination address.

This command requires the Enterprise license.

Examples

This example shows how to set the tunnel source:

```
switch(config-if)# tunnel source 192.0.2.120
```

Related Commands

Command	Description
tunnel destination	Sets the destination of the IP tunnel.
interface tunnel	Creates the IP tunnel.
show interface tunnel	Displays information about the traffic about the specified tunnel interface.

tunnel ttl

To configure the time-to-live value for a tunnel, use the **tunnel ttl** command. To restore the default value, use the **no** form of this command.

tunnel ttl value
no tunnel ttl [**value**]

Syntax Description

value	Time-to-live value for the tunnel. The range is from 1 to 255.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **tunnel ttl** command to configure the time-to-live value for an IP tunnel.

This command requires the Enterprise license.

Examples

This example shows how to configure the time-to-live value for a tunnel interface:

```
switch(config-if)# tunnel ttl 30
```

Related Commands

Command	Description
tunnel destination	Sets the destination of the IP tunnel.
interface tunnel	Creates the IP tunnel.
show interface tunnel	Displays information about the traffic about the specified tunnel interface.

tunnel use-vrf

To specify which virtual routing and forwarding (VRF) instance to use to look up a tunnel destination IP address, use the **tunnel use-vrf** command. To return to the default, use the **no** form of this command.

tunnel use-vrf vrf-name
no tunnel use-vrf vrf-name

Syntax Description

vrf-name	Name of the VRF in which to look up the tunnel destination IP address.

Command Default

Default VRF

Command Modes

Interface configuration mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

You should have the tunnel interface and tunnel destination IP address in the same VRF. You should have the same value for the *vrf-name* parameter in both the **vrf member** and **tunnel use-vrf** command.

This command requires the Enterprise license.

Examples

This example shows how to specify the VRF in which to look up the tunnel destination IP address:

```
switch(config-if)# tunnel use-vrf blue
```

Related Commands

Command	Description
show interface tunnel	Displays information about the traffic about the specified tunnel interface.
show vrf interface tunnel	Displays information about the VRF tunnel interface.