NSX Command Line Interface Reference
VMware NSX for vSphere 6.4
Update 6

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.
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
Contents

Contents 1

About This Book 13

Introduction to the NSX CLI 15
   Logging In and Out of the CLI 15
   Syntax Notation Used in this Document 16
   NSX Manager and NSX Edge CLI Command Modes 16
   NSX Manager and NSX Edge CLI Passwords 16
   Moving Around in the NSX Manager and NSX Edge CLI 17
   Getting Help within the NSX Manager and NSX Edge CLI 17

NSX Manager Commands 19
   cli password 19
   configure terminal 19
   copy running-config startup-config 19
   disable 20
   debug show files 20
   enable 20
   enable password 21
   exit 21
   export tech-support scp 21
   export host-tech-support scp 22
   hostname 22
   interface 23
   ip address 23
   ip route 23
   list 24
   ping 24
   quit 24
   reset 25
   reboot 25
   set clock 25
   setup 26
   show arp 26
   show clock 26
   show ethernet 27
   show filesystem 27
   show log 27
   show running-config 28
   show startup-config 28
   show slots 29
   show tech-support 29
   shutdown 29
   ssh 30
   terminal length 30
   terminal no length 30
   traceroute 31
NSX Command Line Interface Reference

user
user userName privilege web-interface
web-manager
write memory

NSX Central Commands 35
Central Commands Overview 35
Central Common Commands 36
  show cluster 36
  show host hostID 36
  show host hostID health-status 37
  show host hostID health-status detail 37
  show vm vmID 38
  show vnic vnicID 39
Central Controller Commands 39
  show controller list all 39
Central Logical Router Commands 39
  show logical-router controller controllerID dlr dlrID bridge (all | bridgeID) 39
  show logical-router controller controllerID dlr dlrID bridge (all | bridgeID) mac-address-table 40
  show logical-router controller controllerID dlr dlrID brief 40
  show logical-router controller controllerID dlr dlrID interface 40
  show logical-router controller controllerID dlr dlrID route 41
  show logical-router controller controllerID dlr dlrID statistics 41
  show logical-router controller controllerID host hostID connection 42
  show logical-router controller controllerID statistics 42
  show logical-router host hostID connection 43
  show logical-router host hostID dlr dlrID 43
  show logical-router host hostID dlr dlrID arp 44
  show logical-router host hostID dlr dlrID bridge bridgeName mac-address-table 44
  show logical-router host hostID dlr dlrID bridge bridgeName statistics 45
  show logical-router host hostID dlr dlrID bridge bridgeName verbose 46
  show logical-router host hostID dlr dlrID control-plane-statistics 47
  show logical-router host hostID dlr dlrID interface intName brief 48
  show logical-router host hostID dlr dlrID interface intName statistics 49
  show logical-router host hostID dlr dlrID interface intName verbose 50
  show logical-router host hostID dlr dlrID route 50
  show logical-router host hostID dlr dlrID tunable 51
  show logical-router list all 51
  show logical-router list dlr dlrID host 52
  show logical-router resolve 52
Central Logical Switch Commands 52
  show logical-switch controller controllerID host hostID arp 52
  show logical-switch controller controllerID host hostID joined-vnis 53
  show logical-switch controller controllerID host hostID mac 53
  show logical-switch controller controllerID host hostID vtep 53
  show logical-switch controller controllerID vni vni arp 53
  show logical-switch controller controllerID vni vni brief 54
  show logical-switch controller controllerID vni vni connection 54
  show logical-switch controller controllerID vni vni mac 54
  show logical-switch controller controllerID vni vni statistics 55
  show logical-switch controller controllerID vni vni vtep 55
  show logical-switch host hostID config-by-vsm 56
  show logical-switch host hostID statistics 57
  show logical-switch host hostID verbose 57
  show logical-switch host hostID vni vni arp 58
  show logical-switch host hostID vni vni mac 58
show logical-switch host hostID vni vni port portID statistics 59
show logical-switch host hostID vni vni statistics 59
show logical-switch host hostID vni vni verbose 60
show logical-switch host hostID vni vni vtep 60
show logical-switch list all 61
show logical-switch list host hostID vni 61
show logical-switch list vni vni host 61

Central Distributed Firewall Commands 62
  show dfw cluster 62
  show dfw host hostID 62
  show dfw host hostID filter filterID addresses 63
  show dfw host hostID filter filterID discoveredips 63
  show dfw host hostID filter filterID discoveredips stats 63
  show dfw host hostID filter filterID flows 63
  show dfw host hostID filter filterID rules 64
  show dfw host hostID filter filterID stats 64
  show dfw host hostID filter filterID spoofguard 65
  show dfw host hostID filter filterID stats 65
  show dfw host hostID summarize-dvfilter 65
  show dfw vm vmID 67
  show dfw vnic vnicID 67

Central NSX Edge Commands 67
  show edge (all | edgeID) 68
  show edge edgeID arp 68
  show edge edgeID arp-filter 69
  show edge edgeID configuration application-set 69
  show edge edgeID configuration bgp 70
  show edge edgeID configuration certificates 70
  show edge edgeID configuration dhcp 70
  show edge edgeID configuration dns 70
  show edge edgeID configuration firewall 70
  show edge edgeID configuration global 71
  show edge edgeID configuration gslb 71
  show edge edgeID configuration highavailability 71
  show edge edgeID configuration interface 71
  show edge edgeID configuration interface-set 72
  show edge edgeID configuration ipsec 72
  show edge edgeID configuration ipset 72
  show edge edgeID configuration l2vpn 72
  show edge edgeID configuration loadbalancer 73
  show edge edgeID configuration nat 73
  show edge edgeID configuration osfp 73
  show edge edgeID configuration provider-appset 73
  show edge edgeID configuration provider-ipset 73
  show edge edgeID configuration routing-global 74
  show edge edgeID configuration snmp 74
  show edge edgeID configuration sslvpn-plus 74
  show edge edgeID configuration static-routing 74
  show edge edgeID configuration syslog 75
  show edge edgeID eventmgr 75
  show edge edgeID firewall 75
  show edge edgeID firewall flows topN n 75
  show edge edgeID flowtable 76
  show edge edgeID interface 76
  show edge edgeID ip bgp 76
  show edge edgeID ip bgp neighbors 76
  show edge edgeID ip forwarding 77
show edge edgeID ip ospf 77
show edge edgeID ip ospf database 77
show edge edgeID ip ospf interface 77
show edge edgeID ip ospf neighbor 78
show edge edgeID ip route 78
show edge edgeID ipset 78
show edge edgeID log 78
show edge edgeID messagebus 79
show edge edgeID nat 79
show edge edgeID process list 79
show edge edgeID process snapshot 79
show edge edgeID service dhcp 80
show edge edgeID service dns 80
show edge edgeID service highavailability 81
show edge edgeID service highavailability connection-sync 81
show edge edgeID service highavailability link 82
show edge edgeID service ipsec 82
show edge edgeID service ipsec site 83
show edge edgeID service loadbalancer 83
show edge edgeID service loadbalancer error 83
show edge edgeID service l2vpn (on client) 83
show edge edgeID service l2vpn (on server) 84
show edge edgeID service l2vpn site 84
show edge edgeID service l2vpn bridge 84
show edge edgeID service l2vpn conversion-table 85
show edge edgeID service l2vpn etables 86
show edge edgeID service l2vpn trunk-table 86
show edge edgeID service monitor 87
show edge edgeID service monitor service 87
show edge edgeID system cpu 87
show edge edgeID system memory 88
show edge edgeID system network-stats 88
show edge edgeID system storage 88

Central NSX Packet Capture Commands 89
  Capture vNic 89
  Capture pNic 89
  Capture vdrPort 90
  Capture VMKNic 90
  Delete packet capture session 90
  Show all packet capture sessions 91
  Show packet capture session 91
  Show packet capture file content 92
  Stop packet capture session 92
  Stop packet capture session and discard 93
  Transfer packet capture file 93

NSX Edge Commands 95
  clear nat counters 95
  clear arp ipAddress 95
  clear service dhcp lease 95
  clear service ipsec ipsecsa <id> 95
  clear service ipsec ikesa <id> 96
  debug packet capture 96
  debug packet display interface 96
  disable 97
  dnslookup serverName 97
dnslookup serverName (hostname | ipAddress)

enable

export tech-support scp

ping

ping interface addr

ping (ip | ipv6) ipAddress

show arp

show clock

show configuration application-set

show configuration bgp

show configuration certificates

show configuration dhcp

show configuration dns

show configuration firewall

show configuration global

show configuration gslb

show configuration highavailability

show configuration interface

show configuration interface-set

show configuration ipsec

show configuration ipset

show configuration l2vpn

show configuration loadbalancer

show configuration loadbalancer monitor

show configuration loadbalancer pool

show configuration loadbalancer rule

show configuration loadbalancer virtual

show configuration nat

show configuration ospf

show configuration routing-global

show configuration snmp

show configuration sslvpn-plus

show configuration static-routing

show configuration syslog

show configuration vti

show eventmgr

show firewall

show firewall flows

show firewall flows top n

show firewall flows top n sort-by bytes

show firewall flows top n sort-by pkts

show firewall rule-id id

show firewall rule-id id flows

show firewall rule-id id flows top n

show firewall rule-id id flows top n sort-by bytes

show firewall rule-id id flows top n sort-by pkts

show flowstats

show flowtable

show flowtable expect

show flowtable rule-id id

show flowtable rule-id id top n

show flowtable rule-id id top n sort-by bytes

show flowtable rule-id id top n sort-by pkts

show flowtable top n

show flowtable top n sort-by bytes

show flowtable top n sort-by pkts

show flowtimeouts
show hostname 132
show interface 132
show ip address 134
show ip bgp 135
show ip bgp neighbors 135
show ip forwarding 136
show ip ospf 136
show ip ospf database 137
show ip ospf database adv-router 137
show ip ospf database asbr-summary 138
show ip ospf database external 138
show ip ospf database network 139
show ip ospf database nssa-external 139
show ip ospf database opaque-area 139
show ip ospf database router 140
show ip ospf database summary 140
show ip ospf interface 140
show ip ospf neighbor 141
show ip ospf statistics 141
show ip route 141
show ip route bgp 142
show ip route ospf 142
show ipset 142
show ipv6 forwarding 143
show log 144
show log routing 144
show messagebus 145
show nat 146
show nat64 bib 147
show nat64 rules 147
show nat64 sessions 147
show nat64 statistics 148
show netdevice 148
show process 149
show rpfilter 149
show rpfstats 150
show service all 150
show service dhcp 151
show service dns 151
show service highavailability 151
show service highavailability connection-sync 151
show service highavailability internal 152
show service highavailability link 152
show service ipsec 153
show service ipsec cacerts 153
show service ipsec certs 153
show service ipsec crls 153
show service ipsec pubkeys 154
show service ipsec sa 154
show service ipsec site 154
show service ipsec stats 155
show service ipsec stats ikesa 156
show service ipsec stats sa 156
show service ipsec sp 157
show service l2vpn (on client) 157
show service l2vpn (on server) 158
show service l2vpn site 158
show service l2vpn site <sitename>  159
show service l2vpn bridge  160
show service l2vpn conversion table  161
show service l2vpn ebtabels  161
show service l2vpn trunk-table  162
show service loadbalancer error  163
show service loadbalancer monitor  164
show service loadbalancer pool  164
show service loadbalancer session  164
show service loadbalancer table  164
show service loadbalancer virtual  165
show service monitor service  165
show service network-connections  166
show service sslvpn-plus  167
show service sslvpn-plus sessions  168
show service sslvpn-plus stats  168
show service sslvpn-plus tunnels  168
show system cpu  168
show system interrupt  169
show system memory  170
show system network-stats  170
show system storage  171
show system uptime  171
show tech-support  172
show version  172
trace-route  172

Standalone NSX Edge Commands  173
Standalone NSX Edge Overview  173
Standalone NSX Edge Commands  173
ciphers  173
commit  173
configure terminal  174
configure download <From SCP filepath>  174
configure upload <To SCP filepath>  175
dns name-server  175
egress-optimize  175
exit  176
fips enable  176
fips disable  177
ha admin-state  177
ha disable  177
ha get-localnode  178
ha set-config  178
ha set-peernode  178
interface_intfName  179
ip address  179
ip route  179
l2vpn  180
logging  180
mtu  181
no proxy setup  181
no proxy user  181
password  182
peer-ip 182
proxy address 182
proxy username 183
quit 183
rpfILTER 183
server ipAddress [port] 184
show configuration 184
show configuration uncommitted 185
show log 185
show service dns 185
show service highavailability 186
show service highavailability link 186
show service l2vpn 186
show sub-interface 187
ssh (start | stop) 187
sub-interface pairs 187
sub-interface range 188
syslog-server 188
trustca 189
user 189

NSX Host Commands 191

ESXi CLI Commands 191

esxcli network vswitch dvs vmware vxlan config stats get 191
esxcli network vswitch dvs vmware vxlan config stats set 191
esxcli network vswitch dvs vmware vxlan get 191
esxcli network vswitch dvs vmware vxlan list --vds-name value 192
esxcli network vswitch dvs vmware vxlan network list --vds-name value --vxlan-id value 192
esxcli network vswitch dvs vmware vxlan network arp list --vds-name value --vxlan-id value 192
esxcli network vswitch dvs vmware vxlan network arp reset --vds-name value --vxlan-id value 192
esxcli network vswitch dvs vmware vxlan network mac list --vds-name value --vxlan-id value 193
esxcli network vswitch dvs vmware vxlan network mac reset --vxlan-id value --vdsport-id value 193
esxcli network vswitch dvs vmware vxlan network port list --vds-name value --vdsport-id value
--vxlan-id value 193
esxcli network vswitch dvs vmware vxlan network port stats list --vds-name value --vdsport-id value
--vxlan-id value 193
esxcli network vswitch dvs vmware vxlan network stats list --vdsd-name value --vxlan-id value 194
esxcli network vswitch dvs vmware vxlan network stats reset --vxlan-id value --vdsport-id value 195
esxcli network vswitch dvs vmware vxlan network vtep list --vds-name value --vxlan-id value
--segment-id value --vtep-ip value 195
esxcli network vswitch dvs vmware vxlan vmknic list --vds-name value --endpoint-id value
--vmknic-name value --vmknic-ip value 195
esxcli network vswitch dvs vmware vxlan vmknic multicastgroup list --vds-name value --vmknic-id value
--vmknic-name value --vmknic-ip value 195
esxcli network vswitch dvs vmware vxlan vmknic stats list --vds-name value --endpoint-id value
--vmknic-name value --vmknic-ip value 196
esxcli network vswitch dvs vmware vxlan stats reset --vds-name value 197

DVFILTER Commands 197
summarize-dvfILTER 197

NSX Controller Commands 199

restart controller 199
show control-cluster core connection ipAddress 199
show control-cluster core connection-stats ipAddress 199
show control-cluster core log-level 199
show control-cluster core stats 200
show control-cluster logical-routers 200
show control-cluster logical-routers bridge-mac `logicalRouterID_and/or_bridgeID` 200
show control-cluster logical-routers bridges `logicalRouterID_and_bridgeID` 200
show control-cluster logical-routers instance `logicalRouterID` 201
show control-cluster logical-routers interface `logicalRouterID_interfaceName` 201
show control-cluster logical-routers interface-summary `logicalRouterID` 201
show control-cluster logical-routers routes `routerID` 201
show control-cluster logical-routers routes `routerID_and_IPaddress_and_prefixLength` 202
show control-cluster logical-routers stats 202
show control-cluster logical-routers vdr-stats `logicalRouterID` 202
show control-cluster logical-switches arp-records `ipAddress` 202
show control-cluster logical-switches arp-table `vni` 203
show control-cluster logical-switches connection-table `vni` 203
show control-cluster logical-switches joined-vnis `ipAddress` 203
show control-cluster logical-switches mac-records `ipAddress` 203
show control-cluster logical-switches mac-table `vni` 204
show control-cluster logical-switches pkt-cap `pktcap-uuid` display 204
show control-cluster logical-switches pkt-cap `pktcap-uuid` none 205
show control-cluster logical-switches stats 205
show control-cluster logical-switches stats-sample 205
show control-cluster logical-switches vni `vni` 205
show control-cluster logical-switches vni-stats `vni STATS` 206
show control-cluster logical-switches vni-stats-sample `vni` 206
show control-cluster logical-switches vtep-records `ipAddress` 206
show control-cluster logical-switches vtep-table `vni` 206
show control-cluster startup-nodes 207
show network interface 208
show process monitor 208
start control-cluster logical-switches ping 209
start control-cluster logical-switches pktcap 209
start control-cluster logical-switches pktcap-time 210

Hardware Gateway Commands 211

Hardware Gateway Query Commands 211
show hardware-gateway list 211
show hardware-gateway hsc `hardwareGatewayID` brief 212
show hardware-gateway hsc `hardwareGatewayID` certificate 212

Replicator Node Command 212
show hardware-gateway replicator-nodes 212

Bindings Commands 213
show hardware-gateway binding all 213
show hardware-gateway binding hsc `hardwareGatewayID` all 213
show hardware-gateway binding vni `vni` all 213
show hardware-gateway binding `hardwareGatewayID` `vni` 214

Host Commands 214
show hardware-gateway host `hostID` vnis 214
show hardware-gateway host `hostID` bfd-tunnels 214

Controller Commands 215
show hardware-gateway controller `controllerIP` list 215
show hardware-gateway controller `controllerIP` `hardwareGatewayID` certificate 215
show hardware-gateway controller `controllerIP` port-bindings 216
show hardware-gateway controller `controllerIP` control-nodes 216
show hardware-gateway controller `controllerIP` `hardwareGatewayID` inventory 216

Agent Commands 216
show hardware-gateway agent `agentIP` status 217
show hardware-gateway agent `agentIP` replication-cluster 217

VMware, Inc.
show hardware-gateway agent agentIP hardware-gateway [uuid] 217
show hardware-gateway agent agentIP hardware-gateway hardwareGatewayUuid tunnels 218
show hardware-gateway agent agentIP hardware-gateway hardwareGatewayUuid local-macs [vni] 220
show hardware-gateway agent agentIP hardware-gateway hardwareGatewayUuid
  physical-inventory 220
show hardware-gateway agent agentIP hardware-gateway hardwareGatewayUuid bindings 221
show hardware-gateway agent agentIP logical-switches 222
show hardware-gateway agent agentIP logging-level 222
set hardware-gateway agent agentIP logging-level hardwareGatewayAgentLogLevel 222
show hardware-gateway agent agentIP dump 223

Deprecated Commands 225
About This Book

The NSX Command Line Interface Reference describes how to use the NSX Data Center 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 Data Center for vSphere 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 data center operations. This guide assumes familiarity with VMware Infrastructure, 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 for vSphere Installation Guide
- NSX for vSphere Cross-vCenter Installation Guide
- NSX for vSphere Upgrade Guide
- NSX for vSphere Administration Guide
- NSX for vSphere Troubleshooting Guide
- NSX for vSphere Command Line Interface Reference
- NSX for vSphere API Guide
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 or ssh 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.

This chapter includes the following topics:
- “Logging In and Out of the CLI” on page 15
- “Syntax Notation Used in this Document” on page 16
- “NSX Manager and NSX Edge CLI Command Modes” on page 16
- “Moving Around in the NSX Manager and NSX Edge CLI” on page 17
- “Getting Help within the NSX Manager and NSX Edge CLI” on page 17

**Logging In and Out of the CLI**

Before you can run CLI commands, you must initiate a connection 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.

If SSH is enabled, you can also use SSH to access the CLI.
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 [optional] value (requiredA | requiredB) [optionalA | optionalB]
```

<table>
<thead>
<tr>
<th>Format</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>command</td>
<td>Required items, enter as shown.</td>
</tr>
<tr>
<td>[optional]</td>
<td>Optional item.</td>
</tr>
<tr>
<td>value</td>
<td>Placeholder for your value.</td>
</tr>
<tr>
<td>(requiredA</td>
<td>requiredB)</td>
</tr>
<tr>
<td>[optionalA</td>
<td>optionalB]</td>
</tr>
</tbody>
</table>

**NSX Manager and NSX Edge CLI Command Modes**

The commands available to you at any given time depend on the mode you are currently in. Not all appliances have all modes available.

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>NSX Manager</th>
<th>NSX Edge</th>
<th>Standalone NSX Edge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Mode (ssh or console)</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Privileged Mode (enable)</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Configuration Mode (configure terminal)</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Interface Configuration Mode (interface intName)</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>L2 VPN Configuration Mode (l2vpn)</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Save Configuration with</td>
<td>write memory</td>
<td>write memory</td>
<td>commit</td>
</tr>
</tbody>
</table>

Command mode descriptions:

- **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.
- **Configuration**. Configuration mode commands allow you to change the current configuration of utilities on an NSX virtual appliance.
- **Interface Configuration**. Interface configuration mode commands allow you to change the configuration of virtual appliance interfaces. For example, you can change the IP address and IP route for an interface.
- **L2 VPN**. L2 VPN configuration mode commands allow you to change the L2 VPN configuration, including L2 VPN server, L2 VPN username, proxy configuration, and ciphers.

**NSX Manager and NSX Edge CLI Passwords**

The NSX Manager appliance uses different passwords to enter basic mode and privileged mode. When you deploy an NSX Manager appliance from an OVF file you are prompted to configure both passwords. After the NSX Manager appliance has been deployed, you can change the basic mode password with the `cli password` command, and the privileged mode password with the `enable password` command.
The NSX Edge appliance uses the same password to enter basic mode and privileged mode. When you deploy an NSX Edge appliance from NSX Manager via the vSphere Web Client, you are prompted to configure the password. After the NSX Edge appliance has been deployed, you can change the password from the vSphere Web Client (Network & Security > NSX Edges > Select an Edge > Actions > Change CLI Credentials).

The standalone NSX Edge appliance uses different passwords to enter basic mode and privileged mode. When you deploy a standalone NSX Edge appliance from an OVF file you are prompted to configure both passwords. After the standalone NSX Edge appliance has been deployed, you can change the basic and privileged mode passwords with the `password` command.

**Moving Around in the NSX Manager and NSX Edge CLI**

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

<table>
<thead>
<tr>
<th>Keystrokes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTRL+A</td>
<td>Moves the pointer to beginning of the line.</td>
</tr>
<tr>
<td>CTRL+B or the left arrow key</td>
<td>Moves the pointer back one character.</td>
</tr>
<tr>
<td>CTRL+C</td>
<td>Ends any operation that continues to propagate, such as a ping.</td>
</tr>
<tr>
<td>CTRL+D</td>
<td>Deletes the character at the pointer.</td>
</tr>
<tr>
<td>CTRL+E</td>
<td>Moves the pointer to end of the line.</td>
</tr>
<tr>
<td>CTRL+F or the right arrow key</td>
<td>Moves the pointer forward one character.</td>
</tr>
<tr>
<td>CTRL+K</td>
<td>Deletes all characters from the pointer to the end of the line.</td>
</tr>
<tr>
<td>CTRL+N or the down arrow key</td>
<td>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.</td>
</tr>
<tr>
<td>CTRL+P or the up arrow key</td>
<td>Recalls commands in the history, starting with the most recent completed command. Repeat to recall successively older commands.</td>
</tr>
<tr>
<td>CTRL+U</td>
<td>Deletes all characters from the pointer to beginning of the line.</td>
</tr>
<tr>
<td>CTRL+W</td>
<td>Deletes the word to the left of pointer.</td>
</tr>
<tr>
<td>ENTER</td>
<td>Scrolls down one line.</td>
</tr>
<tr>
<td>ESC+B</td>
<td>Moves the pointer back one word.</td>
</tr>
<tr>
<td>ESC+D</td>
<td>Deletes all characters from the pointer to the end of the word.</td>
</tr>
<tr>
<td>ESC+F</td>
<td>Moves the pointer forward one word.</td>
</tr>
<tr>
<td>SPACE</td>
<td>Scrolls down one screen.</td>
</tr>
</tbody>
</table>

**Getting Help within the NSX Manager and NSX Edge CLI**

The CLI contains the following commands to assist you.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Displays a list of available commands.</td>
</tr>
<tr>
<td>sho?</td>
<td>Displays a list of commands that begin with a particular character string (NSX Manager only).</td>
</tr>
<tr>
<td>sho&lt;TAB&gt;</td>
<td>Completes a partial command name.</td>
</tr>
<tr>
<td>show ?</td>
<td>Lists the associated keywords of a command.</td>
</tr>
<tr>
<td>show log ?</td>
<td>Lists the associated arguments of a keyword.</td>
</tr>
<tr>
<td>list</td>
<td>Displays the verbose options of all commands for the current mode (NSX Manager only).</td>
</tr>
</tbody>
</table>
This chapter describes NSX Manager CLI commands. Log in as the user admin to use the NSX Manager commands.

**cli password**

Changes the password of the current command line user. The default command line user is admin.

**Synopsis**

cli password

**CLI Mode**

Configuration

**Example**

nsx-mgr(config)# cli password newpassword

**configure terminal**

Switches to Configuration mode from Privileged mode.

**Synopsis**

configure terminal

**CLI Mode**

Privileged

**Example**

nsx-mgr# configure terminal
nsx-mgr(config)#

**copy running-config startup-config**

Copies the current system configuration to the startup configuration.

**Synopsis**

copy running-config startup-config

**CLI Mode**

Privileged
Example

nsx-mgr# copy running-config startup-config
Building Configuration...
Configuration saved.
[OK]

Related Commands

show running-config
show startup-config

disable

Switches to Basic mode from Privileged mode.

Synopsis
disable

CLI Mode

Basic

Example

nsx-mgr# disable
nsx-mgr>

Related Commands

enable
debug show files

Shows the tcpdump files that have been saved.

Synopsis
debug show files

CLI Mode

Privileged

Example

nsx-mgr# debug show files
total 0
-rw-r--r-- 1 0 Jun 23 16:04 tcpdump.d0.0

Related Commands

enable
enable

Switches to Privileged mode from Basic mode.

Synopsis
enables

CLI Mode

Basic
Example

nsx-mgr> enable
Password:
nsx-mgr#

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
<td>The new password to use.</td>
</tr>
</tbody>
</table>

CLI Mode

Configuration

Example

nsx-mgr# configure terminal
nsx-mgr(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

nsx-mgr(config-if)# exit
nsx-mgr(config)# exit
nsx-mgr#

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. For example, userId@ipAddress/path. Standard scp/ssh syntax is used for username and machine name.

**CLI Mode**
Basic and Privileged

**Example**

nsx-mgr# export tech-support scp user123@host123:file123

**Related Commands**

show tech-support

---

**export host-tech-support scp**

Exports system diagnostics for the specified host ID to a specific location via Secure Copy Protocol (SCP). You can export system diagnostics for ESX command output from the NSX Manager.

**Synopsis**

`export host-tech-support <host-Id> 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**

nsx-mgr# export host-tech-support host-11 scp user123@host123:/file123

**Related Commands**

show tech-support

---

**hostname**

Changes the host name of the machine, which is used as the CLI prompt.

**Synopsis**

`hostname newhostname`

**Option** | **Description**
--- | ---
newhostname | Prompt name to use.

**CLI Mode**
Configuration

**Example**

nsx-mgr(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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>The management port on an NSX virtual machine.</td>
</tr>
</tbody>
</table>

CLI Mode
Configuration

Example

nsx-mgr# configure terminal
nsx-mgr(config)# interface mgmt
nsx-mgr(config-if)#

or

nsx-mgr(config)# no interface mgmt

ip address

Assigns an IP address to an interface. On the NSX Manager appliance, 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 ipAddress/netmask

CLI Mode
Interface Configuration

Example

nsx-mgr(config)# interface mgmt
nsx-mgr(config-if)# ip address 192.168.110.200/24

or

nsx-mgr(config)# 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 ipAddress/netmask gatewayIP

CLI Mode
Configuration
Example

nsx-mgr# configure terminal
nsx-mgr(config)# ip route 0.0.0.0/0 192.168.1.1
or
nsx-mgr(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

nsx-mgr> list
    enable
    exit
    list
    ping WORD
    .

ping

Pings a destination by its hostname or IP address.

Synopsis

ping (hostName | ipAddress)

CLI Mode

Basic, Privileged

Usage Guidelines

Enter CTRL+C to end ping replies.

Example

nsx-mgr# ping 192.168.1.1

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

nsx-mgr(config-if)# quit
nsx-mgr(config)#
Related Commands
exit

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HH:MM:SS</td>
<td>Hours:minutes:seconds</td>
</tr>
<tr>
<td>MM</td>
<td>Month</td>
</tr>
<tr>
<td>DD</td>
<td>Day</td>
</tr>
<tr>
<td>YYYY</td>
<td>Year</td>
</tr>
</tbody>
</table>

CLI Mode
Privileged

Example
nsx-mgr# set clock 23:19:12 04 07 2015
nsx-mgr#
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

Privileged

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 ARP table.

Synopsis

show arp

CLI Mode

Basic, Privileged

Example

nsx-mgr# 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

nsx-mgr# show clock
Tue Apr 7 23:21:10 UTC 2015
Related Commands
set clock

show ethernet
Shows Ethernet information for virtual machine interfaces.

Synopsis
show ethernet

CLI Mode
Basic, Privileged

Example
nsx-mgr# 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
nsx-mgr# 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 log
Shows the appmgmt, manager, or system log of the NSX Manager.

Synopsis
show log (appmgmt | manager | system) [follow | reverse | size | last n]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>follow</td>
<td>Update the displayed log.</td>
</tr>
<tr>
<td>reverse</td>
<td>Show the log in reverse chronological order.</td>
</tr>
<tr>
<td>size</td>
<td>Show the log size.</td>
</tr>
<tr>
<td>last n</td>
<td>Show the last n number of events in the log.</td>
</tr>
</tbody>
</table>
**CLI Mode**

Basic, Privileged

**Example**

```bash
nsx-mgr# show log manager last 3
==========vsm.log=========
2015-04-28 23:10:00.281 GMT  INFO TaskFrameworkExecutor-24 ScheduleSynchronizer:60 -
   Releasing a thread to executor pool and executor pool active count 0
2015-04-28 23:10:25.869 GMT  INFO edgeVseMonitoringThread
   EdgeVseHealthMonitoringThread:219 - Finished Health check for 4 edge vms in
   0 sec
2015-04-28 23:12:25.878 GMT  INFO edgeVseMonitoringThread
   EdgeVseHealthMonitoringThread:219 - Finished Health check for 4 edge vms in
   0 sec
```

**show running-config**

Shows the current running configuration.

**Synopsis**

```
show running-config
```

**CLI Mode**

Basic, Privileged

**Example**

```bash
nsxmgr# show running-config
Building configuration...

Current configuration:
  
ntp server 192.168.110.1
  
ip name server 192.168.110.10
  
hostname nsxmgr-01a
  
interface mgmt
  ip address 192.168.110.15/24
    
ip route 0.0.0.0/0 192.168.110.1
  
web-manager
```

**Related Commands**

- `copy running-config startup-config`
- `show startup-config`

**show startup-config**

Shows the startup configuration.

**Synopsis**

```
show startup-config
```

**CLI Mode**

Basic, Privileged

**Example**

```bash
nsx?mgr# show startup-config
```
Startup Configuration:
!
ntp server 192.168.110.1
!
ip name server 192.168.110.10
!
! Configuration saved
!  2017/01/06 22:35:41
!
hostname nsxmgr-01a
!
interface mgmt
  ip address 192.168.110.15/24
!
ip route 0.0.0.0/0 192.168.110.1
!
web-manager

Related Commands

copy running-config startup-config
show running-config

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

nsx-mgr# 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

nsx-mgr# 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**

nsx-mgr# shutdown

or

nsx-mgr(config)# interface mgmt
nsx-mgr(config-if)# shutdown
nsx-mgr(config-if)# no shutdown

**Related Commands**

reboot

**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 n

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
<td>Enter the number of rows to display, between 0 and 512. If length is 0, no display control is performed.</td>
</tr>
</tbody>
</table>

**CLI Mode**

Privileged

**Example**

manager# terminal length 50

**Related Commands**

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

**traceroute**

Traces the route to a destination.

**Synopsis**

traceroute (hostname | ip_address)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>ip_address</td>
</tr>
</tbody>
</table>

**CLI Mode**

Basic, Privileged

**Example**

nsx-mgr# 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)  0.89 ms  0.913 ms  0.713 ms
  4  10.16.67.118 (10.16.67.118)  1.12 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 NSX Manager user interface admin account and password.

**IMPORTANT** Each NSX 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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Login name of the user.</td>
</tr>
<tr>
<td>hash</td>
<td>Masks the password by using the MD5 hash.</td>
</tr>
<tr>
<td>plaintext</td>
<td>Keeps the password unmasked.</td>
</tr>
<tr>
<td>password</td>
<td>Password to use.</td>
</tr>
</tbody>
</table>
**CLI Mode**

Configuration

**Example**

nsx-mgr(config)# user newuser1 password plaintext abcd1234
or

nsx-mgr(config) no user newuser1

**Related Commands**

cli password

user *userName* privilege web-interface

Allows the specified CLI user to run REST API calls.

**Synopsis**

user *userName* privilege web-interface

**CLI Mode**

Configuration

**Example**

nsx-mgr(config)# user admin privilege web-interface

**web-manager**

Starts the NSX Management Service. To stop the NSX Management Service, use no before the command. When starting the NSX Management Service, it can take a few minutes after getting the OK message for the NSX Management Service to reach the Running state. You can check the status in the NSX Manager Virtual Appliance web interface by clicking View Summary.

**Synopsis**

[no] web-manager

**CLI Mode**

Configuration

**Example**

nsx-mgr(config)# no web-manager
Stopping the web manager ...
OK

nsx-mgr(config)# web-manager
Starting the web manager ...
OK

**write memory**

Writes the current configuration to memory.

**Synopsis**

write memory

**CLI Mode**

Configuration and Interface Configuration
Example

manager# write memory
The chapter includes the following topics:

- “Central Commands Overview” on page 35
- “Central Common Commands” on page 36
- “Central Controller Commands” on page 39
- “Central Logical Router Commands” on page 39
- “Central Logical Switch Commands” on page 52
- “Central Distributed Firewall Commands” on page 62
- “Central NSX Edge Commands” on page 67
- “Central NSX Packet Capture Commands” on page 89

Central Commands Overview

These commands are run from the NSX Manager and retrieve information from the NSX Manager and other devices. The commands allow you to easily compare information from different devices without having to log into each of them. These commands only retrieve information, you must log into the specific device to make configuration changes.

Log in as user admin to use the NSX central commands.

In a cross-vCenter NSX environment, there are multiple NSX Managers. When you log in to an NSX Manager you can retrieve information about objects that are local to that NSX Manager, and information about universal objects. You cannot retrieve information about objects that are local to a different NSX Manager.

You will need some information about your environment in order to use the central commands. The following commands will help you find the appropriate information.

Table 3-1. Finding information to use in central commands

<table>
<thead>
<tr>
<th>Command keyword</th>
<th>Commands to find valid input</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller</td>
<td>show controller list all</td>
</tr>
<tr>
<td>host</td>
<td>Show all clusters:</td>
</tr>
<tr>
<td></td>
<td>show cluster all</td>
</tr>
<tr>
<td></td>
<td>Then show hosts in a specific cluster:</td>
</tr>
<tr>
<td></td>
<td>show cluster clusterID</td>
</tr>
<tr>
<td></td>
<td>Or show all hosts associated with a specific logical router:</td>
</tr>
<tr>
<td></td>
<td>show logical-router list dlr dlrID host</td>
</tr>
<tr>
<td>switch</td>
<td>show logical-switch list all</td>
</tr>
<tr>
<td>dlr</td>
<td>show logical-router list all</td>
</tr>
</tbody>
</table>
Table 3-1. Finding information to use in central commands

<table>
<thead>
<tr>
<th>Command keyword</th>
<th>Commands to find valid input</th>
</tr>
</thead>
<tbody>
<tr>
<td>edge</td>
<td>show edge all (note: lists logical routers and NSX edges)</td>
</tr>
<tr>
<td>filters</td>
<td>Show all clusters: show cluster all  Then show hosts in a specific cluster: show cluster clusterID  Then show all VMs on a host: show host hostID  Then show information for a VM, which includes filters: show vm vmID</td>
</tr>
</tbody>
</table>

Central Common Commands

**show cluster**

Shows all clusters, or shows the hosts in the specified cluster.

**Synopsis**

show cluster (all | clusterID)

**CLI Mode**

Basic

**Example**

nsx-mgr> show cluster all

<table>
<thead>
<tr>
<th>No.</th>
<th>Cluster Name</th>
<th>Cluster Id</th>
<th>Datacenter Name</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Compute Cluster A</td>
<td>domain-c25</td>
<td>ABC Medical</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>Management and Edge Cluster</td>
<td>domain-c7</td>
<td>ABC Medical</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>Compute Cluster B</td>
<td>domain-c27</td>
<td>ABC Medical</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

or

nsx-mgr> show cluster domain-c25

Datacenter: ABC Medical  Cluster: Compute Cluster A

<table>
<thead>
<tr>
<th>No.</th>
<th>Host Name</th>
<th>Host Id</th>
<th>Installation Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>esxcomp-01a.corp.local</td>
<td>host-29</td>
<td>Ready</td>
</tr>
<tr>
<td>2</td>
<td>esxcomp-02a.corp.local</td>
<td>host-34</td>
<td>Ready</td>
</tr>
</tbody>
</table>

**show host hostID**

Shows VMs on the specified host.

**Synopsis**

show host hostID

**CLI Mode**

Basic

**Example**

nsx-mgr> show host host-29

Datacenter: ABC Medical  Cluster: Compute Cluster A  Host: esxcomp-01a.corp.local

<table>
<thead>
<tr>
<th>No.</th>
<th>VM Name</th>
<th>VM Id</th>
<th>Power Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>br-sv-02a</td>
<td>vm-32</td>
<td>off</td>
</tr>
</tbody>
</table>
show host *hostID* health-status

Shows health status of the specified host as HEALTHY/UNHEALTHY/CRITICAL/WARNING.

**Synopsis**

```
show host *hostID* health-status
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show host host-29 health-status
Status: HEALTHY

nsx-mgr> show host host-32 health-status
UNHEALTHY, Host host-29 mount point /vmfs/volumes/58e2c6d5-83319ac1-7830-005056014d86
volume "local_esx-06a" free percentage less than 20%: 0%.
Status: UNHEALTHY

nsx-mgr> show host host-33 health-status
CRITICAL, Control plane agent on host is not in established state with controller. Please
investigate host connection issue with esxcli network ip connection
command.
CRITICAL, VXLAN VDS RegionA01-vDS-MGMT VNI 5007 connection to controller is down: 0.0.0.0 (down).
```

show host *hostID* health-status detail

Shows details of the health status of the specified host.

**Synopsis**

```
show host *hostID* health-status detail
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show host host-33 health-status detail
The host associated cluster check                           [DONE]
The NSX component installation check                        [DONE]
The NSX module VXLAN installation check                     [DONE]
The NSX module DLR installation check                       [DONE]
The NSX VIB installation check                              [DONE]
The control plane agent check                               [DONE]
The firewall agent check                                    [DONE]
The NSX configuration file check                            [DONE]
The host connection to controller check                     [DONE]
The Distributed Switch uplink check                        [DONE]
The Standard Switch uplink check                            [DONE]
The storage volume check                                    [DONE]
UNHEALTHY, Host host-34 mount point /vmfs/volumes/58e2c69b-38d4fa25-b33a-00505601dfe2
volume "local_esx-05a" free percentage less than 20%: 0%.
The Memory overcommit check                                 [DONE]
The physical CPU load check                                 [DONE]
The free memory usage check                                 [DONE]
The VXLAN VDS existence check                               [DONE]
The VXLAN VDS MTU check                                     [DONE]
The VXLAN gateway IP/MAC check                              [DONE]
The VXLAN vmknic check                                      [DONE]
```
The VXLAN uplinks check [DONE]
The VXLAN configuration check [DONE]
The VXLAN vmknic IP address check [DONE]
The VXLAN Overlay settings check [DONE]
The VXLAN vni settings check [DONE]
The host vmnic check [DONE]
The VXLAN vmknic check [DONE]
Status: UNHEALTHY

nsx-mgr> show host host-33 health-status detail
The associated cluster check [DONE]
The NSX component installation check [DONE]
The NSX module VXLAN installation check [DONE]
The NSX module DLR installation check [DONE]
The NSX VIB installation check [DONE]
The control plane agent check [DONE]
The firewall agent check [DONE]
The NSX configuration file check [DONE]
The host connection to controller check [DONE]
CRITICAL, Control plane agent on host is not in established state with controller. Please investigate host connection issue with esxcli network ip connection command.
The Distributed Switch uplink check [DONE]
The Standard Switch uplink check [DONE]
The storage volume check [DONE]
The Memory overcommit check [DONE]
The physical CPU load check [DONE]
The free memory usage check [DONE]
The VXLAN VDS existence check [DONE]
The VXLAN VDS MTU check [DONE]
The VXLAN gateway IP/MAC check [DONE]
The VXLAN vmknic check [DONE]
The VXLAN uplinks check [DONE]
The VXLAN configuration check [DONE]
The VXLAN vmknic IP address check [DONE]
The VXLAN Overlay settings check [DONE]
The VXLAN vni settings check [DONE]
CRITICAL, VXLAN VDS RegionA01-vDS-MGMT VNI 5007 connection to controller is down: 0.0.0.0 (down).
The host vmnic check [DONE]
The VXLAN vmknic check [DONE]
Status: CRITICAL

show vm vmlID

Shows information about the specified VM, including vNIC Name and ID, and filters.

Synopsis

show controller list all

CLI Mode

Basic

Example

nsx-mgr> show vm vm-36
Datacenter: ABC Medical
Cluster: Compute Cluster A
Host: esxcomp-01a.corp.local
VM: web-sv-01a
Virtual Nics List:
1.
  Vnic Name        web-sv-01a - Network adapter 1
  Vnic Id          5026c7cd-b6f3-f4bc-e533-3d4b255c6277.000
  Filters         nic-54466-eth0-vmware-sfw.2
show vnic vnicID

Shows information about the specified vNIC.

Synopsis
show controller list all

CLI Mode
Basic

Example
nsx-mgr> show vnic 5026c7cd-b6f3-f4bc-e533-3d4b255c6277.000
Vnic Name   web-sv-01a - Network adapter 1
Vnic Id      5026c7cd-b6f3-f4bc-e533-3d4b255c6277.000
Mac Address 00:50:56:a6:7a:a2
Port Group Id dvportgroup-198
Filters nic-54466-eth0-vmware-sfw.2

Central Controller Commands

show controller list all

Shows all controllers. This information is retrieved from NSX Manager.

Synopsis
show controller list all

CLI Mode
Basic

Example
nsx-mgr> show controller list all
NAME      IP                        State
controller-4  192.168.110.203     RUNNING
controller-3  192.168.110.202     RUNNING
controller-1  192.168.110.201     RUNNING

Central Logical Router Commands

show logical-router controller controllerID dlr dlrID bridge (all | bridgeID)

Shows information about bridges configured on a logical router. This information is retrieved from the specified controller. Use all to show information for all bridges, or use bridgeID to show information for a specific bridge.

Synopsis
show logical-router controller controllerID dlr dlrID bridge (all | bridgeID)

CLI Mode
Basic

Example
nsx-mgr> show logical-router controller master dlr edge-2 bridge all
LR-Id Bridge-Id Host Active
0x1388 1  192.168.110.53 true
masterControllerIp=192.168.110.203
or
**show logical-router controller controllerID dlr dlrID bridge (all | bridgeID) mac-address-table**

Shows the mac address table for bridges configured on a logical router. This information is retrieved from the specified controller. Use `all` to show the mac address table for all bridges, or use `bridgeID` to show the mac address table for a specific bridge.

**Synopsis**

```
show logical-router controller controllerID dlr dlrID bridge (all | bridgeID) mac-address-table
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-router controller master dlr edge-2 bridge 1 mac-address-table
LR-Id   Bridge-Id   Mac               Vlan-Id Vxlan-Id Port-Id   Source
0x1388   1           68:ef:bd:4e:98:4c 100     0        50331650 vlan
masterControllerIp=192.168.110.203
```

**show logical-router controller controllerID dlr dlrID brief**

Shows information about a logical router. This information is retrieved from the specified controller. `controllerID` can be specified as `master` to retrieve information from the master controller.

**Synopsis**

```
show logical-router controller (master | controllerID) dlr dlrID brief
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-router controller master dlr edge-1 brief
LR-Id   LR-Name          Universal  Service-Controller  Egress-Locale  In-Sync
0x1388   default+edge-1   false      192.168.110.203     local          Yes     NORMAL
masterControllerIp=192.168.110.203
```

**Related Commands**

```
show logical-router host hostID dlr dlrID
```

**show logical-router controller controllerID dlr dlrID interface**

Shows interface information for a logical router. Show information for a single interface by specifying the interface name. This information is retrieved from the specified controller. `controllerID` can be specified as `master` to retrieve information from the master controller.

**Synopsis**

```
show logical-router controller (master | controllerID) dlr dlrID interface [intName]
```

**CLI Mode**

Basic
Example

```
nsx-mgr> show logical-router controller master dlr edge-1 interface
Interface          Type   Id                        IP[
13880000000b       vxlan  5002(0x138a)             172.16.20.1/24
13880000000a       vxlan  5001(0x1389)             172.16.10.1/24
13880000000c       vxlan  5003(0x138b)             172.16.30.1/24
138800000002       vxlan  5000(0x1388)             192.168.10.2/29
masterControllerIp=192.168.110.203
```

or

```
nsx-mgr> show logical-router controller master dlr edge-1 interface 13880000000a
```

```
Interface-Name:   13880000000a
Logical-Router-Id:0x1388
Id:               0x1389
Type:             vxlan
IP:               172.16.10.1/24
DVS-UUID:         88eb0e50-96af-1df1-36fe-c1efa1515149
                  58920e50-931f-c4b2-af82-c947ae1e6250
Mac:              02:50:56:56:44:52
Mtu:              1500
Multicast-IP:     0.0.0.1
Designated-IP:
Flags:            0x280
Bridge-Id:
Bridge-Name:
DHCP-relay-server:
masterControllerIp=192.168.110.203
```

Related Commands

```
show logical-router host hostID dlr dlrID interface intName verbose
show logical-router controller controllerID dlr dlrID route
```

```
show logical-router controller controllerID dlr dlrID route
```

Shows the routes configured on a logical router. Specify the IP address and netmask to see routes configured for a specific network. This information is retrieved from the specified controller. `controllerID` can be specified as master to retrieve information from the master controller.

Synopsis

```
show logical-router controller (master | controllerID) dlr dlrID route [ipAddress/netmask]
```

CLI Mode

Basic

Example

```
nsx-mgr> show logical-router controller master dlr edge-1 route
Destination        Next-Hop[]      Preference Locale-Id                            Source
0.0.0.0/0          192.168.10.1    0          00000000-0000-0000-0000-000000000000
                         CONTROL_VM
masterControllerIp=192.168.110.203
```

Related Commands

```
show logical-router host hostID dlr dlrID route
```

```
show logical-router controller controllerID dlr dlrID statistics
```

Shows statistics for a logical router. This information is retrieved from the specified controller. `controllerID` can be specified as master to retrieve information from the master controller.
Synopsis

show logical-router controller (master | controllerID) dlr dlrID statistics

CLI Mode

Basic

Example

nsx-mgr> show logical-router controller master dlr edge-1 statistics
host.reports.received      6
host.reports.dropped       0
dlrouter.routes.received   6
dlrouter.routes.dropped    0
bridge.reports.received    0
bridge.reports.dropped     0
bridge.macs.received       0
bridge.macs.dropped        0
route.queries.received     0
interface.queries.received 0
mac.queries.received       0
clear.routes.received      1
clear.macs.received        0
errdecode.messages.dropped 0
memfull.messages.dropped   0
errserver.messages.dropped 0
notifications.error        0
masterControllerIP=192.168.110.203

show logical-router controller controllerID host hostIP connection

Shows the IP of a host’s connection to the specified controller.

Synopsis

show logical-router controller controllerID host hostIP connection

CLI Mode

Basic

Example

nsx-mgr> show logical-router controller controller-1 host 192.168.210.51 connection
Version: 6.2

show logical-router controller controllerID statistics

Shows statistics for all logical routers. This information is retrieved from the specified controller.

Synopsis

show logical-router controller controllerID statistics

CLI Mode

Basic

Example

nsx-mgr> show logical-router controller controller-1 statistics
messages.query        0
messages.update       0
messages.flush        0
messages.notification 0
show logical-router host *hostID* connection

Shows all logical router connections on the specified host.

**Synopsis**

text

**CLI Mode**

Basic

**Example**

nsx-mgr> show logical-router host host-29 connection

Host locale Id: 42294beb-799b-4560-3f29-9a5eb70c884a

Connection Information:

```
-------------------------------------
DvsName  VdrPort  NumLifs  VdrVmac
-------  -------  -------  -------
Compute_VDS  vdrPort  4   02:50:56:56:44:52
Teaming Policy: Default Teaming
Uplink : Uplink 1(50331650): 00:50:56:ff:61:12(Team member)
```

Stats : Pkt Dropped  Pkt Replaced  Pkt Skipped
Input : 0 0 1642554
Output : 9 5 591084

show logical-router host *hostID* dlr *dlrID*

Shows information about a logical router. This information is retrieved from the specified host.

**Synopsis**

```
show logical-router host hostID dlr dlrID (brief | verbose)
```

**CLI Mode**

Basic

**Example**

nsx-mgr> show logical-router host host-29 dlr edge-1 brief

VDR Instance Information :

```
-------------------------------------
Vdr Name             Vdr Id     #Lifs   #Routes State      Controller Ip    CP Ip
--------             -------    -----   ------- -----      -------------    -----
default+edge-1       0x1388     4       5       A          192.168.110.203
192.168.210.51
```

or

nsx-mgr> show logical-router host host-29 dlr edge-1 verbose

VDR Instance Information :

```
-------------------------------------
Vdr Name:                   default+edge-1
Vdr Id:                     0x00001388
Number of Lifs:             4
```
Number of Routes: 5
State: Enabled
Controller IP: 192.168.110.203
Control Plane Active: Yes
Num unique nexthops: 1
Generation Number: 0
Edge Active: No

Related Commands

show logical-router controller controllerID dlr dlrID brief

**show logical-router host hostID dlr dlrID arp**

Shows the ARP table for the logical router. This information is retrieved from the specified host.

**Synopsis**

show logical-router host hostID dlr dlrID arp

**CLI Mode**

Basic

**Example**

nsx-mgr> show logical-router host host-29 dlr edge-1 arp

VDR default+edge-1 ARP Information:
Legend: [S: Static], [V: Valid], [P: Proxy], [I: Interface]
Legend: [N: Nascent], [L: Local], [D: Deleted]

<table>
<thead>
<tr>
<th>Network</th>
<th>Mac Interface</th>
<th>Flags</th>
<th>Expiry</th>
<th>SrcPort</th>
<th>Refcnt</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.2</td>
<td>02:50:56:56:44:52</td>
<td>VI</td>
<td>permanent</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>172.16.10.1</td>
<td>02:50:56:56:44:52</td>
<td>VI</td>
<td>permanent</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>172.16.10.11</td>
<td>00:50:56:a6:7a:a2</td>
<td>VL</td>
<td>151</td>
<td>50331657</td>
<td>2</td>
</tr>
<tr>
<td>172.16.30.1</td>
<td>02:50:56:56:44:52</td>
<td>VI</td>
<td>permanent</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>172.16.30.11</td>
<td>00:50:56:a6:ba:09</td>
<td>V</td>
<td>151</td>
<td>50331650</td>
<td>4</td>
</tr>
<tr>
<td>172.16.20.1</td>
<td>02:50:56:56:44:52</td>
<td>VI</td>
<td>permanent</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

**show logical-router host hostID dlr dlrID bridge bridgeName mac-address-table**

Shows MAC address table for a bridge configured on a logical router. This information is retrieved from the specified host.

**Synopsis**

show logical-router host hostID dlr dlrID bridge bridgeName mac-address-table

**CLI Mode**

Basic

**Example**

nsx-mgr> show logical-router host host-100 dlr edge-17 bridge VLAN3 mac-address-table

VDR 'default+edge-17' bridge 'VLAN3' mac address table:
total number of MAC addresses: 2
number of MAC addresses returned: 2

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Address Type</th>
<th>VLAN ID</th>
<th>VXLAN ID</th>
<th>Destination Port</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:50:56:9c:2a:99</td>
<td>Dynamic</td>
<td>0</td>
<td>6</td>
<td>50331653</td>
<td>1</td>
</tr>
<tr>
<td>00:50:56:9c:2a:88</td>
<td>Static</td>
<td>0</td>
<td>6</td>
<td>50331653</td>
<td>20</td>
</tr>
</tbody>
</table>

total number of MAC addresses: 1
number of MAC addresses returned: 1

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Address Type</th>
<th>VLAN ID</th>
<th>VXLAN ID</th>
<th>Destination Port</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:11:11:11:11:11</td>
<td>Static</td>
<td>8</td>
<td>0</td>
<td>9999</td>
<td>103</td>
</tr>
</tbody>
</table>

hostId=host-100

**show logical-router host hostID dlr dlrID bridge bridgeName statistics**

Shows statistics for a bridge configured on a logical-router. This information is retrieved from the specified host.

**Synopsis**

```
show logical-router host hostID dlr dlrID bridge bridgeName statistics
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-router host host-100 dlr edge-17 bridge VLAN3 statistics

VDR 'default+edge-17' bridge 'VLAN3' stats :

Bridge stats:
portNotExist: 0

Network 'vxlan-5000-type-(null)' stats:
  fdbHit: 0
  fdbLearn: 0
  fdbUpdate: 0
  fdbTableFull: 0
  fdbChain: 0
  fdbAged: 0
  fdbMacMoved: 0
  fdbMacHit: 0
  FRPFilterLeafTx: 0
  FRPFilterBridged: 0
  fdbUplinkFilter: 0

  Network port ID '0x3000005' stats:
  pktsTx: 0
  pktsTxMulticast: 0
  pktsTxBroadcast: 0
  pktsRx: 0
  pktsRxMulticast: 0
  pktsRxBroadcast: 0
  droppedTx: 0
  droppedRx: 0
  mappedLenTooShort: 0
  pktSbridged: 0
  pktSdroppedBridged: 0
  pktSdroppedUplink: 0
  droppedTxPortMismatch: 0
  droppedTxVxlanPktToVlan: 0

Network 'vxlan-5000-type-(null)' stats:
```
show logical-router host hostID dlr dlrID bridge bridgeName verbose

Shows information for a bridge configured on a logical router. This information is retrieved from the specified host. bridgeName can be all to show all configured bridges.

Synopsis

show logical-router host hostID dlr dlrID bridge (all | bridgeName) verbose

CLI Mode

Basic

Example

nsx-mgr> show logical-router host host-100 dlr edge-17 bridge VLAN3 verbose

VDR 'default+edge-17' bridge 'VLAN3' config:

Bridge config:
Name:id         VLAN3:1
Portset name:   DemoDSData
Ref count:      2
Number of networks: 2
Number of uplinks: 2

Network 'vxlan-5000-type-(null)' config:
Ref count:      2
Network type:   2
VLAN ID:        0
VXLAN ID:       5000
Ageing time:   300
Fdb entry hold time: 1

Network port ID '0x3000005' stats:
fdbHit:           0
fdbLearn:         0
fdbUpdate:        0
fdbTableFull:     0
fdbChain:         0
fdbAged:          0
fdbMacMoved:      0
fdbMacHit:        0
FRPFilterLeafTx:  0
FRPFilterBridged: 0
fdbUplinkFilter:  0

Network port ID '0x3000005' stats:

pktsTx:                  0
pktsRx:                  0
droppedTx:               0
droppedRx:               0
mappedLenTooShort:       0
pktsBridged:             0
pktsDroppedBridged:      0
pktsDroppedUplink:       0
droppedTxPortMismatch:   0
droppedTxVxlanPktToVlan: 0

show logical-router host hostID dlr dlrID bridge bridgeName verbose
Network 'vxlan-3-type-(null)' config:
Ref count: 2
Network type: 2
VLAN ID: 3
VXLAN ID: 0
Ageing time: 300
Fdb entry hold time: 1
FRP filter enable: 1

Network port ID '0x30000017' config:
Ref count: 1
Port ID: 0x30000017
VLAN ID: 4095
IOChains installed: 0

hostId=host-100

or

nsx-mgr> show logical-router host host-100 dlr edge-17 bridge all verbose

VDR 'LDR-1' bridge 'testbridge' config:

Bridge config:
Name:id testbridge:2
Portset name:
DVS name: opaque-switch-1
Ref count: 1
Number of networks: 2
Number of uplinks: 0

Network 'vxlan-41992-type-bridging' config:
Ref count: 1
Network type: 1
VLAN ID: 0
VXLAN ID: 41992
Ageing time: 300
Fdb entry hold time: 1
FRP filter enable: 1

Network port ID '0x30000005' config:
Ref count: 1
Port ID: 0x30000005
VLAN ID: 4095
IOChains installed: 0

Network 'vxlan-43784-type-bridging' config:
Ref count: 1
Network type: 1
VLAN ID: 0
VXLAN ID: 43784
Ageing time: 300
Fdb entry hold time: 1
FRP filter enable: 1

Network port ID '0x30000005' config:
Ref count: 1
Port ID: 0x30000005
VLAN ID: 4095
IOChains installed: 0

show logical-router host hostID dlr dlrID control-plane-statistics

Shows control plane statistics for a logical router. This information is retrieved from the specified host.
**Synopsis**

`show logical-router host hostID dlr dlrID control-plane-statistics`

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-router host host-29 dlr edge-1 control-plane-statistics

VDR Instance default+edge-1 Control Plane Message Statistics:

Num Link UP RX:              1
Num Link DOWN RX:            0
Num Edge Link UP RX:         0
Num Edge Link DOWN RX:       1
Num Route ADD RX:            10
Err Route ADD:               0
Num Route DEL RX:            6
Err Route DEL:               0
Err Route DEL Match:         2
DUP Route RX:                0
Num Route EOM RX:            1
Err Route Nexthop Add:       0
Err Route Nexthop Del:       0
Num Lif ADD RX:              4
Err Lif ADD:                 0
Num Lif DEL RX:              0
Err Lif Generic:             0
DUP Lif RX:                  2
Num Lif EOM:                 1
Num Lif IP ADD RX:           0
Num Lif IP DEL RX:           0
Num Lif DI Update RX:        0
Num Lif Status Change RX:    0
Num Flush LIF RX:            1
Num Flush Route RX:          2
```

**Synopsis**

`show logical-router host hostID dlr dlrID interface intName brief`

Shows brief information for an interface on a logical router. This information is retrieved from the specified host.

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-router host host-29 dlr edge-1 interface 13880000000a brief

VDR Instance default+edge-1 LIF Information :

State Legend: [A:Active], [d:Deleting], [X:Deleted], [I:Init],[SF-L:Soft Flush LIF]
Modes Legend: [B:Bridging],[E: Empty], [R:Routing],[S:Sedimented],[D:Distributed]
Modes Legend: [In:Internal],[Up:Uplink],[St:Static]

Lif Name     Id           Mode     State     Ip(Mask)
------------- --------- ------ ------ -------------
13880000000a  Vxlan:5001 R,D,In  A  172.16.10.1(255.255.255.0)
Related Commands

show logical-router controller controllerID dlr dlrID interface

show logical-router host hostID dlr dlrID interface intName statistics

Shows statistics for an interface on a logical router. This information is retrieved from the specified host.

Synopsis

show logical-router host hostID dlr dlrID interface intName statistics

CLI Mode

Basic

Example

nsx-mgr> show logical-router host-29 dlr edge-3 interface 13880000000a statistics

VDR default-edge-1 LIF 13880000000a Statistics :

RX Unicast Packets on the interface: 457
RX Unicast Bytes on the interface: 0
TX Unicast Packets on the interface: 0
RX Broadcast Packets on the interface: 0
RX Broadcast Bytes on the interface: 0
TX Broadcast Packets on the interface: 0
TX Broadcast Bytes on the interface: 0
RX Multicast Packets on the interface: 0
RX Multicast Bytes on the interface: 0
RX Packets System Error on interface: 0
TX Ref Errors on the interface: 0
Packets Deferred Free on the interface: 0
RX Packets Dropped on interface: 0

LIF Net Statistics (approx.):

IP & ARP packets RX: 462
IP & ARP packets TX: 4
IP packets Forwarded to Lif: 0
IP packets Consumed: 0
IP packets Fragmented: 0
IP packets Ignored: 0
ARP Request RX: 3
ARP Request TX: 2
ARP Response RX: 2
ARP Response TX: 1
ARP Request for Proxy RX: 0
ARP Request for Proxy My IP RX: 0
GARP RX: 0
GARP TX: 1
ARP Probes TX: 0
ICMP Echo Req RX: 0
ICMP Echo Rsp TX: 0
ICMP Time Exceeded TX: 0
TTL Zero Drops: 0
Bad Checksum Drops: 0
Arp HoldPkts Drops: 0
Packet Allocation Failure: 0
Route not found to Dest: 0
Neighbor not found: 0
show logical-router host hostID dlr dlrID interface intName verbose

Shows information for an interface on a logical router. This information is retrieved from the specified host. `intName` can be all to show verbose information for all interfaces.

**Synopsis**

show logical-router host hostID dlr dlrID interface (all | intName) verbose

**CLI Mode**

Basic

**Example**

nsx-mgr> show logical-router host host-29 dlr edge-1 interface all verbose

VDR default+edge-1 LIF Information:

| Name: | 138800000002 |
| Mode: | Routing, Distributed, uplink |
| Id: | Vxlan:5000 |
| Ip(Mask): | 192.168.10.2(255.255.255.248) |
| Connected Dvs: | Compute_VDS |
| VXLAN Control Plane: | Enabled |
| VXLAN Multicast IP: | 0.0.0.1 |
| State: | Enabled |
| Flags: | 0x2208 |
| DHCP Relay: | Not enabled |

Name: 13880000000a
Mode: Routing, Distributed, Internal
Id: Vxlan:5001
Ip(Mask): 172.16.10.1(255.255.255.0)
Connected Dvs: Compute_VDS

show logical-router host hostID dlr dlrID route

Shows the routes configured on a logical router. This information is retrieved from the specified host.

**Synopsis**

show logical-router host hostID dlr dlrID route

**CLI Mode**

Basic

**Example**

nsx-mgr> show logical-router host host-29 dlr edge-1 route

VDR default+edge-1 Route Table
Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]
Legend: [H: Host], [F: Soft Flush] [!: Reject] [E: ECMP]

<table>
<thead>
<tr>
<th>Destination</th>
<th>GenMask</th>
<th>Gateway</th>
<th>Flags</th>
<th>Ref Origin</th>
<th>UpTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>192.168.10.1</td>
<td>UG</td>
<td>AUTO</td>
<td>272883</td>
</tr>
<tr>
<td>172.16.10.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
<td>UCI</td>
<td>MANUAL</td>
<td>273214</td>
</tr>
<tr>
<td>172.16.20.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
<td>UCI</td>
<td>MANUAL</td>
<td>273241</td>
</tr>
</tbody>
</table>
### Related Commands

```
show logical-router controller controllerID dlr dlrID route
```

### show logical-router host hostID dlr dlrID tunable

Shows tunable parameters for a logical router. This information is retrieved from the specified host.

**Note:** If the control plane agent (netcpa) on a host is down, then wait for the netcpa to come up and resubmit the CLI command.

**Synopsis**

```
show logical-router host hostID dlr dlrID tunable
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-router host host-29 dlr edge-1 tunable
```

**VDR Instance default+edge-1 Tunable Parameters:**

```
enableFLE:            YES
dpLogLevel:           0
enableFrag:           NO
enableIcmpPMTU:       NO
enableIcmpEcho:       YES
enableBcastIcmpEcho:  NO
enableIcmpRateLimit:  NO
defaultTtl:           65
garpSupport:          1
maxArpEntries:        5000
maxFLEntries:         8192
ecmpMethod:           1
rtDeferFlushTimer:    300
vdrARPExpireTime:     600
vdrARPProbeIntvl:     31
vdrARPPreemptTime:    150
```

### show logical-router list all

Shows information about all logical routers. This information is retrieved from NSX Manager.

**Synopsis**

```
show logical-router list all
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-router list all
```

<table>
<thead>
<tr>
<th>Edge Id</th>
<th>Vdr Name</th>
<th>Vdr Id</th>
<th>#Lifs</th>
</tr>
</thead>
<tbody>
<tr>
<td>edge-1</td>
<td>default+edge-1</td>
<td>0x00001388</td>
<td>4</td>
</tr>
</tbody>
</table>
show logical-router list dlr $dlrID$ host

Shows on which hosts the specified logical router is available. This information is retrieved from NSX Manager.

**Synopsis**

show logical-router list dlr $dlrID$ host

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-router list dlr edge-1 host
<table>
<thead>
<tr>
<th>ID</th>
<th>HostName</th>
</tr>
</thead>
<tbody>
<tr>
<td>host-29</td>
<td>esxcomp-01a.corp.local</td>
</tr>
<tr>
<td>host-38</td>
<td>esxcomp-01b.corp.local</td>
</tr>
<tr>
<td>host-10</td>
<td>esx-01a.corp.local</td>
</tr>
<tr>
<td>host-34</td>
<td>esxcomp-02a.corp.local</td>
</tr>
<tr>
<td>host-15</td>
<td>esx-02a.corp.local</td>
</tr>
</tbody>
</table>
```

show logical-router resolve

Shows information about next destination that a logical router will choose when you have configured the logical router with ECMP.

**For example:** You have four NSX Edges. On host-28, you have a source VM 172.17.10.11 that is trying to route to destination 192.168.110.10, and you want to know which of the four NSX Edges will be the next hop for this traffic.

**Synopsis**

show logical-router resolve host $hostID$ dlr show logical-router resolve host $hostID$ dlr

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-router resolve host host-28 dlr default+edge-2 destip 192.168.110.10 srcip 172.17.10.11
VDR default+edge-2 Route Table
Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]
Legend: [H: Host], [F: Soft Flush] [!: Reject] [E: ECMP]

<table>
<thead>
<tr>
<th>Destination</th>
<th>GenMask</th>
<th>Gateway</th>
<th>Flags</th>
<th>Ref Origin</th>
<th>UpTime</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>192.168.5.1</td>
<td>UG</td>
<td>1</td>
<td>AUTO</td>
<td>57</td>
</tr>
</tbody>
</table>
```

**Central Logical Switch Commands**

**show logical-switch controller $controllerID$ host $hostIP$ arp**

Shows the ARP table for a host. This information is retrieved from the specified controller.

**Synopsis**

show logical-switch controller $controllerID$ host $hostIP$ arp
Chapter 3 NSX Central Commands

CLI Mode

Basic

Example

nsx-mgr> show logical-switch controller controller-3 host 192.168.210.51 arp
VNI      IP              MAC               Connection-ID
5001     172.16.10.11    00:50:56:a6:7a:a2 6

show logical-switch controller controllerID host hostIP joined-vnis

Shows connected logical switches on a host. This information is retrieved from the specified controller.

Synopsis

show logical-switch controller controllerID host hostIP connection

CLI Mode

Basic

Example

nsx-mgr> show logical-switch controller controller-3 host 192.168.210.51 joined-vnis
VNI      Controller      BUM-Replication ARP-Proxy Connections
5001     192.168.110.202 Enabled         Enabled   3

show logical-switch controller controllerID host hostIP mac

Shows the MAC address table for a host. This information is retrieved from the specified controller.

Synopsis

show logical-switch controller controllerID host hostIP mac

CLI Mode

Basic

Example

nsx-mgr> show logical-switch controller controller-3 host 192.168.210.51 mac
VNI      MAC               VTEP-IP         Connection-ID
5001     00:50:56:a6:7a:a2 192.168.250.52  6

show logical-switch controller controllerID host hostIP vtep

Shows the VTEP table for a host. This information is retrieved from the specified controller.

Synopsis

show logical-switch controller controllerID host hostIP vtep

CLI Mode

Basic

Example

nsx-mgr> show logical-switch controller controller-3 host 192.168.210.51 vtep
VNI      IP              Segment         MAC               Connection-ID
5001     192.168.250.52  192.168.250.0   00:50:56:60:bb:b6 6

show logical-switch controller controllerID vni vni arp

Shows the ARP table for a logical switch. This information is retrieved from the specified controller. controllerID can be specified as master to retrieve information from the master controller.
**Synopsis**

```
show logical-switch controller (master | controllerID) vni vni arp
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-switch controller master vni 5001 arp
VNI      IP              MAC               Connection-ID
5001     172.16.10.12    00:50:56:a6:a1:e3  7
5001     172.16.10.11    00:50:56:a6:7a:a2   6
masterControllerIp=192.168.110.202
```

**show logical-switch controller controllerID vni vni brief**

Shows information about a logical switch. This information is retrieved from the specified controller. **controllerID** can be specified as master to retrieve information from the master controller.

**Synopsis**

```
show logical-switch controller (master | controllerID) vni vni brief
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-switch controller master vni 5001 brief
VNI      Controller      BUM-Replication ARP-Proxy Connections
5001     192.168.110.202 Enabled         Enabled   3
```

**Related Commands**

```
show logical-switch host hostID vni vni verbose
```

**show logical-switch controller controllerID vni vni connection**

Shows the hosts connected to a logical switch. This information is retrieved from the specified controller. **controllerID** can be specified as master to retrieve information from the master controller.

**Synopsis**

```
show logical-switch controller (master | controllerID) vni vni connection
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-switch controller master vni 5001 connection
Host-IP         Port  ID
192.168.210.51  13335 6
192.168.210.56  35059 7
192.168.210.52  50484 8
masterControllerIp=192.168.110.202
```

**show logical-switch controller controllerID vni vni mac**

Shows the MAC address table for a logical switch. This information is retrieved from the specified controller. **controllerID** can be specified as master to retrieve information from the master controller.

**Synopsis**

```
show logical-switch controller (master | controllerID) vni vni mac
```
Chapter 3  NSX Central Commands

Synopsis

show logical-switch controller (master | controllerID) vni vni mac

CLI Mode

Basic

Example

nsx-mgr> show logical-switch controller master vni 5001 mac
VNI      MAC               VTEP-IP         Connection-ID
5001     00:50:56:a6:a1:e3 192.168.250.53  7
5001     00:50:56:a6:7a:a2 192.168.250.52  6
masterControllerIp=192.168.110.202

show logical-switch controller controllerID vni vni statistics

Shows statistics for a logical switch. This information is retrieved from the specified controller. controllerID can be specified as master to retrieve information from the master controller.

Synopsis

show logical-switch controller (master | controllerID) vni vni statistics

CLI Mode

Basic

Example

nsx-mgr> show logical-switch controller master vni 5001 statistics
update.member         3
update.vtep           5
update.mac            2
update.mac.invalidate 0
update.arp            9
update.arp.duplicate  0
query.mac             1
query.mac.miss        0
query.arp             5
query.arp.miss        5
masterControllerIp=192.168.110.202

show logical-switch controller controllerID vni vni vtep

Shows the VTEP table for a logical switch. This information is retrieved from the specified controller. controllerID can be specified as master to retrieve information from the master controller.

Synopsis

show logical-switch controller (master | controllerID) vni vni vtep

CLI Mode

Basic

Example

nsx-mgr> show logical-switch controller master vni 5001 vtep
VNI      IP              Segment         MAC               Connection-ID
5001     192.168.250.53  192.168.250.0   00:50:56:6c:f5:b8 7
5001     192.168.250.52  192.168.250.0   00:50:56:60:bb:b6 6
5001     192.168.250.51  192.168.250.0   00:50:56:6e:e4:27 8
masterControllerIp=192.168.110.202
Related Commands

```
show logical-switch host hostID vni vni vtep
```

**show logical-switch host hostID config-by-vsm**

Shows controller configuration information. This information is retrieved from the specified host.

**Synopsis**

```
show logical-switch host hostID config-by-vsm
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-switch host host-29 config-by-vsm
<config>
<connectionList>
<connection id="0000">
    <port>1234</port>
    <server>192.168.110.201</server>
    <sslEnabled>true</sslEnabled>
</connection>
<connection id="0001">
    <port>1234</port>
    <server>192.168.110.203</server>
    <sslEnabled>true</sslEnabled>
</connection>
<connection id="0002">
    <port>1234</port>
    <server>192.168.110.202</server>
    <sslEnabled>true</sslEnabled>
</connection>
</connectionList>
<localeId>
    <id>42294BEB-799B-4560-3F29-9A5EB70C884A</id>
</localeId>
<vdrDvsList>
<vdrDvs id="0000">
    <numActiveUplink>1</numActiveUplink>
    <numUpLink>1</numUpLink>
    <teamingPolicy>FAILOVER_ORDER</teamingPolicy>
    <uplinkPortNames>Uplink 1</uplinkPortNames>
    <uuid>88 eb 0e 50 96 af 1d f1-36 fe c1 ef a1 51 51 49</uuid>
    <vxlanOnly>true</vxlanOnly>
</vdrDvs>
</vdrDvsList>
<vdrInstanceId>
<vdrInstanceId id="0000">
    <authToken>28708598-654d-4723-a096-70a474444367</authToken>
    <isUniversal>false</isUniversal>
    <localEgressRequired>False</localEgressRequired>
    <vdrId>5000</vdrId>
    <vdrName>default+edge-1</vdrName>
</vdrInstanceId>
</vdrInstanceIdList>
```
show logical-switch host *hostID* statistics

Shows statistics for a logical switch. This information is retrieved from the specified host.

**Synopsis**

show logical-switch host *hostID* statistics

**CLI Mode**

Basic

**Example**

nsx-mgr> show logical-switch host host-29 statistics
tx.passThrough: 0
tx.vxlanTotal:  0
tx.Clone:  0
tx.tso: 0
tx.csum:    0
tx.drop.invalidFrame:   0
tx.drop.guestTag:   0
tx.drop.noResource: 0
tx.drop.invalidState:   3
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: 3
arpProxy.request.fail: 0
mcastProxy.tx.total:    0
mcastProxy.tx.fail: 0
mcastProxy.rx.total:    0
mcastProxy.rx.fail: 0

show logical-switch host *hostID* verbose

Shows logical switch information. This information is retrieved from the specified host.

**Synopsis**

show logical-switch host *hostID* verbose

**CLI Mode**

Basic

**Example**

nsx-mgr> show logical-switch host host-29 verbose
VXLAN Global States:
  Control plane Out-Of-Sync:  No
  UDP port:  8472
VXLAN VDS:  Compute_VDS
  VDS ID: 88 eb 0e 50 96 af 1d f1-36 fe c1 ef a1 51 51 49
  MTU: 1600
  Segment ID: 192.168.250.0
  Gateway IP: 192.168.250.2
  Gateway MAC: 00:50:56:09:46:07
Vmnic count: 1
VXLAN vmnic: vmk3
  VDS port ID: 44
  Switch port ID: 50331656
  Endpoint ID: 0
  VLAN ID: 0
  IP: 192.168.250.52
  Netmask: 255.255.255.0
  Segment ID: 192.168.250.0
  IP acquire timeout: 0
  Multicast group count: 0

Network count: 4
VXLAN network: 5001
  Multicast IP: N/A (headend replication)
  Control plane: Enabled (multicast proxy,ARP proxy)
  Controller: 192.168.110.202 (up)
  MAC entry count: 2
  ARP entry count: 0
  Port count: 2
VXLAN network: 5002
  Multicast IP: N/A (headend replication)
  Control plane: Enabled (multicast proxy,ARP proxy)
  Controller: 192.168.110.201 (up)
  MAC entry count: 0
  ARP entry count: 0
  Port count: 1
VXLAN network: 5003
  Multicast IP: N/A (headend replication)
  Control plane: Enabled (multicast proxy,ARP proxy)
  Controller: 192.168.110.203 (up)
  MAC entry count: 1
  ARP entry count: 0
  Port count: 1
VXLAN network: 5000
  Multicast IP: 0.0.0.0
  Control plane: Disabled
  MAC entry count: 0
  ARP entry count: 0
  Port count: 1

**show logical-switch host hostID vni vni arp**

Shows the ARP entry count for a logical switch. This information is retrieved from the specified host.

**Synopsis**

show logical-switch host hostID vni vni arp

**CLI Mode**

Basic

**Example**

nsx-mgr> show logical-switch host host-29 vni 5001 arp
ARP entry count: 0

**show logical-switch host hostID vni vni mac**

Shows the MAC entry count for a logical switch. This information is retrieved from the specified host.

**Synopsis**

show logical-switch host hostID vni vni mac

**CLI Mode**

Basic
Example

```
nsx-mgr> show logical-switch host host-29 vni 5001 mac
MAC entry count: 2
  Inner MAC: 00:50:56:e1:3f:db
  Outer MAC: 00:50:56:6e:e4:27
  Outer IP: 192.168.250.51
  Flags: 1
  Inner MAC: 02:50:56:56:44:52
  Outer MAC: 00:50:56:6e:e4:27
  Outer IP: 192.168.250.51
  Flags: D
```

**show logical-switch host hostID vni vni port portID statistics**

Shows the packet statistics for a given VXLAN port on the specified host. You can find VXLAN port numbers with the `show logical-switch host hostID vni vni verbose` command (see VXLAN port field).

**Synopsis**

```
show logical-switch host hostID vni vni port portID statistics
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-switch host host-29 vni 5001 port 68 statistics
  tx.total: 0
  rx.total: 0
```

**Related Commands**

show logical-switch host hostID vni vni verbose

**show logical-switch host hostID vni vni statistics**

Shows statistics for a logical switch. This information is retrieved from the specified host.

**Synopsis**

```
show logical-switch host hostID vni vni statistics
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-switch host host-29 vni 5001 statistics
  tx.total: 0
tx.nonUnicast: 0
tx.crossRouter: 0
tx.drop.total: 1
  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: 4
```
show logical-switch host *hostID* vni *vni* verbose

Shows information about a logical switch. This information is retrieved from the specified host.

**Synopsis**

show logical-switch host *hostID* vni *vni* verbose

**CLI Mode**

Basic

**Example**

nsx-mgr> show logical-switch host host-29 vni 5001 verbose

VXLAN Global States:
   Control plane Out-Of-Sync: No
   UDP port: 8472
VXLAN network: 5001
   Multicast IP: N/A (headend replication)
   Control plane: Enabled (multicast proxy,ARP proxy)
   Controller: 192.168.110.202 (up)
   MAC entry count: 2
   ARP entry count: 0
   Port count: 2
   VXLAN port: 68
      Switch port ID: 50331657
      vmknic ID: 0
   VXLAN port: vdrPort
      Switch port ID: 50331655
      vmknic ID: 0

**Related Commands**

show logical-switch controller *controllerID* vni *vni* brief

show logical-switch host *hostID* vni *vni* vtep

Shows the VTEP count for a logical switch. This information is retrieved from the specified host.

**Synopsis**

show logical-switch host *hostID* vni *vni* vtep

**CLI Mode**

Basic

**Example**

nsx-mgr> show logical-switch host host-29 vni 5001 vtep

VTEP count: 2
   Segment ID: 192.168.250.0
   VTEP IP: 192.168.250.53
   Flags: 0(None)
   Segment ID: 192.168.250.0
Chapter 3 NSX Central Commands

Related Commands

```
show logical-switch controller controllerID vni vni vtep
```

**show logical-switch list all**

Shows all logical switches. This information is retrieved from NSX Manager.

**Synopsis**

```
show logical-switch list all
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-switch list all
NAME                UUID                                   VNI     Trans Zone Name
Transit-Network-01  1f1b49b6-0c1a-4a77-b916-9f3df3e0ff30   5000    Transport-Zone
                vdnscope-1
Web-Tier-01         96c0cfaf-4ae5-43ee-950e-c64cf6d521c3   5001    Transport-Zone
                vdnscope-1
App-Tier-01         d09b79f0-94b5-414e-acb9-5b6ff98e63bb   5002    Transport-Zone
                vdnscope-1
DB-Tier-01          f202a4d3-a036-459d-a2b9-98d8a1cb4e9c   5003    Transport-Zone
                vdnscope-1
```

**show logical-switch list host hostID vni**

Shows all logical switches that are available on a host. This information is retrieved from NSX Manager.

**Synopsis**

```
show logical-switch list host hostID vni
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show logical-switch list host host-29 vni
NAME                UUID                                   VNI     Trans Zone Name
Transit-Network-01  1f1b49b6-0c1a-4a77-b916-9f3df3e0ff30   5000    Transport-Zone
                vdnscope-1
Web-Tier-01         96c0cfaf-4ae5-43ee-950e-c64cf6d521c3   5001    Transport-Zone
                vdnscope-1
App-Tier-01         d09b79f0-94b5-414e-acb9-5b6ff98e63bb   5002    Transport-Zone
                vdnscope-1
DB-Tier-01          f202a4d3-a036-459d-a2b9-98d8a1cb4e9c   5003    Transport-Zone
                vdnscope-1
```

**show logical-switch list vni vni host**

Shows all hosts on which a logical switch is available. This information is retrieved from NSX Manager.

**Synopsis**

```
show logical-switch list vni vni host
```
CLI Mode

Basic

Example

nsx-mgr> show logical-switch list vni 5001 host
ID                   HostName                               VdsName
host-29              esxcomp-01a.corp.local                 Compute_VDS
host-34              esxcomp-02a.corp.local                 Compute_VDS
host-38              esxcomp-01b.corp.local                 Compute_VDS
host-15              esx-02a.corp.local                     Mgmt_Edge_VDS
host-10              esx-01a.corp.local                     Mgmt_Edge_VDS

Central Distributed Firewall Commands

show dfw cluster

Shows clusters protected by distributed firewall.

Synopsis

show dfw cluster (all | clusterID)

CLI Mode

Basic

Example

nsx-mgr> show dfw cluster all
No.  Cluster Name                  Cluster Id               Datacenter Name   Firewall
     Status
 1    Compute Cluster B             domain-c27               ABC Medical       Enabled
 2    Compute Cluster A             domain-c25               ABC Medical       Enabled
 3    Management and Edge Cluster   domain-c7                ABC Medical       Enabled

or

nsx-mgr> show dfw cluster domain-c25
Datacenter: ABC Medical
Cluster: Compute Cluster A
No.  Host Name                Host Id                  Installation Status
1    esxcomp-01a.corp.local   host-29                  Ready
2    esxcomp-02a.corp.local   host-34                  Ready

show dfw host hostID

Shows the VMs protected by distributed firewall on the specified host.

Synopsis

show dfw host hostID

CLI Mode

Basic

Example

nsx-mgr> show dfw host host-29
Datacenter: ABC Medical
Cluster: Compute Cluster A
Host: esxcomp-01a.corp.local
No.  VM Name      VM Id     Power Status
     Status
 1    web-sv-01a   vm-36     on
 2    br-sv-02a    vm-32     off
show dfw host *hostID* filter *filterID* addrsets

Shows address sets (containers) used by the rules on the specified filter.

**Synopsis**

```
show dfw host *hostID* filter *filterID* addrsets
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show dfw host host-29 filter nic-54466-eth0-vmware-sfw.2 addrsets
addrset ip-virtualwire-2 {
  ip 172.16.10.11,
  ip 172.16.10.12,
}
```

show dfw host *hostID* filter *filterID* discoveredips

Shows the discovered VM IPs for the virtual NIC filter as well as detection type. A maximum of 32 IPv4 and 32 IPv6 addresses could be displayed at any time on a filter for detection based on DHCP snooping and 1 IPv4 and 1 IPv6 address could be displayed on a filter for detection based on ARP snooping.

**Synopsis**

```
show dfw host *hostID* filter *filterID* discoveredips
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show dfw host host-29 filter nic-54466-eth0-vmware-sfw.2 discoveredips
Entries found for nic-54466-eth0-vmware-sfw.2: 1
  [1] vlan = 0  mac = 00:50:56:a6:7a:a2  IP = 172.16.10.11 (ARP snooping)
```

show dfw host *hostID* filter *filterID* discoveredips stats

Shows statistics for the discovered VM IPs for the virtual NIC filter including detection types enabled, and counts for additions and deletions.

**Synopsis**

```
show dfw host *hostID* filter *filterID* discoveredips stats
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show dfw host host-29 filter nic-54466-eth0-vmware-sfw.2 discoveredips stats
Features Enabled : 0000000F : (DHCP snooping) (ARP snooping) (DHCPV6 snooping) (ND snooping)
Number of Adds so far : 1
Number of Deletes so far : 0
Last updated time : 294888
Entries found for nic-54466-eth0-vmware-sfw.2: 1
  [1] vlan = 0  mac = 00:50:56:a6:7a:a2  IP = 172.16.10.11 (ARP snooping)
```

show dfw host *hostID* filter *filterID* flows

Shows distributed firewall flows for the specified filter.
**Synopsis**

`show dfw host hostID filter filterID flows`

**CLI Mode**

Basic

**Example**

```plaintext	nsx-mgr> show dfw host host-38 filter nic-54628-eth0-vmware-sfw.2 flows
Count retrieved from kernel active(L3,L4)=2, active(L2)+inactive(L3,L4)=0,
drop(L2,L3,L4)=0
55ce2a2300000003 Active tcp 0800 OUT 1001 0 0 172.16.10.12:Unknown(36768) ->
172.16.20.11:ssh(22) 2609 EST 515817 1576865 9803 9731
55ce2a23000000004 Active icmp 0800 IN 1001 0 0 172.16.30.11 -> 172.16.10.12 8 0 807744
807744 9616 9616
```

**show dfw host hostID filter filterID rule ruleID**

Shows information for a specific firewall rule on the specified filter.

**Synopsis**

`show dfw host hostID filter filterID rule ruleID`

**CLI Mode**

Basic

**Example**

```plaintext	nsx-mgr> show dfw host host-29 filter nic-54466-eth0-vmware-sfw.2 rule 1005
1005 at 3 inout protocol any from addrset ip-virtualwire-2 to addrset ip-virtualwire-2 drop;
```

**show dfw host hostID filter filterID rules**

Shows firewall rules configured on the specified filter.

**Synopsis**

`show dfw host hostID filter filterID rules`

**CLI Mode**

Basic

**Example**

```plaintext	nsx-mgr> show dfw host host-29 filter nic-54466-eth0-vmware-sfw.2 rules
ruleset domain-c25 {
    # Filter rules
    rule 1003 at 1 inout protocol ipv6-icmp icmptype 136 from any to any accept;
    rule 1003 at 2 inout protocol ipv6-icmp icmptype 135 from any to any accept;
    rule 1005 at 3 inout protocol any from addrset ip-virtualwire-2 to addrset ip-virtualwire-2 drop;
    rule 1002 at 4 inout protocol udp from any to any port 68 accept;
    rule 1002 at 5 inout protocol udp from any to any port 67 accept;
    rule 1001 at 6 inout protocol any from any to any accept;
}
ruleset domain-c25_L2 {
    # Filter rules
    rule 1004 at 1 inout ethertype any from any to any accept;
}
show dfw host *hostID* filter *filterID* spoofguard

Shows Spoofguard information for the specified filter.

**Synopsis**

`show dfw host *hostID* filter *filterID* spoofguard`

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show dfw host host-29 filter nic-54466-eth0-vmware-sfw.2 spoofguard
Spoofguard Enabled.
IPv4 Address : 172.16.10.11
MAC Address : 00:50:56:a6:7a:a2
```

show dfw host *hostID* filter *filterID* stats

Shows packet statistics for the specified filter.

**Synopsis**

`show dfw host *hostID* filter *filterID* stats`

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show dfw host host-29 filter nic-54466-eth0-vmware-sfw.2 stats
rule  1003: 31 evals, in 0 out 0 pkts, in 0 out 0 bytes
rule  1003: 0 evals, in 0 out 0 pkts, in 0 out 0 bytes
rule  1005: 31 evals, in 0 out 29 pkts, in 0 out 2268 bytes
rule  1002: 2 evals, in 0 out 0 pkts, in 0 out 0 bytes
rule  1002: 0 evals, in 0 out 0 pkts, in 0 out 0 bytes
rule  1001: 2 evals, in 6273 out 6273 pkts, in 526932 out 526932 bytes
rule  1004: 10 evals, in 6294 out 6321 pkts, in 527898 out 530074 bytes
```

show dfw host *hostID* summarize-dvfilter

Shows a summary of DVFilter information.

**Synopsis**

`show dfw host *hostID* summarize-dvfilter`

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show dfw host host-29 summarize-dvfilter
Fastpaths:
agent: dvfilter-faulter, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter
agent: ESXi-Firewall, refCount: 5, rev: 0x1010000, apiRev: 0x1010000, module: esxfw
agent: dvfilter-generic-vmware, refCount: 2, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter-generic-fastpath
agent: dvfg-igmp, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfg-igmp
agent: dvfilter-generic-vmware-swsec, refCount: 2, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter-switch-security
agent: bridgelearningfilter, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: vdrb
agent: vmware-sfw, refCount: 2, rev: 0x1010000, apiRev: 0x1010000, module: vsip
Slowpaths:
Filters:
```
world 0 <no world>
port 50331650 vmnic0
dvPort slot 0
  name: 41-sw88 eb 0e 50 96 af 1d f1-36 fe c1 ef a1 51 51 49,dvfilter-generic-vmware.0
  agentName: dvfilter-generic-vmware
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
  filter source: Invalid
port 50331652 vmk0
vNic slot 0
  name: nic-0-eth4294967295-ESXi-Firewall.0
  agentName: ESXi-Firewall
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failOpen
  slowPathID: none
  filter source: Invalid
port 50331653 vmk1
vNic slot 0
  name: nic-0-eth4294967295-ESXi-Firewall.0
  agentName: ESXi-Firewall
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failOpen
  slowPathID: none
  filter source: Invalid
port 50331654 vmk2
vNic slot 0
  name: nic-0-eth4294967295-ESXi-Firewall.0
  agentName: ESXi-Firewall
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failOpen
  slowPathID: none
  filter source: Invalid
port 50331656 vmk3
vNic slot 0
  name: nic-0-eth4294967295-ESXi-Firewall.0
  agentName: ESXi-Firewall
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failOpen
  slowPathID: none
  filter source: Invalid
world 54466 vmm0:web-sv-01a vcUuid:'50 26 c7 cd b6 f3 f4 bc-e5 33 3d 4b 25 5e 62 77'
port 50331657 web-sv-01a.eth0
vNic slot 2
  name: nic-54466-eth0-vmware-sfw.2
  agentName: vmware-sfw
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
  filter source: Dynamic Filter Creation
vNic slot 1
  name: nic-54466-eth0-dvfilter-generic-vmware-swsec.1
  agentName: dvfilter-generic-vmware-swsec
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
  filter source: Alternate Opaque Channel
show dfw vm vmID

Shows the vNICs protected by distributed firewall on the specified virtual machine.

**Synopsis**

```
show dfw vm vmID
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show dfw vm vm-36
Datacenter: ABC Medical
Cluster: Compute Cluster A
Host: esxcomp-01a.corp.local
VM: web-sv-01a
Virtual Nics List:
  1.
    Vnic Name      web-sv-01a - Network adapter 1
    Vnic Id        5026c7cd-b6f3-f4bc-e533-3d4b255c6277.000
    Filters        nic-54466-eth0-vmware-sfw.2
```

show dfw vnic vnicID

Shows all filters configured on the specified vNIC.

**Synopsis**

```
show dfw vnic vnicID
```

**CLI Mode**

Basic

**Example**

```
nsx-mgr> show dfw vnic 5026c7cd-b6f3-f4bc-e533-3d4b255c6277.000
Vnic Name      web-sv-01a - Network adapter 1
Vnic Id        5026c7cd-b6f3-f4bc-e533-3d4b255c6277.000
Mac Address    00:50:56:a6:7a:a2
Port Group Id  dvportgroup-198
Filters        nic-54466-eth0-vmware-sfw.2
```

Central NSX Edge Commands

The central edge commands allow you to run a subset of the available edge commands from the NSX Manager command line. The central edge commands have the format `show edge edgeID [keywords and arguments]`, which is the equivalent of running `show [keywords and arguments]` on the NSX Edge appliance, `edgeID`.

`show edge (all | edgeID)` does not have an equivalent command on the NSX Edge appliance.

<table>
<thead>
<tr>
<th>In Central CLI on NSX Manager</th>
<th>In Edge CLI on NSX Edge Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show edge edgeID arp</code></td>
<td><code>show arp</code></td>
</tr>
<tr>
<td><code>show edge edgeID configuration interface [intName]</code></td>
<td><code>show configuration interface [intName]</code></td>
</tr>
<tr>
<td><code>show edge edgeID ip ospf</code></td>
<td><code>show ip ospf</code></td>
</tr>
</tbody>
</table>
The show edge commands can be used to get information from edges in a high availability configuration. show edge edge-1 will retrieve information from the edge appliance that is currently active. To retrieve information from a specific appliance in an high availability configuration, specify the edge by the high availability index, for example, show edge-1.0 or show edge-1.1.

**show edge (all | edgeID )**

Shows information for all edges. To get information for a specific edge, specify the edge ID.

**Synopsis**

`show edge (all | edgeID )`

**CLI Mode**

Basic

**Example**

```bash
nsx-mgr> show edge all
NOTE: CLI commands for Edge ServiceGateway(ESG) start with 'show edge'
CLI commands for Distributed Logical Router(DLR) Control VM start with 'show edge'
CLI commands for Distributed Logical Router(DLR) start with 'show logical-router'

Legend:
Edge Size: Compact - C, Large - L, X-Large - X, Quad-Large - Q

<table>
<thead>
<tr>
<th>Edge ID</th>
<th>Name</th>
<th>Size</th>
<th>Version</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>edge-1</td>
<td>logical-router</td>
<td>C</td>
<td>6.2.0</td>
<td>GREEN</td>
</tr>
<tr>
<td>edge-2</td>
<td>perimeter-gateway</td>
<td>L</td>
<td>6.2.0</td>
<td>GREEN</td>
</tr>
</tbody>
</table>

or

nsx-mgr> show edge edge-2
Id :edge-2
Type :gatewayServices
1) Name :perimeter-gateway-0
Size :large
Host :esx-01a.corp.local
Deploy Status :true
2) Name :perimeter-gateway-1
Size :large
Host :esx-02a.corp.local
Deploy Status :true

-----Services Configuration Status-----
L2VPN :false
Firewall :false
DNS :false
SSLVPN :false
Routing :true
HA :true
Syslog :false
Load Balancer :false
GSLB :false
IPSEC :false
DHCP :false
NAT :true
Bridges :false
```

**show edge edgeID arp**

Shows the Address Resolution Protocol (ARP) table. See `show arp` for an example.

**Synopsis**

`show edge edgeID[.0|.1] arp`
show edge edgeID arp-filter

Displays the ARP packet filter rules that specify what to do with a packet that matches. See show arp for an example.

Synopsis

show edge edgeID arp-filter

CLI Mode

Basic

Example

nsx-mgr>show edge edge-1 arp-filter
haIndex: 0
vShield Edge ARP Filter Table:
Chain IN (policy ACCEPT 2539 packets, 71092 bytes)
pkts bytes target in out source-ip destination-ip source-hw
destination-hw hlen op hrd pro

Chain OUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target in out source-ip destination-ip source-hw
destination-hw hlen op hrd pro

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target in out source-ip destination-ip source-hw
destination-hw hlen op hrd pro

Related Commands

show arp
show edge edgeID arp

show edge edgeID configuration application-set

Shows the application sets (Service Groups) used in the Edge firewall configuration.

Synopsis

show edge edgeID[.0|.1] configuration application-set

CLI Mode

Basic

Related Commands

show configuration application-set
show edge edgeID configuration bgp

Shows the BGP configuration.

**Synopsis**

```
show edge edgeID[.0|.1] configuration bgp
```

**CLI Mode**

Basic

**Related Commands**

show configuration bgp

show edge edgeID configuration certificatestore

Shows the certificate store configuration.

**Synopsis**

```
show edge edgeID[.0|.1] configuration certificatestore
```

**CLI Mode**

Basic

**Related Commands**

show configuration certificatestore

show edge edgeID configuration dhcp

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

**Synopsis**

```
show edge edgeID[.0|.1] configuration dhcp
```

**CLI Mode**

Basic

**Related Commands**

show configuration dhcp

show edge edgeID configuration dns

Shows the DNS configuration.

**Synopsis**

```
show edge edgeID[.0|.1] configuration dns
```

**CLI Mode**

Basic

**Related Commands**

show configuration dns

show edge edgeID configuration firewall

Shows the firewall configuration.
**Synopsis**

`show edge edgeID[.0|.1] configuration firewall`

**CLI Mode**

Basic

**Related Commands**

`show configuration firewall`

---

**show edge edgeID configuration global**

Shows the configuration for all NSX Edge services.

**Synopsis**

`show edge edgeID[.0|.1] configuration global`

**CLI Mode**

Basic

**Related Commands**

`show configuration global`

---

**show edge edgeID configuration gslb**

Show the GSLB (Global Server Load Balancer) configuration.

Note: the show configuration gslb command on the NSX Edge device has more options available.

**Synopsis**

`show edge edgeID[.0|.1] configuration gslb`

**Related Commands**

`show configuration gslb`

---

**show edge edgeID configuration highavailability**

Shows the high availability configuration.

**Synopsis**

`show edge edgeID[.0|.1] configuration highavailability`

**CLI Mode**

Basic

**Related Commands**

`show configuration highavailability`

---

**show edge edgeID configuration interface**

Shows the interface configuration.

**Synopsis**

`show edge edgeID[.0|.1] configuration interface [intName]`

**CLI Mode**

Basic
Related Commands

show configuration interface

show edge edgeID configuration interface-set
Shows the interface set configuration.

Synopsis
show edge edgeID[.0|.1] configuration interface-set

CLI Mode
Basic

Related Commands

show configuration interface-set

show edge edgeID configuration ipsec
Shows certificate configuration for IPSec VPN.

Synopsis
show edge edgeID[.0|.1] configuration ipsec

CLI Mode
Basic

Related Commands

show configuration ipsec

show edge edgeID configuration ipset
Shows IP address groups (IP Sets) configured on the NSX Edge.

Synopsis
show edge edgeID[.0|.1] configuration ipset

CLI Mode
Basic

Related Commands

show configuration ipset

show edge edgeID configuration l2vpn
Shows L2 VPN configuration.

Synopsis
show edge edgeID[.0|.1] configuration l2vpn

CLI Mode
Basic

Related Commands

show configuration l2vpn
show edge edgeID configuration loadbalancer

Shows external, or public, IP address mapped to internal servers for load balancing.

Note: the show configuration loadbalancer command on the NSX Edge device has more options available.

Synopsis

show edge edgeID[.0|.1] configuration loadbalancer

CLI Mode

Basic

Related Commands

show configuration loadbalancer

show edge edgeID configuration nat

Shows the NAT configuration.

Synopsis

show edge edgeID[.0|.1] configuration nat

CLI Mode

Basic

Related Commands

show configuration nat

show edge edgeID configuration osfp

Shows the OSPF configuration.

Synopsis

show edge edgeID[.0|.1] configuration osfp

CLI Mode

Basic

Related Commands

show configuration osfp

show edge edgeID configuration provider-appset

Shows the provider’s application sets (service groups).

Synopsis

show edge edgeID[.0|.1] configuration provider-appset

CLI Mode

Basic

Related Commands

show configuration provider-appset

show edge edgeID configuration provider-ipset

Shows the provider’s IP sets (IP address groups).
Synopsis
show edge edgeID[.0|.1] configuration provider-ipset

CLI Mode
Basic

Related Commands
show configuration provider-ipset

show edge edgeID configuration routing-global
Shows the global routing configuration.

Synopsis
show edge edgeID[.0|.1] configuration routing-global

CLI Mode
Basic

Related Commands
show configuration routing-global

show edge edgeID configuration snmp
Shows the SNMP configuration.

Synopsis
show edge edgeID[.0|.1] configuration snmp

CLI Mode
Basic

Related Commands
show configuration snmp

show edge edgeID configuration sslvpn-plus
Shows the SSL VPN configuration.

Synopsis
show edge edgeID[.0|.1] configuration sslvpn-plus

CLI Mode
Basic

Related Commands
show configuration sslvpn-plus

show edge edgeID configuration static-routing
Shows the static routes defined for the NSX Edge data packets.

Synopsis
show edge edgeID[.0|.1] configuration static-routing
**show edge edgeID configuration syslog**

Shows remote syslog servers defined for the NSX Edge.

**Synopsis**

```
show edge edgeID[.0|.1] configuration syslog
```

**CLI Mode**
Basic

**Related Commands**
show configuration syslog

---

**show edge edgeID eventmgr**

Shows event manager statistics.

**Synopsis**

```
show edge edgeID[.0|.1] eventmgr
```

**CLI Mode**
Basic

**Related Commands**
show eventmgr

---

**show edge edgeID firewall**

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

Note: the show firewall command on the NSX Edge device has more options available.

**Synopsis**

```
show edge edgeID[.0|.1] firewall
```

**CLI Mode**
Basic

**Example**

```
Prompt>
```

**Related Commands**
show firewall

---

**show edge edgeID firewall flows topN n**

Shows firewall packet counters along with top \(n\) number of packet flows.

Note: the show firewall command on the NSX Edge device has more options available.
Synopsis

show edge edgeID[.0|.1] firewall flows topN n

CLI Mode

Basic

Related Commands

show firewall flows

show edge edgeID flowtable
Shows flow table information.

Note: the show flowtable command on the NSX Edge device has more options available.

Synopsis

show edge edgeID[.0|.1] flowtable [rule-id ruleID]

CLI Mode

Basic

Related Commands

show flowtable

show edge edgeID interface
Shows interface information for all interfaces, or a specific interface.

Synopsis

show edge edgeID[.0|.1] interface [intName]

CLI Mode

Basic

Related Commands

show interface

show edge edgeID ip bgp
Shows entries in the Border Gateway Protocol (BGP) routing table.

Synopsis

show edge edgeID[.0|.1] ip bgp

CLI Mode

Basic

Related Commands

show ip bgp

show edge edgeID ip bgp neighbors
Shows BGP neighbors.

Synopsis

show edge edgeID[.0|.1] ip bgp neighbors
**CLI Mode**

Basic

**Related Commands**

show ip bgp neighbors

**show edge edgeID ip forwarding**

Shows forwarding table entries.

**Synopsis**

show edge edgeID[.0|.1] ip forwarding

**CLI Mode**

Basic

**Related Commands**

show ip forwarding

**show edge edgeID ip ospf**

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

**Synopsis**

show edge edgeID[.0|.1] ip ospf

**CLI Mode**

Basic

**Related Commands**

show ip ospf

**show edge edgeID ip ospf database**

Shows IPv4 OSPF database.

Note: the show ip ospf database command on the NSX Edge device has more options available.

**Synopsis**

show edge edgeID[.0|.1] ip ospf database

**CLI Mode**

Basic

**Related Commands**

show ip ospf database

**show edge edgeID ip ospf interface**

Shows IPv4 OSPF interface.

**Synopsis**

show edge edgeID[.0|.1] ip ospf interface

**CLI Mode**

Basic
Related Commands

show ip ospf interface

show edge edgeID ip ospf neighbor
Shows IP addresses of OSPF neighbors.

Synopsis

show edge edgeID[.0|.1] ip ospf neighbor

CLI Mode

Basic

Related Commands

show ip ospf neighbor

show edge edgeID ip route
Shows all routes in the routing information base (RiB).
Note: the show ip route command on the NSX Edge device has more options available.

Synopsis

show edge edgeID[.0|.1] ip route

CLI Mode

Basic

Related Commands

show ip route

show edge edgeID ipset

Synopsis

show edge edgeID[.0|.1] ipset

CLI Mode

Basic

Related Commands

show ipset

show edge edgeID log
Shows the system log.
Note: the show log command on the NSX Edge device has more options available.

Synopsis

show edge edgeID[.0|.1] log

CLI Mode

Basic

Related Commands

show log
show edge edgeID messagebus

Shows message bus statistics.

Synopsis
show edge edgeID[.0|.1] messagebus (forwarder | messages)

CLI Mode
Basic

Related Commands
show messagebus

show edge edgeID nat

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

Synopsis
show edge edgeID[.0|.1] nat

CLI Mode
Basic

Related Commands
show nat

show edge edgeID process list

Shows currently running processes.

Synopsis
show edge edgeID[.0|.1] process list

CLI Mode
Basic

Related Commands
show process

show edge edgeID process snapshot

Shows a snapshot of the process monitor on the specified NSX Edge.

Synopsis
show edge edgeID[.0|.1] process snapshot

CLI Mode
Basic

Example
nsx-mgr> show edge edge-2 process snapshot
haIndex: 0
top - 23:41:21 up 3 days, 5:36, 0 users, load average: 0.00, 0.01, 0.05
Tasks: 88 total, 1 running, 87 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.9%us, 0.4%sy, 0.0%ni, 98.7%id, 0.1%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 1020400k total, 227488k used, 792912k free, 21080k buffers
Swap:  523260k total,  0k used,  523260k free,  58656k cached

PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
23546 root      -2   0 50344 7388 5608 s  0  0.7   0:47.22 heartbeat
1 root      20   0 3956 696 592 s  0  0.0   0:06.32 init
2 root      20   0  0  0  0 s  0  0.0   0:00.00 kthread
3 root      20   0  0  0  0 s  0  0.0   0:01.82 ksoftirqd/0
4 root      20   0  0  0  0 s  0  0.0   0:00.00 kworker/0:0
5 root      20   0  0  0  0 s  0  0.0   0:12.65 kworker/u:0
6 root      RT   0  0  0  0 s  0  0.0   0:02.12 migration/0
7 root      RT   0  0  0  0 s  0  0.0   0:01.93 migration/1
8 root      20   0  0  0  0 s  0  0.0   0:06.58 kworker/1:0
9 root      20   0  0  0  0 s  0  0.0   0:01.13 ksoftirqd/1
10 root     20   0  0  0  0 s  0  0.0   0:25.12 kworker/0:1

or

nsx-mgr> show edge edge-2.1 process snapshot

Related Commands

show process

show edge edgeID service dhcp

Shows whether the DHCP service is running.

Synopsis

show edge edgeID[.0|.1] service dhcp [leaseinfo]

CLI Mode

Basic

Related Commands

show service dhcp

show edge edgeID service dns

Shows whether the DNS service is running.
Note: the show service dns command on the NSX Edge device has more options available.

**Synopsis**

`show edge edgeID[.0|.1] service dns`

**CLI Mode**

Basic

**Related Commands**

`show service dns`

**show edge edgeID service highavailability**

Note: the show service highavailability command on the NSX Edge device has more options available.

**Synopsis**

`show edge edgeID[.0|.1] service highavailability [internal]`

**CLI Mode**

Basic

**Related Commands**

`show service highavailability`

**show edge edgeID service highavailability connection-sync**

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

**Synopsis**

`show edge edgeID service highavailability connection-sync`

**CLI Mode**

Basic

**Example**

```
nsx-mgr>show edge edge-1 service highavailability connection-sync

haIndex:              0
connections local:
current active connections:                0
connections created:                       0    failed:            0
connections updated:                       0    failed:            0
connections destroyed:                     0    failed:            0

connections peer:
current active connections:                0
connections created:                       0    failed:            0
connections updated:                       0    failed:            0
```
connections destroyed: 0  failed: 0

traffic processed:
  0 Bytes 0 Pckts

UDP traffic (active device=vNic_1):
  3432 Bytes sent 3360 Bytes recv
  221 Pckts sent 210 Pckts recv
  0 Error send 0 Error recv

message tracking:
  0 Malformed msgs 0 Lost msgs

Related Commands
  show service highavailability
  show edge edgeID service highavailability

show edge edgeID service highavailability link
Displays HA link information such as IP addresses for peer links and local links.

Synopsis
  show edge edgeID service highavailability link

CLI Mode
  Basic

Example
  nsx-mgr> show edge edge-1 service highavailability link
  haIndex: 0
  Local IP Address: 169.254.1.1/30
  Peer IP Address: 169.254.1.2/30

Related Commands
  show service highavailability
  show edge edgeID service highavailability
  show edge edgeID service highavailability connection-sync

show edge edgeID service ipsec
Shows the VPN service status.

Note: the show service ipsec command on the NSX Edge device has more options available.

Synopsis
  show edge edgeID[.0|.1] service ipsec
show edge edgeID service ipsec site

Synopsis
show edge edgeID[.0|.1] service ipsec site

CLI Mode
Basic

Related Commands
show service ipsec

show edge edgeID service loadbalancer

Shows overall current loadbalancer engine state.

Note: the show service loadbalancer command on the NSX Edge device has more options available.

Synopsis
show edge edgeID[.0|.1] service loadbalancer

CLI Mode
Basic

Related Commands
show service loadbalancer

show edge edgeID service loadbalancer error

Shows the loadbalancer latest errors information.

Note: the show service loadbalancer error command on the NSX Edge device has more options available.

Synopsis
show edge edgeID[.0|.1] service loadbalancer error

CLI Mode
Basic

Related Commands
show service loadbalancer error

show edge edgeID service l2vpn (on client)

Shows the L2 VPN client status.

Synopsis
show edge edgeID service l2vpn
**CLI Mode**

Basic, Privileged

**Example**

```
NSX-edge-1-0> show edge edge-1 service l2vpn
L2 VPN is running
-----------------------------------------------------------------------
L2 VPN type: Client
Tunnel status: up
Total bytes sent: 582
Total bytes received: 408
Tx Packet drop : 0
Rx Packet drop : 0
Encryption Cipher : AES128-GCM-SHA256
```

**show edge edgeID service l2vpn (on server)**

Shows the L2 VPN server status and the tunnel information.

**Synopsis**

```
show edge edgeID service l2vpn
```

**CLI Mode**

Basic

**Example**

```
NSX-edge-1-0> show edge edge-1 service l2vpn
L2 VPN is running
-----------------------------------------------------------------------
L2 VPN type : Server
Tunnel Information :
```

<table>
<thead>
<tr>
<th>CONN ID</th>
<th>SITENAME</th>
<th>USERNAME</th>
<th>INTERFACE</th>
<th>UP TIME</th>
<th>CLIENT</th>
<th>ESG</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Client1</td>
<td>user1</td>
<td>na1</td>
<td>1:19:12</td>
<td>10.172.65.144</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>SiteOne</td>
<td>s1</td>
<td>na2</td>
<td>12:24:28</td>
<td>10.161.95.11</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**show edge edgeID service l2vpn site**

Shows the site status for L2 VPN server. You can run this command on both the client and the server. All sites are displayed, irrespective of the tunnel status.

**Synopsis**

```
show edge edgeID service l2vpn site
```

**CLI Mode**

Basic

**Example**

```
NSX-edge-1> show edge edgeID service l2vpn site
```

<table>
<thead>
<tr>
<th>SITENAME</th>
<th>INTERFACE</th>
<th>TYPE</th>
<th>VLANID/VNI</th>
<th>TUNNELID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SiteOne</td>
<td>vNic_10</td>
<td>VLAN</td>
<td>100</td>
<td>10</td>
</tr>
<tr>
<td>Site Two</td>
<td>vNic_10</td>
<td>VLAN</td>
<td>100</td>
<td>10</td>
</tr>
</tbody>
</table>

**show edge edgeID service l2vpn bridge**

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

show edge edgeID service l2vpn bridge

CLI Mode

Basic

Example

NSX-edge-1-0> show edge edge-1 service l2vpn bridge
bridge name bridge id STP enabled interfaces
br-sub 8000.005056b86b no vNic_2

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

<table>
<thead>
<tr>
<th>INTERFACES</th>
<th>MAC ADDR</th>
<th>VLAN ID</th>
<th>ON BRIDGE?</th>
<th>AGING TIMER</th>
</tr>
</thead>
<tbody>
<tr>
<td>vNic_2</td>
<td>00:50:56:bd:1d:</td>
<td>4094</td>
<td>yes</td>
<td>0:00</td>
</tr>
<tr>
<td>vNic_2</td>
<td>00:50:56:bd:1d:</td>
<td>0</td>
<td>yes</td>
<td>0:00</td>
</tr>
<tr>
<td>vNic_2</td>
<td>00:50:56:bd:1d:</td>
<td>300</td>
<td>yes</td>
<td>0:00</td>
</tr>
<tr>
<td>vNic_2</td>
<td>00:50:56:bd:1d:</td>
<td>2101</td>
<td>yes</td>
<td>0:00</td>
</tr>
<tr>
<td>tap0</td>
<td>82:ef:2e:9d:68:</td>
<td>0</td>
<td>yes</td>
<td>0:00</td>
</tr>
</tbody>
</table>

show edge edgeID 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 edge edgeID service l2vpn conversion-table

CLI Mode

Basic

Example

NSX-edge-1-0> show edge edge-2 service l2vpn conversion-table
vid1 vid2 Tag Type action
=================================
100 10 VLAN TO_VLAN

Egress VLAN Entries
vid1 vid2 Tag Type action
=================================
10 100 VLAN TO_VLAN
VXLAN Table Entries
vid1 vid2 Tag Type action
=================================

show edge edgeID service l2vpn ebtables

*ebtables* is an application program used to set up and maintain the tables of rules that inspect Ethernet frames. To view these rules, run the *ebtables* command.

**Synopsis**

show edge edgeID service l2vpn ebtables

**CLI Mode**

Basic

**Example**

NSX-edge-1-0> show edge edge-1 service l2vpn ebtables

Bridge table: filter
Bridge chain: INPUT, entries: 2, policy: ACCEPT
- i tap0 - j chain_tap0
- i vNic_1 - j chain_vNic_1

Bridge chain: FORWARD, entries: 4, policy: ACCEPT
- o tap0 - j chain_tap0
- i tap0 - j chain_tap0
- o vNic_1 - j chain_vNic_1
- i vNic_1 - j chain_vNic_1

Bridge chain: OUTPUT, entries: 2, policy: ACCEPT
- o tap0 - j chain_tap0
- o vNic_1 - j chain_vNic_1

Bridge chain: chain_vNic_1, entries: 8, policy: ACCEPT
- p 802_1Q - o vNic_1 --vlan-id 4094 - j ACCEPT
- p 802_1Q - i vNic_1 --vlan-id 4094 - j ACCEPT
- p 802_1Q - o vNic_1 --vlan-id 10 - j ACCEPT
- p 802_1Q - i vNic_1 --vlan-id 10 - j ACCEPT
- i vNic_1 - j DROP
- o vNic_1 - j DROP
- i vNic_1 - j DROP
- o vNic_1 - j DROP

Bridge chain: chain_tap0, entries: 4, policy: ACCEPT
- p 802_1Q - o tap0 --vlan-id 10 - j ACCEPT
- p 802_1Q - i tap0 --vlan-id 10 - j ACCEPT
- i tap0 - j DROP
- o tap0 - j DROP

**show edge edgeID 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 edge edgeID service l2vpn trunk-table

**CLI Mode**

Basic

**Example**

NSX-edge-1-0> show edge edge-1 service l2vpn trunk-table
show edge edgeID service monitor

Shows the running status of the health monitor service.

Synopsis

show edge edgeID[0|1] service monitor

CLI Mode

Basic

Related Commands

show service monitor

show edge edgeID service monitor service

Shows the running status of health monitor instances.

Note: the show service monitor command on the NSX Edge device has more options available.

Synopsis

show edge edgeID[0|1] service monitor service [monitorName]

CLI Mode

Basic

Related Commands

show service monitor service

show edge edgeID system cpu

Shows the system CPU details.

Synopsis

show edge edgeID[0|1] system cpu

CLI Mode

Basic

Related Commands

show system cpu
show edge edgeID system memory
Shows the summary of memory utilization.

Synopsis
show edge edgeID[.0|.1] system memory

CLI Mode
Basic

Related Commands
show system memory

show edge edgeID system network-stats
Shows network statistics. For example, statistics for IP, ICMP, TCP and UDP.

Synopsis
show edge edgeID[.0|.1] system network-stats

CLI Mode
Basic

Related Commands
show system network-stats

show edge edgeID system storage
Shows the disk usage details for an NSX Edge.

Synopsis
show edge edgeID[.0|.1] system storage

CLI Mode
Basic

Related Commands
show system storage

show edge edgeID version
Shows the software version running on the virtual machine.

Synopsis
show edge edgeID[.0|.1] version

CLI Mode
Basic

Related Commands
show version
Central NSX Packet Capture Commands

The central packet capture commands allow you to issue packet capture on the NSX Manager from the NSX Manager command line. You can also stop the capture using the CLI command, and transfer the packet capture file.

Optional parameters for packet capture commands are "Filters" used for pktcap-uw on ESX host.

These filters are advanced feature for the central packet capture commands, and is only recommended to be used by users who are familiar with pktcap-uw on ESX host.

NOTE The packet capture central CLI commands requires vSphere 5.5U3 or higher. These commands are not supported on earlier vSphere 5.5 releases.

Capture vNic
Captures packets for a specific VM vNic. Direction has two options, input and output.

Input is for traffic going into vNic, and output is for traffic going out from vNic.

Synopsis

debug packet capture host < host-id > vnic <vnic-id> dir <direction> parameters [optional parameters]

CLI Mode
Privileged

Example

nsx-mgr# debug packet capture host host-32 vnic 502e71fa-1a00-759b-e40f-ce778e915f16.000 dir input parameters
Session: 7cfcb12e-4245-4c08-99ff-5cda50e80b76
Request:
  Capture host: host-32
  Vnic: 502e71fa-1a00-759b-e40f-ce778e915f16.000
  Capture point: vnic
  Capture direction: input
  Session file: /tmp/pktcap/7cfcb12e-4245-4c08-99ff-5cda50e80b76.pcap
  Session status: started

Capture pNic
Captures packets for a specific physical Nic. Direction has two options, input and output.

Input is for traffic going into pNic, and output is for traffic going out from pNic.

Synopsis

debug packet capture host <host-id> vmnic <vmnic-name> dir <direction> parameters [optional parameters]

CLI Mode
Privileged

Example

nsx-mgr# debug packet capture host host-32 vmnic vmnic1 dir input parameters
Session: 7cfcb12e-4245-4c08-99ff-5cda50e80b76
Request:
  Capture host: host-32
  Vnic: vmnic1
  Capture point: vmnic
  Capture direction: input
  Session file: /tmp/pktcap/7cfcb12e-4245-4c08-99ff-5cda50e80b76.pcap
Capture vdrPort

Captures packets for a specific port of virtual distributed router (vDR). Direction has two options, input and output.

Input is for traffic going into vDR, and output is for traffic going out from vDR.

**Synopsis**

```
debug packet capture host <host-id> vdrport dir <direction> parameters [optional parameters]
```

**CLI Mode**

Privileged

**Example**

```
nsx-mgr# debug packet capture host host-32 vdrport dir input parameters
Session: f3a74117-e99c-4ad0-82f4-89aa7f04af7a
Request:
  Capture host: host-32
  Capture point: vdrport
  Capture direction: input
Session file: /tmp/pktcap/f3a74117-e99c-4ad0-82f4-89aa7f04af7a.pcap
Session status: started
```

Capture VMKNic

Captures packets for a specific VM KNic. Direction has two options, input and output.

Input is for traffic going into VMKNic, and output is for traffic going out from VMKNic.

**Synopsis**

```
debug packet capture host <host-id> vmknic <vmknic-name> dir <direction> parameters [optional parameters]
```

**CLI Mode**

Privileged

**Example**

```
nsx-mgr# debug packet capture host host-32 vmknic vmk0 dir input parameters
Session: f0142774-54ec-4a63-9f18-49185e65480e
Request:
  Capture host: host-32
  Vmknic: vmk0
  Capture point: vmknic
  Capture direction: input
Session file: /tmp/pktcap/f0142774-54ec-4a63-9f18-49185e65480e.pcap
Session status: started
```

Delete packet capture session

Deletes a specific packet capture session.

**Synopsis**

```
d debug packet capture clear session <capture-id>
```
CLI Mode
Privileged

Example

nsx-mgr# debug packet capture clear session 7cfcb12e-4245-4c08-99ff-5cda50e80b76
Session: 7cfcb12e-4245-4c08-99ff-5cda50e80b76
Request:  
  Capture host: host-32
  Vnic: 502e71fa-1a00-759b-e40f-ce778e915f16.000
  Capture point: vnic
  Capture direction: input
Session file: /tmp/pktcap/7cfcb12e-4245-4c08-99ff-5cda50e80b76.pcap
Session status: deleted

Show all packet capture sessions

Shows details of all packet capture sessions.

Synopsis

show packet capture sessions

CLI Mode
Privileged

Example

nsx-mgr# show packet capture sessions
Session: 7cfcb12e-4245-4c08-99ff-5cda50e80b76
Request:  
  Capture host: host-32
  Vnic: 502e71fa-1a00-759b-e40f-ce778e915f16.000
  Capture point: vnic
  Capture direction: input
Session file: /tmp/pktcap/7cfcb12e-4245-4c08-99ff-5cda50e80b76.pcap
Session status: started

======================================
Started session: 1
Stopped session: 0
Finished session: 0
Error session: 0
Sessions:

Show packet capture session

Shows a specific packet capture session.

Synopsis

show packet capture session <capture-id>

CLI Mode
Privileged

Example

nsx-mgr# show packet capture session 7cfcb12e-4245-4c08-99ff-5cda50e80b76
Session: 7cfcb12e-4245-4c08-99ff-5cda50e80b76
Request:  
  Capture host: host-32
Show packet capture file content

Shows the packet capture file content.

Synopsis

debag packet capture display session <capture-id> parameters [optional parameters]

CLI Mode

Privileged

Example

nsx-mgr# debug packet capture display session f3a74117-e99c-4ad0-82f4-89aa7f04af7a parameters
Session: f3a74117-e99c-4ad0-82f4-89aa7f04af7a
Request:
  Capture host: host-32
  Capture point: vdrport
  Capture direction: input
  Capture point: vdrport
  Capture direction: input
Session file: /tmp/pktcap/2f118862-c1c2-432c-acb2-208936cd753e.pcap
Session status: finished
Capture packets:
  reading from file /tmp/pktcap/2f118862-c1c2-432c-acb2-208936cd753e.pcap, link-type EN10MB (Ethernet)
    11:10:13.140734 ARP, Reply 192.168.100.12 is-at 00:50:56:ac:d2:eb (oui Unknown), length 46
    11:10:13.143346 IP 192.168.100.12 > 192.168.100.11: ICMP echo reply, id 8449, seq 0, length 64
    11:10:14.130603 IP 192.168.100.12 > 192.168.100.11: ICMP echo reply, id 8449, seq 1, length 64

Stop packet capture session

Stops a specific packet capture session.

Synopsis

no debug packet capture session <capture-id>

CLI Mode

Privileged

Example

nsx-mgr# no debug packet capture session 7cfcb12e-4245-4c08-99ff-5cda50e80b76
Session: 7cfcb12e-4245-4c08-99ff-5cda50e80b76
Request:
  Capture host: host-32
  Vnic: 502e71fa-1a00-759b-e40f-ce778e915f16.000
  Capture point: vnic
  Capture direction: input
Session file: /tmp/pktcap/7cfcb12e-4245-4c08-99ff-5cda50e80b76.pcap
Stop packet capture session and discard

Stops a specific packet capture session, and also discards the session.

**Synopsis**

```bash
no debug packet capture session <capture-id>
```

**CLI Mode**

Privileged

**Example**

```bash
nsx-mgr# no debug packet capture session 7cfcb12e-4245-4c08-99ff-5cda50e80b76 discard
```

Session: 7cfcb12e-4245-4c08-99ff-5cda50e80b76
Request:
- Capture host: host-32
- Vnic: 502e71fa-1a00-759b-e40f-ce778e915f16.000
- Capture point: vnic
- Capture direction: input
Session file: /tmp/pktcap/7cfcb12e-4245-4c08-99ff-5cda50e80b76.pcap
Session status: deleted

Transfer packet capture file

Transfers the packet capture file content to user’s computer. Shows the file content to user when the transfer is complete and file is ready.

**Synopsis**

```bash
depbug packet capture scp session <capture-id> url <user@url:file>
```

**CLI Mode**

Privileged

**Example**

```bash
nsx-mgr# debug packet capture scp session f3a74117-e99c-44d0-82f4-89aa7f04af7a url admin@10.162.210.4:newfile
```

Session: f3a74117-e99c-44d0-82f4-89aa7f04af7a
Request:
- Capture host: host-32
- Capture point: vdrport
- Capture point: vdrport
- Capture direction: input
Session file: /tmp/pktcap/2f118862-c1c2-432c-acb2-208936cd753e.pcap
Session status: finished
Begin SCP:
The authenticity of host '10.162.210.4 (10.162.210.4)' can't be established.
RSA key fingerprint is SHA256:BGiCwphuw1gu97dZB3qg0ZyH/UEy076Ekwcse+kFB3yA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.162.210.4' (RSA) to the list of known hosts.
This chapter describes NSX Edge CLI commands. Log in as the user admin to use the NSX Edge commands.

**clear nat counters**
Resets NAT counters to zeros.

**Synopsis**
```
clear nat counters
```

**CLI Mode**
Privileged

**clear arp ipAddress**
Deletes an entry from the ARP table.

**Synopsis**
```
clear arp ipAddress
```

**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 ipsecsa <id>**
Deletes the SA (Security Association) associated with IPSec.

**NOTE:** You can find out the connection ID from output of the "show service ipsec site" command.

**Synopsis**
```
clear service ipsec ipsecsa <id>
```
CLI Mode
Privileged

Example
nsx-edge # clear service ipsec ipsecsa 8
Closing IPSEC SA 8 succeeded.

clear service ipsec ipxes <id>
Deletes the SA (Security Association) associated with IKE.

NOTE: You can find out the connection ID from output of the "show service ipsec site" command.

Synopsis
clear service ipsec ikesa <id>

CLI Mode
Privileged

Example
nsx-edge # clear service ipsec ikesa 2
Closing IKE SA 2 succeeded.

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]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>intif</td>
<td>The specific NSX Edge interface from which to capture packets.</td>
</tr>
<tr>
<td>expression</td>
<td>A tcpdump-formatted string. You must use an underscore between words in the expression.</td>
</tr>
</tbody>
</table>

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 [intName] [expression]
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>intName</td>
<td>The specific interface from which to capture packets.</td>
</tr>
<tr>
<td>expression</td>
<td>A tcpdump-formatted string. You must use an underscore between words in the expression.</td>
</tr>
</tbody>
</table>

**CLI Mode**

Privileged

**Example**

NSX-edge-1-0# debug packet display interface vNic_0 host_10.10.11.11_and_port_80

disable

Switches to Basic mode from Privileged mode.

**Synopsis**

disable

**CLI Mode**

Basic

**Example**

NSX-edge-1-0# disable
NSX-edge-1-0>

**Related Commands**

enable

dnslookup **servername**

Makes DNS lookup query to the specified DNS server.

**Synopsis**

dnslookup **servername**

**CLI Mode**

Basic

dnslookup **servername** (**hostname** | **ipAddress**)  

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

**Synopsis**

dnslookup **servername** (**hostname** | **ipAddress**)  

**CLI Mode**

Basic

enable

Switches to Privileged mode from Basic mode.

**Synopsis**

enable
**CLI Mode**

Basic

**Example**

```
NSX-edge-1-0> enable
NSX-edge-1-0#
```

**Related Commands**

disable

---

**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**

```
NSX-edge-1-0# export tech-support scp user123@host123:file123
```

---

**ping**

Pings a destination by its hostname or IP address.

Enter CTRL+C to end ping replies.

**Synopsis**

```
ping (hostname | ipAddress)
```

**CLI Mode**

Basic, Privileged

**Example**

```
NSX-edge-1-0# 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. This command is useful for debugging IPSec-related issues.

Enter CTRL+C to end ping replies.

**Synopsis**

```
ping interface addr (sourceHostname | sourceAddress) (destHostname | destAddress)
```
ping (ip | ipv6) ipAddress

Pings a destination by its hostname or IP address. Specify ip to ping an IPv4 address, or ipv6 to ping an IPv6 address.

Optionally you can specify the following:
- **Size**: The data packet size (not including the ICMP header) and “don’t fragment” flag. Enter CTRL+C to end ping replies.
- **Count**: Stop after sending count `ECHO_REQUEST` packets, that you’d like to be recorded and displayed.
- **Timeout**: Time to wait for a response, in seconds.

**Synopsis**

```
ping (ip | ipv6) ipAddress [size packetSize [nofrag]]
```

**CLI Mode**

Basic, Privileged

**Example**

```
vshieldEdge# ping interface addr 192.168.1.1 69.147.76.15
```

```
PING 192.168.110.10 (192.168.110.10) 32(60) bytes of data.
40 bytes from 192.168.110.10: icmp_seq=1 ttl=127 time=9.37 ms
40 bytes from 192.168.110.10: icmp_seq=2 ttl=127 time=10.6 ms
40 bytes from 192.168.110.10: icmp_seq=3 ttl=127 time=2.98 ms
40 bytes from 192.168.110.10: icmp_seq=4 ttl=127 time=2.26 ms
40 bytes from 192.168.110.10: icmp_seq=5 ttl=127 time=3.86 ms ^C
--- 192.168.110.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 2.266/5.832/10.667/3.483 ms
```

```
NSX-edge> ping ip 192.168.110.10 count 2
PING 192.168.110.10 (192.168.110.10) 56(84) bytes of data.
64 bytes from 192.168.110.10: icmp_seq=1 ttl=125 time=1.18 ms
64 bytes from 192.168.110.10: icmp_seq=2 ttl=125 time=1.20 ms
```

```
show arp
```

Shows the ARP table.

**ARP State**

<table>
<thead>
<tr>
<th>ARP State</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERMANENT</td>
<td>The entry is valid forever. It can only be removed administratively</td>
</tr>
</tbody>
</table>
NOARP   The entry is valid. It will not be checked again, but it can be removed when its lifetime expires
REACHABLE The entry is valid until the reachability timeout expires
STALE   The entry is valid but suspicious
DELAY   The kernel is waiting to confirm the state of a stale neighbor

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

NSX-edge-1-0# show clock
wed Apr 29 00:08:24 GMT 2015

show configuration application-set

Show the application sets (Service Groups) used in the Edge firewall configuration.

Synopsis

show configuration application-set

CLI Mode

Basic

Example

NSX-edge-1-0> show configuration
vShield Edge ApplicationSet Config:
{    "applicationSet" : [        {            "application" : [],            "id" : "application-370"        },        {            "application" : [            {"protocol" : ["6"
[ ],
"icmptypenumber" : [],
"sourcePort" : [],
"port" : [ 
  "2100"
]
],
{
  "protocol" : [ 
    "6"
  ],
  "icmptypenumber" : [],
  "sourcePort" : [],
  "port" : [ 
    "1575"
  ]
},
{
  "protocol" : [ 
    "6"
  ],
  "icmptypenumber" : [],
  "sourcePort" : [],
  "port" : [ 
    "8080"
  ]
},
{
  "protocol" : [ 
    "6"
  ],
  "icmptypenumber" : [],
  "sourcePort" : [],
  "port" : [ 
    "2482"
  ]
},
{
  "protocol" : [ 
    "6"
  ],
  "icmptypenumber" : [],
  "sourcePort" : [],
  "port" : [ 
    "1521"
  ]
},
{
  "protocol" : [ 
    "6"
  ],
  "icmptypenumber" : [],
  "sourcePort" : [],
  "port" : [ 
    "2481"
  ]
},
{
  "protocol" : [ 
    "6"
  ],
  "icmptypenumber" : [],
  "sourcePort" : [],
  "port" : [ 
    "1321"
  ]
}
**show configuration bgp**

Shows the BGP configuration.

**Synopsis**

`show configuration bgp`

**CLI Mode**

Basic

**Example**

```
NSX-edge-1-0> show configuration
-----------------------------------------------------------------------
vShield Edge BGP Routing Protocol Config:
{
    "bgp" : {
        "gracefulRestart" : true,
        "redistribute" : {
            "rules" : [
                {
                    "fromOSPF" : false,
                    "fromBGP" : false,
                    "fromStatic" : false,
                    "fromConnected" : true,
                    "action" : "permit",
                    "id" : 0,
                    "prefix" : null
                }
            ],
            "enabled" : true
        },
        "localAS" : 65001,
        "defaultOriginate" : true,
        "neighbours" : [
            {
                "remoteAS" : 65001,
                "protocol" : ["6"],
                "icmpType" : [],
                "sourcePort" : [],
                "port" : ["2481"]
            },
            {
                "protocol" : ["6"],
                "icmpType" : [],
                "sourcePort" : [],
                "port" : ["1526"]
            }
        ],
        "id" : "applicationgroup-22"
    }
}
```
show configuration certificatestore

Shows the certificate store configuration.

Synopsis

CLI Mode

Basic

Example

NSX-edge-1-0> show configuration certificatestore

vShield Edge Certificate Store Config:
{
  "certificateStoreConfig": {
    "certificates": [],
    "caCertificates": [],
    "crls": []
  }
}
**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**

```
NSX-edge-1-0> 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 the DNS configuration.

**Synopsis**

`show configuration dns`

**CLI Mode**

Basic

**Example**

```
NSX-edge-1-0> 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 the firewall configuration.

Synopsis

show configuration firewall

CLI Mode

Basic

Example

NSX-edge-1-0> 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" : [
  "any"
],
"matchTranslated" : false,
"sourcePort" : [],
"description" : "default rule for ingress traffic",
"service" : [
  "any:any:any"
],
"srcIface" : [],
"logging" : {
  "enable" : false,
show configuration global

Shows the configuration for all NSX Edge services.

**Synopsis**

```
show configuration global
```

**CLI Mode**

Basic

**Example**

```
NSX-edge-1-0> show configuration global
-----------------------------------------------------------------------
vShield Edge Global Config:
{
  "global": {
    "edgeAssistId": 0,
    "enableTcpLoose": false,
    "hostname": "NSX-edge-1-0",
    "hypervisorAssist": false,
    "size": "compact",
    "fips": {
      "enable": false
    },
    "enableAesni": true,
    "tenantId": "default",
    "haIndex": "0",
    "distributedRouter": false
  }
}
```

show configuration gslb

Show the GSLB (Global Server Load Balancer) configuration.

**Synopsis**

```
show configuration gslb [gip | monitor | pool | site]
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gip</td>
<td>Show GSLB global IP configuration.</td>
</tr>
<tr>
<td>monitor</td>
<td>Show GSLB health monitor configuration.</td>
</tr>
<tr>
<td>pool</td>
<td>Shows GSLB pools configuration.</td>
</tr>
<tr>
<td>site</td>
<td>Shows GSLB site configuration.</td>
</tr>
</tbody>
</table>

**CLI Mode**

Basic

**Example**

```
NSX-edge-1-0> show configuration gslb
```

-----------------------------------------------------------------------
vShield Edge GSLB Config:
{
  "monitorService": {
    "logging": {
      "enable": true,
      "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_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"
      }
    ]
  },
  "gslb": {
    "ports": null,
    "logging": null,
    "globalIps": null,
    "enable": false,
    "sites": null,
    "serviceTimeout": null,
    "listenOn": null,
    "security": null,
    "persistentCache": null,
  }
}
show configuration highavailability

Shows the high availability configuration.

**Synopsis**

show configuration highavailability

**CLI Mode**

Basic

**Example**

NSX-edge-1-0> 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 the interface configuration.

**Synopsis**

show configuration interface

**CLI Mode**

Basic

**Example**

NSX-edge-1-0> 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_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 interface-set

Shows the interface set configuration.

Synopsis

show configuration interface-set
**CLI Mode**

**Basic**

**Example**

NSX-edge-1-0> show configuration interface-set

vShield Edge InterfaceSet Config:

```
{
  "interfaceSet" : [
    {
      "value" : [
        "vNic_1"
      ],
      "id" : "vnic-index-1"
    },
    {
      "value" : [
        "vNic_0"
      ],
      "id" : "vnic-index-0"
    },
    {
      "value" : [
        "vse"
      ],
      "id" : "vse"
    },
    {
      "value" : [
        "vNic_9"
      ],
      "id" : "vnic-index-9"
    },
    {
      "value" : [
        "vNic_5"
      ],
      "id" : "vnic-index-5"
    },
    {
      "value" : [
        "vNic_8"
      ],
      "id" : "vnic-index-8"
    },
    {
      "value" : [
        "vNic_4"
      ],
      "id" : "vnic-index-4"
    },
    {
      "value" : [
        "vNic_0"
      ],
      "id" : "external"
    },
    {
      "value" : [
        "vNic_7"
      ],
      "id" : "vnic-index-7"
    },
    {
      "value" : [
        "vNic_3"
      ],
      "id" : "vnic-index-3"
    }
  ]
}
```
show configuration ipsec

Shows certificate configuration for IPSec VPN.

Synopsis
show configuration ipsec

CLI Mode
Basic

Example
NSX-edge-1-0> show configuration ipsec
vShield Edge IPSec VPN Config:
{
    "ipsec" : {
        "sites" : [ 

show configuration ipset

Shows IP address groups (IP Sets) configured on the NSX Edge.

**Synopsis**

show configuration ipset

**CLI Mode**

Basic

**Example**

NSX-edge-1-0> show configuration ipset

vShield Edge IpSet Config:

{  
  "ipSet": [  
    {  
      "value": [],  
      "id": "ipset-1"  
    }  
  ]
}
show configuration l2vpn

Shows L2 VPN configuration.

Synopsis

show configuration l2vpn

CLI Mode

Basic

Example for SSL-based L2 VPN

NSX-edge> show configuration l2vpn
---
vShield Edge L2 VPN Config:
{
  "l2vpn" : {
    "l2TunnelsConfig" : null,
    "serverPort" : null,
    "peerSites" : [
      {
        "name" : "Managed Site",
        "l2vpnUser" : {
          "password" : "****",
          "userId" : "managed"
        },
        "vseVnicNames" : [ "vnic_10" ],
        "peerNoneSubInterfaceIp" : "169.254.64.194",
        "peerNoneSubInterfaceNetmask" : "255.255.255.192",
        "filters" : []
      },
      {
        "name" : "Unmanaged Site",
        "l2vpnUser" : {
          "password" : "****",
          "userId" : "unmanaged"
        },
        "vseVnicNames" : [ "vnic_11" ],
        "peerNoneSubInterfaceIp" : "169.254.64.195",
        "peerNoneSubInterfaceNetmask" : "255.255.255.192",
        "filters" : []
      }
    ],
    "clientProxySetting" : null,
    "logging" : {
      "enable" : true,
      "logLevel" : "notice"
    },
    "trunkedVnicIndexes" : [ 1, 2 ],
    "serverVnicIndex" : null,
    "l2Tunnels" : null,
    "listenerPort" : 443,
    "enable" : true,
    "serverAddress" : null,
    "vseVnicNames" : null,
    "ciphers" : ["AES128-GCM-SHA256"],
    "serverCertificate" : "certificate-15",
    "encryptionAlgorithm" : null,
  }
}
Example for IPSec-based L2 VPN

NSX-edge> show configuration l2vpn

```json
{
  "l2vpn": {
    "peerSites": null,
    "l2TunnelsConfig": {
      "mode": "hub"
    },
    "clientProxySetting": null,
    "ciphers": null,
    "listenerIp": null,
    "vseVnicNames": null,
    "encryptionAlgorithm": null,
    "clientVnicIndex": null,
    "filters": [],
    "serverVnicIndex": null,
    "listenerPort": null,
    "l2vpnUsers": [],
    "cacertificate": null,
    "l2Tunnels": [
      {
        "tunnelId": "l2tunnel-38",
        "localEgressGatewayIp": [],
        "stretchedVnics": [
          "vNic_10"
        ],
        "description": "my l2 tunnel",
        "transportSessions": [
          {
            "protocol": "ipsec",
            "tunnelInterfaceLabel": "vti-1",
            "siteId": "ipsecsite-52"
          }
        ],
        "name": "l2tunnel",
        "tap": {
          "type": "gre",
          "dstAddr": "169.254.64.2",
          "mtu": null,
          "label": "l2t-38",
          "srcAddr": "169.254.64.1"
        }
      },
      {
        "description": "my l2 tunnel 2",
        "stretchedVnics": [
          "vNic_11"
        ],
        "tunnelId": "l2tunnel-40",
        "localEgressGatewayIp": [
          "40.40.40.4"
        ],
        "transportSessions": [
          {
            "protocol": "ipsec",
            "siteId": "ipsecsite-53",
            "tunnelInterfaceLabel": "vti-2"
          }
        ]
      }
    ]
  }
}
```
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**

```bash
NSX-edge-1-0> show configuration loadbalancer
```

vShield Edge Loadbalancer Config:

```json
{
    "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"
]}
]
show configuration loadbalancer monitor

Shows service monitor configuration for the load balancer.

Synopsis
show configuration loadbalancer monitor [monitorName]

CLI Mode
Basic

Example
NSX-edge-1-0> 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" : "http",
      "method" : "GET"
    }
  ]
}
show configuration loadbalancer pool

Shows load balancer pool configuration.

Synopsis

show configuration loadbalancer pool [poolName]

CLI Mode

Basic

Example

NSX-edge-1-0> 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

Shows load balancer application rules.

Synopsis

show configuration loadbalancer rule [ruleName]

CLI Mode

Basic

Example

NSX-edge-1-0> show configuration loadbalancer rule
vShield Edge Loadbalancer Config:
{
  "applicationRules" : [
    {
      "script" : "# log the name of the virtual server\ncapture request  header Host
       len 32\n# log the amount of data uploaded during a POST\ncapture request  header Content-Length len 10\n# log the beginning of the
       referrer\ncapture request  header Referer len 20",
      "name" : "advanced-logging"
    }
  ]
}

show configuration loadbalancer virtual

Shows virtual server (Virtual IP) configuration.

Synopsis

show configuration loadbalancer virtual [virtualServerName]

CLI Mode

Basic

Example

NSX-edge-1-0>  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" : http-pool,
      "clientSsl" : null
    }
  ]
}

show configuration nat

Shows the NAT configuration.

Synopsis

show configuration nat

CLI Mode

Basic

Example

NSX-edge-1-0>  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" : "http",
      "ruleId" : 200800,
      "icmpType" : null,
      "internalPort" : "443",
      "logging" : {
        "enable" : false,
        "logLevel" : null
      },
      "interface" : "vNic_0",
      "externalIp" : "10.115.172.18"
    }
  ]
}
"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 the OSPF configuration.

Synopsis

show configuration ospf

CLI Mode

Basic

Example

NSX-edge-1-0> show 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,
      "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 routing-global

Shows the global routing configuration.

Synopsis

CLI Mode

Basic

Example

NSX-edge-1-0> show configuration routing-global
---------------------------------------------------------------
vShield Edge Routing Global Config:
{
  "routingGlobal" : {
    "logging" : {
      "enable" : true,
      "logLevel" : "info"
    },
    "routerId" : "192.168.100.3",
    "ecmp" : true
  }
}
**show configuration snmp**

Shows the SNMP configuration.

**Synopsis**

**CLI Mode**

Basic

**Example**

NSX-edge-1-0> show configuration snmp

vShield Edge SNMP Agent Config:

```
{  
  "snmp" : null
}
```

**show configuration sslvpn-plus**

Shows the SSL VPN configuration.

**Synopsis**

```
show configuration sslvpn-plus
```

**CLI Mode**

Basic

**show configuration static-routing**

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

**Synopsis**

```
show configuration static-routing
```

**CLI Mode**

Basic

**Example**

NSX-edge-1-0> show configuration static-routing

vShield Edge Static Routing Config:

```
{
  "staticRouting" : [
    
    { 
      "gatewayAddress" : null,
      "destinationNetwork" : "0.0.0.0/0",
      "adminDistance" : 0,
      "gatewayAddresses" : [
        "192.168.100.2"
      ],
      "interface" : "vNic_0",
      "description" : null,
      "mtu" : 1500
    }
  ]
}
```

**show configuration syslog**

Shows remote syslog servers defined for the NSX Edge.
**Synopsis**

show configuration syslog

**CLI Mode**

Basic

**Example**

NSX-edge-1-0> show configuration syslog

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

**show configuration vti**

Shows the configuration of the virtual tunnel interface.

**Synopsis**

show configuration vti

**CLI Mode**

Basic

**Example**

NSX-edge> show configuration vti

```
vShield Edge VTI Tunnels Config:
{
   "vtiTunnels" : [
       {
           "enabled" : true,
           "name" : "vti-1",
           "mtu" : 1416,
           "sourceAddress" : "10.109.229.244",
           "label" : "vti-1",
           "mode" : "VTI",
           "tunnelAddresses" : ["2.2.2.2/24"],
           "destinationAddress" : "10.109.229.248"
       }
   ]
}
```

**show eventmgr**

Shows event manager statistics.

**Synopsis**

show eventmgr
CLI Mode

Basic

Example

NSX-edge-1-0> show eventmgr
-----------------------
messagebus     : disabled
debug          : 0
profiling      : 0
cfg_rx         : 1865
cfg_rx_msgbus  : 0
cfg_rx_err     : 0
cfg_exec_err   : 0
cfg_resp       : 0
cfg_resp_err   : 0
cfg_resp_ln_err: 0
fastquery_rx   : 926
fastquery_err  : 1
clearcmd_rx    : 931
clearcmd_err   : 0
ha_rx          : 0
ha_rx_err      : 0
ha_exec_err    : 0
status_rx      : 38
status_rx_err  : 0
status_svr     : 27
status_evt     : 0
status_evt_push: 0
status_ha      : 0
status_ver     : 6
status_sys     : 5
status_cmd     : 0
status_svr_err : 0
status_evt_err : 0
status_sys_err : 0
status_ha_err  : 0
status_ver_err : 0
status_cmd_err : 0
evt_report     : 0
evt_report_err : 0
hc_report      : 0
hc_report_err  : 0
c11_rx         : 1
c11_resp       : 0
c11_resp_err   : 0
counter_reset  : 0
---------- Health Status ------------
system status  : good
ha state       : active
cfg version    : 17
generation     : 0
server status  : 1
syslog-ng      : 1
haproxy        : 0
ipsec          : 0
sslvpn         : 0
l2vpn          : 0
dns            : 0
dhcp           : 0
heartbeat      : 0
monitor        : 0
gs1b           : 0
---------- System Events----------
show firewall

Shows 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

Shows firewall packet counters along with packet flows.

Synopsis

show firewall flows

CLI Mode

Basic

show firewall flows top n

Shows firewall packet counters along with top $n$ number of packet flows.

Synopsis

show firewall flows top $n$

CLI Mode

Basic

show firewall flows top n sort-by bytes

Shows firewall packet counters along with top $n$ number of packet flows sorted by byte numbers.

Synopsis

show firewall flows top $n$ sort-by-bytes

CLI Mode

Basic

show firewall flows top n sort-by pkts

Shows firewall packet counters along with top $n$ number of packet flows sorted by packet numbers.

Synopsis

show firewall flows top $n$ sort-by-pkts

CLI Mode

Basic

show firewall rule-id $id$

Shows firewall rule information filtered by rule-id.

Synopsis

show firewall rule-id $id$
show firewall rule-id *id* flows

Shows firewall rule information and flow information filtered by rule-id.

**Synopsis**

show firewall rule-id *id* flows

**CLI Mode**

Basic

show firewall rule-id *id* flows top *n*

Shows firewall packet counters filtered by rule-id *id* along with top *n* number of packet flows.

**Synopsis**

show firewall rule-id *id* flows top *n*

**CLI Mode**

Basic

show firewall rule-id *id* flows top *n* sort-by bytes

Shows firewall packet counters filtered by rule-id *id* along with top *n* number of packet flows sorted by byte numbers.

**Synopsis**

show firewall rule-id *id* flows top *n* sort-by-bytes

**CLI Mode**

Basic

show firewall rule-id *id* flows top *n* sort-by pkts

Shows firewall packet counters filtered by rule-id *id* along with top *n* number of packet flows sorted by packet numbers.

**Synopsis**

show firewall rule-id *id* flows top *n* sort-by-pkts

**CLI Mode**

Basic

**show flowstats**

Shows metrics related to the internal implementation of the flow-based services provided by NSX Edge.

The following four metrics provide useful operational support indicators, which can be utilized to assist with NSX Edge services capacity monitoring, and as warning signs for presence of corrupted or undesirable traffic that is reaching the Edge:

**Total Flow Capacity** displays the total number of concurrently open connections that the Edge is configured to support.
**Current Flow Entries** displays the total number of current active connections, which includes sockets in ESTABLISHED, SYN_SENT, and TIME_WAIT state. If this counter reaches the Total Flow Capacity, new connections through to Edge services, such as Edge Load Balancer, would be dropped.

**invalid** displays the number of packets seen with Invalid L3, L4 Headers, which could be an indicator of presence of an endpoint (VM or physical) that may be sending corrupted packets, either due to a configuration/defect, or intentionally.

**drop** displays the number of packets dropped due to Edge L3/L4 engine’s inability to handle the packet. This can be caused by Edge resource exhaustion, or by corrupt L3/L4 headers, in which case “invalid” counter will also be increased.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Flow Capacity</td>
<td>Maximum number of concurrent connections that NSX Edge allows</td>
</tr>
<tr>
<td>Current Flow Entries</td>
<td>Current active connections</td>
</tr>
<tr>
<td>searched</td>
<td>Max depth of hash table chain seen so far</td>
</tr>
<tr>
<td>found</td>
<td>Number of entries found through hash table lookup</td>
</tr>
<tr>
<td>new</td>
<td>Number of new connections created so far</td>
</tr>
<tr>
<td>invalid</td>
<td>Number of packets seen with Invalid L3, L4 headers</td>
</tr>
<tr>
<td>ignore</td>
<td>Number of untracked connections: loopback or due to NOTRACK target</td>
</tr>
<tr>
<td>delete</td>
<td>Number of entries deleted so far: done with the connection</td>
</tr>
<tr>
<td>delete_list</td>
<td>Number of entries deleted due to inactivity timeout</td>
</tr>
<tr>
<td>insert</td>
<td>Number of entries successfully inserted into hash table</td>
</tr>
<tr>
<td>insert_failed</td>
<td>Number of entries failed to add to hash table due to a race condition between NAT and conntrack</td>
</tr>
<tr>
<td>drop</td>
<td>Number of packets dropped, L3/L4 protocols unable to handle the packet</td>
</tr>
<tr>
<td>early_drop</td>
<td>Number of dying entries forcefully deleted to make a room for a new connection</td>
</tr>
<tr>
<td>search_restart</td>
<td>Number of times a hash table chain search is restarted due to a change during search operation</td>
</tr>
</tbody>
</table>

The output contains one stats line per CPU.

- Compact: 1 line
- Large: 2 lines
- Quadlarge: 4 lines
- Xlarge: 6 lines

**Synopsis**

```show flowstats```

**CLI Mode**

Basic

**Example**

```
NSX-Edge> show flowstats
Total Flow Capacity: 65536
Current Flow Entries: 3
Current Statistics:
  cpu=0
    searched=0  found=435  new=11  invalid=0  ignore=322  delete=8  delete_list=6
    insert=9  insert_failed=0  drop=0  early_drop=0  error=0  search_restart=0
```
**show flowtable**

Shows packet flows in a table.

**Synopsis**

`show flowtable`

**CLI Mode**

Basic

**Example**

```
NSX-Edge> show flowtable
1: tcp   6 21583 ESTABLISHED src=127.0.0.1 dst=127.0.0.1 sport=34980 dport=10001 pkts=82 bytes=24209
       src=127.0.0.1 dst=127.0.0.1 sport=10001 dport=34980 pkts=34 bytes=3409 [ASSURED] mark=0 rid=0 use=1
2: tcp   6 21599 ESTABLISHED src=10.1.1.254 dst=10.1.1.1 sport=47761 dport=22 pkts=104 bytes=10349
       src=10.1.1.1 dst=10.1.1.254 sport=22 dport=47761 pkts=63 bytes=9441 [ASSURED] mark=0 rid=131076 use=1
3: tcp   6 21552 ESTABLISHED src=127.0.0.1 dst=127.0.0.1 sport=51132 dport=10000 pkts=75 bytes=9262
       src=127.0.0.1 dst=127.0.0.1 sport=10000 dport=51132 pkts=91 bytes=70667 [ASSURED] mark=0 rid=0 use=1
Total flows: 3
```

**show flowtable expect**

Shows expected flows.

**Synopsis**

`show flowtable expect`

**CLI Mode**

Basic

**Example**

```
NSX-Edge> show flowtable expect
Total flows: 0
```

**show flowtable rule-id id**

Shows packet flows matched by rule-id.

**Synopsis**

`show flowtable rule-id id`

**CLI Mode**

Basic

**show flowtable rule-id id top n**

Shows the top \( n \) number of packet flows matched by rule-id.

**Synopsis**

`show flowtable rule-id id top n`

**CLI Mode**

Basic
show flowtable rule-id id top n sort-by bytes

Shows top n number of packet flows matched by rule-id sorted by byte numbers.

Synopsis

show flowtable rule-id id top n sort-by bytes

CLI Mode

Basic

show flowtable rule-id id top n sort-by pkts

Shows the top n number of packet flows matched by rule-id sorted by packet numbers.

Synopsis

show flowtable rule-id id top n sort-by pkts

CLI Mode

Basic

show flowtable top n

Shows top n number of packet flows.

Synopsis

show flowtable top n

CLI Mode

Basic

show flowtable top n sort-by bytes

Shows top n number of packet flows sorted by byte numbers.

Synopsis

show flowtable top n sort-by bytes

CLI Mode

Basic

show flowtable top n sort-by pkts

Shows top n number of packet flows sorted by packet numbers.

Synopsis

show flowtable top n sort-by pkts

CLI Mode

Basic

show flowtimeouts

Shows connection tracking inactivity timeouts.

Synopsis

show flowtimeouts
CLI Mode

Basic

Example

NSX-edge-1-0> show flowtimeouts
nf_contrack_tcp_timeout_syn_sent = 30
nf_contrack_tcp_timeout_syn_recv = 30
nf_contrack_tcp_timeout_established = 3600
nf_contrack_tcp_timeout_fin_wait = 20
nf_contrack_tcp_timeout_last_ack = 30
nf_contrack_tcp_timeout_time_wait = 20
nf_contrack_tcp_timeout_close = 10
nf_contrack_udp_timeout = 30
nf_contrack_udp_timeout_stream = 30
nf_contrack_icmp_timeout = 10
nf_contrack_icmpv6_timeout = 30
nf_contrack_generic_timeout = 120

show hostname

Shows the current hostname for an NSX Edge.

Synopsis

show hostname

CLI Mode

Basic

Example

NSX-edge-1-0# show hostname
NSX-edge-1-0

show interface

Shows the status and statistics of the primary IP address of each edge interface or a specific edge interface. Starting in NSX 6.4, this edge command returns the result of the ifconfig command, which does not include information such as, current speed, duplex mode, secondary IP addresses, and proxy ARP configuration.

To view the current speed and duplex mode, run the show netdevice command. To view the secondary IP addresses, run the show ip address command, and to view the proxy ARP configuration, run the show configuration command.

Synopsis

show interface [intName]

CLI Mode

Basic

Example

NSX-edge-1-0> show interface
Chapter 4 NSX Edge Commands

VDR
Link encap:Ethernet  HWaddr 96:33:56:7B:EE:CD
inet6 addr: fe80::9433:56ff:fe7b:eece/64 Scope:Link
UP BROADCAST RUNNING NOARP  MTU:1500  Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

br-sub
Link encap:Ethernet  HWaddr 5A:EC:41:63:C5:2A
inet6 addr: fe80::58ec:41ff:fe63:c52a/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b)  TX bytes:520 (520.0 b)

lo
Link encap:Local Loopback
inet addr:127.0.0.1  Mask:255.0.0.0
inet6 addr::1/128 Scope:Host
UP LOOPBACK RUNNING  MTU:65536  Metric:1
RX packets:22812 errors:0 dropped:0 overruns:0 frame:0
TX packets:22812 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:2172678 (2.0 Mb)  TX bytes:2172678 (2.0 Mb)

vNic_0
Link encap:Ethernet  HWaddr 00:50:56:BA:B1:0C
inet addr:192.168.10.200  Bcast:192.168.10.255  Mask:255.255.255.0
inet6 addr: fe80::250:56ff:feba:b10c/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:2461 errors:0 dropped:73 overruns:0 frame:0
TX packets:4469 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:208572 (203.6 Kb)  TX bytes:575065 (561.5 Kb)

Or

NSX-edge-1-0> show interface vNic_0

vNic_0
Link encap:Ethernet  HWaddr 00:50:56:BA:B1:0C
inet addr:192.168.10.200  Bcast:192.168.10.255  Mask:255.255.255.0
inet6 addr: fe80::250:56ff:feba:b10c/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:2498 errors:0 dropped:73 overruns:0 frame:0
TX packets:4448 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:205322 (200.5 Kb)  TX bytes:565907 (552.6 Kb)

Related commands
show ip address
show configuration
show netdevice

**show ip address**

Shows the status and statistics of all IP addresses of each edge interface or a specific edge interface.

All IP addresses of an edge interface include primary IP address, secondary IP addresses, and HA IP address.

**Synopsis**

`show ip address [intName]`

**CLI Mode**

Basic

**Example**

`NSX-edge-1-0> show ip address`

```
1:        lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
          link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
          inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
          inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever

2:        vNic_0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
          link/ether 00:50:56:ba:b1:0c brd ff:ff:ff:ff:ff:ff
          inet 192.168.10.200/24 brd 192.168.10.255 scope global vNic_0
            valid_lft forever preferred_lft forever
          inet 192.168.10.220/24 brd 192.168.10.255 scope global secondary vNic_0
            valid_lft forever preferred_lft forever
          inet 192.168.10.230/24 brd 192.168.10.255 scope global secondary vNic_0
            valid_lft forever preferred_lft forever
          inet 192.168.10.210/24 brd 192.168.10.255 scope global secondary vNic_0
            valid_lft forever preferred_lft forever
          inet6 fe80::260:56ff:feba:b10c/64 scope link
            valid_lft forever preferred_lft forever

3:        vNic_4: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
          link/ether 00:50:56:ba:b6:05 brd ff:ff:ff:ff:ff:ff

4:        vNic_8: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
          link/ether 00:50:56:ba:f3:60 brd ff:ff:ff:ff:ff:ff
```

Or

`NSX-edge-1-0> show ip address vNic_0`

```
2:        vNic_0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
          link/ether 00:50:56:ba:b1:0c brd ff:ff:ff:ff:ff:ff
          inet 192.168.10.200/24 brd 192.168.10.255 scope global vNic_0
            valid_lft forever preferred_lft forever
          inet 192.168.10.220/24 brd 192.168.10.255 scope global secondary vNic_0
            valid_lft forever preferred_lft forever
          inet 192.168.10.230/24 brd 192.168.10.255 scope global secondary vNic_0
            valid_lft forever preferred_lft forever
          inet 192.168.10.210/24 brd 192.168.10.255 scope global secondary vNic_0
            valid_lft forever preferred_lft forever
          inet6 fe80::260:56ff:feba:b10c/64 scope link
            valid_lft forever preferred_lft forever
```
show ip bgp

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

**Synopsis**

```
show ip bgp
```

**CLI Mode**

Basic

**Example**

```
NSX-edge-1-0> show ip bgp
```

Status codes: s - suppressed, d - damped, > - best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>AS Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; 0.0.0.0/0</td>
<td>192.168.100.2</td>
<td>0</td>
<td>100</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>&gt; 172.16.100.0/24</td>
<td>192.168.100.3</td>
<td>0</td>
<td>100</td>
<td>60</td>
<td>160</td>
</tr>
<tr>
<td>&gt; 192.168.10.0/24</td>
<td>192.168.100.3</td>
<td>0</td>
<td>100</td>
<td>60</td>
<td>160</td>
</tr>
<tr>
<td>&gt; 192.168.100.0/24</td>
<td>192.168.100.3</td>
<td>0</td>
<td>100</td>
<td>32768</td>
<td>?</td>
</tr>
</tbody>
</table>

show ip bgp neighbors

Shows BGP neighbors. Optionally show neighbor information for only the IP address specified.

**Synopsis**

```
show ip bgp neighbors [ipAddress]
```

**CLI Mode**

Basic

**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. Optionally show forwarding table entries for the specified prefix only.

**Synopsis**

```
show ip forwarding [ipAddress/netmask]
```

**CLI Mode**

Basic

**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

**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: 0x7E66
  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
  NSSA Translator Role: Always
  NSSA Translator State: Disable
  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: 0XBBF5
Number of opaque LSA: 2, Checksum Sum: 0X17F9

**show ip ospf database**

Shows IPv4 OSPF database.

**Synopsis**

show ip ospf database

**CLI Mode**

Basic

**Example**

NSX-edge-1-0> show ip ospf database

**Opaque Area Link States (Area  0.0.0.0)**

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.1</td>
<td>192.168.100.3</td>
<td>668</td>
<td>0x8000003c</td>
<td>0x0000ea87</td>
</tr>
</tbody>
</table>

**Router Link States (Area  0.0.0.1)**

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.11.9</td>
<td>192.168.11.9</td>
<td>610</td>
<td>0x8000003a</td>
<td>0x00009098</td>
</tr>
<tr>
<td>192.168.100.3</td>
<td>192.168.100.3</td>
<td>609</td>
<td>0x8000003c</td>
<td>0x00002663</td>
</tr>
</tbody>
</table>

**Network Link States (Area  0.0.0.1)**

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.11.1</td>
<td>192.168.100.3</td>
<td>614</td>
<td>0x80000039</td>
<td>0x0000603c</td>
</tr>
</tbody>
</table>

**Opaque Area Link States (Area  0.0.0.1)**

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.1</td>
<td>192.168.11.9</td>
<td>621</td>
<td>0x80000039</td>
<td>0x0000c02d</td>
</tr>
<tr>
<td>1.0.0.1</td>
<td>192.168.100.3</td>
<td>263</td>
<td>0x8000003c</td>
<td>0x0000ea87</td>
</tr>
</tbody>
</table>

**AS External Link States**

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>192.168.100.3</td>
<td>263</td>
<td>0x8000003c</td>
<td>0x00008f37</td>
</tr>
<tr>
<td>172.16.10.0</td>
<td>192.168.11.9</td>
<td>616</td>
<td>0x80000039</td>
<td>0x000037a0</td>
</tr>
<tr>
<td>172.16.20.0</td>
<td>192.168.11.9</td>
<td>616</td>
<td>0x80000039</td>
<td>0x0000c805</td>
</tr>
<tr>
<td>172.16.30.0</td>
<td>192.168.11.9</td>
<td>616</td>
<td>0x80000039</td>
<td>0x00005a69</td>
</tr>
</tbody>
</table>

**show ip ospf database adv-router**

Shows OSPF results filtered by advertising router.

**Synopsis**

show ip ospf database adv-router

**CLI Mode**

Basic
Example

NSX-edge-1-0> show ip ospf database adv-router 192.168.100.3

Opaque Area Link States (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.1</td>
<td>192.168.100.3</td>
<td>711</td>
<td>0x8000003c</td>
<td>0x0000ea87</td>
</tr>
</tbody>
</table>

Router Link States (Area 0.0.0.1)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.100.3</td>
<td>192.168.100.3</td>
<td>652</td>
<td>0x8000003c</td>
<td>0x00002663</td>
</tr>
</tbody>
</table>

Network Link States (Area 0.0.0.1)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.11.1</td>
<td>192.168.100.3</td>
<td>657</td>
<td>0x80000039</td>
<td>0x0000603c</td>
</tr>
</tbody>
</table>

Opaque Area Link States (Area 0.0.0.1)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.1</td>
<td>192.168.100.3</td>
<td>306</td>
<td>0x8000003c</td>
<td>0x0000ea87</td>
</tr>
</tbody>
</table>

AS External Link States

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>192.168.100.3</td>
<td>306</td>
<td>0x8000003c</td>
<td>0x00008f37</td>
</tr>
</tbody>
</table>

show ip ospf database asbr-summary

Shows asbr-summary (type 4) LSAs.

Synopsis

show ip ospf database asbr-summary

CLI Mode

Basic

show ip ospf database external

Shows external (type 5) LSAs.

Synopsis

show ip ospf database external

CLI Mode

Basic

Example

NSX-edge-1-0> show ip ospf database external

AS External Link States

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>192.168.100.3</td>
<td>445</td>
<td>0x8000003c</td>
<td>0x00008f37</td>
</tr>
<tr>
<td>172.16.10.0</td>
<td>192.168.11.9</td>
<td>798</td>
<td>0x80000039</td>
<td>0x000037a0</td>
</tr>
<tr>
<td>172.16.20.0</td>
<td>192.168.11.9</td>
<td>798</td>
<td>0x80000039</td>
<td>0x0000c805</td>
</tr>
<tr>
<td>172.16.30.0</td>
<td>192.168.11.9</td>
<td>798</td>
<td>0x80000039</td>
<td>0x00005a69</td>
</tr>
</tbody>
</table>
show ip ospf database network

Shows network (type 2) LSAs.

**Synopsis**

`show ip ospf database network`

**CLI Mode**

Basic

**Example**

```
NSX-edge-1-0> show ip ospf database network

Network Link States (Area 0.0.0.1)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.11.1</td>
<td>192.168.100.3</td>
<td>829</td>
<td>0x80000039</td>
<td>0x0000603c</td>
</tr>
</tbody>
</table>
```

show ip ospf database nssa-external

Shows nssa-external (type 7) LSAs.

**Synopsis**

`show ip ospf database nssa-external`

**CLI Mode**

Basic

**Example**

```
NSX-edge-1-0> show ip ospf database nssa-external

Network Link States (Area 0.0.0.51)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.10.0</td>
<td>192.168.11.9</td>
<td>1143</td>
<td>0x8000001b1</td>
<td>0x00004519</td>
</tr>
<tr>
<td>172.16.20.0</td>
<td>192.168.11.9</td>
<td>1143</td>
<td>0x8000001b1</td>
<td>0x0000d67d</td>
</tr>
<tr>
<td>172.16.30.0</td>
<td>192.168.11.9</td>
<td>1143</td>
<td>0x8000001b1</td>
<td>0x000068e1</td>
</tr>
</tbody>
</table>
```

show ip ospf database opaque-area

Shows opaque-area (type 10) LSAs.

**Synopsis**

`show ip ospf database opaque-area`

**CLI Mode**

Basic

**Example**

```
NSX-edge-1-0> show ip ospf database opaque-area

Opaque Area Link States (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.1</td>
<td>192.168.100.3</td>
<td>908</td>
<td>0x8000003c</td>
<td>0x0000ea87</td>
</tr>
</tbody>
</table>

Opaque Area Link States (Area 0.0.0.1)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
</table>
```
show ip ospf database router

Shows router (type 1) LSAs.

**Synopsis**
show ip ospf database router

**CLI Mode**
Basic

**Example**
NSX-edge-1-0> show ip ospf database router

Router Link States (Area 0.0.0.1)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.11.9</td>
<td>192.168.11.9</td>
<td>894</td>
<td>0x8000003a</td>
<td>0x00009098</td>
</tr>
<tr>
<td>192.168.100.3</td>
<td>192.168.100.3</td>
<td>893</td>
<td>0x8000003c</td>
<td>0x00002663</td>
</tr>
</tbody>
</table>

show ip ospf database summary

Shows summary (type 3) LSAs.

**Synopsis**
show ip ospf database summary

**CLI Mode**
Basic

**Example**
NSX-edge-1-0> show ip ospf database summary

Router Link States (Area 0.0.0)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq Num</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>50.50.50.41</td>
<td>50.50.50.41</td>
<td>841</td>
<td>0x8000006b</td>
<td>0x00001b84</td>
</tr>
<tr>
<td>50.50.50.113</td>
<td>50.50.50.113</td>
<td>841</td>
<td>0x80000068</td>
<td>0x00009039</td>
</tr>
<tr>
<td>60.60.60.3</td>
<td>60.60.60.3</td>
<td>146</td>
<td>0x8000005b</td>
<td>0x00003ba9</td>
</tr>
</tbody>
</table>

show ip ospf interface

Shows IPv4 OSPF interface.

**Synopsis**
show ip ospf interface

**CLI Mode**
Basic

**Example**
NSX-edge-1-0> show ip ospf interface
vNic_1 is activated
Internet Address 192.168.11.1, Network Mask 255.255.255.240, Area 0.0.0.1
Transmit Delay is 1 sec, Network Type BROADCAST, State DR, Priority 128
Designated Router’s Interface Address 192.168.11.1
Backup Designated Router’s Interface Address 192.168.11.10
Timer intervals configured, Hello 1, Dead 4, Retransmit 5

**show ip ospf neighbor**

Shows information about OSPF neighbors.

**Synopsis**

`show ip ospf neighbor`

**CLI Mode**

Basic

**Example**

```
NSX-edge-1-0> show ip ospf neighbor
 Neighbor ID   Priority  Address          Dead Time  State           Interface
192.168.10.2   128       192.168.10.3     37         Full/DR          vNic_1
```

**show ip ospf statistics**

Shows IPv4 OSPF statistics.

**Synopsis**

`show ip ospf statistics`

**CLI Mode**

Basic

**Example**

```
NSX-edge-1-0> show ip ospf statistics
 Area 0.0.0.0:  SPF algorithm executed 60 times
 Area 0.0.0.1:  SPF algorithm executed 59 times
```

**show ip route**

Shows all routes in the routing information base (RiB), or a specific route. The numbers in square brackets in the command output are the administrative distance and the routing metric. For example, the route below for 172.16.10.0/24 has an administrative distance of 110, and a routing metric of 1.

**Synopsis**

`show ip route [ipAddress/netmask]`

**CLI Mode**

Basic

**Example**

```
NSX-edge-1-0> show ip route
 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,
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
Total number of routes: 6
B       0.0.0.0/0               [20/0]      via 192.168.100.2
O   E2  172.16.10.0/24        [110/1]     via 192.168.11.9
O   E2  172.16.20.0/24        [110/1]     via 192.168.11.9
```
NSX Command Line Interface Reference

O   E2  172.16.30.0/24       [110/1]       via 192.168.11.9
C   192.168.11.0/28        [0/0]         via 192.168.11.1
C   192.168.100.0/24       [0/0]         via 192.168.100.3

or

NSX-edge-1-0> show ip route 192.168.110.10

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,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

S   0.0.0.0/0         [0/0]         via 192.168.100.2

show ip route bgp

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

Synopsis

show ip route bgp

CLI Mode

Basic

Example

NSX-edge-1-0> show ip route bgp

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,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

B   0.0.0.0/0         [20/0]        via 192.168.100.2

show ip route ospf

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

Synopsis

show ip route ospf

CLI Mode

Basic

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,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA 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 ipset

Shows IP set information

Synopsis

show ipset
CLI Mode

Example

NSX-edge-1-0> show ipset
Name: 0_131075-ov-v4-1
Type: hash:oservice (Match un-translated Ports)
Revision: 2
Header: hashsize 64 maxelem 65536
Size in memory: 2224
References: 0
Members:
Proto=89, DestPort=Any, SrcPort=Any    (encoded: 0.89.0.0/16,0.89.0.0/16)

Name: 0_131075-ov-v6-1
Type: hash:oservice (Match un-translated Ports)
Revision: 2
Header: hashsize 64 maxelem 65536
Size in memory: 2224
References: 0
Members:
Proto=89, DestPort=Any, SrcPort=Any    (encoded: 0.89.0.0/16,0.89.0.0/16)

Name: 1_131076-os-v4-1
Type: hash:onet (Match un-translated IP addresses)
Revision: 2
Header: family inet hashsize 64 maxelem 65536
Size in memory: 1432
References: 0
Members:
169.254.1.0/30

Name: 1_131076-od-v4-1
Type: hash:onet (Match un-translated IP addresses)
Revision: 2
Header: family inet hashsize 64 maxelem 65536
Size in memory: 1464
References: 0
Members:
169.254.1.0/30
224.0.0.81

show ipv6 forwarding

Shows IPv6 forwarding information

Synopsis

show ipv6 forwarding

CLI Mode

Basic

Example

NSX-edge-1-0> show ipv6 forwarding
IPv6 Routing Table
Codes: C - connected, L - local, S - static
L   fe80::/64
    via ::, VDR
L   fe80::/64
    via ::, vNic_0
L   fe80::/64
    via ::, br-sub
show log

Shows the system log.

Synopsis

show log [follow | reverse]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>follow</td>
<td>Update the displayed log.</td>
</tr>
<tr>
<td>reverse</td>
<td>Show the log in reverse chronological order.</td>
</tr>
</tbody>
</table>

CLI Mode

Basic

Example

NSX-edge-1-0# show log
2015-01-24T05:33:49+00:00 vShieldEdge kernel: Initializing cgroup subsys cpuset
2015-01-24T05:33:49+00:00 vShieldEdge kernel: Initializing cgroup subsys cpu
2015-01-24T05:33:49+00:00 vShieldEdge kernel: Linux version 3.2.31
   (root@build-vm-dhcp221.eng.vmware.com) (gcc version 4.5.3 (GCC) ) #1 SMP
   Wed Nov 26 00:51:39 GMT 2014
2015-01-24T05:33:49+00:00 vShieldEdge kernel: Command line: BOOT_IMAGE=/boot/vmlinuz
   loglevel=3 root=/dev/sda1
2015-01-24T05:33:49+00:00 vShieldEdge kernel: Disabled fast string operations
2015-01-24T05:33:49+00:00 vShieldEdge kernel: BIOS-provided physical RAM map:  
   .
   .

show log routing

Show the routing log.

Synopsis

show log routing [follow | reverse]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>follow</td>
<td>Update the displayed log.</td>
</tr>
<tr>
<td>reverse</td>
<td>Show the log in reverse chronological order.</td>
</tr>
</tbody>
</table>

CLI Mode

Basic

Example

NSX-edge-1-0> show log routing
**** AUDIT       0x2901 - 7    (0001) **** -:-------- F:00000002
ambsmmpi.c 174 :at 18:05:07, 14 August 2015 (100 ms)
SCM initialized successfully.

**** AUDIT 0x1601 - 72 (0000) **** -:-------- F:00000002
asemain.c 1007 :at 18:05:07, 14 August 2015 (100 ms)
Primary System Manager instance started.
Location index = 1

**** AUDIT 0x5701 - 1 (0000) **** -:-------- F:00000002
cssmain.c 141 :at 18:05:07, 14 August 2015 (110 ms)
The CSS component has been initialized successfully.
Process ID = 0X01103000
Interface index = 1

show messagebus

Shows the message bus forwarder counters or message counters.

Synopsis

show messagebus (forwarder | messages)

CLI Mode

Basic

Example

NSX-edge-1-0> show messagebus forwarder
-----------------------
Forwarder Command Channel
vmci_conn : up
app_client_conn : up
vmci_rx : 593
vmci_tx : 591
vmci_rx_err : 0
vmci_tx_err : 0
vmci_closed_by_peer : 0
vmci_tx_no_socket : 0
app_rx : 591
app_tx : 593
app_rx_err : 0
app_tx_err : 0
app_conn_req : 1
app_closed_by_peer : 0
app_tx_no_socket : 0
-----------------------
Forwarder Event Channel
vmci_conn : up
app_client_conn : up
vmci_rx : 179
vmci_tx : 1739
vmci_rx_err : 0
vmci_tx_err : 0
vmci_closed_by_peer : 0
vmci_tx_no_socket : 0
app_rx : 1739
app_tx : 179
app_rx_err : 0
app_tx_err : 0
app_conn_req : 1
app_closed_by_peer : 0
app_tx_no_socket : 0
-----------------------
cntl_rx : 2
cntl_tx : 2
cntl_tx_err : 0
counters_reset : 0

or
NSX Command Line Interface Reference

NSX-edge-1-0> show messagebus messages
-----------------------
Message bus is enabled
 cmd conn state: listening
 init_req : 1
 init_resp : 1
 init_req_err : 0
 init_resp_err : 0
 pwchg_req : 0
 pwchg_resp : 0
 pwchg_req_ok : 0
 pwchg_res_fail : 0
 pwchg_updated : 0
 pwchg_res_err : 0
 pwchg_res_err : 0
 pwchg_res_miss: 0
 cert_change : 0
 cmd_req : 0
 cmd_resp : 0
 cmd_invalid : 0
 cmd_req_err : 0
 cmd_req_abort : 0
 cmd_resp_err : 0
 em_req : 0
 em_resp : 0
 em_req_err : 0
 em_req_invalid: 0
 em_resp_timeout: 0
 em_resp_err : 0
 hb : 573
 hb_rx_err : 0
 hb_ack_err : 0
 cmd_ch_conn : 1
 cmd_login_fail : 0
 msg_thr_rstart : 0
-----------------------
evt conn state: listening
 vse_rx : 1721
 vse_rx_hc : 1720
 vse_rx_evt : 1
 vse_rx_msg : 171
 vse_rx_hc_empty: 0
 vse_rx_err : 0
 vse_tx_hc : 1720
 vse_tx_evt : 1
 vse_tx_hc_err : 0
 vse_tx_evt_err : 0
 evt_rsp : 1
 evt_rsp_no_file: 0
 evt_rsp_more : 0
 evt_rsp_push : 0
 evt_ch_conn : 1
 evt_login_fail : 0
 vse_thr_rstart : 0
-----------------------
c1i_rx : 2
c1i_tx : 2
 c1i_tx_err : 0
 c1i_thr_rstart : 0
 counters_reset : 0
-----------------------

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 nat64 bib
Displays NAT64 Binding Information Base (BIB) information when IPv6 query packets are received.

**Synopsis**
show nat64 bib

**CLI Mode**
Basic

**Example**
NSX-edge> show nat64 bib

<table>
<thead>
<tr>
<th>Protocol</th>
<th>IPv6-6 A</th>
<th>IPv6-DA</th>
<th>SPort</th>
<th>IPv4 SA</th>
<th>SPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>2000::2</td>
<td>2000::2</td>
<td>32479</td>
<td>120.1.1.3</td>
<td>32479</td>
</tr>
</tbody>
</table>

### show nat64 rules
Displays configured NAT64 rules.

**Synopsis**
show nat64 rules

**CLI Mode**
Basic

**Example**
NSX-edge> show nat64 rules

<table>
<thead>
<tr>
<th>Original-Ip</th>
<th>Translated-Ip</th>
<th>Rule-ID</th>
<th>Protocol</th>
<th>Stats</th>
<th>LogLevel</th>
</tr>
</thead>
<tbody>
<tr>
<td>78:ff9b::/96</td>
<td>120.1.1.3/32</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>68:ff9b::/96</td>
<td>120.1.1.9/32</td>
<td>8198</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>64:ff9b::/96</td>
<td>150.1.1.1/32</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### show nat64 sessions
Displays NAT64 active sessions.

**Synopsis**
show nat64 sessions

**CLI Mode**
Basic
Example

NSX-edge> show nat64 sessions

<table>
<thead>
<tr>
<th>Protocol</th>
<th>IPv6-SA</th>
<th>IPv6-DA</th>
<th>SPort</th>
<th>DPort</th>
<th>IPv4-SA</th>
<th>IPv4-DA</th>
<th>SPort</th>
<th>DPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>2000::2</td>
<td>78:ff9b::8201:101</td>
<td>32479</td>
<td>32479</td>
<td>120.1.1.3</td>
<td>130.1.1.1</td>
<td>32479</td>
<td>32479</td>
</tr>
</tbody>
</table>

show nat64 statistics

Displays NAT64 statistics.

Synopsis

show nat64 statistics

CLI Mode

Basic

Example

NSX-edge> show nat64 statistics

NAT64 Feature Statistics
Number of Rules 3
Rule UnMatched Packet-Drop 0
Number of BIB entry 1
Number of Session entry 1
Number of TCP Session entry 0
Number of UDP Session entry 0
Number of ICMP Session entry 1
Number of ICMP Drop entry 0
Number of Illegal address Drop entry 0
Number of Ipv6 Unsupported protocol entry 0
Number of Unsupported ICMP packet drop 0
Number of Ipv4 Unsupported protocol entry 0

show netdevice

Show network device settings.

Synopsis

show netdevice [deviceName]

CLI Mode

Basic

Example

NSX-edge> show netdevice vNic_0

Settings for vNic_0:
Supported ports: [ TP ]
Supported link modes: 1000baseT/Full
                      10000baseT/Full
Supported pause frame use: No
Supports auto-negotiation: No
Advertised link modes: Not reported
Advertised pause frame use: No
Advertised auto-negotiation: No
Speed: 10000Mb/s
Duplex: Full
Port: Twisted Pair
PHYAD: 0
Transceiver: internal
Auto-negotiation: off
MDI-X: Unknown
Supports Wake-on: uag
Wake-on: d
Link detected: yes

show process

Shows information related to NSX Edge processes.

Synopsis

show process (list | monitor)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>List all currently running processes on the NSX Edge.</td>
</tr>
<tr>
<td>monitor</td>
<td>Continuously monitor the list of processes.</td>
</tr>
</tbody>
</table>

CLI Mode

Basic

Example

NSX-edge> show process list

%CPU %MEM VSZ RSZ STAT STARTED TIME COMMAND
0.0 0.1 3956 692 Ss May 05 00:00:02 init [3]
0.0 0.0 0 0 S May 05 00:00:00 [kthreadd]
0.0 0.0 0 0 S May 05 00:00:00 [ksoftirqd/0]
0.0 0.0 0 0 S May 05 00:00:00 [kworker/u:0]
0.0 0.0 0 0 S May 05 00:00:00 [migration/0]
0.0 0.0 0 0 S< May 05 00:00:00 [cpuset]
0.0 0.0 0 0 S< May 05 00:00:00 [khelper]
0.0 0.0 0 0 S< May 05 00:00:00 [netns]

show rpfilter

Shows the reverse path filter settings.

<table>
<thead>
<tr>
<th>Reverse Path Filter Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Disable - no reverse path confirmation will be performed</td>
</tr>
<tr>
<td>1</td>
<td>Strict - confirms the source address is reachable via the same interface from which the packet arrived.</td>
</tr>
<tr>
<td>2</td>
<td>Loose - confirms the source address is reachable via any interface.</td>
</tr>
</tbody>
</table>

Synopsis

show rpfilter

CLI Mode

Basic

Example

NSX-edge-1-0> show rpfilter
net.ipv4.conf.all rp_filter = 1
net.ipv4.conf.default rp_filter = 0
show rpfstats

Shows the reverse path filter statistics.

Synopsis

show rpfstats

CLI Mode

Basic

Example

NSX-edge> show rpfstats
RPF drop packet count: 13301

show service all

Show the status of all services.

Synopsis

show service all

CLI Mode

Basic

Example

NSX-edge> show service all
<table>
<thead>
<tr>
<th>Service</th>
<th>Admin Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIREWALL</td>
<td>Enabled</td>
</tr>
<tr>
<td>SNAT</td>
<td>Enabled</td>
</tr>
<tr>
<td>DNAT</td>
<td>Enabled</td>
</tr>
<tr>
<td>LB</td>
<td>Enabled</td>
</tr>
<tr>
<td>IPSEC</td>
<td>Disabled</td>
</tr>
<tr>
<td>DNS-RELAY</td>
<td>Disabled</td>
</tr>
<tr>
<td>SSLVPN</td>
<td>Disabled</td>
</tr>
<tr>
<td>L2VPN</td>
<td>Disabled</td>
</tr>
<tr>
<td>GSLB</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP</td>
<td>Disabled</td>
</tr>
<tr>
<td>ECMP</td>
<td>Disabled</td>
</tr>
<tr>
<td>OSPF</td>
<td>Enabled</td>
</tr>
<tr>
<td>BGP</td>
<td>Disabled</td>
</tr>
<tr>
<td>ARP-FLTTR</td>
<td>Disabled</td>
</tr>
<tr>
<td>SYSLOG</td>
<td>Disabled</td>
</tr>
<tr>
<td>HA</td>
<td>Enabled</td>
</tr>
<tr>
<td>SSH</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
show service dhcp

Shows whether the DHCP service is running, and shows lease information with the leaseinfo argument.

Synopsis

show service dhcp [leaseinfo]

CLI Mode

Basic

show service dns

Shows whether the DNS service is running.

Synopsis

show service dns

CLI Mode

Basic

show service highavailability

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

Synopsis

show service highavailability

CLI Mode

Basic

Example

NSX-edge> show service highavailability
Highavailability Status: running
Highavailability Unit Name: nsx-edge-2-0
Highavailability Unit State: active
Highavailability Interface(s): vNic_1
Unit Poll Policy:
  Frequency: 3 seconds
  Deadtime: 15 seconds
  Stateful Sync-up Time: 10 seconds
Highavailability Healthcheck Status:
  Peer host [nsx-edge-2-1]: good
  This host [nsx-edge-2-0]: good
Highavailability Stateful Logical Status:
  File-Sync running
  Connection-Sync running
  xmit  xerr  rcv  rerr
  73176  0  71392  0

show service highavailability connection-sync

Shows 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
Example

NSX-edge> show service highavailability connection-sync
connections local:
current active connections: 0
connections created: 0 failed: 0
connections updated: 0 failed: 0
connections destroyed: 0 failed: 0

current active connections: 0
connections created: 0 failed: 0
connections updated: 0 failed: 0
connections destroyed: 0 failed: 0

traffic processed: 0 Bytes 0 Pckts
UDP traffic (active device=vNic_1):
    74080 Bytes sent 72264 Bytes recv
    4676 Pckts sent 4673 Pckts recv
    0 Error send 0 Error recv

message tracking: 0 Malformed msgs 9 Lost msgs

show service highavailability internal

Show high availability internal status information.

Synopsis

CLI Mode

Basic

Example

NSX-edge> show service highavailability internal
Highavailability Internal Status:
Last updated: Mon Aug 17 00:28:50 2015
Current DC: nsx-edge-1-1 (1d263b8a-ff14-f737-a14e-67171e3c2293)
Version: 1.0.9-da7075976b5ff0beef71074385f8fd02f29ec8a3
2 Nodes configured.
1 Resources configured.
Online: [ nsx-edge-1-0 nsx-edge-1-1 ]
vscluser (heartbeat:vseha): Started nsx-edge-1-0

show service highavailability link

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

Synopsis

show service highavailability link

CLI Mode

Basic

Example

Nsx-edge> show service highavailability link
Local IP Address: 169.254.1.1/30
Peer IP Address: 169.254.1.2/30
**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 | crls | pubkeys | sa | sp | stats)`

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cacerts</td>
<td>Show the CA certificates.</td>
</tr>
<tr>
<td>certs</td>
<td>Show the Edge certificates</td>
</tr>
<tr>
<td>crls</td>
<td>Show the CRLs revoke certificates.</td>
</tr>
<tr>
<td>pubkeys</td>
<td>Show the public keys.</td>
</tr>
<tr>
<td>sa</td>
<td>Show the Security Association Database (SAD) entry.</td>
</tr>
<tr>
<td>site</td>
<td>Show the site information.</td>
</tr>
<tr>
<td>sp</td>
<td>Show the Security Policy Database (SPD) entry.</td>
</tr>
<tr>
<td>stats</td>
<td>Show the statistics information.</td>
</tr>
</tbody>
</table>

**CLI Mode**

Basic

**Example**

```
nsx-edge > show service ipsec status
```

**show service ipsec cacerts**

Shows IPSEC CA certificates.

**Synopsis**

`show service ipsec cacerts`

**CLI Mode**

Privileged, Configuration, and Interface Configuration

**show service ipsec certs**

Shows IPSEC certificates.

**Synopsis**

`show service ipsec certs`

**CLI Mode**

Basic

**show service ipsec crls**

Shows Certificate Revocation Lists (CRL).

**Synopsis**

`show service ipsec crls`

**CLI Mode**

Basic
show service ipsec pubkeys

Shows 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

Shows 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

Example

nsx-edge> show service ipsec sa

10.146.97.30[4500] 52.89.185.167[4500]
    esp-udp mode=tunnel spi=3439716288(0xcd05e7c0) reqid=1(0x00000001)
    E: aes-cbc     A: hmac-sha1
    seq=0x00000000 replay=0 flags=0x00000000 state=mature
    created: Feb 27 08:01:33 2018 current: Feb 27 08:44:26 2018
    diff: 2573(s)   hard: 3600(s)   soft: 2708(s)
    last: Feb 27 08:01:34 2018 current: 215712(bytes) hard: 0(bytes) soft: 0(bytes)
    allocated: 2568 hard: 0 soft: 0

52.89.185.167[4500] 10.146.97.30[4500]
    esp-udp mode=tunnel spi=3289622501(0xc413a7e5) reqid=1(0x00000001)
    E: aes-cbc     A: hmac-sha1
    seq=0x00000000 replay=32 flags=0x00000000 state=mature
    created: Feb 27 08:01:33 2018 current: Feb 27 08:44:26 2018
    diff: 2573(s)   hard: 3600(s)   soft: 2959(s)
    last: Feb 27 08:01:34 2018 current: 215712(bytes) hard: 0(bytes) soft: 0(bytes)
    allocated: 2568 hard: 0 soft: 0

show service ipsec site

Shows the IPSec site information along with the IDs for IPSec SA and IKE SA.

Synopsis

show service ipsec site

CLI Mode

Basic

Example 1: Policy-based IPSec VPN

nsx-edge> show service ipsec site

Site: 10.109.229.244/40.40.40.0/24-10.109.229.250/20.0.0.0/24
  | IKE SA: id 2, name 10.109.229.244/40.40.40.0/24-10.109.229.250/20.0.0.0/24, peerip 10.109.229.250, tolocalip 10.109.229.244, UP
  | ipsecsessiontype: policy
Example 2: Route-based IPSec VPN

nsx-edge > show service ipsec site

Site: 10.109.229.244_0.0.0.0/0-10.109.229.246_0.0.0.0/0
   IKE SA: id 1, name 10.109.229.244_0.0.0.0/0-10.109.229.246_0.0.0.0/0, peerip 10.109.229.246, localip 10.109.229.244, UP
   ipsecsessiontype: route, tunnelinterface: vti-2
   dpd: action:restart, delay:30s, timeout:150s| Ike Algorithms:
       AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024 | Version: IKEv2
   ike rekeying in 7 hours
   +->Tunnel 10.109.229.244_0.0.0.0/0-10.109.229.246_0.0.0.0/0: 0.0.0.0/0 <-> 0.0.0.0/0, UP
   IPSec SA: id 3, name 10.109.229.244_0.0.0.0/0-10.109.229.246_0.0.0.0/0, UP
   Out SPI: 0xc96ef41a,In SPI: 0xc246b192 ipsec rekeying in 37 minutes
   AES_CBC_256/HMAC_SHA1_96/MODP_1024

show service ipsec stats

Displays IPSec statistics information.

Synopsis

show service ipsec stats

CLI Mode

Basic

Example

nsx-edge > show service ipsec stats

---------------------------------------------
IPSec packet drop statistics
---------------------------------------------
Inbound Statistics :
No Buffer left for SA : 0
IPSec Header Error : 0
SA not found for packet : 0
Protocol specific error : 0
Mode specific error : 0
Sequence number error : 0
SA Expired : 0
SA mismatch : 0
Invalid SA : 0
No matching policy found for SA : 0
No policy found for SA : 0
Packet discards according to policy : 0
Policy Error : 0
Other Error : 0

Outbound Statistics :
Route or policy not available in cache : 0
show service ipsec stats ikesa

Displays IPSec statistics information for Internet Key Exchange (IKE) protocols to set up a security association (SA).

Synopsis

show service ipsec stats ikesa

CLI Mode

Basic

Example

nsx-edge> show service ipsec stats ikesa

------------------------------------------------------------------------
IKE statistics
------------------------------------------------------------------------
Rekeys Stats
IKEv2 SA Rekeys Initiated : 0
IKEv2 SA Rekeys Responded : 0
IPSec SA Rekeyed : 6

Error Stats
Invalid IKE Packets Received : 0
Packets With Wrong IKE SPI : 0

IKEv2 payload Stats
SA Init Requests Sent : 0
SA Init Responses Received : 0
SA Init Requests Received : 0
SA Init Responses Sent : 0
Auth Requests Sent : 0
Auth Responses Received : 0
Auth Requests Received : 0
Auth Responses Sent : 0
Create Child SA Requests Sent : 0
Create Child SA Responses Received : 0
Create Child SA Requests Received : 0
Create Child SA Responses Sent : 0
Informational Requests Sent : 0
Informational Responses Received : 0
Informational Requests Received : 0
Informational Responses Sent : 0

show service ipsec stats sa

Displays IPSec statistics information for security association (SA).
Synopsis
show service ipsec stats sa

CLI Mode
Basic

Example 1: Policy-based IPSec VPN
nsx-edge > show service ipsec stats sa
Tunnel              : 10.109.229.252_10.0.0.0/24-10.109.229.250_20.0.0.0/24
Status              : UP
IpsecSessionType    : Policy
LocalEndPoint       : 10.109.229.252    PeerEndPoint        : 10.109.229.250
InBound SPI         : 0xc1b94652        OutBoundSPI         : 0xcbf3a23d
Local Subnet        : 10.0.0.0/24       PeerSubnet          : 20.0.0.0/24
Bytes In            : 0                 Bytes Out           : 0
Packets In          : 0                 Packets Out         : 0
Recv Errors         : 0                 Send Errors         : 0
Decryption Failures : 0                 Encryption Failures : 0
Integrity Errors    : 0                 SPI OverFlow Errors : 0
Relay Errors   : 0

Example 2: Route-based IPSec VPN
NSX-edge> show service ipsec stats sa
Tunnel              : 10.109.229.252_0.0.0.0/0-10.109.229.251_0.0.0.0/0
Status              : UP
IpsecSessionType    : Route TunnelInterface : vti-2
LocalEndPoint       : 10.109.229.252    PeerEndPoint        : 10.109.229.251
InBound SPI         : 0xcd9acaf2        OutBoundSPI         : 0xcbc53b9e
Local Subnet        : 0.0.0.0/0         PeerSubnet          : 0.0.0.0/0
Bytes In            : 0                 Bytes Out           : 0
Packets In          : 0                 Packets Out         : 0
Recv Errors         : 0                 Send Errors         : 0
Decryption Failures : 0                 Encryption Failures : 0
Integrity Errors    : 0                 SPI OverFlow Errors : 0
Relay Errors   : 0

show service ipsec sp
Shows 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 l2vpn (on client)
Shows the L2 VPN client status.

Synopsis
show service l2vpn

CLI Mode
Basic, Privileged
Example for SSL-based L2 VPN

NSX-edge-1-0> show service l2vpn
L2 VPN is running
----------------------------------------
L2 VPN type: Server
Tunnel Information:

Example for IPSec-based L2 VPN

NSX-edge> show service l2vpn
L2 VPN is running
----------------------------------------
L2 VPN type: Server/Hub

SITENAME       IPSECSTATUS VTI GRE
l2tunnel       UP       vti-1    l2t-38
l2tunnel       UP       vti-2    l2t-40

show service l2vpn site

Shows the site status for L2 VPN server. You can run this command on both the client and the server.
On server side, all the sites are displayed (irrespective of tunnel status). You can filter to see information about a particular site using the show service l2vpn site <sitename> command. If <sitename> does not exist, then the output will be blank.

On client side, the site is displayed irrespective of the tunnel status. As there is only one site on client side, you cannot filter to see information about a particular site.

**Synopsis**

show service l2vpn site

**CLI Mode**

Basic

**Example**

```
NSX-edge-1> show service l2vpn site
SITENAME INTERFACE TYPE VLANID/VNI TUNNELID
SiteOne vNic_10 VLAN 100 10
Site Two vNic_10 VLAN 100 10

NSX-edge-1> show service l2vpn site sitename
show service l2vpn site SiteOne

SITENAME INTERFACE TYPE VLANID/VNI TUNNELID
SiteOne vNic_10 VLAN 100 10
```

**NOTE** If the site name has spaces, then include the name of the site in quotes.

```
NSX-edge-1> show service l2vpn site "Site Two"

SITENAME INTERFACE TYPE VLANID/VNI TUNNELID
Site Two vNic_10 VLAN 100 10
```

**show service l2vpn site <sitename>**

Shows the site status about a particular site for the L2 VPN server. You can run this command on the server side. If <sitename> does not exist, then the output will be blank. As there is only one site on client side, you cannot filter to see information about a particular site.

**Synopsis**

show service l2vpn site sitename

**CLI Mode**

Basic

**Example**

```
NSX-edge> show service l2vpn site sitename
show service l2vpn site SiteOne

SITENAME INTERFACE TYPE VLANID/VNI TUNNELID
SiteOne vNic_10 VLAN 100 10
```

**NOTE** If the site name has spaces, then include the name of the site in quotes.

```
NSX-edge> show service l2vpn site "Site Two"

SITENAME INTERFACE TYPE VLANID/VNI TUNNELID
Site Two vNic_10 VLAN 100 10
```
show service l2vpn bridge

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

You can filter the output on the following three parameters.

- vlan_id: vlan_id=300
- mac_addr: mac_addr=00:50:56:bd:1d:ff
- interface: interface=vNic_2

You can use them in combination, separated by two underscores. For example: vlan_id=<vlanid>__interface=<interface>__mac_addr=<macaddr>

Synopsis

show service l2vpn bridge

CLI Mode

Basic

Example

NSX-edge> show service l2vpn bridge

bridge name bridge id STP enabled interfaces
br-sub 8000.005056b86b no vNic_2

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

<table>
<thead>
<tr>
<th>INTERFACES</th>
<th>MAC ADDR</th>
<th>VLAN ID</th>
<th>ON BRIDGE?</th>
<th>AGING TIMER</th>
</tr>
</thead>
<tbody>
<tr>
<td>vNic_2</td>
<td>00:50:56:bd:1d:ff</td>
<td>4094</td>
<td>yes</td>
<td>0:00</td>
</tr>
<tr>
<td>vNic_2</td>
<td>00:50:56:bd:1d:ff</td>
<td>0</td>
<td>yes</td>
<td>0:00</td>
</tr>
<tr>
<td>vNic_2</td>
<td>00:50:56:bd:1d:ff</td>
<td>300</td>
<td>yes</td>
<td>0:00</td>
</tr>
<tr>
<td>vNic_2</td>
<td>00:50:56:bd:1d:ff</td>
<td>2101</td>
<td>yes</td>
<td>0:00</td>
</tr>
<tr>
<td>na1</td>
<td>82:ef:2e:9d:68:ff</td>
<td>0</td>
<td>yes</td>
<td>0:00</td>
</tr>
</tbody>
</table>

NSX-edge> show service l2vpn bridge vlan_id=300

<table>
<thead>
<tr>
<th>INTERFACES</th>
<th>MAC ADDR</th>
<th>VLAN ID</th>
<th>ON BRIDGE</th>
<th>AGING TIMER</th>
</tr>
</thead>
<tbody>
<tr>
<td>vNic_2</td>
<td>00:50:56:bd:1d:ff</td>
<td>300</td>
<td>yes</td>
<td>0:00</td>
</tr>
</tbody>
</table>

NSX-edge> show service l2vpn bridge vlan_id=300__interface=vNic_2

<table>
<thead>
<tr>
<th>INTERFACES</th>
<th>MAC ADDR</th>
<th>VLAN ID</th>
<th>ON BRIDGE</th>
<th>AGING TIMER</th>
</tr>
</thead>
<tbody>
<tr>
<td>vNic_2</td>
<td>00:50:56:bd:1d:ff</td>
<td>300</td>
<td>yes</td>
<td>0:00</td>
</tr>
</tbody>
</table>

NSX-edge> show service l2vpn bridge vlan_id=300__mac_addr=00:50:56:bd:1d:ff
## Chapter 4 NSX Edge Commands

### show service l2vpn bridge interface=vNic_2

<table>
<thead>
<tr>
<th>INTERFACES</th>
<th>MAC_ADDR</th>
<th>VLAN ID</th>
<th>ON BRIDGE</th>
<th>AGING TIMER</th>
</tr>
</thead>
<tbody>
<tr>
<td>vNic_2</td>
<td>00:50:56:bd:1d:ff</td>
<td>300</td>
<td>yes</td>
<td>0.00</td>
</tr>
</tbody>
</table>

### show service l2vpn bridge interface=vNic_2__mac_addr=00:50:56:bd:1d:ff

<table>
<thead>
<tr>
<th>INTERFACES</th>
<th>MAC_ADDR</th>
<th>VLAN ID</th>
<th>ON BRIDGE</th>
<th>AGING TIMER</th>
</tr>
</thead>
<tbody>
<tr>
<td>vNic_2</td>
<td>00:50:56:bd:1d:ff</td>
<td>4094</td>
<td>yes</td>
<td>0.00</td>
</tr>
<tr>
<td>vNic_2</td>
<td>00:50:56:bd:1d:ff</td>
<td>0</td>
<td>yes</td>
<td>0.00</td>
</tr>
<tr>
<td>vNic_2</td>
<td>00:50:56:bd:1d:ff</td>
<td>300</td>
<td>yes</td>
<td>0.00</td>
</tr>
<tr>
<td>vNic_2</td>
<td>00:50:56:bd:1d:ff</td>
<td>2101</td>
<td>yes</td>
<td>0.00</td>
</tr>
</tbody>
</table>

For L2 VPN over IPSec client and server, the CLI output is as follows:

```bash
nsx-edge> show service l2vpn bridge
bridge name     bridge id              STP enabled | interfaces
br-sub          8000.005056902e5f       no         | l2t-1     vNic_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**

```bash
show service l2vpn conversion-table
```

**CLI Mode**

Basic

**Example**

```
NSX-edge-1-0> show service l2vpn conversion-table
vid1 vid2 Tag Type action
=================================
100 10 VLAN TO_VLAN
```

**Egress VLAN Entries**

```bash
vid1 vid2 Tag Type action
=================================
10 100 VLAN TO_VLAN
```

**VXLAN Table Entries**

```bash
vid1 vid2 Tag Type action
=================================
```

### show service l2vpn ebtables

ebtables is an application program used to set up and maintain the tables of rules that inspect Ethernet frames. To view these rules, run the `ebtables` command.
Synopsis

show service l2vpn ebtables

CLI Mode

Basic

Example

NSX-edge-1-0> show service l2vpn ebtables
Bridge table: filter

Bridge chain: INPUT, entries: 2, policy: ACCEPT
- i na1 - j chain_na1
- i vNic_2 - j chain_vNic_2

Bridge chain: FORWARD, entries: 4, policy: ACCEPT
- o na1 - j chain_na1
- i na1 - j chain_na1
- o vNic_2 - j chain_vNic_2
- i vNic_2 - j chain_vNic_2

Bridge chain: OUTPUT, entries: 2, policy: ACCEPT
- o na1 - j chain_na1
- o vNic_2 - j chain_vNic_2

Bridge chain: chain_vNic_2, entries: 12, policy: ACCEPT
- p 802_1Q - o vNic_2 --vlan-id 300 - j ACCEPT
- p 802_1Q - i vNic_2 --vlan-id 300 - j ACCEPT
- p 802_1Q - o vNic_2 --vlan-id 4094 - j ACCEPT
- p 802_1Q - i vNic_2 --vlan-id 4094 - j ACCEPT
- p 802_1Q - o vNic_2 --vlan-id 2101 - j ACCEPT
- p 802_1Q - i vNic_2 --vlan-id 2101 - j ACCEPT
- i vNic_2 - j DROP
- o vNic_2 - j DROP
- i vNic_2 - j DROP
- o vNic_2 - j DROP
- i vNic_2 - j DROP
- o vNic_2 - j DROP

Bridge chain: chain_na1, entries: 4, policy: ACCEPT
- p 802_1Q - o na1 --vlan-id 2101 - j ACCEPT
- p 802_1Q - i na1 --vlan-id 2101 - j ACCEPT
- i na1 - j DROP
- o na1 - j DROP

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

Example

NSX-edge-1-0> show service l2vpn trunk-table
show service loadbalancer

Shows overall current loadbalancer engine state.

**Synopsis**

show service loadbalancer

**CLI Mode**

Basic

**Example**

Loadbalancer Services Status:

```
L7 Loadbalancer     : stopped
-----------------------------------------------------------------------
L7 Loadbalancer Statistics:
STATUS    PID        MAX_MEM_MB MAX_SOCK   MAX_CONN   MAX_PIPE   CUR_CONN   CONN_RATE
stopped    0          0          0          0          0          0          0          0
-----------------------------------------------------------------------
L4 Loadbalancer Statistics:
MAX_CONN   ACT_CONN   INACT_CONN TOTAL_CONN
0          0          0          0
```

Prot LocalAddress:Port Scheduler Flags
-> RemoteAddress:Port Forward Weight ActiveConn InActConn

show service loadbalancer error

Shows recent loadbalancer errors.

**Synopsis**

show service loadbalancer error

**CLI Mode**

Basic

**Example**

L7 Loadbalancer     : stopped
show service loadbalancer monitor

Shows health of specified monitor.

Synopsis

show service loadbalancer monitor [monitorName]

CLI Mode

Basic

Example

NSX-edge-1-0> show service loadbalancer monitor
----------------------------------------------
Loadbalancer HealthMonitor Statistics:
POOL MEMBER HEALTH STATUS
http-pool http-Server default_http_monitor:CRITICAL

show service loadbalancer pool

Shows pool member state.

Synopsis

show service loadbalancer pool [poolName]

CLI Mode

Basic

Example

NSX-edge-1-0> 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

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

Synopsis

show service loadbalancer session [l4 | l7]

CLI Mode

Basic

show service loadbalancer table

Shows session persistence table entries.
Synopsis
show service loadbalancer table [tableName]

CLI Mode
Basic

**show service loadbalancer virtual**

Shows virtual server details.

Synopsis
show service loadbalancer virtual [serverName]

CLI Mode
Basic

Example
NSX-edge-1-0> 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 monitor**

Shows the running status of the health monitor service.

Synopsis
show service monitor

CLI Mode
Basic, Privileged

Example
NSX-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 [monitorName]

CLI Mode
Basic, Privileged
Example

NSX-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

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 network-connections

Shows service network connection information. For example, TCP and UDP service information.
### Synopsis

`show service network-connections`

### CLI Mode

**Basic**

#### Example

```
NSX-edge-1-0> show service network-connections
```

#### VShield Edge Service Network-Connection Status:

**Active Internet connections (servers and established)**

<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
<th>PID/Program name</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:2601</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>833/zebra</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:10000</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>1584/vmciproxy</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:10001</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>1586/vmciproxy</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:179</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>1553/sshd</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:15000</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>863/dcsms</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:2812</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>895/monit</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:18566</td>
<td>127.0.0.1:10000</td>
<td>ESTABLISHED</td>
<td>1586/msgmgr</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>192.168.101.3:22</td>
<td>192.168.110.10:51116</td>
<td>ESTABLISHED</td>
<td>31299/sshd: admin</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:36905</td>
<td>127.0.0.1:10001</td>
<td>ESTABLISHED</td>
<td>1586/msgmgr</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>192.168.101.3:50522</td>
<td>192.168.101.2:179</td>
<td>ESTABLISHED</td>
<td>863/dcsms</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:10000</td>
<td>127.0.0.1:18566</td>
<td>ESTABLISHED</td>
<td>1584/vmciproxy</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>192.168.10.2:179</td>
<td>192.168.10.6:50726</td>
<td>ESTABLISHED</td>
<td>863/dcsms</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:10001</td>
<td>127.0.0.1:36905</td>
<td>ESTABLISHED</td>
<td>1584/vmciproxy</td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:1514</td>
<td>0.0.0.0:*</td>
<td></td>
<td>692/syslog-ng</td>
</tr>
</tbody>
</table>

**Active UNIX domain sockets (servers and established)**

<table>
<thead>
<tr>
<th>Proto</th>
<th>RefCnt</th>
<th>Flags</th>
<th>Type</th>
<th>State</th>
<th>I-Node</th>
<th>PID/Program name</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>517</td>
<td>824/fcron</td>
<td>/usr/local/var/run/fcron.fifo</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>DGRAM</td>
<td></td>
<td>7950</td>
<td>1586/msgmgr</td>
<td>/var/run/vmware/vshield/msgmgr/vse_event.sock</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>538</td>
<td>833/zebra</td>
<td>/var/run/zserv.api</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>DGRAM</td>
<td></td>
<td>545</td>
<td>833/zebra</td>
<td>/var/run/zebra.vty</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>DGRAM</td>
<td></td>
<td>8779</td>
<td>1586/msgmgr</td>
<td>/var/run/vmware/vshield/msgmgr/msgmgr_client_server</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>DGRAM</td>
<td></td>
<td>217</td>
<td>692/syslog-ng</td>
<td>/var/run/vmware/vshield/eventmgr/evmgr_client_server.sock</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>DGRAM</td>
<td></td>
<td>630</td>
<td>897/eventmgr</td>
<td>/var/run/vmware/vshield/vmciproxy_client_server.sock</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>DGRAM</td>
<td></td>
<td>221</td>
<td>692/syslog-ng</td>
<td>/var/run/syslog-ngctl</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>DGRAM</td>
<td></td>
<td>6630</td>
<td>897/eventmgr</td>
<td>/var/run/vmware/vshield/vse_config.sock</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>DGRAM</td>
<td></td>
<td>7912</td>
<td>1586/msgmgr</td>
<td></td>
</tr>
</tbody>
</table>

**show service sslvpn-plus**

Shows SSL VPN-Plus service information.
Synopsis
show service sslvpn-plus

CLI Mode
Basic

**show service sslvpn-plus sessions**
Shows SSL VPN-Plus active sessions.

Synopsis
show service sslvpn-plus sessions

CLI Mode
Basic

**show service sslvpn-plus stats**
Shows SSL VPN-Plus statistic information.

Synopsis
show service sslvpn-plus stats

CLI Mode
Basic

**show service sslvpn-plus tunnels**
Shows SSL VPN-Plus tunnel information.

Synopsis
show service sslvpn-plus tunnels

CLI Mode
Basic

**show system cpu**
Shows the system CPU details.

Synopsis
show system cpu

CLI Mode
Basic

Example
NSX-edge-1-0# show system cpu
processor : 0
vendor_id : GenuineIntel
cpu family : 6
model : 45
model name : Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz
stepping : 7
microcode : 0x710
cpu MHz : 2700.000
cache size : 20480 KB
show system interrupt

Shows system interrupt and affinity information.

Synopsis

show system interrupt [affinity irqID]

CLI Mode

Basic

Example

NSX-edge-1-0> show system interrupt

CPU0  CPU1
0:    796  0    IO-APIC-edge  timer
1:    4    4    IO-APIC-edge  i8042
4:    11   0    IO-APIC-edge  serial
8:    52   0    IO-APIC-edge  rtc0
9:    0    0    IO-APIC-fasteoi  acpi
12:   0    114  IO-APIC-edge  i8042
17:   54063 30548 IO-APIC-fasteoi  ioc0
72:   1475   0    PCI-MSI-edge  vmci
73:    0    0    PCI-MSI-edge  vmci
74:   47791   2    PCI-MSI-edge  vNic_0:v0-Rx
75:    1   3379  PCI-MSI-edge  vNic_0:v1-Rx
76:    0    0    PCI-MSI-edge  vNic_0:v2-event
83:   44052   0    PCI-MSI-edge  vNic_1:v0-Rx
84:    0   3696  PCI-MSI-edge  vNic_1:v1-Rx
85:    0    0    PCI-MSI-edge  vNic_1:v2-event
NMI:    0    0    Non-maskable interrupts
LOC: 1112749 5490722 Local timer interrupts
SPU:    0    0    Spurious interrupts
PMI:    0    0    Performance monitoring interrupts
IWT:    0    0    IRQ work interrupts
RES: 317633 324946 Rescheduling interrupts
CAL:  395  358 Function call interrupts
TLB: 144492 147028 TLB shootdowns
TRM:    0    0    Thermal event interrupts
THR:    0    0    Threshold APIC interrupts
MCE:    0    0    Machine check exceptions
show system memory

Shows the summary of memory utilization.

**Synopsis**

show system memory

**CLI Mode**

Basic, Privileged

**Example**

NSX-edge-1-0# show system mem
MemTotal: 2072204 kB
MemFree: 1667248 kB
Buffers: 83120 kB
...

show system network-stats

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

**Synopsis**

show system network-stats

**CLI Mode**

Basic

**Example**

NSX-edge-1-0> show system network-stats
Ip:
    45198 total packets received
    0 forwarded
    0 incoming packets discarded
    43765 incoming packets delivered
    42232 requests sent out
Icmp:
    23 ICMP messages received
    0 input ICMP message failed.
    ICMP input histogram:
        destination unreachable: 6
        echo requests: 11
        echo replies: 6
    36 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 6
        echo request: 19
        echo replies: 11
IcmpMsg:
    InType0: 6
    InType3: 6
    InType8: 11
show system storage

Shows the disk usage details for an NSX Edge.

Synopsis

show system storage

CLI Mode

Basic, Privileged

Example

NSX-edge-1-0# show system storage
Filesystem Size Used Avail Use% Mounted on
/dev/sda1 372M 327M 27M 93% /
/dev/sda2 47M 5.0M 40M 12% /var/db
/dev/sda3 31M 4.5M 25M 15% /var/dumpfiles
/dev/sda4 34M 7.0M 26M 22% /var/log

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

NSX-edge-1-0# show system uptime
01:58:15 up 1 day, 23:38, 2 users, load average: 0.00, 0.01, 0.05
show tech-support

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

**Synopsis**

show tech-support

**CLI Mode**

Basic

**Related Commands**

export tech-support scp

show version

Shows the software version running on the virtual machine.

**Synopsis**

show version

**CLI Mode**

Basic, Privileged

**Example**

NSX-edge-1-0> show version
Name:                 vShield Edge
Version:              6.2.0
Build number:         2697212
Kernel:               3.2.62

**Related Commands**

show edge edgeID version

traceroute

Traces the route from the NSX Edge to a target system.

**Synopsis**

traceroute (hostname | ipAddress)

**CLI Mode**

Basic, Privileged

**Example**

NSX-edge-1-0# 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
Standalone NSX Edge Overview

A standalone NSX Edge appliance can be deployed as a L2 VPN client in a vCenter that does not use NSX. The L2VPN client connects to an NSX Edge L2VPN server that is part of an NSX installation.

You deploy a standalone edge using an OVF file. After deployment, all configuration changes must be made using the command line interface.

A standalone NSX Edge appliance has the same basic and privileged modes as an NSX Edge that is deployed in an NSX environment. In addition, it has configuration, interface configuration and L2VPN configuration modes.

Log in as the user admin to use the standalone NSX Edge commands.

Standalone NSX Edge Commands

ciphers

Add ciphers to the configuration. Available options are 3DES, AES, AES256, GCM, and NULL. List multiple ciphers separated by a colon (:). To remove a cipher, use no before the command.

Synopsis

[no] ciphers cipherName1[:cipherName2][:...]

CLI Mode

L2VPN

Example

nsx-l2vpn-edge(config-l2vpn)# ciphers 3DES
or
nsx-l2vpn-edge(config-l2vpn)# ciphers 3DES:AES
or
nsx-l2vpn-edge(config-l2vpn)# no ciphers 3DES

Related Commands

show configuration l2vpn

commit

Applies changes made in configuration, interface configuration, or L2VPN mode to the system. Uncommitted changes are persistent across reboots. You can view uncommitted changes with show configuration uncommitted.
**Synopsis**

commit

**CLI Mode**

Configuration, Interface Configuration, L2VPN

**Example**

```
nsx-l2vpn-edge(config)# commit
```

**Related Commands**

show configuration uncomitted

---

**configure terminal**

Switches to Configuration mode from Privileged mode.

**Synopsis**

configure terminal

**CLI Mode**

Privileged

**Example**

```
nsx-l2vpn-edge# configure terminal
nsx-l2vpn-edge(config)#
```

**Related Commands**

exit
quit
interface intName
l2vpn
commit

---

**configure download < From SCP filepath>**

The `configure` command helps in importing and exporting the configuration on an existing standalone edge. Use the `configure download` command to import the HA configuration. Use the same key for decryption that you used for encryption.

**Synopsis**

configure download <from SCP filepath>:

**CLI Mode**

Configuration

**Example**

```
nsx-l2vpn-edge# configure terminal
nsx-l2vpn-edge(config)# configure download <scp filepath>
nsx-l2vpn-edge(config)# configure download user 1@10.108.161.87:/tmp/backup.conf
```

The authenticity of host '10.108.160.12 (10.108.160.12)' can't be established.
RSA key fingerprint is SHA256:Z/C64IKiplifHtvL30SupWDE/Gua5krungYoWccEwCg.
Are you sure you want to continue connecting (yes/no)? yes
user1@10.108.161.87's password:
Please provide key for decryption:
Please provide Ha Index for the appliance ('0'/ '1') : 0
Imported Configuration has HA feature enabled. Please verify uncommitted configuration before commit.

nsx-l2vpn-edge(config)# commit

Related Commands

commit
configure upload <To SCP filepath>

configure upload <To SCP filepath>

The `configure` command helps in importing and exporting the configuration on an existing standalone edge. Use the `configure upload` command to export the encrypted HA configuration. You need to provide the encryption key and use the same key for decryption.

Note: When the configuration is imported on a standalone edge, you must make changes to the Index and MAC addresses, which are editable.

Synopsis

configure upload <to scp filepath>:

CLI Mode

Configuration

Example

nsx-l2vpn-edge# configure terminal
nsx-l2vpn-edge(config)# configure upload <scp filepath>
nsx-l2vpn-edge(config)# configure upload user1@10.108.161.87:/tmp/backup.conf
Please provide key for encryption:
The authenticity of host '10.108.161.87 (10.108.161.87)' can't be established.
RSA key fingerprint is SHA256:Z/C64IKiplifHtv130SupwOE/Gua5krungYiWccEWcg.
Are you sure you want to continue connecting (yes/no)? yes
user1@10.108.161.87's password:
nsx-l2vpn-edge(config)# commit

Related Commands

commit
configure download < From SCP filepath>

dns name-server

Configures DNS servers. To remove a DNS server, use `no` before the command.

Synopsis

[no] dns name-server ipAddressPrimary [ipAddressSecondary]

CLI Mode

Configuration

Example

nsx-l2vpn-edge(config)# dns name-server 192.168.110.10

Related Commands

show configuration global

egress-optimize

Adds one or more IP addresses to the egress-optimize IP list. To remove an IP address, use `no` before the command.
**Synopsis**

```
[no] egress-optimize ipAddress1[:ipAddress2:[...]]
```

**CLI Mode**

L2VPN

**Example**

```
nsx-l2vpn-edge(config-l2vpn)# no egress-optimize 192.168.1.1
or
nsx-l2vpn-edge(config-l2vpn)# egress-optimize 192.168.1.1:192.168.2.1:192.168.3.1
```

**Related Commands**

```
show configuration l2vpn
```

---

**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, Interface Configuration, L2VPN

**Example**

```
nsx-l2vpn-edge(config)# exit
nsx-l2vpn-edge#
```

or

```
nsx-l2vpn-edge# exit
Connection to 192.168.100.200 closed.
```

**Related Commands**

```
quit
disable
```

---

**fips enable**

Enable FIPS mode for the standalone edge. You must reboot standalone edge after committing the changes.

**Synopsis**

```
fips enable
```

**CLI Mode**

Configuration

**Example**

```
nsx-l2vpn-edge# configure terminal
nsx-l2vpn-edge(config)# fips enable
nsx-l2vpn-edge(config)# commit
```

**Related Commands**

```
configure terminal
commit
fips disable
```
fips disable

Disable FIPS mode for the standalone edge. You must reboot standalone edge after committing the changes.

Synopsis
fips disable

CLI Mode
Configuration

Example
nsx-l2vpn-edge# configure terminal
nsx-l2vpn-edge(config)# fips disable
nsx-l2vpn-edge(config)# commit

Related Commands
configure terminal
commit
fips enable

ha admin-state

Set Admin state as **UP** or **Down** for the appliance. To start HA, run the ha admin-state UP command on each node. This command does not show the status of the NSX Edge virtual appliance.

Synopsis
ha admin-state

CLI Mode
Configuration

Example
nsx-l2vpn-edge(config)# ha admin-state

For example, on both Node-1 and Node-2:
nsx-l2vpn-edge(config)# ha admin-state UP
Note: Make sure that you type UP in uppercase, as shown in the example.
nsx-l2vpn-edge(config)# commit

ha disable

Disable HA for the appliance. You can switch from HA mode to non HA mode.

Synopsis
ha disable

CLI Mode
Configuration

Example
nsx-l2vpn-edge(config)# ha disable
nsx-l2vpn-edge(config)# commit
ha get-localnode
Get MAC information for vNICs of the local node. Log in to each node, and run the ha get-local node command on both nodes individually to retrieve the MAC addresses of the three vNIC interface cards.

Synopsis
ha get-localnode

CLI Mode
Configuration

Example
nsx-l2vpn-edge(config)# ha get-localnode

For example, on Node-1:
nsx-l2vpn-edge(config)# ha get-localnode

For example, on Node-2:
nsx-l2vpn-edge(config)# ha get-localnode
00:50:56:90:1c:75  00:50:56:90:34:c1  00:50:56:90:36:80

ha set-config
Set HA IP address for the local node and the peer node, and set HA index for the appliance. Log in to each node, and run the ha set-config command on both nodes individually to set the IP addresses of the HA vNIC interface.

Synopsis
ha set-config

CLI Mode
Configuration

Example
nsx-l2vpn-edge(config)# ha set-config

For example, on Node-1:
nsx-l2vpn-edge(config)# ha set-config 192.168.1.1  192.168.1.2 0 15 vNic_2

For example, on Node-2:
nsx-l2vpn-edge(config)# ha set-config 192.168.1.2  192.168.1.1 1 15 vNic_2
nsx-l2vpn-edge(config)# commit

ha set-peernode
Set peer node with the MAC information. Run the ha set-peernode command on both nodes individually to assign the MAC address of Node-1 to Node-2, and MAC address of Node-2 to Node-1.

Synopsis
ha set-peernode

CLI Mode
Configuration
Example

nsx-l2vpn-edge(config)# ha set-peernode

For example, assign the MAC address of Node-2 on Node-1:
nsx-l2vpn-edge(config)# ha set-peernode 00:50:56:90:1c:75 00:50:56:90:34:c1
00:50:56:90:36:80

For example, assign the MAC address of Node-1 to Node-2:
nsx-l2vpn-edge(config)# ha set-peernode 0:50:56:90:12:ea 00:50:56:90:97:ca
00:50:56:90:d9:69

nsx-l2vpn-edge(config)# commit

interface intName

Switches to Interface Configuration mode for the specified interface. Changing the configuration of the uplink interface is the only supported option.

Synopsis
interface intName

CLI Mode
Configuration

Example

nsx-l2vpn-edge(config)# interface uplink
nsx-l2vpn-edge(config-if)#

Related Commands

show configuration interface

ip address

Assigns an IP address to an interface. To remove an IP address from an interface, use no before the command.
It is recommended to change the IP address setting from the console only.

Synopsis

[no] ip address ipAddress/netmask

CLI Mode
Interface Configuration

Example

nsx-l2vpn-edge(config-if)# ip address 192.168.100.200/24

Related Commands

show configuration interface

ip route

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

Synopsis

[no] ip route ipAddress/netmask gatewayIP
CLI Mode
Configuration

Example

nsx-l2vpn-edge(config)# ip route 0.0.0.0/0 192.168.100.2

Related Commands

show configuration static-routing

l2vpn

Switches to L2VPN mode from Configuration mode.

Synopsis

12vpn

CLI Mode
Configuration

Example

nsx-l2vpn-edge(config)# l2vpn
nsx-l2vpn-edge(config-l2vpn)#

Related Commands

commit
exit
quit
show configuration l2vpn

logging

Configure log level for L2VPN for an unmanaged edge from Configuration mode. Default logging of L2VPN is enabled, and level is set to "notice".

Synopsis

logging

CLI Mode
Configuration

Example

nsx-l2vpn-edge(config)# l2vpn
nsx-l2vpn-edge(config-l2vpn)#

1 **Enabling l2vpn log level**

nsx-l2vpn-edge(config-l2vpn)# logging
  LEVEL  Set logging level. Options : 'emergency', 'alert', 'critical', 'error', 'warning', 'notice', 'info', 'debug'
nsx-l2vpn-edge(config-l2vpn)# logging info
nsx-l2vpn-edge(config-l2vpn)# commit

2 **Changing log level**

nsx-l2vpn-edge(config-l2vpn)# logging debug
nsx-l2vpn-edge(config-l2vpn)# commit
3  **Disabling log level**

nsx-l2vpn-edge(config-l2vpn)# no logging
nsx-l2vpn-edge(config-l2vpn)# commit

NOTE After commit, logging of l2vpn service gets disabled and no logs will be printed.

**Related Commands**

commit
exit
quit
show configuration l2vpn

**mtu**

Specify MTU for an interface. Valid values are between 60 and 9000.

**Synopsis**

mtu IntName mtuSize

**CLI Mode**

Configuration

**Example**

nsx-l2vpn-edge(config)# mtu uplink 1500

**Related Commands**

show configuration interface

**no proxy setup**

Remove the proxy setup including proxy user setup.

**Synopsis**

no proxy setup

**CLI Mode**

L2VPN

**Example**

nsx-l2vpn-edge(config-l2vpn)# no proxy setup

**Related Commands**

show configuration l2vpn
proxy address
proxy username

**no proxy user**

Remove the proxy user configuration.

**Synopsis**

no proxy user

**CLI Mode**

L2VPN
Example

```
nsx-l2vpn-edge(config-l2vpn)# no proxy user
```

**Related Commands**

```
show configuration l2vpn
proxy username
```

### password

Change the password of the admin, enable, or root user. The password command takes effect immediately without having to commit the change.

**Synopsis**

```
password userName
```

**CLI Mode**

Configuration

**Example**

```
nsx-l2vpn-edge(config)# password admin
```

### peer-ip

Set the peer IP address and peer code for IPSec-based L2 VPN.

**NOTE**: Peer code contains the sensitive pre-shared key (PSK) in plain text format. Therefore, this peer code must be kept securely according to the client security.

**Synopsis**

```
peer-ip ipAddress peer-code code
```

**CLI Mode**

L2VPN

**Example**

```
nsx-l2vpn-edge(config)# peer-ip 20.20.20.4 peer-code M3MTcOLHsi270ZU5hbWUkJGaX3zdFpGUiJLCJzcmNUYXBCcCI6I
```

### proxy address

Set the proxy IP address and port.

**Synopsis**

```
proxy address ipAddress portNumber
```

**CLI Mode**

L2VPN

**Example**

```
nsx-l2vpn-edge(config-l2vpn)# proxy address 10.10.1.1 port 553
```

**Related Commands**

```
proxy username
no proxy setup
show configuration l2vpn
```
proxy username

Sets the proxy authentication username and password. There can be only one user configured. If you run this command when a user is already configured, the previous user configuration will be overwritten.

Synopsis

proxy username userName password password

CLI Mode

L2VPN

Example

nsx-l2vpn-edge(config-l2vpn)# proxy username test password test

Related Commands

no proxy user
show configuration l2vpn

quit

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

Synopsis

quit

CLI Mode

Configuration, Interface Configuration, L2VPN

Example

nsx-l2vpn-edge(config-l2vpn)# quit
nsx-l2vpn-edge(config)#

or

nsx-l2vpn-edge# exit
Connection to 192.168.100.200 closed.

Related Commands

exit

rpfilter

Specify an reverse path filter value for an interface. Specifying all sets all the rpfilter policy for all interfaces. Specifying default sets the rpfilter policy for any new interfaces.

Synopsis

rpfilter interfaceName policy

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Disable - no reverse path confirmation will be performed</td>
</tr>
<tr>
<td>1</td>
<td>Strict - confirms the source address is reachable via the same interface from which the packet arrived.</td>
</tr>
<tr>
<td>2</td>
<td>Loose - confirms the source address is reachable via any interface.</td>
</tr>
</tbody>
</table>
CLI Mode
Configuration

Example
nsx-l2vpn-edge(config)# rpfilter uplink 2

**server ipAddress [port]**
Configure the remote L2VPN server IP address, and optionally port. If no port is specified, the default port of 443 is used.

To delete a remote L2VPN server, use no before the command.

**Synopsis**
[no] server ipAddress [port]

CLI Mode
L2VPN

Example
nsx-l2vpn-edge(config-l2vpn)# server 10.10.10.1 553

**Related Commands**
show configuration l2vpn

**show configuration**
Show configuration information. With no arguments, it shows all configuration. You can optionally specify which section of the configuration to view: certificatestore, global, interface, l2vpn, routing-global, and static-routing. Specifying uncommitted will show any configuration that has been entered but not yet committed. Uncommitted configuration is persistent across reboots.

**Synopsis**
show configuration [configType]

CLI Mode
Configuration, Interface Configuration, L2VPN

Example
nsx-l2vpn-edge(config-if)# show configuration static-routing

vShield Edge Static Routing Config:
{
  "staticRouting" : [
    {
      "gatewayAddress" : null,
      "destinationNetwork" : "0.0.0.0/0",
      "interface" : "vNic_0",
      "gatewayAddresses" : [
        "192.168.100.2"
      ],
      "description" : "",
      "mtu" : 1500
    }
  ]
}
show configuration uncommitted

Shows unsaved configuration information for the edge.

**Synopsis**

```
show configuration uncommitted
```

**CLI Mode**

Configuration

**Example**

```
nsx-l2vpn-edge(config)# show configuration uncommitted
```

show log

Show system log file.

**Synopsis**

```
show log
```

**CLI Mode**

Configuration, Interface Configuration, L2VPN

**Example**

```
nsx-l2vpn-edge(config)# show log
2015-08-13T21:04:17+00:00 vShieldEdge kernel: Initializing cgroup subsys cpuset
2015-08-13T21:04:17+00:00 vShieldEdge kernel: Initializing cgroup subsys cpu
2015-08-13T21:04:17+00:00 vShieldEdge kernel: Linux version 3.2.62
    (root@sc-d01-255-093.eng.vmware.com) (gcc version 4.5.3 (GCC) ) #1 SMP Fri
    Jul 17 23:38:44 GMT 2015
2015-08-13T21:04:17+00:00 vShieldEdge kernel: Command line: BOOT_IMAGE=/boot/vmlinuz
    loglevel=3 root=/dev/sda1
2015-08-13T21:04:17+00:00 vShieldEdge kernel: Disabled fast string operations
2015-08-13T21:04:17+00:00 vShieldEdge kernel: BIOS-provided physical RAM map:
    2015-08-13T21:04:17+00:00 vShieldEdge kernel: BIOS-e820: 0000000000000000 -
        000000000009f800 (usable)
    2015-08-13T21:04:17+00:00 vShieldEdge kernel: BIOS-e820: 000000000009f800 -
        00000000000a0000 (reserved)
    2015-08-13T21:04:17+00:00 vShieldEdge kernel: BIOS-e820: 00000000000a0000 -
        00000000000ca000 (reserved)
    2015-08-13T21:04:17+00:00 vShieldEdge kernel: BIOS-e820: 00000000000ca000 -
        00000000000dc000 (reserved)
    2015-08-13T21:04:17+00:00 vShieldEdge kernel: BIOS-e820: 00000000000dc000 -
        0000000000100000 (reserved)
2015-08-13T21:04:17+00:00 vShieldEdge syslog-ng[730]: syslog-ng starting up;
    version='3.3.11'
```

show service dns

Show DNS service status information.

**Synopsis**

```
show service dns
```

**CLI Mode**

Configuration, Interface Configuration, L2VPN
Example

```
nsx-l2vpn-edge(config)# show service dns
vShield Edge DNS Server Status:
DNS is not running.
```

### show service highavailability

Shows details of nodes that are active and standby in high availability (HA).

**Synopsis**

```
show service highavailability
```

**CLI Mode**

Configuration

**Example**

```
nsx-l2vpn-edge(config)# show service highavailability
```

### show service highavailability link

To check the link status of the HA, run the `show service highavailability link` command on each node. This command lists the local and peer /30 IP subnet addresses that you had configured while deploying the standalone L2VPN nodes.

**Synopsis**

```
show service highavailability link
```

**CLI Mode**

Configuration

**Example**

```
nsx-l2vpn-edge(config)# show service highavailability
Local IP address: 192.168.1.1/30
Peer IP Address: 192.168.1.2/30
```

### show service l2vpn

Show L2VPN service status information.

**Synopsis**

```
show service l2vpn [bridge | conversion-table | trunk-table]
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge</td>
<td>Shows L2VPN bridge information.</td>
</tr>
<tr>
<td>conversion-table</td>
<td>Shows conversion table for tunnel IDs to VLAN/VNI IDs, if they are not the same.</td>
</tr>
<tr>
<td>trunk-table</td>
<td>Shows trunk information for interfaces.</td>
</tr>
</tbody>
</table>

**CLI Mode**

Configuration, Interface Configuration, L2VPN
Example

```
nsx-l2vpn-edge(config)# show service l2vpn
L2 VPN is running.
```

```
L2 VPN type : Client
Tunnel status : down
Total bytes sent : 0
Total bytes received : 0
```

show sub-interface

Show sub-interfaces configured on the trunk interface. An NSX Edge can have 10 interfaces (vNic_0 - vNic_9), so the sub-interface numbering starts at 10. The interface index is the TunnelId plus 10.

Synopsis

```
show sub-interface
```

CLI Mode

Configuration, Interface Configuration, L2VPN

Example

```
nsx-l2vpn-edge(config)# show sub-interface
Name   Index  TunnelId  NetworkId
-------- ----- --------  ---------
vNic_210 210    200       200
```

```
--------- total 1  ---------
```

ssh (start | stop)

Start or stop the ssh service. It is recommended to stop the ssh service from the console only.

Synopsis

```
ssh (start | stop)
```

CLI Mode

Configuration

Example

```
nsx-l2vpn-edge(config)# ssh stop
nsx-l2vpn-edge(config)# commit
```

sub-interface pairs

Add a sub-interface with VLAN ID to tunnel ID mapping. The VLAN ID and tunnel ID must be separated by a colon (:). Multiple vlan-tunnel pairs can be specified in the same command, with each pair separated by a space, and the group of pairs enclosed in quotes.

Synopsis

```
sub-interface pairs "vlanID1:tunnelID1 [vlanID2:tunnelID2] [...]
```

CLI Mode

Configuration

Example

```
nsx-l2vpn-edge(config)# sub-interface pairs 250:20
or
```

```
nsx-l2vpn-edge(config)# sub-interface pairs "300:30 400:31 500:32 600:33"
```
Related Commands

- show sub-interface
- sub-interface range

sub-interface range

Add a range of sub-interfaces with VLAN ID to tunnel ID mapping. The VLAN ID and tunnel ID of each sub-interface is the same when created with this command.

**Synopsis**

```
sub-interface range startID endID
```

**CLI Mode**

Configuration

**Example**

```
nsx-l2vpn-edge(config)# sub-interface range 10 15
nsx-l2vpn-edge(config)# commit
nsx-l2vpn-edge(config)# show sub-interface
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Index</th>
<th>TunnelId</th>
<th>NetworkId</th>
</tr>
</thead>
<tbody>
<tr>
<td>vNic_20</td>
<td>20</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>vNic_21</td>
<td>21</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>vNic_22</td>
<td>22</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>vNic_23</td>
<td>23</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>vNic_24</td>
<td>24</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>vNic_25</td>
<td>25</td>
<td>15</td>
<td>15</td>
</tr>
</tbody>
</table>

------------- total 6 -----------

Related Commands

- show sub-interface
- sub-interface pairs

syslog-server

You can configure the syslog server using the syslog server IP address and the protocol to be used. Supported protocols are of UDP and TCP each. You can configure two syslog servers. After commit, the command overwrites the syslog server(s) configured earlier.

- If you give one syslog server IP address, command overwrites the previous first IP address.
- If you give two new IP addresses, command overwrites both the IP addresses.

**Synopsis**

```
syslog-server
```

**CLI Mode**

Configuration

**Example**

```
nsx-l2vpn-edge(config)# syslog-server
```

1  **Configure One Syslog Server**

```
nsx-l2vpn-edge(config-l2vpn)# syslog-server PROTOCOL
# Protocol for syslog server. It can be udp or tcp.
nsx-l2vpn-edge(config-l2vpn)# syslog-server tcp
```
### IP1: IP address of syslog server 1
nsx-l2vpn-edge(config)# syslog-server tcp 10.160.255.180
nsx-l2vpn-edge(config-l2vpn)# commit

2 **Configure Two Syslog Servers**

nsx-l2vpn-edge(config-l2vpn)# syslog-server tcp # IP1 and IP2: IP addresses of both syslog servers
nsx-l2vpn-edge(config-l2vpn)# syslog-server tcp 10.160.255.180 10.109.243.190
nsx-l2vpn-edge(config-l2vpn)# commit

3 **Remove Syslog Server Configuration**

nsx-l2vpn-edge(config-l2vpn)# no syslog-server
nsx-l2vpn-edge(config-l2vpn)# commit

### trustca

Import one or more CA certificates. Each run of trustca command overwrites the previous configuration. The certificates must be in PEM format. To remove all certificates, use no before the command.

**Synopsis**

[n] trustca

**CLI Mode**

L2VPN

**Example**

nsx-l2vpn-edge(config-l2vpn)# trustca
-----BEGIN CERTIFICATE-----
MIID9zCCAt+gAwIBAg...
.
.
.
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDjjCCAnagAwIBAgI...
.
.
.
-----END CERTIFICATE-----
nsx-l2vpn-edge(config-l2vpn)# quit

**Related Commands**

show configuration l2vpn
show configuration certificatestore

### user

Sets the L2VPN username and password. To remove a user, use no before the command.

**Synopsis**

[n] user userName password password

**CLI Mode**

L2VPN
Example

```
nsx-l2vpn-edge(config-l2vpn)# user vpn password vpntest
```

Related Commands

```
show configuration l2vpn
```
The chapter includes the following topics:
- “ESXi CLI Commands” on page 191
- “DVFilter Commands” on page 197

**ESXi CLI Commands**

This section describes the ESXi CLI commands 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

<table>
<thead>
<tr>
<th>VDS ID</th>
<th>VDS Name</th>
<th>MTU</th>
<th>Segment ID</th>
<th>Gateway IP</th>
<th>Gateway MAC</th>
<th>Network Count</th>
<th>Vmknic Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>35 fe 34 50 d4 59 27 dc-e7 9f</td>
<td>dvSwitch</td>
<td>1600</td>
<td></td>
<td>192.168.0.0</td>
<td>192.168.0.254</td>
<td>00:00:0c:00:11:22</td>
<td>1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>VXLAN ID</th>
<th>Multicast IP</th>
<th>Control Plane</th>
<th>Controller</th>
<th>Connection</th>
<th>Port Count</th>
<th>MAC Entry Count</th>
<th>ARP Entry Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>5000</td>
<td>N/A (headend replication)</td>
<td>Enabled (multicast proxy,ARP proxy)</td>
<td>192.168.100.1</td>
<td>(up)</td>
<td>1</td>
<td>11</td>
<td>1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>IP</th>
<th>MAC</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.200.1</td>
<td>00:50:56:00:11:22</td>
<td>00000000</td>
</tr>
</tbody>
</table>

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

Resets VXLAN network ARP table for specified vDS.
Synopses

```
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
```

```
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 --vxlan-id value --vdsport-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
```

```
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
```
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
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>tx.total</td>
<td>0</td>
</tr>
<tr>
<td>rx.total</td>
<td>0</td>
</tr>
<tr>
<td>tx.nonUnicast</td>
<td>0</td>
</tr>
<tr>
<td>tx.crossRouter</td>
<td>0</td>
</tr>
<tr>
<td>tx.drop.total</td>
<td>0</td>
</tr>
<tr>
<td>rx.total</td>
<td>0</td>
</tr>
<tr>
<td>rx.mcastEncap</td>
<td>0</td>
</tr>
<tr>
<td>rx.crossRouter</td>
<td>0</td>
</tr>
<tr>
<td>rx.drop.wrongDest</td>
<td>0</td>
</tr>
<tr>
<td>rx.drop.invalidEncap</td>
<td>0</td>
</tr>
<tr>
<td>rx.drop.total</td>
<td>0</td>
</tr>
<tr>
<td>mac.lookup.found</td>
<td>0</td>
</tr>
<tr>
<td>mac.lookup.flood</td>
<td>0</td>
</tr>
<tr>
<td>mac.lookup.full</td>
<td>0</td>
</tr>
<tr>
<td>mac.update.learn</td>
<td>0</td>
</tr>
<tr>
<td>mac.update.extend</td>
<td>0</td>
</tr>
<tr>
<td>mac.update.full</td>
<td>0</td>
</tr>
<tr>
<td>mac.age</td>
<td>0</td>
</tr>
<tr>
<td>mac.renew</td>
<td>0</td>
</tr>
<tr>
<td>arp.lookup.found</td>
<td>0</td>
</tr>
<tr>
<td>arp.lookup.unknown</td>
<td>0</td>
</tr>
<tr>
<td>arp.lookup.full</td>
<td>0</td>
</tr>
<tr>
<td>arp.lookup.wait</td>
<td>0</td>
</tr>
<tr>
<td>arp.lookup.timeout</td>
<td>0</td>
</tr>
<tr>
<td>arp.update.update</td>
<td>0</td>
</tr>
<tr>
<td>arp.update.unknown</td>
<td>0</td>
</tr>
<tr>
<td>arp.update.notFound</td>
<td>0</td>
</tr>
<tr>
<td>arp.age</td>
<td>0</td>
</tr>
<tr>
<td>arp.renew</td>
<td>0</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>IP</th>
<th>Segment ID</th>
<th>Is MTEP</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.2</td>
<td>192.168.0.0</td>
<td>False</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Vmknic Name</th>
<th>Switch Port ID</th>
<th>VDS PortID</th>
<th>Endpoint ID</th>
<th>VLAN ID</th>
<th>IP</th>
<th>Netmask</th>
<th>IP Acquire</th>
<th>Multicast Group Count</th>
<th>Segment ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmk2</td>
<td>67108868</td>
<td>100</td>
<td>0</td>
<td>0</td>
<td>192.168.0.1</td>
<td>255.255.255.0</td>
<td>34960</td>
<td>0</td>
<td>192.168.0.0</td>
</tr>
</tbody>
</table>

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
**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
```

<table>
<thead>
<tr>
<th>Vmnic Name</th>
<th>Vmnic ID</th>
<th>VXLAN IP</th>
<th>Multicast IP</th>
<th>Joined</th>
<th>Port Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmk2</td>
<td>0</td>
<td>192.168.0.1</td>
<td>239.0.0.1</td>
<td>YES</td>
<td>1</td>
</tr>
</tbody>
</table>

**Name** | **Value**
---|---
tx.passThrough | 0
tx.vxlanTotal | 0
tx.clone | 0
tx.tso | 0
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**

Shows 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
```

**Related Commands**

show dfw host *hostID*
This section describes NSX Controller CLI commands. Log in as the user admin to use the NSX Controller commands.

**NOTE** Using the NSX Controller CLI commands to enable or disable IPSec is not supported. Use NSX API to enable or disable IPSec. For details, refer to *NSX API Guide*.

### restart controller

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

**Synopsis**

```
restart controller
```

### show control-cluster core connection *ipAddress*

Shows status of specified connection.

**Synopsis**

```
show control-cluster core connection 11.11.111.11
```

**Example**

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

### show control-cluster core connection-stats *ipAddress*

Shows statistics for the specified controller.

**Synopsis**

```
show control-cluster core connection-stats ipAddress
```

**Example**

```
nsx-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 log-level

Shows log level for the specified controller.
show control-cluster core log-level

Example

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

show control-cluster core stats

Shows controller statistics.

Synopsis

show control-cluster core stats

Example

nsx-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 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

$logicalRouterID_and/or_bridgeID$

Shows 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

nsx-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

$logicalRouterID_and_bridgeID$

Shows 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

nsx-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`

Shows logical router information. `logicalRouterID` can be all.

**Synopsis**

```
show control-cluster logical-routers instance logicalRouterID
```

**Example**

```
nsx-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 interfaceName`

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

**Synopsis**

```
show control-cluster logical-routers interface logicalRouterID interfaceName
```

**Example**

```
nsx-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`

Shows interface summary for specified logical router.

**Synopsis**

```
show control-cluster logical-routers interface-summary logicalRouter_ID
```

**Example**

```
nsx-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`

Shows static route for router specified by ID. `routerID` can be all.

**Synopsis**

```
show control-cluster logical-routers routes routerID
```

**Example**

```
nsx-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**

Shows 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**

```
nsx-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

Shows statistics of all logical routers on this controller.

**Synopsis**

```
show control-cluster logical-routers stats
```

**Example**

```
nsx-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**

Shows statistics of the specified logical router.

**Synopsis**

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

**Example**

```
nsx-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 logical-switches arp-records

**ipAddress**

Shows the ARP records updated from the specified connection.

**Synopsis**

```
show control-cluster logical-switches arp-records ipAddress
```
Example

```
nsx-controller # show control-cluster logical-switches arp-records 192.168.110.52
VNI   IP              MAC               Connection-ID
5000  192.168.10.6    00:50:56:8e:f5:8b 2
5000  192.168.10.1    00:50:56:8e:6a:04 2
5000  192.168.10.2    00:50:56:8e:9d:88 2
```

**show control-cluster logical-switches arp-table vni**

Shows the ARP records for the specified VNI.

**Synopsis**

```
show control-cluster logical-switches arp-table vni
```

**Example**

```
nsx-controller # show control-cluster logical-switches arp-table 5000
VNI   IP              MAC               Connection-ID
5000  192.168.10.6    00:50:56:8e:f5:8b 2
5000  192.168.10.1    00:50:56:8e:6a:04 2
5000  192.168.10.2    00:50:56:8e:9d:88 2
```

**show control-cluster logical-switches connection-table vni**

Shows the hosts that are connected to the specified VNI.

**Synopsis**

```
show control-cluster logical-switches connection-table vni
```

**Example**

```
nsx-controller # show control-cluster logical-switches connection-table 5000
Host-IP         Port  ID
192.168.110.52  32141 2
192.168.110.51  34692 3
192.168.210.56  33323 4
192.168.210.52  12074 5
192.168.210.51  35441 6
192.168.210.57  56744 7
```

**show control-cluster logical-switches joined-vnis ipAddress**

Shows which VNIs the specified host has joined.

**Synopsis**

```
show control-cluster logical-switches joined-vnis ipAddress
```

**Example**

```
nsx-controller # show control-cluster logical-switches joined-vnis 192.168.110.52
VNI      Controller      BUM-Replication ARP-Proxy Connections VTEPs
5002     192.168.110.202 Enabled         Enabled   6           3
5000     192.168.110.202 Enabled         Enabled   6           2
```

**show control-cluster logical-switches mac-records ipAddress**

Shows the MAC records updated from the specified connection.

**Synopsis**

```
show control-cluster logical-switches mac-records ipAddress
```

**Example**

```
nsx-controller # show control-cluster logical-switches mac-records 192.168.110.52
VNI   Controller  BUM-Replication ARP-Proxy Connections VTEPs
5002  192.168.110.202 Enabled         Enabled   6           3
5000  192.168.110.202 Enabled         Enabled   6           2
```
### Example

```
nsx-controller # show control-cluster logical-switches mac-records 192.168.110.52
VNI      MAC               VTEP-IP         Connection-ID
5000     00:50:56:8e:f5:8b  192.168.150.52  2
5000     00:50:56:8e:6a:04  192.168.150.52  2
5000     00:50:56:8e:9d:88  192.168.150.52  2
```

### show control-cluster logical-switches mac-table vni

Shows MAC records of the specified VNI.

### Synopsis

```
show control-cluster logical-switches mac-table vni
```

### Example

```
nsx-controller # show control-cluster logical-switches mac-table 5000
VNI      MAC               VTEP-IP         Connection-ID
5000     00:50:56:8e:f5:8b  192.168.150.52  2
5000     00:50:56:8e:6a:04  192.168.150.52  2
5000     00:50:56:8e:9d:88  192.168.150.52  2
```

### show control-cluster logical-switches pkt-cap pktcap-uuid display

Shows packet capture data for the specified packet capture operation.

### Synopsis

```
show control-cluster logical-switches pkt-cap pktcap-uuid display
```

### Example

```
nsx-controller # show control-cluster logical-switches pkt-cap 24301920-126f-4255-bf1b-02f42e001389 display
Time-Stamp Source-IP       Dest-IP         TX/RX Type  Comments
358836241 192.168.250.53  192.168.250.52  TX    REQ   CAPPT PktFree TSO 0 CSUM 0 CSUMVFD
0 ENCAP 0 VXLAN 5001 SEGS 1 [ 142 ] +0us:EtherswitchDispatch +4us:EtherswitchOutput +0us:PortOutput +3us:IOChain +0us:PreDVFilter +1us:PostDVFilter +85us:PktFree
3588339300 192.168.250.53  192.168.250.52  TX    REQ   CAPPT PktFree TSO 0 CSUM 0 CSUMVFD
0 ENCAP 0 VXLAN 5001 SEGS 1 [ 142 ] +0us:EtherswitchDispatch +4us:EtherswitchOutput +0us:PortOutput +3us:IOChain +0us:PreDVFilter +1us:PostDVFilter +82us:PktFree
3588342671 192.168.250.53  192.168.250.52  TX    REQ   CAPPT PktFree TSO 0 CSUM 0 CSUMVFD
0 ENCAP 0 VXLAN 5001 SEGS 1 [ 142 ] +0us:EtherswitchDispatch +4us:EtherswitchOutput +0us:PortOutput +3us:IOChain +0us:PreDVFilter +1us:PostDVFilter +85us:PktFree
3588662506 192.168.250.53  192.168.250.52  RX    REQ   CAPPT PktFree TSO 0 CSUM 0 CSUMVFD
0 ENCAP 0 VXLAN 5001 SEGS 1 [ 92 ] +0us:EtherswitchDispatch +4us:EtherswitchOutput +0us:PortOutput +3us:IOChain +0us:PreDVFilter +1us:PostDVFilter +85us:PktFree
```

### Related Commands

- show control-cluster logical-switches pkt-cap pktcap-uuid none
- start control-cluster logical-switches ping
- start control-cluster logical-switches pktcap
- start control-cluster logical-switches pktcap-time
**show control-cluster logical-switches pkt-cap pktpcap-uuid none**

Shows all available packet capture files.

**Synopsis**

`show control-cluster logical-switches pkt-cap pktpcap-uuid none`

**Example**

```
nsx-controller # show control-cluster logical-switches pkt-cap 24301920-126f-4255-bf1b-02f42e001389 none
```

**Trace-File-Name**

- file1-24301920-126f-4255-bf1b-02f42e001389-192.168.250.53-TX.pcapng
- file1-24301920-126f-4255-bf1b-02f42e001389-192.168.250.52-RX.pcapng
- file1-24301920-126f-4255-bf1b-02f42e001389-192.168.250.52-TX.pcapng
- file1-24301920-126f-4255-bf1b-02f42e001389-192.168.250.53-RX.pcapng

**Related Commands**

- `show control-cluster logical-switches pkt-cap pktpcap-uuid display`
- `start control-cluster logical-switches ping`
- `start control-cluster logical-switches pktpcap`
- `start control-cluster logical-switches pktpcap-time`

**show control-cluster logical-switches stats**

Shows statistics for all logical switches on this controller.

**Synopsis**

`show control-cluster logical-switches stats`

**Example**

```
nsx-controller # show control-cluster logical-switches stats
messages.query        2144
messages.update       64
messages.flush        1
messages.notification 0
```

**show control-cluster logical-switches stats-sample**

Shows the latest samples of node statistics.

**Synopsis**

`show control-cluster logical-switches stats-sample`

**Example**

```
nsx-controller # show control-cluster logical-switches stats-sample
03:44:10   03:44:20   03:44:30   03:44:40   03:44:50
messages.query        2144       2144       2144       2144       2145
messages.update       64         64         64         64         64
messages.flush        1          1          1          1          1
messages.notification 0          0          0          0          0
```

**show control-cluster logical-switches vni vni**

Shows controller, configuration, and status of the specified VNI.

**Synopsis**

`show control-cluster logical-switches vni vni`

**Example**

```
nsx-controller # show control-cluster logical-switches vni 5000
```
show control-cluster logical-switches vni-stats vni

Shows statistics for the specified VNI.

Synopsis

show control-cluster logical-switches vni-stats vni

Example

nsx-controller # show control-cluster logical-switches vni-stats 5000
update.member 6
update.vtep 12
update.mac 1
update.mac.invalidate 0
update.arp 1
update.arp.duplicate 0
query.mac 716
query.mac.miss 0
query.arp 3
query.arp.miss 1

show control-cluster logical-switches vni-stats-sample vni

Shows the latest statistics samples for the specified VNI.

Synopsis

show control-cluster logical-switches vni-stats-sample vni

Example

nsx-controller # show control-cluster logical-switches vni-stats-sample 5000
03:00:00 03:10:00 03:20:00 03:30:00 03:40:00
update.member 0 0 0 0 0
update.vtep 0 0 0 0 0
update.mac 0 0 0 0 0
update.mac.invalidate 0 0 0 0 0
update.arp 0 0 0 0 0
update.arp.duplicate 0 0 0 0 0
query.mac 1 2 1 1 2
query.mac.miss 0 0 0 0 0
query.arp 0 0 0 0 0
query.arp.miss 0 0 0 0 0

show control-cluster logical-switches vtep-records ipAddress

Shows the VTEP records updated from the specified connection.

Synopsis

show control-cluster logical-switches vtep-records ipAddress

Example

nsx-controller # show control-cluster logical-switches vtep-records 192.168.110.52
VNI IP Segment MAC Connection-ID
5000 192.168.150.52 192.168.150.0 00:50:56:60:1e:dd 2

show control-cluster logical-switches vtep-table vni

Shows the VTEP table for the specified VNI.
Synopsis

show control-cluster logical-switches vtep-table vni

Example

nsx-controller # show control-cluster logical-switches vtep-table 5000

<table>
<thead>
<tr>
<th>VNI</th>
<th>IP</th>
<th>Segment</th>
<th>MAC</th>
<th>Connection-ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>5000</td>
<td>192.168.250.52</td>
<td>192.168.250.0</td>
<td>00:50:56:6b:37:64</td>
<td>5</td>
</tr>
<tr>
<td>5000</td>
<td>192.168.150.52</td>
<td>192.168.150.0</td>
<td>00:50:56:60:1e:dd</td>
<td>2</td>
</tr>
</tbody>
</table>

**show control-cluster startup-nodes**

Shows the set of NSX Controller nodes that this node will attempt to connect to upon startup in order to rejoin its NSX Controller cluster. This is not an accurate list of active nodes in the controller cluster and may include nodes that are inactive, or may exclude nodes that are active.

Synopsis

show control-cluster startup-nodes

Example

nsx-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

nsx-controller # show control-cluster status

<table>
<thead>
<tr>
<th>Type</th>
<th>Status</th>
<th>Since</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join status:</td>
<td>Join complete</td>
<td>12/29 00:43:17</td>
</tr>
<tr>
<td>Majority status:</td>
<td>Connected to cluster majority</td>
<td>01/09 20:21:33</td>
</tr>
<tr>
<td>Restart status:</td>
<td>This controller can be safely restarted</td>
<td>01/09 20:21:23</td>
</tr>
<tr>
<td>Cluster ID:</td>
<td>b29a7ae3-576a-4c18-bed5-c5c8442a0903</td>
<td></td>
</tr>
<tr>
<td>Node UUID:</td>
<td>5113b115-4363-4ca0-bc61-6ff924163f07</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>Configured status</td>
<td>Active status</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>api_provider</td>
<td>enabled</td>
<td>activated</td>
</tr>
<tr>
<td>persistence_server</td>
<td>enabled</td>
<td>activated</td>
</tr>
<tr>
<td>switch_manager</td>
<td>enabled</td>
<td>activated</td>
</tr>
<tr>
<td>logical_manager</td>
<td>enabled</td>
<td>activated</td>
</tr>
<tr>
<td>directory_server</td>
<td>enabled</td>
<td>activated</td>
</tr>
</tbody>
</table>

Cluster status from vnet-controller:

| Active cluster members    | isMaster: true    | uuId=9122d3ca-feld-4e50-94ec-a5f054843824, ip=192.168.110.32 |
| uuId=5113b115-4363-4ca0-bc61-6ff924163f07, ip=192.168.110.33 |
| uuId=b29a7ae3-576a-4c18-bed5-c5c8442a0903, ip=192.168.110.31 |

Configured cluster members

| uuId=9122d3ca-feld-4e50-94ec-a5f054843824, ip=192.168.110.32 |
| uuId=5113b115-4363-4ca0-bc61-6ff924163f07, ip=192.168.110.33 |
| uuId=b29a7ae3-576a-4c18-bed5-c5c8442a0903, ip=192.168.110.31 |
controllerd.info
0000000: 5113 b115 4363 4ca0 bc61 6ff9 2416 3f07 Q...CcL..ao.$?.
0000010: 0500 0000 0000 0000 0300 0000 0000 0000  ................
0000020: 7a6b 636c 6973 3000 0031 3932 2e31 3638 zkclis0..192.168
0000030: 2e31 3130 2e33 31:3737 3737 2c31 3932  .110.33:7777,192
0000040: 2e31 3638 2e31 3130 2e33 323a 3737 3737  .168.110.32:7777
0000050: 2c31 3932 2e31 3638 2e31 3130 2e33 333a  ,192.168.110.33:
0000060: 3737 3737 0000 0000 0000 0000 0000 0000  7777......
0000070: 0000 0000 0000 0000 0000 0000 0000 0000  ........................
0000080: 0000 0000 7a6b 7376 3000 0000 0031 3932  ....zksv0....192
0000090: 2e31 3638 2e31 3130 2e33 333a 3737 3737  .168.110.33:7777
00000a0: 2c31 3932 2e31 3638 2e31 3130 2e33 313a  ,192.168.110.33:
00000b0: 3737 3737 0000 0000 0000 0000 0000 0000  7777......

----------------------------
/var/log is writable: True
/var/cloudnet/data is writable: True
/var/cloudnet/cluster is writable: True

show network interface

Shows the IP address of the controller.

Synopsis

show network interface

CLI Mode

Basic, Privileged

show process monitor

Shows the process information on the controller. This command is equivalent to the top command that is used to debug the processes on the controller that cause high CPU issues.

Synopsis

show process monitor

CLI Mode

Basic

Example

Tasks: 174 total: 1 running: 172 sleeping: 0 stopped: 1 zombie
%CPU0 : 1.3/0.7 2[[
%CPU1 : 1.3/0.0 1[|
%CPU2 : 0.7/1.3 2[|
%CPU3 : 3.3/0.7 4[|||
GiB Mem : 38.0/3.858 [
GiB Swap: 0.0/2.000 [

PID USER PR NI VIRT RES %CPU%MEM TIME+ COMMAND
1 root 20 0 32.7m 5.8m 0.0 0.1 0:20.95 systemd
1139 root 20 0 45.2m 22.4m 0.0 0.6 0:24.54 -systemd-journal
start control-cluster logical-switches ping

Starts a ping capture to test connectivity between VTEPs.

**Synopsis**

start control-cluster logical-switches ping vni vtepIP1 vtepIP2 scheme packetNum
packetsize trace fileName

**Example**
	nsx-controller# start control-cluster logical-switches ping 5001 192.168.250.52
192.168.250.53 uni 3 50 trace file1

**Operation Status**

Operation in progress: 24301920-126f-4255-bf1b-02f42e001389

Capture stage StartCaptureHostRx, failure time-out is 63 seconds

Retrieve results with command: show control-cluster logical-switches pkt-cap

24301920-126f-4255-bf1b-02f42e001389 <display|none>

**Related Commands**

show control-cluster logical-switches pkt-cap pktcap-uuid none
show control-cluster logical-switches pkt-cap pktcap-uuid display
start control-cluster logical-switches pktcap
start control-cluster logical-switches pktcap-time

start control-cluster logical-switches pktcap

Starts packet capture on the host identified by the VTEP IP. The package capture runs for maxPackets packets.

See pktcap-uw for supported command arguments. The pktcap-uw command arguments must be surrounded by single quotes.

**Synopsis**

start control-cluster logical-switches pktcap vni vtep maxPackets fileName
commandArguments
Example

```
nsx-controller # start control-cluster logical-switches pktcap 5001 192.168.250.53 3
file2 ' --vmk vmk3'
```

Operation Status
Operation in progress: c77a1eeb-33a9-48c4-9676-988913001389
Capture for 300 seconds or 3 packets
Retrieve results with command: show control-cluster logical-switches pkt-cap
c77a1eeb-33a9-48c4-9676-988913001389 none

Related Commands

```
show control-cluster logical-switches pkt-cap pktcap-uuid none
show control-cluster logical-switches pkt-cap pktcap-uuid display
start control-cluster logical-switches ping
start control-cluster logical-switches pktcap-time
```

**start control-cluster logical-switches pktcap-time**

Starts packet capture on the host identified by the VTEP IP. See pktcap-uw for supported command arguments. The package capture runs for `maxTime` seconds.

**Synopsis**

```
start control-cluster logical-switches pktcap-time vni vtepIP maxTime FileName
commandArguments
```

**Example**

```
nsx-controller # start control-cluster logical-switches pktcap-time 5001 192.168.250.53
20 file3 ' --vmk vmk3'
```

Operation Status
Operation in progress: 0e9389c8-d1a4-480f-a582-e5d937001389
Capture for 20 seconds or 10000 packets
Retrieve results with command: show control-cluster logical-switches pkt-cap
0e9389c8-d1a4-480f-a582-e5d937001389 none

Related Commands

```
show control-cluster logical-switches pkt-cap pktcap-uuid none
show control-cluster logical-switches pkt-cap pktcap-uuid display
start control-cluster logical-switches ping
start control-cluster logical-switches pktcap
```

VMware, Inc.
This section describes CLI commands used to troubleshoot common issues with a hardware gateway deployment. Log in as the user admin to use these commands. This chapter includes the following sections:

- “Hardware Gateway Query Commands” on page 211
- “Replicator Node Command” on page 212
- “Bindings Commands” on page 213
- “Host Commands” on page 214
- “Controller Commands” on page 215
- “Agent Commands” on page 216

For additional information about hardware gateways, see:

- “Configuring Hardware Gateways” in the NSX for vSphere Administration Guide
- “Managing Hardware Gateways” in the NSX for vSphere API Reference Guide
- Documentation from your hardware gateway vendor

Hardware Gateway Query Commands

Use these commands to query hardware gateways.

**show hardware-gateway list**

Shows a list of known hardware gateways (regardless of status).

**Synopsis**

```
show hardware-gateway list
```

**CLI Mode**

Basic

**Example**

```
nsx?mgr> show hardware-gateway list

ID       UUID         Name               BFD Enabled Management IP
---       -------      --------           -------          ---------
torgateway-1       3e5ffd66-448d-4e54-82ec-92fffd46d4af torgateway1       true           10.144.137.91
```

VMware, Inc.
show hardware-gateway hsc *hardwareGatewayID* brief

Shows the relevant data of the specified hardware gateway in a brief format.

**Synopsis**

show hardware-gateway hsc *hardwareGatewayID* brief

**CLI Mode**

Basic

**Example**

```bash	nsx?mgr> show hardware-gateway hsc torgateway-1 brief
ID                  Name                BFD Enabled    Management IP
UUID
1766-1766-1766-1766-1766-1766-1766-1766
3e5ffd66-448d-4e54-82ec-92fffd46d4af
```

show hardware-gateway hsc *hardwareGatewayID* certificate

Shows the certificate of the specified hardware gateway.

**Synopsis**

show hardware-gateway hsc *hardwareGatewayID* certificate

**CLI Mode**

Basic

**Example**

```bash	nsx?mgr> show hardware-gateway hsc torgateway-1 certificate
-----BEGIN CERTIFICATE-----
MIIDeDCCAmACAQEwDQYJKoZIhvcNAQEFBQAwYEXCZAJBgNVBAYTA1VTMQswCQYDVQQIEwY
Q0ExCzAJBgNVBAYTB0NMMRAwDgYDVQQLEw9zd2l0Y2hjYTE7MDkGA1UEAxMyTlZTHN3aXJr
jaGHBiEiIcKjGiGIDkMKc9JXoIIFo5RZw8DBOQ6Y2FwaQ==
-----END CERTIFICATE-----
```

### Replicator Node Command

Use this command to query replicator nodes.

**show hardware-gateway replicator-nodes**

Shows all replicator nodes on the hardware gateway.

**Synopsis**

show hardware-gateway replicator-nodes
Bindings Commands

Use these commands to query bindings on the hardware gateway.

**show hardware-gateway binding all**

Shows all bindings on the hardware gateway.

**Synopsis**

`show hardware-gateway binding all`

**CLI Mode**

Basic

**Example**

```bash
nsx?mgr> show hardware-gateway binding all
```

<table>
<thead>
<tr>
<th>Switch Name</th>
<th>Port Name</th>
<th>VLAN ID</th>
<th>VNI</th>
<th>Hardware Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-switch-603</td>
<td>p1</td>
<td>0</td>
<td>8823</td>
<td>torgateway-1</td>
</tr>
<tr>
<td>1-switch-603</td>
<td>p2</td>
<td>0</td>
<td>8824</td>
<td>torgateway-1</td>
</tr>
<tr>
<td>1-switch-168</td>
<td>p1</td>
<td>0</td>
<td>8823</td>
<td>torgateway-2</td>
</tr>
<tr>
<td>1-switch-168</td>
<td>p2</td>
<td>0</td>
<td>8824</td>
<td>torgateway-2</td>
</tr>
</tbody>
</table>

**show hardware-gateway binding hsc hardwareGatewayID all**

Shows all bindings for the specified hardware gateway.

**Synopsis**

`show hardware-gateway binding hsc hardwareGatewayID all`

**CLI Mode**

Basic

**Example**

```bash
nsx?mgr> show hardware-gateway binding hsc torgateway-1 all
```

<table>
<thead>
<tr>
<th>Switch Name</th>
<th>Port Name</th>
<th>VLAN ID</th>
<th>VNI</th>
<th>Hardware Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-switch-603</td>
<td>p1</td>
<td>0</td>
<td>8823</td>
<td>torgateway-1</td>
</tr>
<tr>
<td>1-switch-603</td>
<td>p2</td>
<td>0</td>
<td>8824</td>
<td>torgateway-1</td>
</tr>
</tbody>
</table>

**show hardware-gateway binding vni vni all**

Shows all bindings for the specified virtual network instance.

**Synopsis**

`show hardware-gateway binding vni vni all`

**CLI Mode**

Basic
Example

```bash
nsx?mgr> show hardware-gateway binding vni 8823 all
```

<table>
<thead>
<tr>
<th>Switch Name</th>
<th>Port Name</th>
<th>VLAN ID</th>
<th>VNI</th>
<th>Hardware Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-switch-603</td>
<td>p1</td>
<td>0</td>
<td>8823</td>
<td>torgateway-1</td>
</tr>
<tr>
<td>1-switch-168</td>
<td>p1</td>
<td>0</td>
<td>8823</td>
<td>torgateway-2</td>
</tr>
</tbody>
</table>

**show hardware-gateway binding hsc hardwareGatewayID vni vni**

Shows all bindings for the specified virtual network instance on the specified hardware gateway.

**Synopsis**

```bash
show hardware-gateway binding hsc hardwareGatewayID vni vni
```

**CLI Mode**

Basic

**Example**

```bash
nsx?mgr> show hardware-gateway binding hsc torgateway-1 vni 8823
```

<table>
<thead>
<tr>
<th>Switch Name</th>
<th>Port Name</th>
<th>VLAN ID</th>
<th>VNI</th>
<th>Hardware Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-switch-603</td>
<td>p1</td>
<td>0</td>
<td>8823</td>
<td>torgateway-1</td>
</tr>
</tbody>
</table>

**Host Commands**

Use these commands to query host information.

**show hardware-gateway host hostID vnis**

Shows the virtual network instances on the specified host.

**Synopsis**

```bash
show hardware-gateway host hostID vnis
```

**CLI Mode**

Basic

**Example**

```bash
nsx?mgr> show hardware-gateway host host-21 vnis
```

<table>
<thead>
<tr>
<th>Is PTEP:</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VXLAN count:</td>
<td>2</td>
</tr>
<tr>
<td>VXLAN IDs:</td>
<td></td>
</tr>
<tr>
<td>8824</td>
<td></td>
</tr>
<tr>
<td>8823</td>
<td></td>
</tr>
</tbody>
</table>

**show hardware-gateway host hostID bfd-tunnels**

Shows the tunnels (BFD configuration) on the specified host.

**Synopsis**

```bash
show hardware-gateway host hostID bfd-tunnels
```

**CLI Mode**

Basic

**Example**

```bash
nsx?mgr> show hardware-gateway host host-21 bfd-tunnels
```

<table>
<thead>
<tr>
<th>BFD count:</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.18.171.169</td>
<td>--&gt; 172.21.145.84 , Inner Dest IP: 169.254.1.0 , Inner Dest Mac: 00:23:20:00:00:01 , Local State: up, Remote State: up</td>
</tr>
</tbody>
</table>
Controller Commands

Use these commands to query information about the hardware gateway controller.

**show hardware-gateway controller controllerIP list**

Shows details on the specified hardware gateway controller. Output of the `UtepProbeInterval` parameter is in milliseconds.

**Synopsis**

```bash
show hardware-gateway controller controllerIP list
```

**CLI Mode**

Basic

**Example**

```bash
nsx?mgr> show hardware-gateway controller 10.144.136.210 list
Tor-uuid                       bfd-Enabled     UtepProbeInterval
3e5ffd66-448d-4e54-92fffd46d4af true            300
6c43af48-7d42-43b4-9416-10c508edbcf true            300
```

**show hardware-gateway controller controllerIP hsc hardwareGatewayID certificate**

Shows the certificate of the specified hardware gateway.

**Synopsis**

```bash
show hardware-gateway controller controllerIP hsc hardwareGatewayID certificate
```

**CLI Mode**

Basic

**Example**

```bash
nsx?mgr> show hardware-gateway controller 10.144.136.211 hsc torgateway-1 certificate
-----BEGIN CERTIFICATE-----
MIIDeDCCAmACAQEwDQYJKoZIhvcNAQEFBQAwgYExCzAJBgNVBAYTAlVTMQswCQYD
VQQIEwJDQTEVMBMGA1UEChMMT3BlbiB2U3dpdGNoMREwDwYDVQQEwDVQElEBENlcnRpZmljYXRlICgyMDE2IEFwciAwMDo0
YXZlcnR5cGVzYW1vdWxlcxI0MSwGCSqGSIb3DQEBAQUAA4IBAQC2
-----END CERTIFICATE-----
```
show hardware-gateway controller controllerIP port-bindings

Shows the port bindings (logical port attachment configuration) of the specified hardware gateway controller.

Synopsis

show hardware-gateway controller controllerIP port-bindings

CLI Mode

Basic

Example

nsx?mgr> show hardware-gateway controller 10.144.136.211 port-bindings
Vni   Vlan Switch-Name     Port-Id         ToR-Uuid
8823  0     1-switch-603    p1              3e5ffd66-448d-4e54-82ec-92fffd46d4af
8823  0     1-switch-168    p1              6c43af48-d742-43b4-9416-10c508edbdcf
8824  0     1-switch-168    p2              6c43af48-d742-43b4-9416-10c508edbdcf
8824  0     1-switch-603    p2              3e5ffd66-448d-4e54-82ec-92fffd46d4af

show hardware-gateway controller controllerIP control-nodes

Shows all controller nodes of the specified hardware gateway controller.

Synopsis

show hardware-gateway controller controllerIP control-nodes

CLI Mode

Basic

Example

nsx?mgr> show hardware-gateway controller 10.144.136.211 control-nodes
Node-Uuid                                IP                        Port
94ecd027-a210-452f-8e98-77d6100f2fc3     10.144.136.212            1234
e37a1fcc-2c72-4b87-9487-e700b6fbc3d6     10.144.136.211            1234
7a90d58e-6224-46f6-bd8b-69746ba4e128     10.144.136.210            1234

show hardware-gateway controller controllerIP hsc hardwareGatewayID inventory

Shows all inventory information of the specified hardware gateway.

Synopsis

show hardware-gateway controller controllerIP hsc hardwareGatewayID inventory

CLI Mode

Basic

Example

nsx?mgr> show hardware-gateway controller 10.144.136.212 hsc torgateway-1 inventory
Switch-Name     Port-Id
1-switch-603    p4
1-switch-603    p3
1-switch-603    p2
1-switch-603    p1

Agent Commands

Use these commands to query hardware gateway agent information.
show hardware-gateway agent *agentIP* status

Shows the connection status of the specified hardware gateway.

**Synopsis**

`show hardware-gateway agent *agentIP* status`

**CLI Mode**

Basic

**Example**

```
nsx?mgr> show hardware-gateway agent 10.144.136.212 status
controller IP              connection status
10.144.136.210              connected
10.144.136.212              connected
10.144.136.211              connected
```

---

show hardware-gateway agent *agentIP* replication-cluster

Shows the PTEP list for a specified VNI on the specified hardware gateway agent.

**Synopsis**

`show hardware-gateway agent *agentIP* replication-cluster`

**CLI Mode**

Basic

**Example**

```
nsx?mgr> show hardware-gateway agent 10.144.136.212 replication-cluster
172.18.175.120
172.18.175.119
172.19.226.89
```

---

show hardware-gateway agent *agentIP* hardware-gateway [uuid]

Show details about the master hardware gateway agent for the specified hardware gateway instance on the specified master gateway agent.

The `<uuid>` of the hardware gateway instance is optional. If unspecified, then this command returns a list of all hardware hardware gateways mastered by this hardware gateway agent.

Output of the `Bfd Probe Interval` parameter is in milliseconds.

**Synopsis**

`show hardware-gateway agent *agentIP* hardware-gateway [uuid]`

**CLI Mode**

Basic

**Example**

```
nsx?mgr> show hardware-gateway agent 10.144.136.212 hardware-gateway 3e5ffd66-448d-4e54-82ec-92fffd46d4af

UUID                            3e5ffd66-448d-4e54-82ec-92fffd46d4af
Ip                              10.144.137.91
Instance Id                     1
Connected                       true
Physical Master                 true
Bfd Enabled                     true
```
show hardware-gateway agent agentIP hardware-gateway hardwareGatewayUuid tunnels

Shows the tunnel table (including BFD) on the specified hardware gateway agent.

Synopsis
show hardware-gateway agent agentIP hardware-gateway hardwareGatewayUuid tunnels

CLI Mode
Basic

Example
nsx?mgr> show hardware-gateway agent 192.161.126.22 hardware-gateway 1e100ec0-b15a-4727-ba9f-ebdb74e357f2 tunnels

Endpoints
Local Ip                        172.21.145.85
Remote Ip                       172.19.152.225
Local config
Destination Ip                  169.254.1.0
Destination Mac                 00:23:20:00:00:01
Remote config
Destination Ip
Destination Mac
BFD parameters
Enable                         false
Min Rx
Min Tx
Forwarding If Rx               false
BFD status
Diagnostic
Enabled                         false
Forwarding
false
Remote diagnostic
State
Info

Endpoints
Local Ip                        172.21.145.85
Remote Ip                       172.19.152.225
### Local config
- **Destination Ip**: 169.254.1.0
- **Destination Mac**: 00:23:20:00:00:01

### Remote config
- **Destination Ip**: 172.18.171.168
- **Destination Mac**: 00:00:00:00:00:00

### BFD parameters
- **Enable**: true
- **Min Rx**: 300
- **Min Tx**: 300
- **Forwarding If Rx**: true

### BFD status
- **Diagnostic**: Control Detection Time Expired
- **Enabled**: true
- **Forwarding**: true
- **Remote diagnostic**: Control Detection Time Expired
- **Remote state**: up
- **State**: up

### Endpoints
- **Local Ip**: 172.21.145.85
- **Remote Ip**: 172.18.171.168

### Local config
- **Destination Ip**: 169.254.1.0
- **Destination Mac**: 00:23:20:00:00:01

### Remote config
- **Destination Ip**: 172.18.171.168
- **Destination Mac**: 00:00:00:00:00:00

### BFD parameters
- **Enable**: true
- **Min Rx**: 300
- **Min Tx**: 300
- **Forwarding If Rx**: true

### BFD status
- **Diagnostic**: Neighbor Signaled Session Down
- **Enabled**: true
- **Forwarding**: true
- **Remote diagnostic**: Control Detection Time Expired
- **Remote state**: up
- **State**: up

### Endpoints
- **Local Ip**: 172.21.145.85
- **Remote Ip**: 172.18.171.169

### Local config
- **Destination Ip**: 169.254.1.0
- **Destination Mac**: 00:23:20:00:00:01

### Remote config
- **Destination Ip**: 172.18.171.169
- **Destination Mac**: 00:00:00:00:00:00

### BFD parameters
- **Enable**: true
- **Min Rx**: 300
- **Min Tx**: 300
- **Forwarding If Rx**: true

### BFD status
- **Diagnostic**: Neighbor Signaled Session Down
- **Enabled**: true
- **Forwarding**: true
- **Remote diagnostic**: Control Detection Time Expired
- **Remote state**: up
- **State**: up

### Info
show hardware-gateway agent agentIP hardware-gateway hardwareGatewayUuid local-macs [vni]

Shows the local MAC tables (unicast and multicast) on the specified hardware gateway agent.

Synopsis

show hardware-gateway agent agentIP hardware-gateway hardwareGatewayUuid local-macs [vni]

CLI Mode

Basic

Example

nsx?mgr> show hardware-gateway agent 10.144.136.212 hardware-gateway 3e5fffd66-448d-4e54-82ec-92fffd46d4af local-macs

Hardware Gateway UUID           3e5fffd66-448d-4e54-82ec-92fffd46d4af
Local Unicast Macs
Mac                           Empty
Local Multicast Macs
VNI                             8823
Macs

Mac                         unknown-dst
Ip
Logical Switch UUID          6c752ceb-b3e9-3bbb-82cb-59c3e19a27bf
VNI                           8823
Vtep Ips

VNI                             8824
Macs

Mac                         unknown-dst
Ip
Logical Switch UUID          801a0897-5938-3ea9-ba5f-77ecc339f4be
VNI                           8824
Vtep Ips

show hardware-gateway agent agentIP hardware-gateway hardwareGatewayUuid physical-inventory

Shows the hardware gateway physical inventory (switches and ports) on the specified hardware gateway agent.

Synopsis

show hardware-gateway agent agentIP hardware-gateway hardwareGatewayUuid physical-inventory

CLI Mode

Basic

Example

nsx?mgr> show hardware-gateway agent 10.144.136.212 hardware-gateway 3e5fffd66-448d-4e54-82ec-92fffd46d4af physical-inventory

Hardware Gateway UUID           3e5fffd66-448d-4e54-82ec-92fffd46d4af
Physical Switches

Name                   1-switch-603
Description            OVS VTEP Emulator
Management Ips         Empty
Tunnel Ips
show hardware-gateway agent agentIP hardware-gateway hardwareGatewayUuid bindings

Shows hardware gateway attachments of logical ports (physical switch and port, VNI, VLAN) on the specified hardware gateway agent.

Synopsis

show hardware-gateway agent agentIP hardware-gateway hardwareGatewayUuid bindings

CLI Mode

Basic

Example

nsx?mgr> show hardware-gateway agent 10.144.136.212 hardware-gateway 3e5ffd66-448d-4e54-82ec-92fffd46d4af bindings

UUID f04348e8-90b4-3f83-bf2e-82b44a43e55d
Logical Switch UUID 6c752ceb-b3e9-3bbb-82cb-59c3e19a27bf
VNI 8823
Hardware Gateway UUID 3e5ffd66-448d-4e54-82ec-92fffd46d4af
Switch Name 1-switch-603
Port Name p1
VLAN 0
Statistics
Packets from local 3518
Bytes from local 566017
Packets to local 11742
Bytes to local 3427838

UUID b6e273de-bff8-3c43-a4c7-9e42a671f004
Logical Switch UUID 801a0897-5938-3ea9-ba5f-77ecc339f4be
VNI 8824
Hardware Gateway UUID 3e5ffd66-448d-4e54-82ec-92fffd46d4af
Switch Name 1-switch-603
Port Name p2
VLAN 0
Statistics
Packets from local 759119
Bytes from local 107781854
Packets to local 8287
Bytes to local 2824944

**show hardware-gateway agent agentIP logical-switches**

Shows the list of logical switches (UUID, VNI) known to the specified hardware gateway agent.

**Synopsis**

`show hardware-gateway agent agentIP logical-switches`

**CLI Mode**

Basic

**Example**

```
nsx?mgr> show hardware-gateway agent 10.144.136.212 logical-switches
```

```
UUID                            801a0897-5938-3ea9-ba5f-77ecc339f4be
VNI                             8824

UUID                            6c752ceb-b3e9-3bbb-82cb-59c3e19a27bf
VNI                             8823
```

**show hardware-gateway agent agentIP logging-level**

Gets the current logging level on the specified hardware gateway agent. One of the following values:

- ERROR
- WARN
- INFO
- DEBUG
- TRACE

**Synopsis**

`show hardware-gateway agent agentIP logging-level`

**CLI Mode**

Basic

**Example**

```
nsx?mgr> show hardware-gateway agent 10.144.136.212 logging-level
Log level: INFO
```

**set hardware-gateway agent agentIP logging-level**

**hardwareGatewayAgentLogLevel**

Sets logging on the specified hardware gateway agent to one of the following levels:

- ERROR
- WARN
- INFO
- DEBUG
- TRACE

**Synopsis**

`set hardware-gateway agent agentIP logging-level hardwareGatewayLogLevel`
CLI Mode
Basic

Example
nsx?mgr> set hardware-gateway agent 10.144.136.212 logging-level DEBUG

show hardware-gateway agent agentIP dump

Shows a full information dump of the specified hardware gateway agent.

Synopsis
show hardware-gateway agent agentIP dump

CLI Mode
Basic

Example
nsx?mgr> show hardware-gateway agent agentIP dump
The following table lists deprecated commands.

**Table 9-1. Deprecated Commands**

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>cli ssh allow</td>
</tr>
<tr>
<td>clear firewall counters</td>
</tr>
<tr>
<td>clear vmwall rules</td>
</tr>
<tr>
<td>clear vty</td>
</tr>
<tr>
<td>close support-tunnel</td>
</tr>
<tr>
<td>copy http URL slot (1</td>
</tr>
<tr>
<td>copy http URL temp</td>
</tr>
<tr>
<td>copy scp URL slot (1</td>
</tr>
<tr>
<td>copy scp URL temp</td>
</tr>
<tr>
<td>debug copy</td>
</tr>
<tr>
<td>debug export snapshot</td>
</tr>
<tr>
<td>debug import snapshot</td>
</tr>
<tr>
<td>debug service</td>
</tr>
<tr>
<td>debug service flow src</td>
</tr>
<tr>
<td>debug snapshot list</td>
</tr>
<tr>
<td>debug snapshot remove</td>
</tr>
<tr>
<td>debug snapshot restore</td>
</tr>
<tr>
<td>default web-manager password</td>
</tr>
<tr>
<td>duplex auto</td>
</tr>
<tr>
<td>duplex (half</td>
</tr>
<tr>
<td>http server</td>
</tr>
<tr>
<td>ip name server</td>
</tr>
<tr>
<td>ip policy-address</td>
</tr>
<tr>
<td>link-detect</td>
</tr>
<tr>
<td>linkwatch interval &lt;5-60&gt;</td>
</tr>
<tr>
<td>manager key</td>
</tr>
<tr>
<td>mode policy-based-forwarding</td>
</tr>
<tr>
<td>ntp server</td>
</tr>
<tr>
<td>open support-tunnel</td>
</tr>
<tr>
<td>set support key</td>
</tr>
</tbody>
</table>
### Table 9-1. Deprecated Commands

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>show alerts</td>
</tr>
<tr>
<td>show debug log</td>
</tr>
<tr>
<td>show dv-support</td>
</tr>
<tr>
<td>show hardware</td>
</tr>
<tr>
<td>show gateway rules</td>
</tr>
<tr>
<td>show interface</td>
</tr>
<tr>
<td>show ip addr</td>
</tr>
<tr>
<td>show iptables</td>
</tr>
<tr>
<td>show kernel message</td>
</tr>
<tr>
<td>show kernel message last</td>
</tr>
<tr>
<td>show log alerts</td>
</tr>
<tr>
<td>show log events</td>
</tr>
<tr>
<td>show service helpers</td>
</tr>
<tr>
<td>show service statistics</td>
</tr>
<tr>
<td>show services</td>
</tr>
<tr>
<td>show session-manager counters</td>
</tr>
<tr>
<td>show session-manager sessions</td>
</tr>
<tr>
<td>show stacktrace</td>
</tr>
<tr>
<td>show raid</td>
</tr>
<tr>
<td>show raid detail</td>
</tr>
<tr>
<td>show realms</td>
</tr>
<tr>
<td>show syslog</td>
</tr>
<tr>
<td>show system events</td>
</tr>
<tr>
<td>show system network_connections</td>
</tr>
<tr>
<td>show syslog</td>
</tr>
<tr>
<td>show vmwall log</td>
</tr>
<tr>
<td>show vmwall rules</td>
</tr>
<tr>
<td>ssh end</td>
</tr>
<tr>
<td>syslog</td>
</tr>
<tr>
<td>telnet</td>
</tr>
<tr>
<td>vm validation</td>
</tr>
<tr>
<td>vm validation log</td>
</tr>
<tr>
<td>vmwall log suppression</td>
</tr>
</tbody>
</table>