NSX Command Line Interface Reference

NSX 6.1 for vSphere

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001589-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About This Book

The *NSX Command Line Interface Reference* describes how to use the NSX for vSphere Command Line Interface (CLI) and includes examples and command overviews.

Intended Audience

This guide is intended for anyone who wants to install or use NSX in a VMware vCenter environment. The information in this guide is written for experienced system administrators who are familiar with virtual machine technology and virtual datacenter operations. This guide assumes familiarity with VMware Infrastructure 4.x, including VMware ESX, vCenter Server, and the vSphere Client.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation go to http://www.vmware.com/support/pubs.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

NSX Documentation

The following documents comprise the NSX documentation set:

- *NSX Administration Guide*
- *NSX Installation and Upgrade Guide*
- *NSX API Programming Guide*

Introduction to the NSX CLI 1

IT organizations have gained significant benefits as a direct result of server virtualization. Server consolidation reduced physical complexity, increased operational efficiency and the ability to dynamically re-purpose underlying resources to quickly and optimally meet the needs of increasingly dynamic business applications.

VMware's Software Defined Data Center (SDDC) architecture is now extending virtualization technologies across the entire physical data center infrastructure. VMware NSX®, the network virtualization platform, is a key product in the SDDC architecture. With NSX, virtualization delivers for networking what it has already delivered for compute and storage. In much the same way that server virtualization programmatically creates, snapshots, deletes and restores software-based virtual machines (VMs), NSX network virtualization programmatically creates, snapshots, deletes, and restores software-based virtual networks. The result is a completely transformative approach to networking that not only enables data center managers to achieve orders of magnitude better agility and economics, but also allows for a vastly simplified operational model for the underlying physical network. With the ability to be deployed on any IP network, including both existing traditional networking models and next-generation fabric architectures from any vendor, NSX is a completely non-disruptive solution. In fact, with NSX, the physical network infrastructure you already have is all you need to deploy a software-defined data center.

To use the NSX virtual appliance CLI, you must have console access to an NSX virtual appliance. Each NSX virtual appliance contains a command line interface (CLI). The viewable modes in the NSX CLI can differ based on the assigned role and rights of a user. If you are unable to access an interface mode or issue a particular command, consult your NSX administrator.

NOTE User account management in the CLI is separate from user account management in the NSX Manager user interface.

This chapter includes the following topics:

CLI Command Modes

The commands available to you at any given time depend on the mode you are currently in.

NOTE NSX Edge virtual machines have Basic mode only.

- **Basic**. Basic mode is a read-only mode. To have access to all commands, you must enter Privileged mode.

- **Privileged**. Privileged mode commands allow support-level options such as debugging and system diagnostics. To save configuration changes you have made in Privileged mode, you must run the write memory command. Otherwise, the changes are lost upon reboot.
- **Configuration**. Configuration mode commands allow you to change the current configuration of utilities on an NSX virtual appliance. You can access Configuration mode from Privileged mode. From Configuration mode, you can enter Interface configuration mode.
- **Interface Configuration**. Interface Configuration mode commands allow you to change the configuration of virtual machine interfaces. For example, you can change the IP address and IP route for the management port of the NSX Manager.

Logging In and Out of the CLI

Before you can run CLI commands, you must initiate a console session to an NSX virtual appliance. To open a console session within the vSphere Client, select the NSX virtual appliance from the inventory panel and click the **Console** tab. You can log in to the CLI by using the default user name admin and the password you specified while installing NSX Manager.

You can also use SSH to access the CLI. If you did not enable SSH while installing NSX Manager, you can use the ssh command to enable and disable the SSH service on an NSX virtual appliance. See "ssh" on page 29.

To log out, type exit from either Basic or Privileged mode.

Syntax Notation Used in this Document

Run commands at the prompt as shown. Do not type the ( ), < >, or [ ] symbols.

command A.B.C.D (option1 | option2) <0-512> [WORD]

- Required numerical ranges are enclosed in angle brackets.
- Required text is presented in all capital letters.
- Multiple, required keywords or options are enclosed in parentheses and separated by a pipe character.
- An optional keyword or value is enclosed in square brackets.

Moving Around in the CLI

The following commands move the pointer around on the command line.

Keystrokes	Description
CTRL+A	Moves the pointer to beginning of the line.
CTRL+B or the left arrow key	Moves the pointer back one character.
CTRL+C	Ends any operation that continues to propagate, such as a ping.
CTRL+D	Deletes the character at the pointer.
CTRL+E	Moves the pointer to end of the line.
CTRL+F or the right arrow key	Moves the pointer forward one character.
CTRL+K	Deletes all characters from the pointer to the end of the line.
CTRL+N or the down arrow key	Displays more recent commands in the history buffer after recalling commands with CTRL+P (or the up arrow key). Repeat to recall other recently run commands.
CTRL+P or the up arrow key	Recalls commands in the history, starting with the most recent completed command. Repeat to recall successively older commands.
CTRL+U	Deletes all characters from the pointer to beginning of the line.

Keystrokes	Description
CTRL+W	Deletes the word to the left of pointer.
ENTER	Scrolls down one line.
ESC+B	Moves the pointer back one word.
ESC+D	Deletes all characters from the pointer to the end of the word.
ESC+F	Moves the pointer forward one word.
SPACE	Scrolls down one screen.

Getting Help within the CLI

The CLI contains the following commands to assist you.

Command	Description
?	Moves the pointer to the beginning of the line.
sho?	Displays a list of commands that begin with a particular character string.
exp+TAB	Completes a partial command name.
show ?	Lists the associated keywords of a command.
show log ?	Lists the associated arguments of a keyword.
list	Displays the verbose options of all commands for the current mode.

Securing CLI User Accounts 2

Each NSX virtual appliance comes with a default user account and password.

NOTE User account management in the CLI is separate from user account management in the NSX Manager user interface.

This chapter includes the following topics:

CLI User Account Management

You must manage CLI user accounts separately on each NSX virtual appliance. By default, you use the admin user account to log in to the CLI of each NSX virtual appliance.

The Privileged mode password is managed separately from the admin user account password. The default Privileged mode password is the same for each CLI user account.

IMPORTANT Each NSX virtual appliance has a built-in CLI user account (nobody) for system use. Do not delete or modify this account. If this account is deleted or modified, the virtual machine will not work.

You can create new CLI user accounts. Each created user account has administrator-level access to the CLI.

Hardening the CLI of an NSX Virtual Appliance

To harden access to the CLI of an NSX virtual appliance, you must change the admin user account and Privileged mode passwords after initial login.

Change the admin User Account Password

To change the admin user account password

1 Log in to the vSphere Client and select an NSX virtual appliance from the inventory.

2 Click the **Console** tab to open a CLI session.

3 Log in to the CLI and switch to Privileged mode.

```
manager> enable
password:
manager#
```

4 Switch to Configuration mode.

```
manager# configure terminal
```

5 Change the admin account password.

```
manager(config)# cli password PASSWORD
```

where PASSWORD is replaced with the new password you want to use.

6 Save the configuration.

```
manager(config)# write memory
Building Configuration...
Configuration saved.
[OK]
```

Change the CLI Privileged Mode Password

You can change the Privileged mode password to secure access to the configuration options of the CLI.

To change the Privileged mode password

1 Log in to the vSphere Client and select an NSX virtual appliance from the inventory.

2 Click the **Console** tab to open a CLI session.

3 Log in to the CLI and switch to Privileged mode.

```
manager> enable
password:
manager#
```

4 Switch to Configuration mode.

```
manager# configure terminal
```

5 Change the Privileged mode password.

```
manager(config)# enable password PASSWORD
```

6 Save the configuration.

```
manager(config)# write memory
Building Configuration...
Configuration saved.
[OK]
```

7 Run the exit command twice to log out of the CLI.

```
manager(config)# exit
manager# exit
```

8 Log in to the CLI and switch to Privileged mode by using the new password.

```
manager> enable
password:
manager#
```

Add a CLI User Account

You can add CLI user accounts for each NSX virtual appliance.

To add a CLI user account

1 Log in to the vSphere Client and select an NSX virtual appliance from the inventory.

2 Click the **Console** tab to open a CLI session.

3 Log in by using the admin account.

```
manager login: admin
password:
manager>
```

4 Switch to Privileged mode.

```
manager> enable
password:
manager#
```

5 Switch to Configuration mode.

```
manager# configure terminal
```

6 Add a user account.

```
manager(config)# user abc password plaintext PASSWORD
```

where abc is replaced with the username and PASSWORD is replaced with the desired password.

7 Save the configuration.

```
manager(config)# write memory
Building Configuration...
Configuration saved.
[OK]
```

8 Exit the CLI.

```
manager(config)# exit
manager# exit
```

Delete the admin User Account from the CLI

Do not delete the admin user account until you add a user account to replace the admin account. This prevents you from being locked out of the CLI.

To delete the admin user account

1 Log in to the vSphere Client and select an NSX virtual appliance from the inventory.

2 Click the **Console** tab to open a CLI session.

3 Log in by using a user account other than admin.

4 Switch to Privileged mode.

```
manager> enable
password:
manager#
```

5 Switch to Configuration mode.

```
manager# configure terminal
```

6 Delete the admin user account.

```
manager(config)# no user admin
```

7 Save the configuration.

```
manager(config)# write memory
Building Configuration...
Configuration saved.
[OK]
```

8 Run the exit command twice to log out of the CLI.

```
manager(config)# exit
manager# exit
```

NSX CLI Commands 3

The chapter includes the following topics:

NSX Manager Commands

This section describes NSX Manager CLI commands.

configure terminal

Switches to Configuration mode from Privileged mode.

Synopsis

configure terminal

CLI Mode

Privileged

Example

```
vShield# configure terminal
vShield(config)#
```

Related Commands

interface

database erase

Erases the NSX Manager database, resetting the database to factory defaults. This command clears all configuration data from the NSX Manager user interface. The NSX Manager CLI configuration is not affected by this command.

Synopsis

database erase

CLI Mode

Privileged

Example

manager# database erase

disable

Switches to Basic mode from Privileged mode.

Synopsis

disable

CLI Mode

Basic

Example

vShield# disable
vShield>

Related Commands

enable

enable

Switches to Privileged mode from Basic mode.

Synopsis

enable

CLI Mode

Basic

Example

vShield> enable
password:
vShield#

Related Commands

disable

enable password

Changes the Privileged mode password. You should change the Privileged mode password for each NSX virtual machine. CLI user passwords and the Privileged mode password are managed separately. The Privileged mode password is the same for each CLI user account.

Synopsis

enable password PASSWORD

Option	Description
PASSWORD	Password to use. The default password is default.

CLI Mode

Configuration

Example

```
vShield# configure terminal
vShield(config)# enable password abcd123
```

Related Commands

enable

exit

Exits from the current mode and switches to the previous mode, or exits the CLI session if run from Privileged or Basic mode.

Synopsis

```
exit
```

CLI Mode

Basic, Privileged, Configuration, and Interface Configuration

Example

```
vShield(config-if)# exit
vShield(config)# exit
vShield#
```

Related Commands

quit

export tech-support scp

Exports the system diagnostics to a specific location via Secure Copy Protocol (SCP). You can also export system diagnostics for an NSX virtual machine from the NSX Manager user interface.

Synopsis

```
export tech-support scp URL
```

Option	Description
URL	Enter the username and complete path of the destination. Standard scp /ssh syntax is used for username and machine name.

CLI Mode

Basic and Privileged

Example

```
vShield# export tech-support scp user123@host123:file123
```

hostname

Changes the host name of the machine, which is used as the CLI prompt. The default prompt name for the NSX Manager is `manager`.

Synopsis

```
hostname WORD
```

Option	Description
WORD	Prompt name to use.

CLI Mode

Configuration

Example

```
vShield(config)# hostname vs123
vs123(config)#
```

interface

Switches to Interface Configuration mode for the specified interface.

To delete the configuration of an interface, use no before the command.

Synopsis

```
[no] interface mgmt
```

Option	Description
mgmt	The management port on an NSX virtual machine.

CLI Mode

Configuration

Example

```
vShield# configure terminal
vShield(config)# interface mgmt
vShield(config-if)#
```

or

```
vShield(config)# no interface mgmt
```

ip address

Assigns an IP address to an interface. On the NSX virtual machines, you can assign an IP address to the management interface only.

To remove an IP address from an interface, use no before the command.

Synopsis

```
[no] ip address A.B.C.D/M
```

Option	Description
A.B.C.D	IP address to use.
M	Subnet mask to use.

CLI Mode

Interface Configuration

Example

```
vShield(config)# interface mgmt
vShield(config-if)# ip address 192.168.110.200/24
```

or

```
vShield(config)# interface mgmt
vShield(config-if)# no ip address 192.168.110.200/24
```

ip route

Adds a static route.

To delete an IP route, use no before the command.

Synopsis

[no] ip route A.B.C.D/M W.X.Y.Z

Option	Description
A.B.C.D	IP address to use.
M	Subnet mask to use.
W.X.Y.Z	IP address of network gateway.

CLI Mode

Configuration

Example

```
vShield# configure terminal
vShield(config)# ip route 0.0.0.0/0 192.168.1.1
```

or

```
vShield(config)# no ip route 0.0.0.0/0 192.168.1.1
```

list

Lists all in-mode commands.

Synopsis

list

CLI Mode

Basic, Privileged, Configuration, Interface Configuration

Examples

```
NSXMgr> list
  enable
  exit
  list
  ping WORD
...
```

ping

Pings a destination by its hostname or IP address.

Synopsis

ping (HOSTNAME | A.B.C.D)

Option	Description
HOSTNAME | A.B.C.D	The hostname or IP address of the target system.

CLI Mode

Basic, Privileged

Usage Guidelines

Enter CTRL+C to end ping replies.

Example

vShield# ping 192.168.1.1

reset

Resets the terminal settings to remove the current screen output and return a clean prompt.

Synopsis

reset

CLI Mode

Basic, Privileged, Configuration

Example

manager# reset

Related Commands

terminal length

terminal no length

quit

Quits Interface Configuration mode and switches to Configuration mode, or quits the CLI session if run from Privileged or Basic mode.

Synopsis

quit

CLI Mode

Basic, Privileged, and Interface Configuration

Example

vShield(config-if)# quit
vShield(config)#

Related Commands

exit

reboot

Reboots an NSX virtual appliance.

Synopsis

reboot

CLI Mode

Privileged

Related Commands

shutdown

set clock

Sets the date and time if not using an NTP server.

Synopsis

set clock HH:MM:SS MM DD YYYY

Option	Description
HH:MM:SS	Hours:minutes:seconds
MM	Month
DD	Day
YYYY	Year

CLI Mode

Privileged

Example

```
vShield# show  clock
Mon Apr  7 05:26:49 UTC 2014
```

Related Commands

show clock

setup

Opens the CLI initialization wizard for NSX virtual machine installation. You configure multiple settings by using this command. You run the setup command during NSX Manager installation. Press ENTER to accept a default value.

Synopsis

setup

CLI Mode

Basic

Example

```
manager(config)# setup
Default settings are in square brackets '[]'.
Hostname [manager]:
IP Address (A.B.C.D or A.B.C.D/MASK): 192.168.0.253
Default gateway (A.B.C.D): 192.168.0.1
Old configuration will be lost, and system needs to be rebooted
Do you want to save new configuration (y/[n]): y
Please log out and log back in again.
```

show arp

Shows the contents of the ARP cache.

Synopsis

show arp

CLI Mode

Basic, Privileged

Example

```
vShield# show arp
IP address       HW type     Flags       HW address            Mask     Device
192.0.2.130      0x1         0x6         00:00:00:00:00:81     *        virteth1
192.168.110.1    0x1         0x2         00:0F:90:D5:36:C1     *        mgmt
```

show clock

Shows the current time and date of the virtual machine. If you use an NTP server for time synchronization, the time is based on Coordinated Universal Time (UTC).

Synopsis

show clock

CLI Mode

Basic, Privileged

Example

```
vShield# show clock
Wed Feb  9 13:04:50 UTC 2005
```

Related Commands

set clock

show ethernet

Shows Ethernet information for virtual machine interfaces.

Synopsis

show ethernet

CLI Mode

Basic, Privileged

Example

```
vShield# show ethernet
Settings for mgmt:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised auto-negotiation: Yes
        Speed: 100Mb/s
        Duplex: Full
```

show filesystem

Shows the hard disk drive capacity for an NSX virtual machine. NSX Manager has two disk drives.

Synopsis

show filesystem

CLI Mode

Basic, Privileged

Example

```
vShield# show filesystem
Filesystem            Size  Used Avail Use% Mounted on
/dev/hda3             4.9G  730M  3.9G  16% /
/dev/hda6             985M   17M  919M   2% /tmp
/dev/hda7              24G  1.7G   21G   8% /common
```

show manager log

Shows the system log of the NSX Manager.

Synopsis

show manager log [follow | reverse]

Option	Description
follow	Update the displayed log every 5 seconds.
reverse	Show the log in reverse chronological order.
size	Display manager log size.
last *n*	Display the last *n* number of events in the NSX Manager log.

CLI Mode

Basic, Privileged

Example

```
vShield# show manager log
SEM Debug Nov 15, 2005 02:46:23 PM PropertyUtils Prefix:applicationDir

SEM Debug Nov 15, 2005 02:46:23 PM PropertyUtils Props Read:[]
SEM Info Nov 15, 2005 02:46:23 PM RefreshDb UpdateVersionNumbers info does not exist

SEM Debug Nov 15, 2005 02:46:23 PM RefreshDb Applications: []
SEM Info Nov 15, 2005 02:46:23 PM RefreshDb Compiler version pairs found: []
```

Related Commands

show manager log last

show manager log last

Shows the last *n* number of events in the NSX Manager log.

Synopsis

show manager log last NUM

Option	Description
NUM	Number of events to display.

CLI Mode

Basic, Privileged

Example

```
manager# show manager log last 10
```

Related Commands

show network interface

show slots

Shows the software images on the slots of an NSX virtual machine. Boot indicates the image that is used to boot the virtual machine.

Synopsis

show slots

CLI Mode

Basic, Privileged

Example

```
manager# show slots
Recovery:  System Recovery v0.3.2
Slot 1:    13Aug09-09.49PDT
Slot 2:    * 16Aug09-23.52PDT (Boot)
```

show tech-support

Shows the system diagnostic log that can be sent to technical support by running the export tech-support scp command.

Synopsis

show tech-support

CLI Mode

Basic, Privileged

Example

```
vShield# show tech-support
```

shutdown

In Privileged mode, the shutdown command powers off the virtual machine. In Interface Configuration mode, the shutdown command disables the interface.

To enable a disabled interface, use no before the command.

Synopsis

[no] shutdown

CLI Mode

Privileged, Interface Configuration

Example

```
vShield# shutdown
```

or

```
vShield(config)# interface mgmt
vShield(config-if)# shutdown
vShield(config-if)# no shutdown
```

Related Commands

reboot

The feature commands help you monitor NSX Edge states and statistics.

ssh

Starts or stops the SSH service on an NSX virtual appliance.

Synopsis

ssh (start | stop)

CLI Mode

Privileged

Example

manager# ssh start

or

manager# ssh stop

terminal length

Sets the number of rows to display at a time in the CLI terminal.

Synopsis

terminal length <0-512>

Option	Description
0-512	Enter the number of rows to display. If length is 0, no display control is performed.

CLI Mode

Privileged

Example

manager# terminal length 50

Related Commands

terminal length

terminal no length

terminal no length

Negates the terminal length command.

Synopsis

terminal no length

CLI Mode

Privileged

Example

manager# terminal no length

Related Commands

terminal length

terminal length

traceroute

Traces the route to a destination.

Synopsis

traceroute (HOSTNAME | A.B.C.D)

Option	Description
HOSTNAME | A.B.C.D	The hostname or IP address of the target system.

CLI Mode

Basic, Privileged

Example

```
vShield# traceroute 10.16.67.118
traceroute to 10.16.67.118 (10.16.67.118), 30 hops max, 40 byte packets
 1  10.115.219.253 (10.115.219.253)  128.808 ms  74.876 ms  74.554 ms
 2  10.17.248.51 (10.17.248.51)  0.873 ms  0.934 ms  0.814 ms
 3  10.16.101.150 (10.16.101.150)  0.890 ms  0.913 ms  0.713 ms
 4  10.16.67.118 (10.16.67.118)  1.120 ms  1.054 ms  1.273 ms
```

user

Adds a CLI user account. The user admin is the default user account. The CLI admin account and password are separate from the vShield Manager user interface admin account and password.

IMPORTANT Each vShield virtual machine has two built-in CLI user accounts for system use: nobody and vs_comm. Do not delete or modify these accounts. If these accounts are deleted or modified, the virtual machine will not work.

To remove a CLI user account, use no before the command.

Synopsis

[no] user USERNAME password (hash | plaintext) PASSWORD

Option	Description
USERNAME	Login name of the user.
hash	Masks the password by using the MD5 hash. You can view and copy the provided MD5 hash by running the show running-config command.
plaintext	Keeps the password unmasked.
PASSWORD	Password to use.

CLI Mode

Configuration

Example

```
vShield(config)# user newuser1 password plaintext abcd1234
```

or

```
vShield(config) no user newuser1
```

write

Writes the running configuration to memory. This command performs the same operation as the write memory command.

Synopsis

write

CLI Mode

Privileged

Example

manager# write

Related Commands

write memory

write erase

Resets the CLI configuration to factory default settings.

Synopsis

write erase

CLI Mode

Privileged

Example

manager# write erase

write memory

Writes the current configuration to memory. This command is identical to the write command.

Synopsis

write memory

CLI Mode

Privileged, Configuration, and Interface Configuration

Example

manager# write memory

Related Commands

write

NSX Edge Commands

This section describes NSX Edge CLI commands.

clear nat counters

Resets NAT counters to zeros.

Synopsis

clear nat counters

CLI Mode

Privileged, Configuration, and Interface Configuration

clear arp WORD

Deletes an ARP entry from the ARP table, which is associated with the specified IP address.

Synopsis

clear arp WORD

CLI Mode

Privileged

clear service dhcp lease

Removes DHCP lease information from the DHCP service.

Synopsis

clear service dhcp lease

CLI Mode

Privileged

clear service ipsec sa

Deletes the SA (Security Association) associated with the specified peer name.

Synopsis

clear service ipsec sa WORD

CLI Mode

Privileged

debug packet capture

Captures all packets processed by an NSX Edge, similar to a tcpdump. Enabling this command can slow NSX Edge performance. Packet debug capture is disabled by default. To disable packet capture, use no before the command.

Synopsis

[no] debug packet capture (intif| extif)) [EXPRESSION]

intif | extif	The specific NSX Edge interface from which to capture packets.
EXPRESSION	A tcpdump-formatted string. You must use an underscore between words in the expression.

CLI Mode

Privileged

debug packet display interface

Displays all packets captured by an NSX Edge interface, similar to a tcpdump. Enabling this command can impact NSX Edge performance. To disable the display of packets, use no before the command.

Synopsis

[no] debug packet display interface (intif | extif) [EXPRESSION]

intif | extif	The specific NSX Edge interface from which to display packets.
EXPRESSION	A tcpdump-formatted string. You must use an underscore between words in the expression.

CLI Mode

Privileged

dnslookup *serverName*

Makes DNS lookup query to the specified DNS server.

Synopsis

dnslookup ABC

CLI Mode

Basic

dnslookup *serverName* | *address*

Makes DNS lookup query for the specified host or IP address.

Synopsis

dnslookup *server name_or_address*

CLI Mode

Basic

debug crashdump

Activates crash dump support and triggers a reboot. After the reboot, NSX Edge runs with crashkernel support active. When a kernel panic occurs, NSX Edge boots the crash kernel and stores the kernel dump to the file system. Edge then reboots again back into the standard kernel, with crashdump still enabled.

To view the kernel dump file, use debug show files.

To copy the kernel dump file, use debug copy [ftp|scp] ....

To delete the kernel dump file, use debug remove [<filename>|all].

When crashdump is enabled, the available NSX Edge memory is reduced by 64MB. To disable crashdump support, type no debug crashdump.

The debug crashdump command is not supported for the 64 bit X-Large NSX Edge.

Synopsis

debug crashdump

CLI Mode

Privileged

debug packet display interface

Displays all packets captured by an NSX Edge interface, similar to a tcpdump. Enabling this command can impact NSX Edge performance.

To disable the display of packets, use no before the command.

Synopsis

[no] debug packet display interface mgmt [EXPRESSION]

Option	Description
mgmt	The specific interface from which to capture packets.
EXPRESSION	A tcpdump-formatted string. You must use an underscore between words in the expression.

NSX Edge

[no] debug packet display interface (intif | extif) [EXPRESSION]

Option	Description
intif | extif	The specific NSX Edge interface from which to capture packets.
EXPRESSION	A tcpdump-formatted string. You must use an underscore between words in the expression.

CLI Mode

Privileged

Example

vShield# debug packet display interface mgmt host_10.10.11.11_and_port_80

export tech-support scp

Exports the system diagnostics to a specific location via Secure Copy Protocol (SCP). You can also export system diagnostics for an NSX virtual machine from the NSX Manager user interface.

Synopsis

export tech-support scp URL

Option	Description
URL	Enter the complete path of the destination.

CLI Mode

Basic and Privileged

Example

vShield# export tech-support scp user123@host123:file123

ping

Pings a destination by its hostname or IP address.

Synopsis

ping (HOSTNAME | A.B.C.D)

Option	Description
HOSTNAME | A.B.C.D	The hostname or IP address of the target system.

CLI Mode

Basic, Privileged

Usage Guidelines

Enter CTRL+C to end ping replies.

Example

vShield# ping 192.168.1.1

ping interface addr

Pings an external destination from the internal address of a virtual machine protected by an NSX Edge.

Synopsis

ping interface addr (SOURCE_HOSTNAME | A.B.C.D) (DEST_HOSTNAME | A.B.C.D)

Option	Description
SOURCE_HOSTNAME | A.B.C.D	The hostname or internal IP address of a virtual machine protected by an NSX Edge.
DEST HOSTNAME | A.B.C.D	The hostname or IP address of the destination.

CLI Mode

Basic, Privileged

Usage Guidelines

This command is useful for debugging IPSec-related issues.

Enter CTRL+C to end ping replies.

Example

vshieldEdge# ping interface addr 192.168.1.1 69.147.76.15

show arp

Shows the Address Resolution Protocol (ARP) settings for the NSX Edge.

Synopsis

show arp

CLI Mode

Basic

Example

vShield Edge ARP Cache:

IP Address	Interface	MAC Address	State
10.115.172.1	vNic_0	00:00:0c:07:ac:01	DELAY
10.115.172.161	vNic_0	00:0c:29:ee:40:b9	STALE

show clock

Shows the current time and date of the virtual machine. If you use an NTP server for time synchronization, the time is based on Coordinated Universal Time (UTC).

Synopsis

show clock

CLI Mode

Basic, Privileged

Example

vShield# show clock

Wed Feb 9 13:04:50 UTC 2005

Related Commands

set clock

show configuration

Shows either the current global configuration or the configuration for a specified service on an NSX Edge.

Synopsis

show configuration (dhcp | firewall | ipsec | loadbalancer | nat | syslog | loadbalancer)

Option	Description
dhcp	Show the current DHCP configuration.
firewall	Show the current firewall configuration.
ipsec	Show the current VPN configuration.
l2vpn	Show the current L2 VPN configuration
loadbalancer	Show the current Load Balancer configuration.
nat	Show the current NAT configuration.
syslog	Show the current syslog configuration.

Usage for each option is shown in the command descriptions below.

CLI Mode

Basic

Example

vShieldEdge# show configuration dhcp

show configuration dhcp

Shows NSX Edge IP address pooling and one-to-one static IP address allocation.

Synopsis

show configuration dhcp

CLI Mode

Basic

Example

```
vShield-edge-2-0> show configuration dhcp
-----------------------------------------------------------------------
vShield Edge DHCP Config:
{
  "dhcp" : {
    "relay" : null,
    "logging" : {
      "enable" : false,
      "logLevel" : "info"
    },
    "enable" : true,
    "bindings" : {
      "vNic_1" : {
        "staticBindings" : [],
        "ipPools" : [
          {
```

```
            "subnetMask" : "255.255.255.0",
            "maxLeaseTime" : "86400",
            "endIp" : "11.1.1.100",
            "primaryNameServer" : null,
            "defaultGateway" : "11.1.1.1",
            "defaultLeaseTime" : "86400",
            "domainName" : null,
            "secondaryNameServer" : null,
            "startIp" : "11.1.1.2"
          }
        ]
      }
    }
  }
}
```


show configuration dns

Shows external DNS servers.

Synopsis

show configuration dns

CLI Mode

Basic

Example


```
vShield-edge-2-0>  show configuration dns
--------------------------------------------------------------------------------
vShield Edge DNS Config:
{
  "dns" : {
    "views" : [
      {
        "recursion" : true,
        "enableForwarding" : true,
        "name" : "vsm-default-view",
        "zones" : null,
        "forwarders" : [
          "10.112.0.1",
          "10.112.0.2"
        ],
        "matchInterfaces" : [
          "any"
        ],
        "matchClients" : [
          "any"
        ]
      }
    ],
    "logging" : {
      "enable" : false,
      "logLevel" : "info"
    },
    "enable" : true,
    "listenOn" : [
      "10.115.172.18",
      "11.1.1.1"
    ],
    "cacheSize" : 16,
    "zones" : null,
    "forwarders" : [
      "10.112.0.1",
      "10.112.0.2"
```

```
    ]
  }
}
```

show configuration firewall

Shows NSX Edge firewall configuration.

Synopsis

show configuration firewall

CLI Mode

Basic

Example

```
vShield-edge-2-0> show configuration firewall
--------------------------------------------------------------------------------
vShield Edge Firewall Config:
{
  "firewall" : {
    "globalConfig" : {
      "ipGenericTimeout" : 120,
      "icmp6Timeout" : 10,
      "tcpPickOngoingConnections" : false,
      "tcpAllowOutOfWindowPackets" : false,
      "tcpTimeoutEstablished" : 3600,
      "disableFirewall" : false,
      "dropInvalidTraffic" : true,
      "tcpTimeoutClose" : 30,
      "icmpTimeout" : 10,
      "udpTimeout" : 60,
      "tcpTimeoutOpen" : 30,
      "tcpSendResetForClosedVsePorts" : true,
      "logInvalidTraffic" : false
    },
    "rules" : [
      {
        "source" : [
          "vse"
        ],
        "dstIface" : [],
        "destination" : [
          "any"
        ],
        "matchTranslated" : false,
        "sourcePort" : [],
        "description" : "firewall",
        "service" : [
          "any:any:any"
        ],
        "srcIface" : [],
        "logging" : {
          "enable" : false,
          "logLevel" : null
        },
        "action" : "accept",
        "id" : 131074
      },
      {
        "source" : [
          "vnic-index-1"
        ],
        "dstIface" : [],
        "destination" : [
```

```
            "vse"
          ],
          "matchTranslated" : false,
          "sourcePort" : [],
          "description" : "dhcp",
          "service" : [
            "17:67:any"
          ],
          "srcIface" : [],
          "logging" : {
            "enable" : false,
            "logLevel" : null
          },
          "action" : "accept",
          "id" : 131075
        },
        {
          "source" : [
            "any"
          ],
          "dstIface" : [],
          "destination" : [
            "10.115.172.18"
          ],
          "matchTranslated" : false,
          "sourcePort" : [],
          "description" : "sslvpn",
          "service" : [
            "6:443:any"
          ],
          "srcIface" : [],
          "logging" : {
            "enable" : false,
            "logLevel" : null
          },
          "action" : "accept",
          "id" : 131076
        },
        {
          "source" : [
            "any"
          ],
          "dstIface" : [],
          "destination" : [
            "any"
          ],
          "matchTranslated" : false,
          "sourcePort" : [],
          "description" : "default rule for ingress traffic",
          "service" : [
            "any:any:any"
          ],
          "srcIface" : [],
          "logging" : {
            "enable" : false,
            "logLevel" : null
          },
          "action" : "accept",
          "id" : 131073
        }
      ]
    }
  }
```


show configuration global

Shows configuration for all NSX Edge services.

Synopsis

show configuration global

CLI Mode

Basic

Example

```
vShield-edge-2-0> show configuration global
------------------------------------------------------------------------
vShield Edge Global Config:
{
  "global" : {
    "edgeAssistId" : 0,
    "enableTcpLoose" : false,
    "hostname" : "vShield-edge-2-0",
    "hypervisorAssist" : false,
    "size" : "compact",
    "fips" : {
      "enable" : false
    },
    "enableAesni" : true,
    "tenantId" : "default",
    "haIndex" : "0",
    "distributedRouter" : false
  }
}
```

show configuration highavailability

Shows high availability configuration for the NSX Edge.

Synopsis

show configuration highavailability

CLI Mode

Basic

Example

```
vShield-edge-2-0> show configuration highavailability
------------------------------------------------------------------------
vShield Edge High Availability Config:
{
  "highAvailability" : {
    "enable" : false,
    "heartbeatInterval" : 0,
    "logging" : null,
    "interface" : null,
    "heartbeatDeadTime" : 0,
    "security" : {
      "psk" : "****",
      "enable" : false,
      "encryptionAlgorithm" : null,
      "authenticationSignature" : {
        "type" : "sha1",
        "key" : "962215d5d6a49a1ae738f5c99087cb2efd87fd65"
      }
    },
    "nodes" : [],
    "heartbeatWarnTime" : 0,
    "heartbeatInitDead" : 0
  }
}
```

show configuration interface

Shows interfaces configured for the NSX Edge.

Synopsis

show configuration interface

CLI Mode

Basic

Example

```
vShield-edge-2-0> show configuration interface
------------------------------------------------------------------------
vShield Edge Interface Config:
{
  "interfaceConfig" : {
    "vNic_0" : {
      "status" : "up",
      "name" : "uplink",
      "sendRedirects" : false,
      "index" : 0,
      "enableProxyArp" : false,
      "lifName" : null,
      "mac" : "00:50:56:a2:57:f9",
      "subnets" : [
        {
          "primary" : "10.115.172.18",
          "address" : [
            "10.115.172.18"
          ],
          "subnet" : "10.115.172.0/24"
        }
      ],
      "mtu" : 1500
    },
    "vNic_9" : {
      "status" : "down",
      "name" : "vnic9",
      "sendRedirects" : true,
      "index" : 9,
      "enableProxyArp" : false,
      "lifName" : null,
      "mac" : "00:50:56:a2:73:98",
      "subnets" : [],
      "mtu" : 1500
    },
    "vNic_4" : {
      "status" : "down",
      "name" : "vnic4",
      "sendRedirects" : true,
      "index" : 4,
      "enableProxyArp" : false,
      "lifName" : null,
      "mac" : "00:50:56:a2:76:06",
      "subnets" : [],
      "mtu" : 1500
    },
    "vNic_7" : {
      "status" : "down",
      "name" : "vnic7",
      "sendRedirects" : true,
      "index" : 7,
      "enableProxyArp" : false,
      "lifName" : null,
      "mac" : "00:50:56:a2:58:c5",
      "subnets" : [],
```

```
    "mtu" : 1500
  },
  "vNic_3" : {
    "status" : "down",
    "name" : "vnic3",
    "sendRedirects" : true,
    "index" : 3,
    "enableProxyArp" : false,
    "lifName" : null,
    "mac" : "00:50:56:a2:f8:e0",
    "subnets" : [],
    "mtu" : 1500
  },
  "vNic_5" : {
    "status" : "down",
    "name" : "vnic5",
    "sendRedirects" : true,
    "index" : 5,
    "enableProxyArp" : false,
    "lifName" : null,
    "mac" : "00:50:56:a2:ce:f7",
    "subnets" : [],
    "mtu" : 1500
  },
  "vNic_8" : {
    "status" : "down",
    "name" : "vnic8",
    "sendRedirects" : true,
    "index" : 8,
    "enableProxyArp" : false,
    "lifName" : null,
    "mac" : "00:50:56:a2:6e:07",
    "subnets" : [],
    "mtu" : 1500
  },
  "vNic_2" : {
    "status" : "down",
    "name" : "vnic2",
    "sendRedirects" : true,
    "index" : 2,
    "enableProxyArp" : false,
    "lifName" : null,
    "mac" : "00:50:56:a2:2b:ec",
    "subnets" : [],
    "mtu" : 1500
  },
  "vNic_6" : {
    "status" : "down",
    "name" : "vnic6",
    "sendRedirects" : true,
    "index" : 6,
    "enableProxyArp" : false,
    "lifName" : null,
    "mac" : "00:50:56:a2:38:33",
    "subnets" : [],
    "mtu" : 1500
  },
  "vNic_1" : {
    "status" : "up",
    "name" : "int",
    "sendRedirects" : false,
    "index" : 1,
    "enableProxyArp" : false,
    "lifName" : null,
    "mac" : "00:50:56:a2:75:f0",
    "subnets" : [
      {
        "primary" : "11.1.1.1",
```

```
            "address" : [
              "11.1.1.1"
            ],
            "subnet" : "11.1.1.0/24"
          }
        ],
        "mtu" : 1500
      }
    }
}
```


show configuration ipsec

Shows certificate configuration for IPSec VPN.

Synopsis

show configuration ipsec

CLI Mode

Basic

Example


```
vShield-edge-2-0>  show configuration ipsec
-----------------------------------------------------------------------------
vShield Edge IPsec VPN Config:
{
  "ipsec" : {
    "sites" : [
      {
        "certificate" : null,
        "encryptionAlgorithm" : "aes",
        "enabled" : true,
        "mtu" : null,
        "psk" : "****",
        "extension" : null,
        "peerSubnets" : [
          "192.168.2.0/24"
        ],
        "peerIp" : "10.115.172.19",
        "name" : "IPsec",
        "description" : null,
        "localSubnets" : [
          "11.1.1.0/24"
        ],
        "dhGroup" : "dh2",
        "peerId" : "10.115.172.19",
        "enablePfs" : true,
        "localIp" : "10.115.172.18",
        "authenticationMode" : "psk",
        "localId" : "10.115.172.18"
      }
    ],
    "enable" : true,
    "logging" : {
      "enable" : false,
      "logLevel" : "info"
    },
    "global" : {
      "extension" : null,
      "crlCertificates" : [],
      "serviceCertificate" : null,
      "pskForDynamicIp" : null,
      "id" : null,
      "caCertificates" : []
    }
```

```
  }
}
```

show configuration ipset

Shows IP address groups defined at the NSX Edge scope.

Synopsis

show configuration ipset

CLI Mode

Basic

Example

```
vShield-edge-2-0>  show configuration ipset
------------------------------------------------------------------------
vShield Edge IpSet Config:
{
  "ipSet" : []
}
```

show configuration l2vpn

Shows L2 VPN configuration.

Synopsis

show configuration l2vpn

CLI Mode

Basic

Example

```
vShield-edge-2-0>  show configuration l2vpn
------------------------------------------------------------------------
{
  "l2vpn" : {
    "ciphers" : [
      "AES256-SHA"
    ],
    "listenerPort" : 443,
    "clientVnicIndex" : null,
    "filters" : [],
   "serverPort" : null,
    "caCertificate" : null,
    "encryptionAlgorithm" : null,
    "listenerIp" : "10.110.18.190",
    "peerSites" : [
      {
        "vseVnicNames" : [
          "vNic_10",
          "vNic_11",
          "vNic_12",
          "vNic_13",
          "vNic_14",
          "vNic_15",
          "vNic_16",
          "vNic_17",
          "vNic_18",
          "vNic_19"
        ],
        "name" : "site1",
        "filters" : [],
```

```
        "l2vpnUser" : {
          "password" : "****",
          "userId" : "user1"
        }
      },
      {
        "vseVnicNames" : [
          "vNic_20",
          "vNic_21",
          "vNic_22",
          "vNic_23",
          "vNic_24",
          "vNic_25",
          "vNic_26",
          "vNic_27",
          "vNic_28",
          "vNic_29"
        ],
        "name" : "site2",
        "filters" : [],
        "l2vpnUser" : {
          "password" : "****",
          "userId" : "user2"
        }
      } ],
    "clientProxySetting" : null,
    "enable" : true,
    "trunkedVnicIndexes" : [
      1
    ],
    "serverVnicIndex" : null,
    "l2vpnUsers" : [],
    "serverAddress" : null,
    "logging" : {
      "enable" : true,
      "logLevel" : "info"
    },
    "vseVnicNames" : null,
    "serverCertificate" : null
  }
}
```


show configuration loadbalancer

Shows external, or public, IP address mapped to internal servers for load balancing. Note that there are a number of specialized show configuration loadbalancer sub-commands explained after this one.

Synopsis

show configuration loadbalancer

CLI Mode

Basic

Example


```
vShield-edge-2-0>  show configuration loadbalancer
------------------------------------------------------------------------
vShield Edge Loadbalancer Config:
{
  "monitorService" : {
    "logging" : {
      "enable" : false,
      "logLevel" : "info"
    },
    "enable" : true,
    "healthMonitors" : [
```

```
      {
        "extension" : null,
        "send" : null,
        "expected" : null,
        "maxRetries" : 3,
        "name" : "default_tcp_monitor",
        "interval" : 5,
        "receive" : null,
        "timeout" : 15,
        "url" : null,
        "type" : "tcp",
        "method" : null
      },
      {
        "extension" : null,
        "send" : null,
        "expected" : null,
        "maxRetries" : 3,
        "name" : "default_http_monitor",
        "interval" : 5,
        "receive" : null,
        "timeout" : 15,
        "url" : "/",
        "type" : "http",
        "method" : "GET"
      },
      {
        "extension" : null,
        "send" : null,
        "expected" : null,
        "maxRetries" : 3,
        "name" : "default_https_monitor",
        "interval" : 5,
        "receive" : null,
        "timeout" : 15,
        "url" : "/",
        "type" : "https",
        "method" : "GET"
      }
    ]
  },
  "loadBalancer" : {
    "logging" : {
      "enable" : false,
      "logLevel" : "info"
    },
    "enable" : true,
    "vips" : [
      {
        "maxConn" : 0,
        "rateLimit" : 0,
        "applicationRules" : null,
        "mode" : "http",
        "name" : "VSIP",
        "accelerationEnabled" : false,
        "redirection" : null,
        "serverSsl" : null,
        "serverSslEnabled" : false,
        "insertXForwardedFor" : false,
        "sessionPersistence" : null,
        "ipAddresses" : [
          "[10.115.172.18]:80"
        ],
        "defaultPool" : null,
        "clientSsl" : null
      }
    ],
    "applicationRules" : null,
```

```
    "objectSet" : null,
    "accelerationEnabled" : false,
    "pools" : [
      {
        "members" : [
          {
            "maxConn" : 0,
            "minConn" : 0,
            "name" : "http-Server",
            "objectId" : null,
            "ipAddress" : "11.1.1.2",
            "port" : 80,
            "weight" : 1,
            "monitorPort" : 80,
            "healthMonitors" : [
              "default_http_monitor"
            ],
            "condition" : "enabled"
          }
        ],
        "algorithm" : "round-robin",
        "transparent" : {
          "enable" : false
        },
        "name" : "http-pool"
      }
    ]
  }
}
```


show configuration loadbalancer monitor

Shows monitor details.

Synopsis

show configuration loadbalancer monitor

CLI Mode

Basic

Example


```
vShield-edge-2-0>  show configuration loadbalancer monitor
-----------------------------------------------------------------------
vShield Edge Loadbalancer Config:
{
  "healthMonitors" : [
    {
      "extension" : null,
      "send" : null,
      "expected" : null,
      "maxRetries" : 3,
      "name" : "default_tcp_monitor",
      "interval" : 5,
      "receive" : null,
      "timeout" : 15,
      "url" : null,
      "type" : "tcp",
      "method" : null
    },
    {
      "extension" : null,
      "send" : null,
      "expected" : null,
      "maxRetries" : 3,
      "name" : "default_http_monitor",
```

```
      "interval" : 5,
      "receive" : null,
      "timeout" : 15,
      "url" : "/",
      "type" : "http",
      "method" : "GET"
    },
    {
      "extension" : null,
      "send" : null,
      "expected" : null,
      "maxRetries" : 3,
      "name" : "default_https_monitor",
      "interval" : 5,
      "receive" : null,
      "timeout" : 15,
      "url" : "/",
      "type" : "https",
      "method" : "GET"
    }
  ]
}
```


show configuration loadbalancer pool *poolName*

Shows pool details.

Synopsis

show configuration loadbalancer pool poolname

CLI Mode

Basic

Example


```
vShield-edge-2-0>  show configuration loadbalancer pool
--------------------------------------------------------------------------------
vShield Edge Loadbalancer Config:
{
  "pools" : [
    {
      "members" : [
        {
          "maxConn" : 0,
          "minConn" : 0,
          "name" : "http-Server",
          "objectId" : null,
          "ipAddress" : "11.1.1.2",
          "port" : 80,
          "weight" : 1,
          "monitorPort" : 80,
          "healthMonitors" : [
            "default_http_monitor"
          ],
          "condition" : "enabled"
        }
      ],
      "algorithm" : "round-robin",
      "transparent" : {
        "enable" : false
      },
      "name" : "http-pool"
    }
  ]
}
```

show configuration loadbalancer rule *ruleName*

Shows rule details.

Synopsis

show configuration loadbalancer rule *rulename*

CLI Mode

Basic

show configuration loadbalancer virtual *virtualServerName*

Shows virtual server details.

Synopsis

show configuration loadbalancer virtual *virtualServerName*

CLI Mode

Basic

Example

```
vShield-edge-2-0>  show configuration loadbalancer virtual
------------------------------------------------------------------------
vShield Edge Loadbalancer Config:
{
  "vips" : [
    {
      "maxConn" : 0,
      "rateLimit" : 0,
      "applicationRules" : null,
      "mode" : "http",
      "name" : "VSIP",
      "accelerationEnabled" : false,
      "redirection" : null,
      "serverSsl" : null,
      "serverSslEnabled" : false,
      "insertXForwardedFor" : false,
      "sessionPersistence" : null,
      "ipAddresses" : [
        "[10.115.172.18]:80"
      ],
      "defaultPool" : null,
      "clientSsl" : null
    }
  ]
}
```

show configuration nat

Shows NAT rules defined for the NSX Edge.

Synopsis

show configuration nat

CLI Mode

Basic

Example

```
vShield-edge-2-0>  show configuration nat
------------------------------------------------------------------------
vShield Edge NAT Config:
```

```
{
  "dnat" : [
    {
      "protocol" : "17",
      "internalIp" : "10.115.172.18",
      "externalPort" : "500",
      "comments" : "ipsec",
      "ruleId" : 200706,
      "icmpType" : null,
      "internalPort" : "500",
      "logging" : {
        "enable" : false,
        "logLevel" : null
      },
      "interface" : "vNic_0",
      "externalIp" : "10.115.172.18"
    },
    {
      "protocol" : "17",
      "internalIp" : "10.115.172.18",
      "externalPort" : "4500",
      "comments" : "ipsec",
      "ruleId" : 200707,
      "icmpType" : null,
      "internalPort" : "4500",
      "logging" : {
        "enable" : false,
        "logLevel" : null
      },
      "interface" : "vNic_0",
      "externalIp" : "10.115.172.18"
    },
    {
      "protocol" : "50",
      "internalIp" : "10.115.172.18",
      "externalPort" : "any",
      "comments" : "ipsec",
      "ruleId" : 200708,
      "icmpType" : null,
      "internalPort" : "any",
      "logging" : {
        "enable" : false,
        "logLevel" : null
      },
      "interface" : "vNic_0",
      "externalIp" : "10.115.172.18"
    },
    {
      "protocol" : "51",
      "internalIp" : "10.115.172.18",
      "externalPort" : "any",
      "comments" : "ipsec",
      "ruleId" : 200709,
      "icmpType" : null,
      "internalPort" : "any",
      "logging" : {
        "enable" : false,
        "logLevel" : null
      },
      "interface" : "vNic_0",
      "externalIp" : "10.115.172.18"
    },
    {
      "protocol" : "6",
      "internalIp" : "10.115.172.18",
      "externalPort" : "443",
      "comments" : "sslvpn",
      "ruleId" : 196609,
```

```
      "icmpType" : null,
      "internalPort" : "443",
      "logging" : {
        "enable" : false,
        "logLevel" : null
      },
      "interface" : "vNic_0",
      "externalIp" : "10.115.172.18"
    },
    {
      "protocol" : "6",
      "internalIp" : "10.115.172.18",
      "externalPort" : "80",
      "comments" : "loadBalancer",
      "ruleId" : 200710,
      "icmpType" : null,
      "internalPort" : "80",
      "logging" : {
        "enable" : false,
        "logLevel" : null
      },
      "interface" : "vNic_0",
      "externalIp" : "10.115.172.18"
    }
  ],
  "snat" : []
}
```


show configuration ospf

Shows OSPF configuration.

Synopsis

show configuration ospf

CLI Mode

Basic

Example


```
vShield-edge-1-0> sh configuration ospf
vShield Edge OSPF Routing Protocol Config:
{
  "ospf" : {
    "defaultOriginate" : false,
    "forwardingAddress" : null,
    "gracefulRestart" : true,
    "interfaces" : [
      {
        "cost" : 1,
        "priority" : 128,
        "areaId" : 51,
        "mtuIgnore" : false,
        "vnic" : "vNic_1",
        "deadInterval" : 40,
        "helloInterval" : 10
      },
      {
        "cost" : 1,
        "priority" : 128,
        "areaId" : 0,
        "mtuIgnore" : false,
        "vnic" : "vNic_2",
        "deadInterval" : 40,
        "helloInterval" : 10
      }
```

```
    ],
    "redistribute" : {
      "rules" : [
        {
          "fromOSPF" : false,
          "fromBGP" : false,
          "fromISIS" : false,
          "fromStatic" : true,
          "fromConnected" : false,
          "action" : "permit",
          "id" : 0,
          "prefix" : null
        }
      ],
      "enabled" : true
    },
    "protocolAddress" : null,
    "areas" : [
      {
        "areaId" : 51,
        "authenticationType" : "none",
        "authenticationSecret" : null,
        "type" : "nssa"
      },
      {
        "areaId" : 0,
        "authenticationType" : "none",
        "authenticationSecret" : null,
        "type" : "normal"
      },
      {
        "areaId" : 1,
        "authenticationType" : "none",
        "authenticationSecret" : null,
        "type" : "normal"
      }
    ],
    "enabled" : true
  }
}
```


show configuration static_routing

Shows the static routes defined for the NSX Edge data packets.

Synopsis

show configuration static_routing

CLI Mode

Basic

show configuration syslog

Shows remote syslog servers defined for the NSX Edge.

Synopsis

show configuration syslog

CLI Mode

Basic

Example

vShield-edge-2-0> show configuration syslog

```
-------------------------------------------------------------------------
vShield Edge Syslog Config:
{
  "syslog" : {
    "protocol" : "tcp",
    "destinationHost" : [
      "11.1.1.100",
      "11.1.1.2"
    ]
  }
}
```

show configuration sslvpn-plus

Shows the SSL VPN configuration.

Synopsis

show configuration sslvpn-plus

CLI Mode

Basic

show fips

Indicates whether fips (Federal Information Processing Standard) is enabled for the specified NSX Edge.

Synopsis

show fips

CLI Mode

Basic

show firewall

Displays firewall packet counters along with firewall rules that specify what to do with a packet that matches.

Synopsis

show firewall

CLI Mode

Basic

show firewall flows

Displays the firewall packet counters along with packet flows.

Synopsis

show firewall flows

CLI Mode

Basic

show firewall flows top *number*

Displays firewall packet counters along with top N number of packet flows.

Synopsis

show firewall flows top 10

CLI Mode

Basic

show firewall flows top *number* sort-by pkts

Displays firewall packet counters along with top N number of packet flows sorted by packet numbers.

Synopsis

show firewall flows top 10 sort-by-pkts

CLI Mode

Basic

show firewall flows top *number* sort-by bytes

Displays firewall packet counters along with top N number of packet flows sorted by byte numbers.

Synopsis

show firewall flows top 10 sort-by-bytes

CLI Mode

Basic

show firewall rule-id *ID*

Displays firewall packet counters filtered by rule-id.

Synopsis

show firewall rule-id 25

CLI Mode

Basic

show firewall rule-id *ID* flows

Displays firewall packet counters filtered by rule-id.

Synopsis

show firewall rule-id 25 flows

CLI Mode

Basic

show firewall rule-id *ID* flows top *number*

Displays firewall packet counters filtered by rule-id along with top N number of packet flows.

Synopsis

show firewall rule-id 25 flows top 10

CLI Mode

Basic

show firewall rule-id *ID* flows top *number* sort-by pkts

Displays firewall packet counters filtered by rule-id along with top N number of packet flows sorted by packet numbers.

Synopsis

show firewall rule-id 25 flows top 10 sort-by-pkts

CLI Mode

Basic

show firewall rule-id ID flows top *number* sort-by-bytes

Displays firewall packet counters filtered by rule-id along with top N number of packet flows sorted by byte numbers.

Synopsis

show firewall rule-id 25 flows top 10 sort-by-bytes

CLI Mode

Basic

show flowtable

Displays packet flows in a table.

Synopsis

show flowtable

CLI Mode

Basic

show flowtable rule-id *ID*

Displays packet flows matched by rule-id.

Synopsis

show flowtable rule-id 25

CLI Mode

Basic

show flowtable rule-id *ID* top *number*

Displays the top N number of packet flows matched by rule-id.

Synopsis

show flowtable rule-id 25 top 30

CLI Mode

Basic

show flowtable rule-id *ID* top *number* sort-by pkts

Displays the top N number of packet flows matched by rule-id sorted by packet numbers.

Synopsis

show flowtable rule-id 25 top 30 sort-by pkts

CLI Mode

Basic

show flowtable rule-id *ID* top *number* sort-by bytes

Displays top N number of packet flows matched by rule-id sorted by byte numbers.

Synopsis

show flowtable rule-id 25 top 30 sort-by bytes

CLI Mode

Basic

show flowtable top *number*

Displays top N number of packet flows.

Synopsis

show flowtable top 10

CLI Mode

Basic

show flowtable top *number* sort-by pkts

Displays top N number of packet flows sorted by packet numbers.

Synopsis

show flowtable top 10 sort-by pkts

CLI Mode

Basic

show flowtable top *number* sort-by bytes

Displays top N number of packet flows sorted by byte numbers.

Synopsis

show flowtable top 10 sort-by bytes

CLI Mode

Basic

show hostname

Shows the current hostname for an NSX Edge.

Synopsis

show hostname

CLI Mode

Basic, Privileged

Example

vshieldEdge# show hostname

show interface

Displays interface information like IP addresses.

Synopsis

show interface

CLI Mode

Basic

show interface *name*

Displays interface information for the specified interface.

Synopsis

show interface TEST

CLI Mode

Basic

show ip bgp

Shows entries in the Border Gateway Protocol (BGP) routing table.

Synopsis

show ip bgp

CLI Mode

Basic, Privileged

Example

```
Status codes: s - suppressed, d - damped, > - best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop        Metric  LocPrf  Weight  Origin
 >  50.50.50.0/24      0.0.0.0          0     100   32768     i
 >  60.60.60.0/24      50.50.50.3       0     100   32768     i
    80.80.80.0/24      20.20.20.1       0     100      60     ?
 >  80.80.80.0/24      70.70.70.1       0     100      60     ?
 >  90.90.90.0/24      50.50.50.3       0     100   32768     i
```

show ip bgp neighbors

Shows BGP neighbors.

Synopsis

show ip bgp neighbors

CLI Mode

Basic, Privileged

Example

```
BGP neighbor is 20.20.20.1,   remote AS 200,
BGP state = Established, up
Hold time is 180, Keep alive interval is 60 seconds
```

```
Neighbor capabilities:
        Route refresh: advertised and received
        Address family IPv4 Unicast:advertised and received
        Graceful restart Capability:advertised and received
            Restart remain time: 0
Received 3034 messages, Sent 3033 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
        Index 1 Identifier 0x9ac9f52c
        Route refresh request:received 0 sent 0
        Prefixes received 1 sent 3 advertised 3
Connections established 2, dropped 57
Local host: 20.20.20.113, Local port: 43886
Remote host: 20.20.20.1, Remote port: 179
BGP neighbor is 70.70.70.1,   remote AS 200,
BGP state = Established, up
Hold time is 180, Keep alive interval is 60 seconds
Neighbor capabilities:
        Route refresh: advertised and received
        Address family IPv4 Unicast:advertised and received
        Graceful restart Capability:advertised and received
            Restart remain time: 0
Received 3085 messages, Sent 3075 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
        Index 2 Identifier 0x9ac9f52c
        Route refresh request:received 0 sent 0
        Prefixes received 1 sent 3 advertised 3
Connections established 1, dropped 9
Local host: 70.70.70.113, Local port: 179
Remote host: 70.70.70.1, Remote port: 26563
```

show ip forwarding

Shows forwarding table entries.

Synopsis

```
show ip forwarding
```

CLI Mode

Basic, Privileged

Example

```
Codes: C - connected, R - remote,
     > - selected route, * - FIB route

R>* 0.0.0.0/0 via 10.24.31.253, vNic_3
C>* 10.24.28.0/22 is directly connected, vNic_3
C>* 20.20.20.0/24 is directly connected, vNic_2
C>* 50.50.50.0/24 is directly connected, vNic_0
R>* 60.60.60.0/24 via 50.50.50.3, vNic_0
C>* 70.70.70.0/24 is directly connected, vNic_1
R>* 80.80.80.0/24 via 70.70.70.1, vNic_2
R>* 90.90.90.0/24 via 50.50.50.3, vNic_0
```

show ip ospf

Shows information about Open Shortest Path First (OSPF) routing process.

Synopsis

```
show ip ospf
```

CLI Mode

Basic, Privileged

Example

```
OSPF routing process with Router ID 50.50.50.113
Supports opaque LSA
SPF schedule delay: 5 secs, Hold time between two SPFs: 10 secs
Minimum LSA interval: 5 secs, Minimum LSA arrival: 1 secs
Number of external LSA: 4, Checksum Sum: 0X119C0
Number of opaque AS LSA: 0, Checksum Sum: 0
  Area BACKBONE(0)
    SPF algorithm executed 292 times
    Number of area border routers reachable within area: 0
    Number of LSA: 9, Checksum Sum: 0X32360
    Number of router LSA: 3, Checksum Sum: 0XE766
    Number of network LSA: 1, Checksum Sum: 0X5808
    Number of summary network LSA: 0, Checksum Sum: 0
    Number of summary ASB LSA: 0, Checksum Sum: 0
    Number of external NSSA LSA: 0, Checksum Sum: 0
    Number of opaque LSA: 5, Checksum Sum: 0X1E3F2
  Area 0.0.0.51
    It is a NSSA area
    SPF algorithm executed 292 times
    Number of area border routers reachable within area: 0
    Number of LSA: 3, Checksum Sum: 0X203EE
    Number of router LSA: 0, Checksum Sum: 0
    Number of network LSA: 0, Checksum Sum: 0
    Number of summary network LSA: 0, Checksum Sum: 0
    Number of summary ASB LSA: 0, Checksum Sum: 0
    Number of external NSSA LSA: 1, Checksum Sum: 0X8BF5
    Number of opaque LSA: 2, Checksum Sum: 0X177F9
```

show ip ospf database

Shows IPv4 OSPF database.

Synopsis

```
show ip ospf database
```

CLI Mode

Basic, Privileged

Example

```
adv-ro uter      Filtered by advertising router.
  asbr-summary   Show asbr-summary (type 4) LSAs.
  external       Show external (type 5) LSAs.
  network        Show network (type 2) LSAs.
  nssa-external  Show nssa-external (type 7) LSAs.
  opaque-area    Show opaque-area (type 10) LSAs.
  router         Show router (type 1) LSAs.
  summary        Show summary (type 3) LSAs.
```

show ip ospf database adv-router

Filters OSPF results by advertising router.

Synopsis

```
show ip ospf database adv-router
```

CLI Mode

Basic, Privileged

Example

```
Router Link States (Area  0.0.0.0)
Link ID         ADV Router      Age         Seq Num       Checksum
50.50.50.113    50.50.50.113    866         0x80000068    0x00009039
Network Link States (Area  0.0.0.0)
Link ID         ADV Router      Age         Seq Num       Checksum
50.50.50.113    50.50.50.113    866         0x80000067    0x00005808
Opaque Area Link States (Area  0.0.0.0)
Link ID         ADV Router      Age         Seq Num       Checksum
1.0.0.1         50.50.50.113    737         0x8000005a    0x000003a6
1.0.0.2         50.50.50.113    692         0x8000005a    0x000029ab
Type-7 AS External Link States (Area  0.0.0.51)
Link ID         ADV Router      Age         Seq Num       Checksum
80.80.80.0      50.50.50.113    1317        0x80000059    0x00008bf5
Opaque Area Link States (Area  0.0.0.51)
Link ID         ADV Router      Age         Seq Num       Checksum
1.0.0.1         50.50.50.113    737         0x8000005a    0x0000a8fa
1.0.0.2         50.50.50.113    692         0x8000005a    0x0000ceff
AS External Link States
Link ID         ADV Router      Age         Seq Num       Checksum
80.80.80.0      50.50.50.113    1317        0x80000059    0x000089f7
```

show ip ospf database asbr-summary

Shows asbr-summary (type 4) LSAs.

Synopsis

show ip ospf database asbr-summary

CLI Mode

Basic, Privileged

show ip ospf database external

Shows external (type 5) LSAs.

Synopsis

show ip ospf database external

CLI Mode

Basic, Privileged

Example

```
AS External Link States
Link ID         ADV Router      Age         Seq Num       Checksum
60.60.60.0      60.60.60.3      183         0x8000005b    0x00004130
80.80.80.0      50.50.50.41     475         0x80000059    0x00003b8e
80.80.80.0      50.50.50.113    1279        0x80000059    0x000089f7
90.90.90.0      60.60.60.3      1769        0x80000054    0x0000130b
```

show ip ospf database network

Shows network (type 2) LSAs.

Synopsis

show ip ospf database network

CLI Mode

Basic, Privileged

Example

```
Network Link States (Area  0.0.0.0)
Link ID         ADV Router      Age         Seq Num       Checksum
50.50.50.113    50.50.50.113    832         0x80000067    0x00005808
```

show ip ospf database nssa-external

Shows nssa-external (type 7) LSAs.

Synopsis

show ip ospf database nssa-external

CLI Mode

Basic, Privileged

Example

```
Type-7 AS External Link States (Area  0.0.0.51)
Link ID         ADV Router      Age         Seq Num       Checksum
80.80.80.0      50.50.50.113    1286        0x80000059    0x00008bf5
```

show ip ospf database opaque-area

Shows opaque-area (type 10) LSAs.

Synopsis

show ip ospf database opaque-area

CLI Mode

Basic, Privileged

Example

```
Type-7 AS External Link States (Area  0.0.0.51)
Link ID         ADV Router      Age         Seq Num       Checksum
80.80.80.0      50.50.50.113    1286        0x80000059    0x00008bf5
```

show ip ospf database router

Shows router (type 1) LSAs.

Synopsis

show ip ospf database router

CLI Mode

Basic, Privileged

Example

```
Router Link States (Area  0.0.0.0)
Link ID         ADV Router      Age         Seq Num       Checksum
50.50.50.41     50.50.50.41     841         0x8000006b    0x00001b84
50.50.50.113    50.50.50.113    841         0x80000068    0x00009039
60.60.60.3      60.60.60.3      146         0x8000005b    0x00003ba9
```

show ip ospf database summary

Shows summary (type 3) LSAs.

Synopsis

show ip ospf database summary

CLI Mode

Basic, Privileged

Example

```
Router Link States (Area  0.0.0.0)
Link ID         ADV Router      Age         Seq Num       Checksum
50.50.50.41     50.50.50.41     841         0x8000006b    0x00001b84
50.50.50.113    50.50.50.113    841         0x80000068    0x00009039
60.60.60.3      60.60.60.3      146         0x8000005b    0x00003ba9
```

show ip ospf interface

Shows IPv4 OSPF interface.

Synopsis

show ip ospf interface

CLI Mode

Basic, Privileged

Example

```
vNic_0 is activated
  Internet Address 50.50.50.113, Network Mask 255.255.255.0, Area 0.0.0.0
  Transmit Delay is 1 sec, Network Type BROADCAST, State DR, Priority 128
  Designated Router's Interface Address 50.50.50.113
  Backup Designated Router's Interface Address 50.50.50.4
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
```

show ip ospf ne

Shows IP addresses of OSPF neighbors.

Synopsis

show ip ospf ne

CLI Mode

Basic, Privileged

Example

```
Neigbhor ID      Priority   Address          Dead Time   State
60.60.60.3       128        50.50.50.4       34          Full/BDR
50.50.50.41      128        50.50.50.41      36          Full/DROTHER
```

show ip ospf statistics

Shows IPv4 OSPF statistics.

Synopsis

show ip ospf statistics

CLI Mode

Basic, Privileged

Example

```
Area 0.0.0.0:  SPF algorithm executed 292 times
Area 0.0.0.51:  SPF algorithm executed 292 times
vShield-edge-6-0> sh ip ospf database
                Router Link States (Area  0.0.0.0)
Link ID         ADV Router      Age         Seq Num       Checksum
50.50.50.41     50.50.50.41     822         0x8000006b    0x00001b84
50.50.50.113    50.50.50.113    822         0x80000068    0x00009039
60.60.60.3      60.60.60.3      127         0x8000005b    0x00003ba9
Network Link States (Area  0.0.0.0)
Link ID         ADV Router      Age         Seq Num       Checksum
50.50.50.113    50.50.50.113    822         0x80000067    0x00005808
Opaque Area Link States (Area  0.0.0.0)
Link ID         ADV Router      Age         Seq Num       Checksum
1.0.0.1         50.50.50.41     154         0x8000005a    0x0000ff76
1.0.0.1         50.50.50.113    693         0x8000005a    0x000003a6
1.0.0.1         60.60.60.3      237         0x8000005a    0x0000671f
1.0.0.2         50.50.50.41     827         0x80000063    0x0000500c
1.0.0.2         50.50.50.113    648         0x8000005a    0x000029ab
Type-7 AS External Link States (Area  0.0.0.51)
Link ID         ADV Router      Age         Seq Num       Checksum
80.80.80.0      50.50.50.113    1273        0x80000059    0x00008bf5
Opaque Area Link States (Area  0.0.0.51)
Link ID         ADV Router      Age         Seq Num       Checksum
1.0.0.1         50.50.50.113    693         0x8000005a    0x0000a8fa
1.0.0.2         50.50.50.113    648         0x8000005a    0x0000ceff
AS External Link States
Link ID         ADV Router      Age         Seq Num       Checksum
60.60.60.0      60.60.60.3      177         0x8000005b    0x00004130
80.80.80.0      50.50.50.41     469         0x80000059    0x00003b8e
80.80.80.0      50.50.50.113    1273        0x80000059    0x000089f7
90.90.90.0      60.60.60.3      1763        0x80000054    0x0000130b
```

show ip route

Shows all routes in the routing information base (RiB).

Synopsis

show ip route [A.B.C.D/M]

Option	Description
A.B.C.D	IP address to use.
M	Subnet mask to use.

CLI Mode

Basic, Privileged

Example

```
vShield# show ip route
Codes: K - kernel route, C - connected, S - static,
       > - selected route, * - FIB route
S>* 0.0.0.0/0 [1/0] via 192.168.110.1, mgmt
C>* 192.168.110.0/24 is directly connected, mgmt
```

Related Commands

ip route

show ip route ospf

Shows routes in routing information base (RiB) learnt through OSPF protocol.

Synopsis

show ip route ospf

CLI Mode

Basic, Privileged

Example

```
Codes: O - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2
O   E2  60.60.60.0/24       [110/1]      via 50.50.50.3
O   E2  90.90.90.0/24       [110/1]      via 50.50.50.3
```

show ip route bgp

Shows routes in routing information base (RiB) learnt through the BGP protocol.

Synopsis

show ip route bgp

CLI Mode

Basic, Privileged

Example

```
Codes: O - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2
B      80.80.80.0/24       [20/0]       via 20.20.20.1
B      80.80.80.0/24       [20/0]       via 70.70.70.1
```

show ip route A.B.C.D/M

Displays a route entry matched by the specified prefix.

Synopsis

show ip route A.B.C.D

CLI Mode

Privileged, Configuration, and Interface Configuration

show log

Shows the system log.

Synopsis

show log [follow | reverse]

Option	Description
follow	Update the displayed log every 5 seconds.
reverse	Show the log in reverse chronological order.

CLI Mode

Basic, Privileged

Example

```
vShield# show log
Aug  7 17:32:37 vShield_118 syslog-ng[27397]: Configuration reload request received, reloading configuration;
Aug  7 17:32:37 vShield_118 udev[21427]: removing device node '/dev/vcs12'
Aug  7 17:32:37 vShield_118 udev[21429]: removing device node '/dev/vcsa12'
Aug  7 17:32:37 vShield_118 udev[21432]: creating device node '/dev/vcs12'
Aug  7 17:32:37 vShield_118 udev[21433]: creating device node '/dev/vcsa12'
Aug  7 17:33:37 vShield_118 ntpdate[21445]: adjust time server 10.115.216.84 offset 0.011031 sec
Aug  7 17:34:37 vShield_118 ntpdate[21466]: adjust time server 10.115.216.84 offset 0.002739 sec
Aug  7 17:35:37 vShield_118 ntpdate[21483]: adjust time server 10.115.216.84 offset 0.010884 sec
...
```

Related Commands

show log last

show log follow

Displays the log as it gets log contents.

Synopsis

```
show log follow
```

CLI Mode

Basic

show log last

Shows last *n* lines of the log.

Synopsis

```
show log last NUM
```

Option	Description
NUM	Number of log lines to display

CLI Mode

Basic, Privileged

Example

```
vShield# show log last 2
Feb  9 12:30:55 localhost ntpdate[24503]: adjust time server 192.168.110.199 off
set -0.000406 sec
Feb  9 12:31:54 localhost ntpdate[24580]: adjust time server 192.168.110.199 off
set -0.000487 sec
```

Related Commands

show log

show log reverse

Displays the log in reverse chronolgical order.

Synopsis

```
show log reverse
```

CLI Mode

Basic

show nat

Displays NAT packet counters along with the NAT rules that specify how to translate network addresses for a packet that matches.

Synopsis

show nat

CLI Mode

Basic

show process

Shows information related to NSX Edge processes.

Synopsis

show process (list | monitor)

Option	Description
list	List all currently running processes on the NSX Edge.
monitor	Continuously monitor the list of processes.

CLI Mode

Basic, Privileged

Example

vShieldEdge# show process list

show route

Shows the current routes configured on an NSX Edge.

Synopsis

show route

CLI Mode

Basic, Privileged

Example

vShieldEdge# show route

show service

Shows the status of the specified NSX Edge service.

Synopsis

show service (dhcp | ipsec | lb)

Option	Description
dhcp	Show the status of the DHCP service.
ipsec	Show the status of the VPN service.
lb	Show the status of the Load Balancer service.

CLI Mode

Basic

Example

vShieldEdge# show service dhcp

show service l2vpn (on server)

Shows the L2 VPN server status and tunnel information along with the encryption algorithm that is being used in the communication.

Synopsis

show service l2vpn

CLI Mode

Basic, Privileged

Example

```
vShield-edge-1-0> show service l2vpn
L2 VPN is running
------------------------------------------------------------------------------
L2 VPN type: Server
Tunnel information: 1 ABC na 1 1402561453 AES128-SHA
```

show service l2vpn (on client)

Shows the L2 VPN client status.

Synopsis

show service l2vpn

CLI Mode

Basic, Privileged

Example

```
vShield-edge-1-0> show service l2vpn
L2 VPN is running
------------------------------------------------------------------------------
L2 VPN type: Client
Tunnel status: up
Total bytes sent: 582
Total bytes received: 408
```

show service l2vpn bridge

Shows the L2 VPN bridge configuration. You can run this command on both the client and the server.

Synopsis

show service l2vpn bridge

CLI Mode

Basic, Privileged

Example

vShield-edge-1-0> show service l2vpn bridge

bridge name	bridge id	STP enabled	interfaces
br-sub	8000.005056b86b46	no	vnic1 na1

List of learned MAC addresses for L2 VPN bridge br-sub

port no	mac addrr	is local?	vlan id	ageing timer
1	00:50:56:b8:6b:46	yes	0	);00
2	c2:2b:0e:8b:b3:ba	yes	0	0:00

show service l2vpn trunk-table

Lists the interfaces of the Edge and shows the trunk interfaces. You can run this command on both the client and the server.

Synopsis

show service l2vpn trunk-table

CLI Mode

Basic, Privileged

Example

vShield-edge-1-0> show service l2vpn trunk-table

ifindex	iface	trunk flag
01	lo	0
02	VDR	0
03	vNIC_0	0
04	vNIC_4	0
...	...	...
...	...	...
06	vNIC_1	1

show service l2vpn conversion table

Lists the tunnel ID to which the network is mapped. Also indicates whether the network is VLAN or VXLAN.

Synopsis

show service l2vpn trunk-table

CLI Mode

Basic, Privileged

Example

vShield-edge-1-0> show service l2vpn trunk-table

TunnelId	VLAN/VNI	Type
10	100	VLAN

show service monitor

Shows the running status of health monitor service.

Synopsis

show service monitor

CLI Mode

Basic, Privileged

Example

```
vShield-edge-1-0> show service monitor
Network Monitor Service Status:
Network Monitor : running
PID : 18578
Total Services : 7
Monitored Services Status:
Services in OK/WARNING/UNKNOWN/CRITICAL : 1 / 0 / 0 / 6
Services Scheduled : 7
Services Checked : 7
Service Checks Last 1/5/15 min : 45 / 45 / 45
Total Service State Change : 0.000 / 0.000 / 0.000 %
```

show service monitor service

Shows the running status of health monitor instances.

Synopsis

show service monitor service

CLI Mode

Basic, Privi leged

Example

```
vShield-edge-1-0> show service monitor service
Network Monitor: Monitored Services Statistics:
MONITOR default_tcp_monitor
| TOTAL SERVICES MONITORED: 5
+->SERVICE [0]
+->SERVICE METADATA INFORMATION:
| MONITOR: default_tcp_monitor
| POOL: iis-pool
| MEMBER: m1
| HOST ADDRESS: 10.117.5.62
| CHECK EXECUTION TIME (s): 15.033
| CHECK LATENCY (s): 0.627
| CHECK ATTEMPTS (CUR/MAX): 1/1
| CHECK RESULT: CRITICAL - Socket timeout after 15 seconds
+->SERVICE [1]
+->SERVICE METADATA INFORMATION:
| MONITOR: default_tcp_monitor
| POOL: tcp-pool-shared-l4-l7
| MEMBER: 192.168.1.100
| HOST ADDRESS: 192.168.1.100
| CHECK EXECUTION TIME (s): 3.036
| CHECK LATENCY (s): 0.652
| CHECK ATTEMPTS (CUR/MAX): 1/1
| CHECK RESULT: No route to host
+->SERVICE [2]
+->SERVICE METADATA INFORMATION:
| MONITOR: default_tcp_monitor
| POOL: tcp-pool
| MEMBER: m1
```

| HOST ADDRESS: 192.168.1.100
| CHECK EXECUTION TIME (s): 2.036
| CHECK LATENCY (s): 0.653
| CHECK ATTEMPTS (CUR/MAX): 1/1
| CHECK RESULT: No route to host
+->SERVICE [3]
+->SERVICE METADATA INFORMATION:
| MONITOR: default_tcp_monitor
| POOL: tcp-pool
| MEMBER: m2
| HOST ADDRESS: 192.168.1.40
| CHECK EXECUTION TIME (s): 0.015
| CHECK LATENCY (s): 0.654
| CHECK ATTEMPTS (CUR/MAX): 1/1
| CHECK RESULT: Connection refused
+->SERVICE [4]
+->SERVICE METADATA INFORMATION:
| MONITOR: default_tcp_monitor
| POOL: tcp-pool
| MEMBER: m3
| HOST ADDRESS: 192.168.1.50
| CHECK EXECUTION TIME (s): 0.035
| CHECK LATENCY (s): 0.652
| CHECK ATTEMPTS (CUR/MAX): 1/1
| CHECK RESULT: Connection refused
MONITOR HC-WEB
| TOTAL SERVICES MONITORED: 2
+->SERVICE [0]
+->SERVICE METADATA INFORMATION:
| MONITOR: HC-WEB
| POOL: http-pool
| MEMBER: m1
| HOST ADDRESS: 192.168.1.100
| CHECK EXECUTION TIME (s): 3.037
| CHECK LATENCY (s): 0.652
| CHECK ATTEMPTS (CUR/MAX): 1/1
| CHECK RESULT: No route to host
+->SERVICE [1]
+->SERVICE METADATA INFORMATION:
| MONITOR: HC-WEB
| POOL: http-pool
| MEMBER: m2
| HOST ADDRESS: 192.168.1.40
| CHECK EXECUTION TIME (s): 0.009
| CHECK LATENCY (s): 0.654
| CHECK ATTEMPTS (CUR/MAX): 1/1
| CHECK RESULT: HTTP OK: Status line output matched "HTTP/1.1 200 OK" - 329 bytes in 0.002 second response time

show service dhcp

Displays whether the DHCP service is running.

Synopsis

show service dhcp

CLI Mode

Basic

show service dns

Displays whether the DNS service is running.

Synopsis

show service dns

CLI Mode

Basic

show service ipsec

Shows the VPN service details. For an explanation of the various sub-modes of this command, see the sections that follow this one.

Synopsis

show service ipsec (cacerts | certs | ctrls | pubkeys | sa | sp | status)

Option	Description
cacerts	Show the CA certificates.
certs	Show the Edge certificates
ctrls	Show the CRLs revoke certificates.
pubkeys	Show the public keys.
sa	Show the Ssecurity Association Database (SAD) entry.
sp	Show the Ssecurity Policy Database (SPD) entry.
status	Show the status of the ipsec server.

CLI Mode

Basic

Example

vShieldEdge# show service ipsec status

show service ipsec cacerts

Displays IPSEC CA certificates.

Synopsis

show service ipsec cacerts

CLI Mode

Privileged, Configuration, and Interface Configuration

show service ipsec certs

Displays IPSEC certificates.

Synopsis

show service ipsec certs

CLI Mode

Basic

show service ipsec crls

Displays Certificate Revocation Lists (CRL).

Synopsis

show service ipsec crls

CLI Mode

Basic

show service ipsec pubkeys

Displays all installed public keys that are either received from peers or loaded locally.

Synopsis

show service ipsec pubkeys

CLI Mode

Basic

show service ipsec sa

Displays the security association database, which contains a set of security information that describes a particular kind of secure connection between one device and another.

Synopsis

show service ipsec sa

CLI Mode

Basic

show service ipsec sp

Displays the security policy database, which contains a set of rules that are programmed into the IPSec implementation that tells it how to process different packets received by the device.

Synopsis

show service ipsec sp

CLI Mode

Basic

show service highavailability

Displays high availability (HA) service information such as HA status and Healthcheck status, etc.

Synopsis

show service highavailability

CLI Mode

Basic

show service highavailability link

Displays HA link information such as IP addresses for peer links and local links.

Synopsis

show service highavailability link

CLI Mode

Basic

show service highavailability connection-sync

Displays HA connection sync-up status information. For example, statistics about current active connections of both local and peer device.

Synopsis

show service highavailability connection-sync

CLI Mode

Basic

show service loadbalancer

Display overall current loadbalancer engine state.

Synopsis

show service loadbalancer

CLI Mode

Basic

show service loadbalancer monitor *monitorName*

Displays health of specified monitor.

Synopsis

show service loadbalancer monitor *monitorName*

CLI Mode

Basic

Example

```
vShield-edge-2-0> show service loadbalancer monitor
------------------------------------------------------------------------------
Loadbalancer HealthMonitor Statistics:

POOL                 MEMBER               HEALTH STATUS
http-pool            http-Server          default_http_monitor:CRITICAL
```

show service loadbalancer pool *poolName*

Displays pool member state.

Synopsis

show service loadbalancer pool *name*

CLI Mode

Basic

Example

```
vShield-edge-2-0> show service loadbalancer pool
------------------------------------------------------------------------------
Loadbalancer Pool Statistics:

POOL http-pool
|  LB METHOD round-robin
|  LB PROTOCOL L7
|  Transparent disabled
```

```
| SESSION (cur, max, limit, total) = (0, 0, 1, 0)
| BYTES in = (0), out = (0)
  +->POOL MEMBER: http-pool/http-Server, STATUS: DOWN
  | | STATUS = DOWN, MONITOR STATUS = default_http_monitor:CRITICAL
  | | SESSION (cur, max, limit, total) = (0, 0, , 0)
  | | BYTES in = (0), out = (0)
```

show service loadbalancer session

Displays concurrent sessions for both L4 and L7 load balancer engines.

Synopsis

show service loadbalancer session

CLI Mode

Basic

show service loadbalancer table

Displays session persistence table entries.

Synopsis

show service loadbalancer table

CLI Mode

Basic

show service loadbalancer virtual *serverName*

Displays virtual server details.

Synopsis

show service loadbalancer virtual *serverName*

CLI Mode

Basic

Example

```
vShield-edge-2-0> show service loadbalancer virtual
--------------------------------------------------------------------------------
Loadbalancer VirtualServer Statistics:

VIRTUAL VSIP
| ADDRESS [10.115.172.18]:80
| SESSION (cur, max, limit, total) = (0, 0, 1024, 0)
| RATE (cur, max, limit) = (0, 0, 0)
| BYTES in = (0), out = (0)
```

show service network connections

Displays service network connection information. For example, TCP and UDP service information.

Synopsis

show service network connections

CLI Mode

Basic

show service sslvpn-plus

Displays SSL VPN-Plus service information.

Synopsis

show service sslvpn-plus

CLI Mode

Basic

show service sslvpn-plus stats

Displays SSL VPN-Plus statistic information.

Synopsis

show service sslvpn-plus stats

CLI Mode

Basic

show service sslvpn-plus sessions

Displays SSL VPN-Plus active sessions.

Synopsis

show service sslvpn-plus sessions

CLI Mode

Basic

show service sslvpn-plus tunnels

Displays SSL VPN-Plus tunnel information.

Synopsis

show service sslvpn-plus tunnels

CLI Mode

Basic

show system load

Shows the average processing load on an NSX Edge.

Synopsis

show system load

CLI Mode

Basic, Privileged

Example

```
vShield# show system mem
MemTotal:      2072204 kB
MemFree:       1667248 kB
Buffers:         83120 kB
```

show system network-stats

Displays network statistics. For example, statistics for IP, ICMP, TCP and UDP, etc.

Synopsis

show system network-stats

CLI Mode

Basic

show system cpu

Shows the system cpu details.

Synopsis

show system cpu

CLI Mode

Basic

Example

vShield# show system cpu

Related Commands

show system memory

show system uptime

show system log size

Shows the total size of the system log files.

Synopsis

show system log size

CLI Mode

Basic

Example

vShield# show system log size
1M

show system memory

Shows the summary of memory utilization.

Synopsis

show system memory

CLI Mode

Basic, Privileged

Example

vShield# show system mem
MemTotal: 2072204 kB
MemFree: 1667248 kB
Buffers: 83120 kB

show system storage

Shows the disk usage details for an NSX Edge.

Synopsis

show system storage

CLI Mode

Basic, Privileged

Example

vShield# show system storage

show system uptime

Shows the length of time the NSX virtual machine has been operational since last reboot.

Synopsis

show system uptime

CLI Mode

Basic, Privileged

Example

vShield# show system uptime
0 day(s), 8 hour(s), 50 minute(s), 26 second(s)

show tech-support

Displays system information for tech-support. It shows all the information contained in tech-support tarball file.

Synopsis

show tech-support

CLI Mode

Basic

show version

Shows the software version currently running on the virtual machine.

Synopsis

show version

CLI Mode

Basic, Privileged

Example

vShield# show version

traceroute

Traces the route to a destination.

Synopsis

traceroute (HOSTNAME | A.B.C.D)

Option	Description
HOSTNAME | A.B.C.D	The hostname or IP address of the target system.

CLI Mode

Basic, Privileged

Example

```
vShield# traceroute 10.16.67.118
traceroute to 10.16.67.118 (10.16.67.118), 30 hops max, 40 byte packets
 1  10.115.219.253 (10.115.219.253)  128.808 ms  74.876 ms  74.554 ms
 2  10.17.248.51 (10.17.248.51)  0.873 ms  0.934 ms  0.814 ms
 3  10.16.101.150 (10.16.101.150)  0.890 ms  0.913 ms  0.713 ms
 4  10.16.67.118 (10.16.67.118)  1.120 ms  1.054 ms  1.273 ms
```

NSX Controller Commands

This section describes controller commands. Log in as the controller admin to use the controller CLI commands.

restart controller

Restarts a controller. You must restart only one controller in a cluster at a time.

Synopsis

restart contoller

set control-cluster core log-level *value*

Sets log level for the controller cluster. Possible values are:

- error
- warn
- info
- debug
- trace

Synopsis

set control-cluster core log-level value

Example

nsx-controller # set control-cluster core error

show control-cluster core

Lists all available properties, the required parameters, and their descriptions for the controller framework.

Synopsis

show control-cluster core

show control-cluster core stats

Displays controller statistics.

Synopsis

show control-cluster core stats

Example

```
nvp-controller # show control-cluster core stats
messages.received               40
messages.received.dropped       0
messages.transmitted            22
messages.transmit.dropped       0
messages.processing.dropped     0
connections.up                  2
connections.down                0
connections.timeout             0
connections.active              2
connections.sharding.subscribed 0
```

show control-cluster core connection-stats *ipAddress*

Displays statistics for the specified controller.

Synopsis

show control-cluster core connection-stats 11.11.111.11

Example

```
nvp-controller # show control-cluster core connection-stats 10.24.106.158
messages.received         22
messages.received.dropped 0
messages.transmitted      10
messages.transmit.dropped 0
```

show control-cluster core connection *ipAddress*

Displays status of specified connection.

Synopsis

show control-cluster core log-level 11.11.111.11

Example

```
nvp-controller # show control-cluster core connection 11.11.111.11
Host-IP         Port  ID
10.24.106.158   53540 3
```

show control-cluster core log-level

Displays log level for the specified controller.

Synopsis

show control-cluster core log-level

Example

```
nvp-controller # show control-cluster core log-level
Log level: INFO
```

show control-cluster logical-routers

Lists all available properties, the required parameters, and their descriptions for logical routers.

Synopsis

show control-cluster logical-routers

show control-cluster logical-routers bridge-mac *logicalRouterID*_and/or_*bridgeID*

Displays bridge mac records for a bridge of a logical router. *logical_router_ID* and/or *bridge_ID* can be all.

Synopsis

show control-cluster logical-routers bridge-mac *logicalRouterID_and_bridgeID*

Example

```
nvp-controller # show control-cluster logical-routers bridge-mac 1 all
LR-Id      Bridge-Id  Mac               Vlan-Id Vxlan-Id Port-Id  Source
1          1001       01:00:00:01:00:00 0       65535   1        vxlan
```

show control-cluster logical-routers bridges *logicalRouterID*_and_*bridgeID*

Displays bridge instance information for a logical router. *logical_router_id* and/or *bridge-id* can be all.

Synopsis

show control-cluster logical-routers bridges *logicalRouterID_and_bridgeID*

Example

```
nvp-controller # show control-cluster logical-routers bridges 1 all
LR-Id      Bridge-Id  Host           Active
1          1001       10.24.106.158  true
```

show control-cluster logical-routers instance *logicalRouterID*

Displays logical router information. *logicalRouterID* can be all.

Synopsis

show control-cluster logical-routers instance *logicalRouterID*

Example

```
nvp-controller # show control-cluster logical-routers instance 1
LR-Id  LR-Name   Hosts[]          Edge-Connection Service-Controller
1      perftest  10.24.106.158                    10.24.105.58
```

show control-cluster logical-routers interface *logicalRouterID*_and_*logicalRouterName*

Displays interface details for logical router specified by ID and name.

Synopsis

show control-cluster logical-routers interface *logicalRouterID_and_logicalRouterName*

Example

```
nvp-controller # show control-cluster logical-routers interface 1 lif0
Interface-Name:   lif0
Logical-Router-Id:1
Id:               0
Type:             vlan
IP:               10.0.0.0/24
DVS-UUID:         64767331-0000-0000-0000-000000000000
Mac:              00:00:00:00:00:00
Mtu:              1500
Multicast-IP:
Designated-IP:    10.24.106.158
Is-Sedimented:    false
Bridge-Id:
```

Bridge-Name:

show control-cluster logical-routers interface-summary *logicalRouterID*

Displays interface summary for specified logical router.

Synopsis

show control-cluster logical-routers interface-summary *logicalRroute_ID*

Example

```
nvp-controller # show control-cluster logical-routers interface-summary 1
Interface                Type   Id          IP[]
lif0                     vlan   0           10.0.0.0/24
lif1                     vlan   1           10.0.1.0/24
```

show control-cluster logical-routers routes *routerID*

Displays static route for router specified by ID. *routerID* can be all.

Synopsis

show control-cluster logical-routers routes *routerID*

Example

```
nvp-controller # show control-cluster logical-routers routes 1
LR-Id      Destination       Next-Hop
1          70.70.70.0/24     10.0.1.2
1          80.80.80.0/24     10.0.0.2
```

show control-cluster logical-routers routes *routerID_and_IPaddress_*and*_prefixLength*

Displays static route for router specified by ID, IP address, and prefix length. *router_ID* can be all.

Synopsis

show control-cluster logical-routers routes *routerID_and_IPaddress_and_prefixLength*

Example

```
nvp-controller # show control-cluster logical-routers route 1 70.70.70.0 24
LR-Id      Destination       Next-Hop
1          70.70.70.0/24     10.0.1.2
```

show control-cluster logical-routers stats

Displays statistics of all logical routers on this controller.

Synopsis

show control-cluster logical-routers stats

Example

```
nvp-controller # show control-cluster logical-routers stats
messages.query        0
messages.update       4
messages.flush        0
messages.notification 0
```

show control-cluster logical-routers vdr-stats *logicalRouterID*

Displays statistics of the specified logical router.

Synopsis

show control-cluster logical-routers vdr-stats *logicalRouterID*

Example

```
nvp-controller # show control-cluster logical-routers vdr-stats 1
host.reports.received      1
host.reports.dropped       0
edge.routes.received       2
edge.routes.dropped        0
bridge.reports.received    1
bridge.reports.dropped     0
bridge.macs.received       1
bridge.macs.dropped        0
route.queries.received     0
interface.queries.received 0
mac.queries.received       0
clear.routes.received      0
clear.macs.received        0
errdecode.messages.dropped 0
memfull.messages.dropped   0
errserver.messages.dropped 0
notifications.error        0
```

show control-cluster startup-nodes

Shows the IP addresses of active controllers in the cluster.

Synopsis

show control-cluster startup-nodes

Example

```
nvp-controller # show control-cluster startup-nodes
10.24.105.59
```

show control-cluster status

Shows control-cluster status. The example below shows that the controller status is normal. All controllers in the cluster should have the same cluster ID as the first controller.

Synopsis

show control-cluster status

Example

```
nvp-controller # show control-cluster status
Type Status Since
--------------------------------------------------------------------------------
Join status: Join complete 08/15 00:39:57
Majority status: Connected to cluster majority 08/15 00:39:33
Restart status: This controller can be safely restarted 08/15 00:40:03
Cluster ID: 2105ad76-0449-47ef-9f99-83e7ddd14cd0
Node UUID: 2105ad76-0449-47ef-9f99-83e7ddd14cd0
Role Configured status Active status
--------------------------------------------------------------------------------
api_provider enabled activated
persistence_server enabled activated
switch_manager enabled activated
logical_manager enabled activated
directory_server enabled activated
```

show network interface

Shows the IP address of the controller.

Synopsis

show network interface

CLI Mode

Basic, Privileged

ESXi CLI Commands

This section describes the ESXi CLI commads for NSX vSphere. For additional ESX CLI commands, see *vSphere Command-Line Interface Documentation*.

esxcli network vswitch dvs vmware vxlan config stats get

Shows statistics.

Synopsis

esxcli network vswitch dvs vmware vxlan config stats get

Example

```
# esxcli network vswitch dvs vmware vxlan config stats get
Level: 1
```

esxcli network vswitch dvs vmware vxlan config stats set

Enable statistics. Adding level=0 disables statistics.

Synopsis

esxcli network vswitch dvs vmware vxlan config stats set

esxcli network vswitch dvs vmware vxlan get

Shows VXLAN global states on the system.

Synopsis

esxcli network vswitch dvs vmware vxlan get

Example

```
# esxcli network vswitch dvs vmware vxlan get
Controlplane Out Of Sync: No
UDPport: 8472
```

esxcli network vswitch dvs vmware vxlan list --vds-name *value*

Shows VXLAN switches information for the specified vDS.

Synopsis

esxcli network vswitch dvs vmware vxlan list

Example

esxcli network vswitch dvs vmware vxlan list

VDS ID	VDS Name	MTU	Segment ID	Gateway IP	Gateway MAC	Network Count	Vmknic Count
35 fe 34 50 d4 59 27 de-e7 9f c0 3d c8 c7 a0 84	dvSwitch	1600	192.168.0.0	192.168.0.254	00:00:0c:00:11:22	1	1

esxcli network vswitch dvs vmware vxlan network list --vds-name *value* vxlan-id *value*

Shows VXLAN network information with specified vDS.

Synopsis

esxcli network vswitch dvs vmware vxlan network list --vds-name *value* [--vxlan-id *value*]

Example

esxcli network vswitch dvs vmware vxlan network list --vds-name dvSwitch

VXLAN ID	Multicast IP	Control Plane	Controller	Connection	Port Count	MAC Entry Count	ARP Entry Count
5000	N/A (headend replication)	Enabled (multicast proxy,ARP proxy)	192.168.100.1	(up)	1	11	1

esxcli network vswitch dvs vmware vxlan network arp list --vds-name *value* --vxlan-id *value*

Retrieves VXLAN network ARP table for specified vDS.

Synopsis

esxcli network vswitch dvs vmware vxlan network arp list --vds-name *value* --vxlan-id *value* --vdsport-id *value*

Example

esxcli network vswitch dvs vmware vxlan network arplist --vds-name dvSwitch --vxlan-id 5000 --vdsport-id=101

IP	MAC	Flags
192.168.200.1	00:50:56:00:11:22	00000000

esxcli network vswitch dvs vmware vxlan network arp reset -vds-name *value* --vxlan-id *value*

Resets VXLAN network ARP table for specified vDS.

Synopsis

esxcli network vswitch dvs vmware vxlan network are reset -vds-name *value* --vxlan-id *value* --vdsport-id *value*

esxcli network vswitch dvs vmware vxlan network mac list --vds-name *value* --vxlan-id *value*

Retrieves VXLAN network MAC table for specified vDS.

Synopsis

esxcli network vswitch dvs vmware vxlan network mac ABC 500

Example

esxcli network vswitch dvs vmware vxlan network mac --vds-name dvSwitch --vxlan-id 5000

Inner MAC	Outer MAC	Outer IP	Flags
00:50:56:00:11:23	00:50:56:01:23:45	192.168.0.2	00000000

esxcli network vswitch dvs vmware vxlan network mac reset --vxlan-id *value* --vdsport-id *value*

Resets VXLAN network MAC table for specified vDS.

Synopsis

esxcli network vswitch dvs vmware vxlan network mac reset -vxlan-id=value --vdsport-id=value

esxcli network vswitch dvs vmware vxlan network port list --vds-name *value* --vdsport-id *value* --vxlan-id *value*

Shows VXLAN port information with specified network.

Synopsis

esxcli network vswitch dvs vmware vxlan network port list --vds-name *value* --vxlan-id *value* [--vdsport-id *value*]

Example

esxcli network vswitch dvs vmware vxlan network port list --vds-name dvSwitch --vxlan-id 5000

Switch Port ID	VDS Port ID	VMKNIC ID
67108869	101	0

esxcli network vswitch dvs vmware vxlan network port stats list --vds-name *value* --vdsport-id *value* --vxlan-id *value*

Shows VXLAN port statistics information with specified network.

Synopsis

esxcli network vswitch dvs vmware vxlan network port stats list --vds-name *value* --vxlan-id *value* --vdsport-id *value*

Example

esxcli network vswitch dvs vmware vxlan network port stats list --vds-name dvSwitch --vxlan-id 5000 --vdsport-id=101

Name	Value
tx.total	0
rx.total	0

esxcli network vswitch dvs vmware vxlan network stats list --vdsd-name *value* --vxlan-id *value*

Shows VXLAN network statistics.

Synopsis

esxcli network vswitch dvs vmware vxlan network stats list --vds-name *value* --vxlan-id *value*

Example

esxcli network vswitch dvs vmware vxlan network stats list --vds-name dvSwitch --vxlan-id 5000

Name	Value
tx.total	0
tx.nonUnicast	0
tx.crossRouter	0
tx.drop.total	0

Name	Value
rx.total	0
rx.mcastEncap	0
rx.crossRouter	0
rx.drop.wrongDest	0
rx.drop.invalidEncap	0
rx.drop.total	0
mac.lookup.found	0
mac.lookup.flood	0
mac.lookup.full	0
mac.update.learn	0
mac.update.extend	0
mac.update.full	0
mac.age	0
mac.renew	0
arp.lookup.found	0
arp.lookup.unknown	0
arp.lookup.full	0
arp.lookup.wait	0
arp.lookup.timeout	0
arp.update.update	0
arp.update.unkown	0
arp.update.notFound	0
arp.age	0
arp.renew	0

esxcli network vswitch dvs vmware vxlan network stats reset --vxlan-id *value* --vdsport-id *value*

Resets VXLAN network statistics.

Synopsis

esxcli network vswitch dvs vmware vxlan network stats reset -vxlan-id *value* --vdsport-id *value*

esxcli network vswitch dvs vmware vxlan network vtep list --vds-name *value* --vxlan-id *value* --segment-id *value* --vtep-ip *value*

Retrieves VXLAN network VTEP table for specified vDS. To retrieve VTEP information for a specific segment or VTEP IP address, specify the segmentID or vtepIP parameter.

Synopsis

esxcli network vswitch dvs vmware vxlan network mac --vds-name value --vxlan-id value [--segment-id *value* --vtep-ip *value*]

Example

esxcli network vswitch dvs vmware vxlan network mac --vds-name dvSwitch --vxlan-id 5000

IP	Segment ID	Is MTEP
192.168.0.2	192.168.0.0	False

esxcli network vswitch dvs vmware vxlan vmknic list --vds-name *value* --endpoint-id *value* --vmknic-name *value* --vmknic-ip *value*

Retrieves VXLAN vmknic multicast group information. To retrieve multicast group information for a specific vmknic, specify the vmknic ID, IP, or name using the appropriate parameter.

Synopsis

esxcli network vswitch dvs vmware vxlan vmknic list --vds-name *value* [--endpoint-id *value* --vmknic-name *value* --vmknic-ip *value*]

Example

esxcli network vswitch dvs vmware vxlan vmknic list --vds-name dvSwitch

Vmknic Name	Switch Port ID	VDS Port ID	Endpoint ID	VLAN ID	IP	Netmask	IP Acquire Timeout	Multicast Group Count	Segment ID
vmk2	67108868	100	0	0	192.168.0.1	255.255.255.0	34960	0	192.168.0.0

esxcli network vswitch dvs vmware vxlan vmknic multicastgroup list --vds-name *value* --vmknic-id *value* --vmknic-name *value* --vmknic-ip *value*

Retrieves VXLAN network VTEP table for specified vDS. To retrieve VTEP information for a specific segment or VTEP IP address, specify the segmentID or vtepIP parameter.

Synopsis

esxcli network vswitch dvs vmware vxlan vmknic multicastgroup list --vds-name *value* [--vmknic-id *value* --vmknic-name *value* --vmknic-ip *value*]

Example

esxcli network vswitch dvs vmware vxlan network mac --vds-name dvSwitch --vmknic-name vmk2

Vmknic Name	Vmknic ID	VXLAN IP	Multicast IP	Joined	Port Count
vmk2	0	192.168.0.1	239.0.0.1	YES	1

esxcli network vswitch dvs vmware vxlan stats list --vds-name *value* --endpoint-id *value* --vmknic-name *value* --vmknic-ip *value*

Retrieves VXLAN vmknic statistics. To retrieve statistics for a specific vmknic, specify the Endpoint ID, IP, or name using the appropriate parameter.

Synopsis

esxcli network vswitch dvs vmware vxlan stats list -vds-name *value* [--endpoint-id *value* --vmknic-name *value* --vmknic-ip *value*]

Example

esxcli network vswitch dvs vmware vxlan stats list --vds-name dvSwitch

Name	Value
tx.passThrough	0
tx.vxlanTotal	0
tx.clone	0
tx.tso	0

Name	Value
tx.csum	0
tx.drop.invalidFrame	0
tx.drop.guestTag	0
tx.drop.noResource	0
tx.drop.invalidState	0
rx.passThrough	0
rx.vxlanTotal	0
rx.clone	0
rx.drop.invalidFrame	0
rx.drop.notExist	0
rx.drop.noResource	0
forward.pass	0
forward.reject	0
forward.rpf	0
arpProxy.reply.total	0
arpProxy.reply.fail	0
arpProxy.request.total	0
arpProxy.request.fail	0
mcastProxy.tx.total	0
mcastProxy.tx.fail	0
mcastProxy.rx.total	0
mcastProxy.rx.fail	0

esxcli network vswitch dvs vmware vxlan stats reset --vds-name *value*

Resets VXLAN vDS statistics.

Synopsis

esxcli network vswitch dvs vmware vxlan stats reset -vds-name *value*

DVFilter Commands

To use the DVFilter command, log in to the host CLI terminal as root with the password that you specified while installing NSX Manager.

summarize-dvfilter

Displays fast-path and slow-path agents of the DVFilters that are deployed on the host.

Synopsis

summarize-dvfilter

Example

```
# summarize-dvfilter
Fastpaths:
agent: dvfilter-faulter, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter
agent: dvfg-igmp, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfg-igmp
agent: dvfilter-generic-vmware, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter-generic-fastpath
```

agent: vmware-sfw, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: vsip
agent: dvfilter-generic-vmware-swsec, refCount: 2, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter-switch-security

Slowpaths:

Filters:
world 1000672395 vmm0:pro-vm vcUuid:'50 07 6c 09 c9 18 c5 9a-bb 78 37 70 e0 52 bd b6'
port 67108869 pro-vm.eth1
vNic slot 0
name: nic-1000672395-eth1-dvfilter-generic-vmware-swsec.0
agentName: dvfilter-generic-vmware-swsec
state: IOChain Attached
vmState: Detached
failurePolicy: failOpen
slowPathID: none
filter source: Alternate Opaque Channel

Deprecated Commands

The following table lists deprecated commands.

Table 3-1. Deprecated Commands

Command
cli ssh allow
clear firewall counters
clear vmwall rules
clear vty
close support-tunnel
copy http URL slot (1|2)
copy http URL temp
copy scp URL slot (1|2)
copy scp URL temp
debug copy
debug export snapshot
debug import snapshot
debug service
debug service flow src
debug show files
debug snapshot list
debug snapshot remove
debug snapshot restore
default web-manager password
duplex auto
duplex (half|full) speed (10|100|1000)
htp server
ip name server
ip policy-address
link-detect
linkwatch interval <5-60>
manager key

Table 3-1. Deprecated Commands

Command
mode policy-based-forwarding
ntp server
open support-tunnel
set support key
show alerts
show debug log
show dv-support
show hardware
show gateway rules
show interface
shop ip addr
show iptables
show kernel message
show kernel message last
show log alerts
show log events
show service helpers
show service statistics
show services
show session-manager counters
show session-manager sessions
show stacktrace
show startup-config
show raid
show raid detail
show realms
copy running-config startup-config
show running-config
show syslog
show system events
show system network_connections
show syslog
show vmwall log
show vmwall rules
ssh end
syslog
telnet
vm validation
vm validation log
vmwall log suppression
web-manager

Index

L

P

Q

R

S

T

U

W