T Commands

This chapter describes the Cisco Nexus 1000V commands that begin with T.

table-map

To create or modify a QoS table map, use the **table-map** command. To remove the table map, use the **no** form of this command.

table-map *table-map-name*

no table-map *table-map-name*

Syntax Description

table-map-name	Specify the table map name.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

Examples

This example shows how to create or access the my_table1 table map for configuration:

```
n1000v# configure terminal
n1000v(config)# table-map my_table1
```

```
n1000v(config-tmap)#
```

This example shows how to remove the my_table1 table map:

```
n1000v(config)# no table-map my_table1
n1000v(config)#
```

Related Commands

Command	Description
from *src* **to** *dest*	Maps input field values to output field values in a QoS table map.
show table-map	Displays table maps.
policy-map	Creates and configures QoS policy maps.
class-map	Creates or modifies a QoS class map that defines a class of traffic.

tac-pac

To generate troubleshooting information in a compressed file format for TAC. You can specify the target location where the file is saved using the command parameter.

tac-pac {bootflash | ftp | modflash | scp | sftp | tftp | volatile}

Note Before you open a TAC case, always generate troubleshooting information file using the **tac-pac** command along with feature specific command outputs and attach the files to the case. The troubleshooting information contains complete information for the Cisco TAC engineers to understand the issue. The troubleshooting information file, in compressed file format, is easier to share and transfer.

Syntax Description

bootflash	Sets bootflash as destination location to save the troubleshooting information file.
ftp	Sets FTP server as destination location to save the troubleshooting information file.
modflash	Sets modflash as destination location to save the troubleshooting information file.
scp	Sets SCP as destination location to save the troubleshooting information file.
sftp	Sets a secured FTP server as destination location to save the troubleshooting information file.
tftp	Sets TFTP server as destination location to save the troubleshooting information file.
volatile	Sets volatile memory as destination location to save the troubleshooting information file.

Defaults

volatile

Command Modes

any

SupportedUserRoles

network admin

Command History

Release	Modification
5.2(1)SV3(1.1)	This command was introduced.

Examples

This example shows how generate troubleshooting information file for TAC and save it in the bootflash:

```
pri_vsm# tac-pac bootflash:
pri_vsm# dir bootflash:
      1006479    Nov 23 00:07:00 2015  show_tech_out.gz
```

This example shows how generate troubleshooting information file for TAC and save it in the volatile memory:

```
pri_vsm# tac-pac volatile
pri_vsm# dir volatile:
374382 Nov 23 00:07:00 2015  show_tech_out.gz
```

You can copy the troubleshooting information file to bootflash, FTP, or TFTP server using the **copy** command. For example:

```
pri_vsm#  copy volatile:show_tech_out.gz bootflash:
```

Related Commands

Command	Description
show tech-support	To collect switch information for Cisco TAC.

tacacs+ enable

To enable TACACS+, use the **tacacs+ enable** command. To disable TACACS+, use the **no** form of this command.

tacacs+ enable

no tacacs+ enable

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to enable TACACS+:

```
n1000v(config)# tacacs+ enable
n1000v(config)#
```

This example shows how to disable TACACS+:

```
n1000v(config)# no tacacs+ enable
n1000v(config)#
```

Related Commands

Command	Description
tacacs-server key	Designates the global key shared between the Cisco Nexus 1000V and the TACACS+ server hosts.
tacacs-server host	Designates the key shared between the Cisco Nexus 1000V and this specific TACACS+ server host.
show tacacs-server	Displays the TACACS+ server configuration.

tacacs-server deadtime

To set a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the **tacacs-server deadtime** command. To disable the monitoring of the nonresponsive TACACS+ server, use the **no** form of this command.

tacacs-server deadtime *minutes*

no tacacs-server deadtime *minutes*

Syntax Description

time	Specifies the time interval in minutes. The range is from 1 to 1440.

Defaults

0 minutes

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

Setting the time interval to zero disables the timer. If the dead-time interval for an individual TACACS+ server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead-time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead-time interval for the group is greater than 0 minutes.

In global configuration mode, you must first enable the TACACS+ feature, using the **tacacs+ enable** command, before you can use any of the other TACACS+ commands to configure the feature.

Examples

This example shows how to configure the dead-time interval and enable periodic monitoring:

```
n1000v# config terminal
n1000v(config)# tacacs-server deadtime 10
```

This example shows how to revert to the default dead-time interval and disable periodic monitoring:

```
n1000v# config terminal
n1000v(config)# no tacacs-server deadtime 10
```

Related Commands

Command	Description
deadtime	Sets a dead-time interval for monitoring a nonresponsive TACACS+ server.
show tacacs-server	Displays TACACS+ server information.
tacacs+ enable	Enables TACACS+.

tacacs-server directed-request

To allow users to send authentication requests to a specific TACACS+ server when logging in, use the **radius-server directed request** command. To revert to the default, use the **no** form of this command.

tacacs-server directed-request

no tacacs-server directed-request

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

In global configuration mode, you must first enable the TACACS+ feature, using the **tacacs+ enable** command, before you can use any of the other TACACS+ commands to configure the feature.

The user can specify the *username@vrfname*:*hostname* during login, where *vrfname* is the virtual routing and forwarding (VRF) name to use and *hostname* is the name of a configured TACACS+ server. The username is sent to the server name for authentication.

Note If you enable the directed-request option, the NX-OS device uses only the RADIUS method for authentication and not the default local method.

Examples

This example shows how to allow users to send authentication requests to a specific TACACS+ server when logging in:

```
n1000v# config t
n1000v(config)# tacacs-server directed-request
```

This example shows how to disallow users to send authentication requests to a specific TACACS+ server when logging in:

```
n1000v# config t
n1000v(config)# no tacacs-server directed-request
```

Related Commands

Command	Description
show tacacs-server directed request	Displays a directed request TACACS+ server configuration.
tacacs+ enable	Enables TACACS+.

tacacs-server host

To configure TACACS+ server host parameters, use the **tacacs-server host** command in configuration mode. To revert to the defaults, use the **no** form of this command.

tacacs-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret*] [**port** *port-number*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds*]

no tacacs-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret*] [**port** *port-number*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds*]

Syntax Description

hostname	TACACS+ server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
ipv4-address	TACACS+ server IPv4 address in the *A.B.C.D* format.
ipv6-address	TACACS+ server IPv6 address in the *X*:*X*:*X*:*X* format.
key	(Optional) Configures the TACACS+ server's shared secret key.
0	(Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
shared-secret	Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters.
port *port-number*	(Optional) Configures a TACACS+ server port for authentication. The range is from 1 to 65535.
test	(Optional) Configures parameters to send test packets to the TACACS+ server.
idle-time *time*	(Optional) Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
password *password*	(Optional) Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.
username *name*	(Optional) Specifies a user name in the test packets. The username is alphanumeric, case sensitive, and has a maximum of 32 characters.
timeout *seconds*	(Optional) Configures a TACACS+ server timeout period (in seconds) between retransmissions to the TACACS+ server. The range is from 1 to 60 seconds.

Defaults

Parameter	Default
Idle-time	disabled
Server monitoring	disabled
Timeout	1 seconds
Test username	test
Test password	test

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

You must use the **tacacs+ enable** command before you configure TACACS+.

When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

Examples

This example shows how to configure TACACS+ server host parameters:

```
n1000v# config terminal
n1000v(config)# tacacs-server host 10.10.2.3 key HostKey
n1000v(config)# tacacs-server host tacacs2 key 0 abcd
n1000v(config)# tacacs-server host tacacs3 key 7 1234
n1000v(config)# tacacs-server host 10.10.2.3 test idle-time 10
n1000v(config)# tacacs-server host 10.10.2.3 test username tester
n1000v(config)# tacacs-server host 10.10.2.3 test password 2B9ka5
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
tacacs+ enable	Enables TACACS+.

tacacs-server key

To configure a global TACACS+ shared secret key, use the **tacacs-server key** command. To removed a configured shared secret, use the **no** form of this command.

tacacs-server key [**0** | **7**] *shared-secret*

no tacacs-server key [**0** | **7**] *shared-secret*

Syntax Description

0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the TACACS+ client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text to authenticate communication between the TACACS+ client and server.
shared-secret	Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

You must configure the TACACS+ preshared key to authenticate the device on the TACACS+ server. The length of the key is restricted to 63 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all TACACS+ server configurations on the device. You can override this global key assignment by using the **key** keyword in the **tacacs-server host** command.

You must use the **tacacs+ enable** command before you configure TACACS+.

Examples

The following example shows how to configure TACACS+ server shared keys:

```
n1000v# config terminal
n1000v(config)# tacacs-server key AnyWord
n1000v(config)# tacacs-server key 0 AnyWord
n1000v(config)# tacacs-server key 7 public
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
tacacs+ enable	Enables TACACS+.

tacacs-server timeout

To specify the time between retransmissions to the TACACS+ servers, use the **tacacs-server timeout** command. To revert to the default, use the **no** form of this command.

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

Syntax Description

seconds	Seconds between retransmissions to the TACACS+ server. The range is from 1 to 60 seconds.

Defaults

5 seconds

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

You must use the **tacacs+ enable** command before you configure TACACS+.

Examples

This example shows how to configure the TACACS+ server timeout value:

```
n1000v# config terminal
n1000v(config)# tacacs-server timeout 3
```

This example shows how to revert to the default TACACS+ server timeout value:

```
n1000v# config terminal
n1000v(config)# no tacacs-server timeout 3
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
tacacs+ enable	Enables TACACS+.

tail

To display the last lines of a file, use the **tail** command.

tail [*filesystem***:**[*//module/*]][*directory/*]*filename lines*]

Syntax Description		
	*filesystem***:**	(Optional) Name of a file system. The name is case sensitive.
	//module/	(Optional) Identifier for a supervisor module. Valid values are **sup-active**, **sup-local**, **sup-remote**, or **sup-standby**. The identifiers are case sensitive.
	directory/	(Optional) Name of a directory. The name is case sensitive.
	filename	Name of the command file. The name is case sensitive.
	lines	(Optional) Number of lines to display. The range is from 0 to 80.

Defaults 10 lines

Command Modes Any

SupportedUserRoles network-admin

Command History	Release	Modification
	4.0(4)SV1(1)	This command was introduced.

Examples This example shows how to display the last 10 lines of a file:

```
n1000v# tail bootflash:startup.cfg
ip arp inspection filter marp vlan 9
ip dhcp snooping vlan 13
ip arp inspection vlan 13
ip dhcp snooping
ip arp inspection validate src-mac dst-mac ip
ip source binding 10.3.2.2 0f00.60b3.2333 vlan 13 interface Ethernet2/46
ip source binding 10.2.2.2 0060.3454.4555 vlan 100 interface Ethernet2/10
logging level dhcp_snoop 6
logging level eth_port_channel 6
```

This example shows how to display the last 20 lines of a file:

```
n1000v# tail bootflash:startup.cfg 20
area 99 virtual-link 1.2.3.4
router rip Enterprise
router rip foo
  address-family ipv4 unicast
router bgp 33.33
event manager applet sdtest
monitor session 1
monitor session 2
```

```
ip dhcp snooping vlan 1
ip arp inspection vlan 1
ip arp inspection filter marp vlan 9
ip dhcp snooping vlan 13
ip arp inspection vlan 13
ip dhcp snooping
ip arp inspection validate src-mac dst-mac ip
ip source binding 10.3.2.2 0f00.60b3.2333 vlan 13 interface Ethernet2/46
ip source binding 10.2.2.2 0060.3454.4555 vlan 100 interface Ethernet2/10
logging level dhcp_snoop 6
logging level eth_port_channel 6
```

Related Commands

Command	Description
cd	Changes the current working directory.
copy	Copies files.
dir	Displays the directory contents.
pwd	Displays the name of the current working directory.

telnet

To create a Telnet session, use the **telnet** command.

telnet {*ipv4-address* | *hostname*} [*port-number*] [**vrf** *vrf-name*]

Syntax Description

ipv4-address	IPv4 address of the remote device.
hostname	Hostname of the remote device. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
port-number	(Optional) Port number for the Telnet session. The range is from 1 to 65535.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the Telnet session. The name is case sensitive.

Defaults

Port 23

Default VRF

Command Modes

Any

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Telnet server using the **feature telnet** command.

Examples

This example shows how to start a Telnet session using an IPv4 address:

```
n1000v# telnet 10.10.1.1 vrf management
```

Related Commands

Command	Description
clear line	Clears Telnet sessions.
feature telnet	Enables the Telnet server.

template data timeout

To designate a timeout period for resending NetFlow template data, use the **template data timeout** command. To remove the timeout period, use the **no** form of this command.

template data timeout *time*

no template data timeout

Syntax Description

time	A time period between 1 and 86400 seconds.

Defaults

None

Command Modes

Netflow flow exporter version 9 configuration (config-flow-exporter-version-9)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to configure a 3600-second timeout period for resending NetFlow flow exporter template data:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)# template data timeout 3600
```

This example shows how to remove the timeout period for resending NetFlow flow exporter template data:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)# no template data timeout
n1000v(config-flow-exporter)#
```

Related Commands

Command	Description
flow exporter	Creates a Flexible NetFlow flow exporter.
flow record	Creates a Flexible NetFlow flow record.
flow monitor	Creates a Flexible NetFlow flow monitor.
show flow exporter	Displays information about the NetFlow flow exporter.
show flow record	Displays information about NetFlow flow records.
show flow monitor	Displays information about the NetFlow flow monitor.
version 9	Designates NetFlow export version 9 in the NetFlow exporter.

terminal event-manager bypass

To bypass the CLI event manager, use the **terminal event-manager bypass** command.

terminal event-manager bypass

Syntax Description

This command has no arguments or keywords.

Defaults

Event manager is enabled.

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

CommandHistory

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to disable the CLI event manager:

```
n1000v# terminal event-manager bypass
n1000v#
```

Related Commands

Command	Description
show terminal	Displays terminal configuration.

terminal length

To set the number of lines that appear on the screen, use the **terminal length** command.

terminal length *number*

Syntax Description

number	Number of lines. The range of valid values is 0 to 511.

Defaults

28 lines

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

Set *number* to 0 to disable pausing.

Examples

This example shows how to set the number of lines that appear on the screen:

```
n1000v# terminal length 60
n1000v#
```

Related Commands

Command	Description
show terminal	Displays the terminal configuration.

terminal monitor

To enable logging for Telnet or Secure Shell (SSH), use the **terminal monitor** command. To disable logging, use the **no** form of this command.

terminal monitor

no terminal monitor

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

This command does not disable all messages from being printed to the console. Messages such as "module add" and "remove events" will still be logged to the console.

Examples

This example shows how to enable logging for Telnet or SSH:

```
n1000v# terminal monitor
n1000v#
```

Related Commands

Command	Description
show terminal	Displays the terminal configuration.
terminal length	Sets the number of lines that appear on the screen.
terminal width	Sets the terminal width.
terminal type	Specifies the terminal type.
terminal session-timeout	Sets the session timeout.

terminal session-timeout

To set session timeout, use the **terminal session-timeout** command.

terminal session-timeout *time*

Syntax Description

time	Timeout time, in seconds. The range of valid values is 0 to 525600.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

Set *time* to 0 to disable timeout.

Examples

This example shows how to set session timeout:

```
n1000v# terminal session-timeout 100
n1000v#
```

Related Commands

Command	Description
show terminal	Displays the terminal configuration.

terminal terminal-type

To specify the terminal type, use the **terminal terminal-type** command.

terminal terminal-type *type*

Syntax Description		
	type	Terminal type.

Defaults None

Command Modes Any

SupportedUserRoles network-admin
network-operator

Command History	Release	Modification
	4.0(4)SV1(1)	This command was introduced.

Examples This example shows how to specify the terminal type:

```
n1000v# terminal terminal-type vt100
n1000v#
```

Related Commands	Command	Description
	show terminal	Displays the terminal configuration.

terminal tree-update

To update the main parse tree, use the **terminal tree-update** command.

terminal tree-update

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to update the main parse tree:

```
n1000v# terminal tree-update
n1000v#
```

Related Commands

Command	Description
show terminal	Displays the terminal configuration.

terminal width

To set terminal width, use the **terminal width** command.

terminal width *number*

Syntax Description		
	number	Number of characters on a single line. The range of valid values is 24 to 511.

Defaults

102 columns

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to set terminal width:

```
n1000v# terminal width 60
n1000v#
```

Related Commands

Command	Description
show terminal	Displays the terminal configuration.

test aaa

To test for AAA on a RADIUS server or server group, use the **test aaa** command.

test aaa {**group** *group-name user-name password* | **server radius** *address* {*user-name password* | **vrf** *vrf-name user-name password*]}}

Syntax Description

group	Specifies an AAA server group.
group-name	AAA server group name. The range of valid values is 1 to 32.
user-name	User name. The range of valid values is 1 to 32.
password	User password. The range of valid values is 1 to 32.
server	Specifies an AAA server.
radius	Specifies a RADIUS server.
address	IP address or DNS name.
vrf	Specifies a virtual route.
vrf-name	Virtual route.name.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to test for AAA on RADIUS server:

```
n1000v# test aaa server radius ts1 vrf route1 user1 9w8e7r
n1000v#
```

Related Commands

Command	Description
show aaa	Displays AAA information.

timers bgp <keepalive-timer> <hold-timer>

To configure Keepalive interval timer and holdtimer for bgp, use the t**imers bgp <keepalive-timer> <hold-timer>** command.

timers bgp <keepalive-timer> <hold-timer>

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
5.2(1)SV3(1.1)	This command was introduced.

Examples

This example shows how to configure Keepalive interval timer and holdtimer for bgp:

```
n1000v(config-router)# timers bgp 180 180
```

Related Commands

Command	Description
show aaa	Displays AAA information.

track network-state enable

To enable Network State Tracking for all VEMs configured with a vPC-HM port-profile , use the **track network-state enable** command. To disable Network State Tracking, use the **no** form of this command.

track network-state enable

no track network-state

Syntax Description

This command has no arguments or keywords.

Defaults

disabled

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV1(4)	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to enable Network State Tracking for all VEMs configured with a vPC-HM port-profile:

```
n1000v# config t
n1000v(config)# track network-state enable
n1000v(config)#
```

This example shows how to disable Network State Tracking:

```
n1000v(config)# no track network-state
n1000v(config)#
```

Related Commands

Command	Description
show network-state tracking config	Displays the Network State Tracking configuration for verification.
show network-state tracking {**module** *modID* | **interface** *channelID*}	Displays the Network State Tracking status for a module or interface.

track network-state interval

To specify an interval of time, from 1 to 10 seconds, between which Network State Tracking broadcasts are sent to pinpoint link failure on a port channel configured for vPC-HM, use the **track network-state interval** command. To remove the configured interval, use the **no** form of this command.

track network-state interval *intv*

no track network-state interval

Syntax Description

intv	Broadcast interval (from 1 to 10 seconds). The default is 5 seconds.

Defaults

5 seconds

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV1(4)	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to specify an interval for sending broadcasts:

```
n1000v(config)# track network-state interval 8
n1000v(config)#
```

This example shows how to remove the broadcast interval configuration:

```
n1000v(config)# no track network-state interval
n1000v(config)#
```

Related Commands

Command	Description
show network-state tracking	Displays the Network State Tracking status for a module or interface.
show network-state tracking config	Displays the Network State Tracking configuration for verification.
tracking enable	Enables Network State Tracking for all VEMs configured with a vPC-HM port-profile.

track network-state threshold miss-count

To specify the maximum number of Network State Tracking broadcasts that can be missed consecutively before a split network is declared, use the **track network-state threshold miss-count** command. To remove the configuration, use the **no** form of this command.

track network-state threshold miss-count *count*

no track network-state threshold miss-count

Syntax Description

count	Specifies the number of Network State Tracking broadcasts that can be missed from 3 to 7. The default is 5.

Defaults

5 missed broadcasts

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV1(4)	This command was introduced.

Examples

This example shows how to configure the maximum number of Network State Tracking broadcasts that can be missed:

```
n1000v# config t
n1000v(config)# network-state tracking threshold miss-count 7
n1000v(config)#
```

This example shows how to remove the configuration:

```
n1000v(config)# no network-state tracking threshold miss-count
n1000v(config)#
```

Related Commands

Command	Description
show network-state tracking	Displays the Network State Tracking status for a module or interface.
show network-state tracking config	Displays the Network State Tracking configuration for verification.
tracking enable	Enables Network State Tracking for all VEMs configured with a vPC-HM port-profile.

track network-state split action

To specify the action to take if a split network is detected by Network State Tracking, use the **track network-state split action** command. To remove the configuration, use the **no** form of this command.

track network-state split action

no track network-state split action

Syntax Description

repin	If a split network is detected by Network State Tracking, the traffic is pinned to another uplink. (the default)
log-only	If a split network is detected by Network State Tracking, traffic is not repinned, and system messages are logged only.

Defaults

repin

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV1(4)	This command was introduced.

Examples

This example shows how to specify the action to take if Network State Tracking detects a split network:

```
n1000v# config t
n1000v(config)# track network-state split action repin
n1000v(config)#
```

This example shows how to remove the configuration:

```
n1000v(config)# no track network-state split action repin
n1000v(config)#
```

Related Commands

Command	Description
show network-state tracking	Displays the Network State Tracking status for a module or interface.
show network-state tracking config	Displays the Network State Tracking configuration for verification.
tracking enable	Enables Network State Tracking for all VEMs configured with a vPC-HM port-profile.

traceroute

To discover the routes that packets take when traveling to an IPv4 address, use the **traceroute** command.

traceroute {*dest-ipv4-addr* | *hostname*} [**vrf** *vrf-name*] [**show-mpls-hops**] [**source** *src-ipv4-addr*]

Syntax Description

dest-ipv4-addr	IPv4 address of the destination device. The format is *A.B.C.D*.
hostname	Name of the destination device. The name is case sensitive.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) to use. The name is case sensitive.
show-mpls-hops	(Optional) Displays the Multiprotocol Label Switching (MPLS) hops.
source *src-ipv4-addr*	(Optional) Specifies a source IPv4 address. The format is *A.B.C.D*.

Defaults

Uses the default VRF.
Does not show the MPLS hops.
Uses the management IPv4 address for the source address.

Command Modes

Any

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

To use IPv6 addressing for discovering the route to a device, use the **traceroute6** command.

Examples

This example shows how to discover a route to a device:

```
n1000v# traceroute 172.28.255.18 vrf management
traceroute to 172.28.255.18 (172.28.255.18), 30 hops max, 40 byte packets
 1  172.28.230.1 (172.28.230.1)  0.746 ms  0.595 ms  0.479 ms
 2  172.24.114.213 (172.24.114.213)  0.592 ms  0.51 ms  0.486 ms
 3  172.20.147.50 (172.20.147.50)  0.701 ms  0.58 ms  0.486 ms
 4  172.28.255.18 (172.28.255.18)  0.495 ms  0.43 ms  0.482 ms
```

Related Commands

Command	Description
traceroute6	Discovers the route to a device using IPv6 addressing.

transport ip address A.B.C.D gateway A.B.C.D

Configures VXLAN termination or a VTEP on the VXLAN gateway. Creating VTEP port-profile is similar to the steps described under *Configuring vmknics for VXLAN Encapsulation* except the vmware port-group command which is not supported on the VXLAN gateway.

[no] transport ip address *A.B.C.D* **gateway** *A.B.C.D*

Note Starting with Release 5.2(1)SV3(1.15), Cisco Nexus 1000V for VMware vSphere does not support the VXLAN gateway feature.

Syntax Description

A.B.C.D	IPv4 address of the encapsulation device.
A.B.C.D	IPv4 default gateway address of the encapsulation device.

Defaults

None.

Command Modes

Port-profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV2(2.1)	This command was introduced.

Usage Guidelines

Configures VXLAN termination or a VTEP on the VXLAN gateway.

Examples

This example shows how to configure transport ip address:

```
n1000v# config t
n1000v(config)# port-profile type vethernet vmknic_vtep
n1000v(config-port-prof)# transport ip address 192.168.10.100 255.255.255.0 gateway
192.168.10.1
```

This example shows how to remove transport ip address:

```
n1000v# config t
n1000v(config)# port-profile type vethernet vmknic_vtep
n1000v(config-port-prof)# no transport ip address 192.168.10.100 255.255.255.0 gateway
192.168.10.1
```

Related Commands None.

transport udp (NetFlow)

To add a destination UDP port from the NetFlow exporter to the collector, use the **transport udp** command. To remove the port, use the **no** form of this command.

transport udp *portnumber*

no transport udp

portnumber	Destination UDP number from 1 to 65535.

Defaults

None

Command Modes

Netflow flow exporter configuration (**config-flow-exporter**)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

Avoid using well-known ports 1-1024 when possible.

Examples

This example shows how to add UDP 200 to the flow exporter:

```
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# transport udp 200
```

This example shows how to remove UDP 200 from the flow exporter:

```
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# no transport udp 200
```

Related Commands

Command	Description
flow exporter	Creates a Flexible NetFlow flow exporter.
flow record	Creates a Flexible NetFlow flow record.
flow monitor	Creates a Flexible NetFlow flow monitor.
show flow exporter	Displays information about the NetFlow flow exporter.
show flow record	Displays information about NetFlow flow records.
show flow monitor	Displays information about the NetFlow flow monitor.

type

To define the network segmentation policy type, use the **type** command. To remove the network segmentation policy type, use the **no** form of this command.

type {*nw_type*}

no type [{*nw_type*}]

Syntax Description

nw_type	The type of the network segmentation policy.

Defaults

None

Command Modes

Network Segment Policy configuration (config-network-segment-policy)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV1(5.1)	This command was introduced.

Usage Guidelines

The policy type can be Segmentation or VLAN. For segmentation policy, VXLAN is used. For more information, see the *Cisco Nexus 1000V VXLAN Configuration Guide, Release 4.2(1)SV2(1.1)*.

The policy type corresponds to the network pools in the vCloud Director. The policy type Segmentation corresponds to the network isolation-backed network pool in the vCloud Director. The policy type VLAN corresponds to the VLAN-backed network pool in the vCloud Director.

Once configured, the type cannot be changed.

Examples

This example shows how to define the network segmentation policy type:

```
n1000v# configure terminal
n1000v(config)# network-segment policy abc-policy-vxlan
n1000v(config-network-segment-policy)# type segmentation
n1000v(config-network-segment-policy)
```

Related Commands

Command	Description
network-segment policy	Creates a network segmentation policy.
show run network-segment policy	Displays the network segmentation policy configuration.