Pluribus Netvisor ONE

Version 5.2.1 - Command Reference A-O

June 2020

Table of contents

Legal Notice

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR PLURIBUS NETWORKS REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE ARE PROVIDED "AS IS" WITH ALL FAULTS. PLURIBUS NETWORKS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL PLURIBUS NETWORKS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA, ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF PLURIBUS NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Version 5.2.1	June 2020
Version 5.2.0	March 2020
Version 5.1.2	February 2020
Version 5.1.1	December 2019
Version 5.1.0	September 2019

A Commands

aaa-tacacs-create

Use this command to add a TACACS+ server for authorization and authentication on the network.

Syntax `aaa-tacacs-create`

`name` *`name-string`*	Specify the name, up to 60 characters, of the TACACS service.
`scope fabric|local`	Specify the scope to apply to the TACACS server.
`server` *`server-string`*	Specify the name, up to 60 characters, of the TACACS server.
`port` *`port-number`*	Specify the port that connects to the server. The default port is 49.
`secret` *`secret-string`*	Specify the secret (password) to access the server.
`timeout` *`timeout-number`*	Specify the number of seconds for the server to time out a request. The default value is 10 seconds.
`priority` *`priority-number`*	Specify the priority for the server. The priority can be 1 (highest) to X (lowest priority).
`authen|no-authen`	Specify if the server authenticates clients on the network.
`authen-method pap|chap|ms-chap`	Specify the authentication method for clients. PAP, CHAP, and MS-CHAP are supported methods with CHAP as the default method.
`sess-acct|no-sess-acct`	Specify if you want to use session accounting. The TACACS+ server is notified when a user logs in or out of the network.
`cmd-acct|no-cmd-acct`	Specify if you want to use command accounting. The TACACS+ server is notified when ever a user, including the network administrator, runs a non-show command.
`sess-author|no-sess-author`	Specify if you want to use session authorization. The TACACS+ server configured for session authorization determines if a user can initiate a session on the network after logging in.
`cmd-author|no-cmd-author`	Specify if you want to use command authorization. The TACACS+ server determines if a user can run certain commands on the network.
`acct-local|no-acct-local`	Specify accounting for local users
`author-local|no-author-local`	Specify authorization for local users.
`service` *`service-string`*	Specify the service name used for TACACS+ requests sent from Netvisor to the TACACS+ server for commands run at the Netvisor CLI, and the Java,

	C, and REST APIs. The default value is `shell`.
`service-shell` *service-shell-string*	Specify the service name used for TACACS+ requests sent from Netvisor to the TACACS+ server for commands run from a UNIX shell.
`service-vtysh` *service-vtysh-string*	Specify the service name used for TACACS+ requests sent from Netvisor to the TACACS+ server for commands run from vtysh.

Defaults None.

Access CLI

History

Version 1.2.1	Command introduced.
Version 2.6.0	The parameters, `acct-local`, `author-local`, `service`, `service-shell`, and `service-vtyesh`, added.

Usage Use this command to allow a TACACS+ server authenticate and authorize clients on the network. The TACACS+ can also provide accounting for sessions and commands.

Examples To add the TACACS+ server, TACserver1, with scope **local** on port **33** and secret, **p@ssw0rd**, use the following commands:

```
CLI network-admin@switch > aaa-tacacs-create name TACserver1 scope local port 33 p@ssw0rd
```

To add the authentication method, MS-CHAP, use the following command:

```
CLI network-admin@switch > aaa-tacacs-create name TACserver1 authen-method ms-chap
```

aaa-tacacs-delete

This command is used to remove a TACACS+ server from the configuration.

Syntax `aaa-tacacs-delete name` *name-string*

`name` *name-string*	Specify the name of the TACACS+ server to remove from the configuration.

Defaults None.

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage Use this command to remove a TACACS+ server.

Examples To remove the TACACS+ server, TACserver1, use the following command:

```
CLI network-admin@switch > aaa-tacacs-delete name TACserver1
```

aaa-tacacs-modify

This command is used to modify a TACACS+ server configuration on the network.

Syntax `aaa-tacacs-modify`

`name` *`name-string`*	Specify the name of the TACACS service.
Specify one or more of the following options to modify:	
`scope fabric|local`	Specify the scope to apply to the TACACS server.
`server` *`server-string`*	Specify the name of the TACACS server.
`port` *`port-number`*	Specify the port that connects to the server.
`secret secret-string`	Specify the secret (password) to access the server.
`timeout` *`timeout-number`*	Specify the number of seconds for the server to time out a request. The default value is 10 seconds.
`priority` *`priority-number`*	Specify the priority for the server. The priority can be 1 (highest) to X (lowest priority).
`authen|no-authen`	Specify if the server authenticates clients on the network.
`authen-local|no-authen-local`	Specify if the server authentication overrides the local users.
`authen-method pap|chap|ms-chap`	Specify the authentication method for clients. PAP, CHAP, and MS-CHAP are supported methods.
`sess-acct|no-sess-acct`	Specify if you want to use session accounting. The TACACS+ server is notified when a user logs in or out of the network.
`cmd-acct|no-cmd-acct`	Specify if you want to use command accounting. The TACACS+ server is notified when ever a user, including the network administrator, runs a non-show command.
`sess-author|no-sess-author`	Specify if you want to use session authorization. The TACACS+ server configured for session authorization determines if a user can initiate a session on the network after logging in.
`cmd-author|no-cmd-author`	Specify if you want to use command authorization. The TACACS+ server determines if a user can run certain commands on the network.
`acct-local|no-acct-local`	Specify accounting for local users
`author-local|no-author-local`	Specify authorization for local users.
`service` *`service-string`*	Specify the service name used for TACACS+

	requests sent from Netvisor to the TACACS+ server for commands run at the Neetvisor CLI, and the Java, C, and REST APIs. The default value is `shell`.
`service-shell` *service-shell-string*	Specify the service name used for TACACS+ requests sent from Netvisor to the TACACS+ server for commands run from a UNIX shell.
`service-vtysh` *service-vtysh-string*	Specify the service name used for TACACS+ requests sent from Netvisor to the TACACS+ server for commands run from vtysh.

Defaults None.

Access CLI.

History

Version 1.2.1	Command introduced.
Version 2.6.0	The parameters, `acct-local`, `author-local`, `service`, `service-shell`, and `service-vtyesh`, added.

Usage Use this command to modify how a TACACS+ server authenticates and authorizes clients on the network. The TACACS+ can also provide accounting for sessions and commands.

Examples To modify the TACACS+ server, **TACserver1**, and change the secret, **p@ssw0rd**, to m0nk3ys, use the following commands:

```
CLI network-admin@switch > aaa-tacacs-modify name TACserver1 secret @m0nk3ys
```

aaa-tacacs-show

Use this command to display the configuration parameters of the TACACS+ server.

Syntax `aaa-tacacs-show`

`name` *name-string*	Specifies the name of the TACACS service.
`scope fabric|local`	Specifies the scope to apply to the TACACS server.
`server` *server-string*	Specify the name of the TACACS server.
`port` *port-number*	Specifies the port that connects to the server.
`secret` *secret-string*	Specifies the secret (password) to access the server.
`timeout` *timeout-number*	Specifies the number of seconds for the server to time out a request. The default value is 10 seconds.
`priority` *priority-number*	Specifies the priority for the server. The priority can be 1 (highest) to X (lowest priority).
`authen|no-authen`	Specifies if the server authenticates clients on the network.

`authen-local|no-authen-local`	Specifies if the server authentication overrides the local users.
`authen-method pap|chap|ms-chap`	Specifies the authentication method for clients. PAP, CHAP, and MS-CHAP are supported methods.
`sess-acct|no-sess-acct`	Specifies if you use session accounting. The TACACS+ server is notified when a user logs in or out of the network.
`cmd-acct|no-cmd-acct`	Specifies if you use command accounting. The TACACS+ server is notified when ever a user, including the network administrator, runs a non-show command.
`acct-local|no-acct-local`	Specify accounting for local users
`sess-author|no-sess-author`	Specifies if you use session authorization. The TACACS+ server configured for session authorization determines if a user can initiate a session on the network after logging in.
`cmd-author|no-cmd-author`	Specifies if you use command authorization. The TACACS+ server determines if a user can run certain commands on the network.
`author-local|no-author-local`	Specify authorization for local users.
`timed-out yes|no`	Specifies if the server has timed out.
`error-start date/time:yyyy-mm-ddTHH:mm:ss`	Specifies the time of first error.
`num-errors num-errors-number`	Specifies the number of errors.
`errors-logged yes|no`	Specifies if gthe errors are logged or not.
`service` *`service-string`*	Specify the service name used for TACACS+ requests sent from Netvisor to the TACACS+ server for commands run at the Neetvisor CLI, and the Java, C, and REST APIs. The default value is `shell`.
`service-shell` *`service-shell-string`*	Specify the service name used for TACACS+ requests sent from Netvisor to the TACACS+ server for commands run from a UNIX shell.
`service-vtysh` *`service-vtysh-string`*	Specify the service name used for TACACS+ requests sent from Netvisor to the TACACS+ server for commands run from vtysh.

Defaults None.

Access CLI.

History

Version 1.2.1	Command introduced.
Version 2.6.0	The parameters, `acct-local`, `author-local`, `service`, `service-shell`, and `service-vtyesh`, added.

Usage Use this command to display information about a TACACS+ server

Examples To display the information about a TACACS+ server, use the following command:

```
CLI network-admin@switch > aaa-tacacs-show layout vertical
```

aaa-tacacs-status

This command is used to display the status of the TACACS+ service.

Syntax `aaa-tacacs-status name name-string`

`name name-string`	Specify the name of the TACACS service.

Defaults None.

Access CLI

Usage Use this command to display TACACS status.

Examples To display the status of tacacs-service, use the following command:

```
CLI network-admin@switch > aaa-tacacs-status name tacacs-service
```

access-list-create

This command creates an access list for the Router Advertisement (RA) Guard feature.

Syntax `access-list-create name name-string scope local|fabric`

`name name-string`	Specify a name for the access list.
`scope local|fabric`	Specify the scope for the access list.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to create an access list for RA Guard.

Examples To create an access list with the name, **ra-guard-list**, and the scope as **fabric** use the following syntax:

```
CLI network-admin@switch > access-list-create name ra-guard-list scope fabric
```

access-list-delete

This command deletes an access list for the Router Advertisement (RA) Guard feature.

Syntax `access-list-create name name-string`

`name name-string`	Specify a name for the access list.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to delete an access list for RA Guard.

Examples To delete an access list with the name, **ra-guard-list** , use the following syntax:

```
CLI network-admin@switch > access-list-delete name ra-guard-list
```

access-list-show

This command displays access lists for the Router Advertisement (RA) Guard feature.

Syntax `access-list-show name name-string scope local|fabric`

`name name-string`	Specify a name for the access list.
`scope local|fabric`	Specify the scope for the access list.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to display an access list for RA Guard.

Examples To display an access list with the name, **ra-guard-list** , use the following syntax:

```
CLI network-admin@switch > access-list-show name ra-guard-list

  switch       name              scope
  ---------- -----------    -----
  Spine-1    ra-guard-list  local
```

access-list-ip-add

This command adds an IPv6 address to the access list for the Router Advertisement (RA) Guard feature.

Syntax `access-list-ip-add name` *`name-string`* `ip` *`ip-address`*

`name` *`name-string`*	Specify a name for the access list.
`ip` *`ip-address`*	Specify the IPv6 address associated with the access list.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to add an IPv6 IP address to an access list for RA Guard. .

Examples To add an IPv6 address to the access list, **ra-guard-list**, IPv6 address **2001:0db8:85a3:0000:0000:8a2e:0370:7334**, use the following syntax:

```
CLI network-admin@switch > access-list-ip-add name ra-guard-list ip
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

access-list-ip-remove

This command removes an IPv6 address from the access list for the Router Advertisement (RA) Guard feature.

Syntax `access-list-ip-remove name` *`name-string`* `ip` *`ip-address`*

`name` *`name-string`*	Specify the name of the access list.
`ip` *`ip-address`*	Specify the IPv6 address to remove from the access list.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to add an IPv6 IP address to an access list for RA Guard,

Examples To remove an IPv6 address to an access list with the name, **ra-guard-list**,IPv6 address **2001:0db8:85a3:0000:0000:8a2e:0370:7334**, use the following syntax:

```
CLI network-admin@switch > access-list-ip-add name ra-guard-list ip
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

access-list-ip-show

This command displays access list IP addresses for the Router Advertisement (RA) Guard feature.

Syntax `access-list-ip-show name` *`name-string`* `ip` *`ip-address`*

`name` *`name-string`*	Specify a name for the access list.
`ip` *`ip-address`*	Specify the IPv6 address for the access list.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to display IP addresses assigned to an access list for RA Guard.

Examples To display an access list with the name, **ra-guard-list** , use the following syntax:

```
CLI network-admin@switch > access-list-ip-show  name  ra-guard-list

  switch       name             ip
  ----------   -------------   ----------------------------------------
  Spine-1           ra-guard-list   2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

acl-ip-create

Use this command to create an IP address for an Access Control List (ACL). ACLs are rules that you apply to allow or deny access to hosts or IP addresses.

Syntax `acl-ip-create`

`name` *`name-string`*	Specify the name of the ACL.
`action` `permit | deny`	Specify the permission of the ACL as either permit or deny.
`scope` `local|fabric`	Specify the scope of the ACL.
Specify at least one of the following options:	
`src-ip` *`ip-address`*	Specify the source IP address of the ACL.
`src-ip-mask` *`netmask`*	Specify the source IP mask of the ACL.
`dst-ip` *`ip-address`*	Specify the destination IP address of the ACL.
`dst-ip-mask` *`netmask`*	Specify the destination IP mask of the ACL.
Then any of the following options:	
`proto [tcp|udp|icmp|igmp|ip|icmpv6`	Specify the protocol flag filter of the ACL.
`src-port` *`src-port-number`*	Specify the source port number.
`dst-port` *`dst-port-number`*	Specify the destination port number
`vnet` *`vnet-name`*	Specify the name of the VNET.
`bd` *`bridge-domain name`*	Specify the domain name of the bridge.
`vlan` *`vlan-id`*	Specify the VLAN to apply the ACL. This is a numeric value between 0 and 4095.
`port` *`port-number`*	If the scope is local, Specify the switch port of the ACL.

Defaults None

Access CLI

History

Version 1.2.	Command introduced.
Version 2.4	The option, `igmp`, added to the parameter, `protocol`.
Version 2.4.1	The parameter, `vnet`, added.

Usage IP ACLs can be used to filter network traffic. Use this command to create a new IP ACL.

Informational Note: The source or destination IP address/mask of 0.0.0.0/255.255.255.255 means any address.
The source or destination IP address/mask of 208.74.182.229/0.0.0.0 is the same as "host 208.74.182.229" .

Examples This example shows how to create a fabric-wide ACL named MyWebACL allowing HTTP traffic (port 80) from any host to the web server with IP address 208.74.182.229.

```
CLI network-admin@switch > ip-acl-create name MyWebACL action permit scope fabric src-ip
0.0.0.0 src-msk 255.255.255.255 dst-ip 208.74.182.229 dst-msk 0.0.0.0 prot tcp src-port 80
dst-port 80
```

acl-ip-delete

Use this command to delete an ACL from the network configuration.

Syntax `acl-ip-delete name name-string id`

`name name-string`	Specify the name of the ACL.
`id`	Specify the identifier assigned to the ACL.

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage Deletes an ACL from the existing network configuration.

Examples To delete the ACL, `net-traffic`, use the following command:

```
CLI network-admin@switch > acl-ip-delete  net-traffic
```

acl-ip-modify

This command allows you to change an existing ACL rule on the switch.

Syntax `acl-ip-modify`

`name name-string`	Specifies the name of the ACL.
`id id`	Specifies the ID assigned by ONVL to the ACL.
The following parameter is optional:	
`action permit | deny`	Specifies the permission of the ACL to be either permit or deny.
`src-ip ip-address`	Specifies the source IP address of the ACL.
`src-ip-mask netmask`	Specifies the source IP mask of the ACL.
`dst-ip ip-address`	Specifies the destination IP address of the ACL.

`dst-ip-mask` *`netmask`*	Specifies the destination IP mask of the ACL.
Then any of the following options:	
`proto [tcp|udp|icmp| igmp|ip|icmpv6]`	Specifies the protocol flag filter of the ACL.
`src-port` *`src-port-number`*	Specifies the source port number.
`dst-port` *`dst-port-number`*	Specifies the destination port number
`vnet` *`vnet-name`*	Specify the name of the VNET.
`bd` *`bridge-domain name`*	Specify the domain name of the bridge.
`vlan` *`vlan-id`*	Specifies the VLAN to apply the ACL. This is a numeric value between 0-4095.
`port` *`port-number`*]	If the scope is local, specifies the switch port of the ACL.

Defaults None.

Access network-admin

History

Version 1.2	Command introduced.
Version 2.3.0	Added the parameters to modify the ACL.
Version 2.4	The option, `igmp`, added to the parameter, `protocol`.
Version 2.4.1	The parameter, `vnet`, added.

Usage Use this command to modify an existing IP ACL.

Informational Note: The source or destination IP address/mask of 0.0.0.0/255.255.255.255 means any address.
The source or destination IP address/mask of 208.74.182.229/0.0.0.0 is the same as "host 208.74.182.229" .

Examples To modify the ACL, `net-traffic`, from `deny` to `permit`, use the following command:

```
CLI network-admin@switch > acl-ip-modify net-traffic action permit
```

acl-ip-show

Use this command to display information about ACLs configured on the switch.

Syntax `acl-ip-show`

`name` *`name-string`*	Specifies the name of the ACL.
`id`	Species the ID assigned to the ACL.

`action permit | deny`	Specifies the permission of the ACL to be either permit or deny.
`scope local|fabric`	Specifies the scope of the ACL.
`src-ip` *`ip-address`*	Specifies the source IP address of the ACL.
`src-ip-mask` *`netmask`*	Specifies the source IP mask of the ACL.
`dst-ip` *`ip-address`*	Specifies the destination IP address of the ACL.
`dst-ip-mask` *`netmask`*	Specifies the destination IP mask of the ACL.
`protocol [tcp|udp|icmp|igmp|ip|icmpv6`	Specifies the protocol flag filter of the ACL.
`src-port` *`src-port-number`*`]`	Specifies the source port number.
`dst-port` *`dst-port-number`*	Specifies the destination port number
`vnet` *`vnet-name`*	Specify the name of the VNET.
`bd` *`bridge-domain name`*	Specify the bridge domain name assigned to the ACL.
`vlan` *`vlan-id`*	Specifies the VLAN (0-4095) to apply the ACL.
`port` *`port-number`*	If the scope is local, specifies the switch port of the ACL.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.3.0	Added the parameters to modify the ACL.
Version 2.4	The option, `igmp`, added to the parameter, `protocol`.
Version 2.4.1	The parameter, `vnet`, added.

Usage Displays the list of IP ACLS in the configuration. .

Informational Note: The source or destination IP address/mask of 0.0.0.0/255.255.255.255 means any address.
The source or destination IP address/mask of 208.74.182.229/0.0.0.0 is the same as “host 208.74.182.229” .

Examples This example shows how to display all IP ACLs.

```
CLI network-admin@switch > acl-ip-show
```

```
name  id  action  prot  sip  smsk  sprt  dip  dmsk  dprt  vlan  scope  unit  slot  p
ort

test1 54147812341841995 deny udp 192.192.100.100 0.0.0.0 20 192.168.1.100

0.0.0.0 40 0 local 0 0 0


test2 54147812341841996 deny udp 192.192.100.100 0.255.255.255 20

192.168.1.100 0.0.255.255 40 0 local 0 0 0
```

acl-mac-create

This command is used to create Access Control Lists (ACLs) based on MAC addresses.

Syntax `acl-mac-create`

`name` *`name-string`*	Specifies the name of the ACL.
`action permit|deny`	Specifies the permission of the ACL to be either permit or deny.
`src-mac` *`mac-address`*	Specifies the source MAC address of the ACL. The value can be any to match all MAC addresses
`src-mac-mask` *`mac-address`*	Specifies the source MAC address mask.
`dst-mac` *`mac-address`*	Specifies the destination MAC address of the ACL. The value can be any to match all MAC addresses.
`dst-mac-mask` *`mac-address`*	Specifies the destination MAC address mask.
`ether-type ipv4|arp|wake|rarp|vlan| ipv6|lacp|mpls-uni|mpls-multi|jumbo| dot1X|aoe|lldp|qinq|macsec|ecp| ptp|fcoe|fcoe-init|qinq-old`	Specifies the EtherType value.
`vnet` *`vnet-name`*	Specify the name of the VNET.
`bd bridge-domain name`	Specify the bridge domain name assigned to the ACL.
`vlan` *`vlan-id`*	Specifies the VLAN identifier, a value between 0-4095.
`scope local|fabric`	Specifies the scope of the ACL.
`port` *`port-number`*	Specifies the switch port number.

Defaults None

Access CLI

History

Version 1.2.1	Command introduced.
Version 2.4.1	The parameter, `vnet`, added.

Usage MAC access control lists (ACLs) can be used to filter network traffic. This command creates a new ACL.

Examples This example shows how to create a fabric-wide ACL named `MyMacACL` allowing IPv4 traffic from the host with the MAC address `e0:f8:47:14:3c:2e` to any host.

```
CLI network-admin@switch > mac-acl-create name MyMacACL action permit scope fabric src
e0:f8:47:14:3c:2e dst any type ipv4
```

acl-mac-delete

This command is used to delete an existing MAC ACL from the switch.

Syntax `acl-mac-delete name` *`name-string`* `id` *`acl-id`*

`name` *`string`*	Specify the name of the ACL to delete.
`id` *`acl-id`*	Specify the ACL identifier. This is automatically generated by ONVL.

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage MAC access control lists (ACLs) can be used to filter network traffic. This command deletes an existing MAC ACL.

Examples To delete the MAC ACL named `MyMacACL`, use the following command:

```
CLI network-admin@switch > acl-mac-delete name MyMacACL
```

acl-mac-modify

This command is used to modify Access Control Lists (ACLs) based on MAC addresses.

Syntax `acl-mac-modify name` *`name-string`*

Defaults

`name name` *`string`*	Specifies the name of the ACL.
`id`	Specifies the ID associated with the ACL.
Specify one or more of the following options:	
`action permit|deny`	Specifies the permission of the ACL to be either permit or deny.
`src-mac` *`mac-address`*	Specifies the source MAC address of the ACL. The value can be any to match all MAC addresses
`src-mac-mask` *`mac-address`*	Specifies the source MAC address mask.
`dst-mac` *`mac-address`*	Specifies the destination MAC address of the ACL. The value can be any to match all MAC addresses.
`dst-mac-mask` *`mac-address`*	Specifies the destination MAC address mask.
`ether-type ipv4|arp|wake|rarp|vlan|ipv6|mpls-uni|mpls-multi|jumbo|aoe|dot1X|lldp|lacp|ecp|macsec|ptp|fcoe|fcoe-init|qinq-old`	Specifies the EtherType value.
`vnet` *`vnet-name`*	Specify the name of the VNET.
`bd bridge-domain name`	Specifies the bridge domain name assigned to the ACL

vlan *vlan-id*	Specifies the VLAN identifier.
scope local|fabric|cluster	Specifies the scope of the ACL.
port *port-number*	Specifies the switch port number.

Defaults None

Access CLI

History

Version 1.2.1	Command introduced.
Version 2.4.1	The parameter, vnet, added.
Version 2.5.2	The parameter, scope local|fabric|cluster, deprecated.

Usage MAC access control lists (ACLs) can be used to filter network traffic. This command modifies a new ACL.

Examples This example shows how to modify a fabric-wide ACL named MyMacACL allowing IPv4 traffic from the host with the MAC address e0:f8:47:14:3c:2e to any host.

```
CLI network-admin@switch > mac-acl-modify name MyMacACL action permit scope fabric src
e0:f8:47:14:3c:2e dst any type ipv4
```

acl-mac-show

Displays information about the ACLs using MAC addresses as a parameter.

Syntax acl-mac-show

name *name-string*	Specifies the name of the ACL.
id	Specifies the ID generated by ONVL.
action permit|deny	Specifies the permission of the ACL to be either permit or deny.
src-mac *mac-address*	Specifies the source MAC address of the ACL. The value can be any to match all MAC addresses
src-mac-mask *mac-address*	Specifies the source MAC address mask.
dst-mac *mac-address*	Specifies the destination MAC address of the ACL. The value can be any to match all MAC addresses.
dst-mac-mask *mac-address*	Specifies the destination MAC address mask.
ether-type ipv4|arp|wake|rarp|vlan| ipv6|mpls-uni|mpls-multi|jumbo|aoe| dot1X|lldp|lacp|ecp|macsec|ptp|fcoe| fcoe-init||qinq-old	Specifies the EtherType value.
vnet *vnet-name*	Specify the name of the VNET.
bd *bridge-domain name*	Specify the bridge domain name assigned to the ACL.

`vlan` *`vlan-id`*	Specifies the VLAN identifier, a value between 0-4095.
`scope local|fabric`	Specifies the scope of the ACL.
`port` *`port-number`*	Specifies the switch port number.

Defaults None

Access CLI

History

Version 1.2.1	Command introduced.
Version 2.4.1	The parameter, `vnet`, added.
Version 2.5.2	The parameter, `cluster`,deprecated.

Usage MAC access control lists (ACLs) filter network traffic. This command displays a list of MAC ACLs.

Examples This example shows how to list all MAC ACLs.

```
CLI network-admin@switch > acl-mac-show

name       id                  action   src                   dst   type                 vlan   scope
--------    ---------------    ------    -----------------    --------------------      -----  -----
MyMacACl 54147812341841957 deny     e0:f8:47:14:3c:2e ff:ff:ff:ff:ff:ffipv4    0       local   0
```

admin-service-modify

This command is used to modify the services on the switch.

Syntax `admin-service-modify`

`if` *`if-string`*	Specify the interface to modify.
Specify one or more of the following options:	
`ssh|no-ssh`	Specify if you want to connect to the switch using Secure Shell (SSH).
`nfs|no-nfs`	Specify if you want to use Network Files System (NFS) for the admin service.
`web|no-web`	Specify if you want to enable Web management.
`web-ssl|` `no-web-ssl`	Specify if you want to use SSL and certificates for Web services.
`web-ssl-port` *`web-ssl-port-number`*	Specify the Web SSL port.
`web-port` *`web-port-number`*	Specify the port for Web management.
`web-log|no-web-log`	Specify if you want to turn on or off Web logging.
`snmp|no-snmp`	Specify if SNMP is allowed as a service.
`net-api|no-net-api`	Specify if APIs are allowed as a service.
`icmp|no-icmp`	Specify if Internet Control Message Protocol (ICMP) is allowed as a service.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 3.0.0	The parameter, `web-log|no-web-log`, added.

Usage Use this command to modify the administrative services on the switch.

Examples To modify the admin service to enable SNMP, use the following command:

```
CLI network-admin@switch > admin-service-modify if eth.0 scope fabric snmp
```

admin-service-show

This command is used to display information about admin services configuration.

Syntax `admin-service-show`

if *if-string*	Specifies the interface.

ssh|no-ssh	Specifies if the switch is running Secure Shell (SSH) as a service.
nfs|no-nfs	Specifies if the switch is running Network File System (NFS) as a service.
web|no-web	Specifies if Web is running as a service.
web-ssl|no-web-ssl	Specifies if SSL and certificates are used for Web services.
web-ssl-port *web-ssl-port-number*	Specifies the Web SSL port.
web-port *web-port-number*	Specifies the port for Web management.
web-log|no-web-log	Specify if you want to turn on or off Web logging.
snmp|no-snmp	Specifies if SNMP is running as a service.
net-api|no-net-api	Specifies if APIs are running as a service.
icmp|no-icmp	Specifies if Internet Control Message Protocol (ICMP) is running as a service.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 3.0.0	The parameter, web-log|no-web-log, added.

Usage Use this command to display information about admin services on the switch.

Examples To display admin service information, use the following command:

```
CLI network-admin@switch > admin-service-show

switch       if    ssh nfs web web-ssl web-ssl-port web-port web-log snmp net-api icmp
------------ ---- --- --- --- ------- ------------ -------- ------- ---- ------- ----
draco-dev01 mgmt on   on   on   off      443           80        off      off   on       on
draco-dev01 data on   on   on   off      443           80        off      off   on       on
```

admin-session-timeout-modify

Modify administrator timeouts for login sessions.

Syntax `admin-session-timeout-modify timeout duration:#d#h#m#s`

`timeout duration:#d#h#m#s`	Configure the maximum time to wait for user activity before terminating the login session.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to configure administrator session timeouts.

Examples To set the session timeout to five minutes, use the following syntax:

```
CLI network-admin@switch > admin-session-timout-modify timeout 5m
```

admin-session-timeout-show

Display the session timeout for administrator sessions.

Syntax `admin-session-timeout-show`

`timeout duration:#d#h#m#s`	Configure the maximum time to wait for user activity before terminating the login session.

Defaults None

Access Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to display administrator sessions timeouts.

Examples To display the session timeout, use the following syntax:

```
CLI network-admin@switch > admin-session-timeout-show
```

admin-sftp-modify

This command allows you to modify SFTP functionality for the network administrator.

Syntax `admin-sftp-modify enable|disable`

Defaults Disabled.

Access CLI

History Command introduced in Version 1.2.

Usage Use this command to enable or disable secure file transport protocol (SFTP).

Examples To enable SFTP, use the following command:

```
CLI network-admin@switch > admin-sftp-modify  enable

  sftp  password:
```

Enter a password for the SFTP server.

admin-sftp-show

This command allows you to display SFTP functionality for the administrator.

Syntax `admin-sftp-show`

Defaults None

Access CLI

History Command introduced in Version 1.2.

Usage Use this command to display SFTP functionality on the switch.

Examples Use the following command to display SFTP,

```
CLI network-admin@switch > admin-sftp-show

  switch:           pleiades24
  sftp-user:        sftp
```

admin-syslog-create

This command is used to create the scope and other parameters of syslog event collection.

Syntax `admin-syslog-create`

`name` *`name-string`*	The name of the syslog file for the syslog event collection.
`scope local|fabric`	The scope of the syslog for the syslog event collection.
`host` *`host-string`*	The host name for the syslog event collection..
`port` *`port-number`*	The port for the syslog event collection.
`transport tcp-tls|udp`	The type of transport for log events - `tcp/tls` or `udp`
`message-format structured|legacy`	The message format you want to use in the syslog event collection. The default format is legacy.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.5	The parameter, `transport`, added.

Usage Used to create a syslog file.

Examples To create the syslog file, `engoct12`, with the scope `local` on port `24` and message format `structured`, use the following command:

```
CLI network-admin@switch > admin-syslog-create name engoct12 scope local port 24 message-format structured
```

admin-syslog-delete

This command is used to delete a syslog from the configuration.

Syntax `admin-syslog-delete`

name *name-string*	Specify the name of the syslog file to delete.

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.

Usage Used to delete a syslog file.

Examples To delete the syslog file, `eng-local`, use the following command:

```
CLI network-admin@switch > admin-syslog-delete  eng-local
```

admin-syslog-modify

This command is used to modify the scope and other parameters of syslog event collection.

Syntax `admin-syslog-modify`

name *name-string*	Specify the name of the syslog file to modify.
Specify one or more of the following options:	
`scope local|fabric`	Specify the scope of the syslog to modify
host *host-string*	Specify the host to modify.
port *port-number*	Specify the port you want to modify.
`transport tcp-tls|udp`	The type of transport for log events - `tcp/tls` or `udp`
`message-format structured|legacy`	Specify the message format you want to modify.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.5	The parameter, `transport`, added.

Usage Used to modify an existing syslog file.

Examples To modify the port from port 24 to port 83 for syslog file, `engoct12`, use the following command:

```
CLI network-admin@switch > admin-syslog-modify name engoct12 port 83
```

admin-syslog-show

This command is used to display parameters about a syslog file.

Syntax `admin-syslog-show`

`name` *`name-string`*	Specifies the name of the syslog file.
`scope local|fabric`	Specifies the scope of the syslog file.
`host` *`host-string`*	Specifies the host for the syslog file.
`port` *`port-number`*	Specifies the port for the syslog file.
`transport tcp-tls|udp`	The type of transport for log events - `tcp/tls` or `udp`
`message-format structured|legacy`	Specifies the message format for the syslog file.
`status` *`status-string`*	Specifies the syslog export status

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.5	The parameter, `transport`, added.

Usage Use this command to display information about a syslog file.

Examples Use this command to display administrative log information.

```
CLI network-admin@switch > admin-syslog-show

  switch    name    scope host      port message-format
  --------- ------ ----- -------- ---- --------------
  pubdev01 syslog local pubdev01 25    legacy
```

admin-syslog-match-add

This command is used to search a syslog file for specific events logged to it.

Syntax `admin-syslog-match-add`

`syslog-name`*`name-string`*	Specify the name of the syslog file to use for matching an event or adding an event.
Specify the following match arguments:	
name *`name-string`*	Specify the name of the log file.
Specify any of the following options:	
`msg-category event|audit|system|perror|container|os-logs`	Specify the category of the message to match or add in the systlog file.
`msg-program` *`program-string`*	Specify the name of the program used to generate log messages.
`msg-name` *`name-string`*	Specify the type of message to match or add.
`msg-code` *`code-number`*	Specify the message code to match or add.
`msg-level critical|error|warn|note`	Specify the message level to match or add.
`msg-event-type system|port|tcp|stp|igmp| lldp||lacp|vdp|ecp|evb|ptp|openflow|storage| tacacs|openstack|mld| mroute|vport|lacp-port-event`	Specify the type of event to match or add.
`msg-vnet` *`vnet-name`*	Specify the name of a VNET to match or add.
`msg-remote-switch node` *`name`*	Specify the name of a remote switch node to match or add.
`msg-user` *`user-name`*	Specify user name to match or add.
`msg-client-addr ip-address`	Specify the client IP address.
`msg-port` *`port-number`*	Specify the port to match or add.
`msg-vlan` *`vlan-id`*	Specify the VLAN ID to match or add.
`msg-bd` *`bridge-domain name`*	Specify the bridge domain to match.

`msg-vxlan` *`vxlan-name`*	Specify the VXLAN name to match or add.
`msg-args` *`args-string`*	Specify a message argument to match or add.
`msg-starting-point` *`starting-point-number`*	Specify a starting point number for a message.
`msg-length` *`length-number`*	Specify the length of a message.
`msg-show-time` *`show-time-string`*	Specify the time the message appeared.
`msg-since-last-reset|no-msg-since-last-reset`	Specify the messages since the last reset.
`set-facility kern|user|mail|daemon|auth| syslog|lpr|news|uucp|clock|security|ftp|ntp| audit|alert|cron|local0|local1|local2| local3|local4|local5|local6|local7|0..23`	Specify the facility type to match or add.
`set-severity emerg|alert|crit|err|warning| notice|info|debug|0..7`	Specify the severity of the event to match or add.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.3	The parameters, `mld` and `mroute`, added.
Version 2.3.3	The parameter, `vport`, added to message event type.

Usage Use this command to search a syslog file and match on a certain keyword.

Examples To add the message level `critical`, in the syslog file, `logevents-aug13`, use the following command:

```
CLI network-admin@switch > admin-syslog-match-add syslog-name logevents-aug13 msg-level
critical
```

admin-syslog-match-modify

This command is used to modify a syslog file for specific events logged to it.

Syntax `admin-syslog-match-modify`

`syslog-name` *`name-string`*	The name of the syslog file to use for matching an event or adding an event.
Specify the following match arguments:	

`name` *`name-string`*	Specify the name of the syslog file.
Specify any of the following options:	
`msg-category event|audit|system|perror|container|os-logs`	The category of the message to match or add in the systlog file.
`msg-program` *`program-string`*	The name of the program used to generate log messages.
`msg-name` *`name-string`*	The type of message to match or add.
`msg-code` *`code-number`*	The message code to match or add.
`msg-level critical|error| warn|note`	The message level to match or add.
`msg-event-type systm|port|tcp|stp|igmp|lldp| lacp|vdp|ecp|evb|ptp| openflow|storage|tacacs|openstack|mld|mroute| vport|lacp-port-event`	The type of event to match or add.
`msg-vnet` *`vnet-name`*	The name of a VNET to match or add.
`msg-remote-switch node` *`name`*	The name of a remote switch node to match or add.
`msg-user` *`user-name`*	User name to match or add.
`msg-client-addr` *`ip-address`*	The client IP address to match.
`msg-port` *`port-number`*	The port to match or add.
`msg-vlan` *`vlan-id`*	The VLAN ID to match or add.
`msg-bd` *`bridge-domain name`*	The bridge domain name to match.
`msg-vxlan` *`vxlan-name`*	The VXLAN name to match or add.
`msg-args` *`args-string`*	Specify a message argument to match or add.
`msg-starting-point` *`starting-point-number`*	Specify a starting point number for a message.
`msg-length` *`length-number`*	Specify the length of a message.
`msg-reverse|no-msg-reverse`	Specify if the message is reversed or not.
`msg-show-time` *`show-time-string`*	The time the message appeared.

`msg-since-last-reset|no-msg-since-last-reset`	Messages since the last reset log.
`set-facility kern|user|mail|daemon|auth|syslog|lpr|news|uucp|clock|security|ftp|ntp|audit|alert|cron|local0|local1|local2|local3|local4|local5|local6|local7|0..23`	The facility type to match or add.
`set-severity emerg|alert|crit|err|warning|notice|info|debug|0..7`	The severity of the event to match or add.

Access CLI

History

Version 1.2	Command introduced.
Version 2.3	The parameters, `mld` and `mroute`, added.
Version 2.3.3	The parameter, `vport`, added to message event type.

Usage Use this command to modify a search term for a syslog file and match on a certain keyword.

Examples To modify the syslog to capture messages with the level `critical`, in the syslog file, `logevents-aug13`, use the following command:

```
CLI network-admin@switch > admin-syslog-match-modify syslog-name logevents-aug13 msg-level
critical
```

admin-syslog-match-remove

This command is used to remove a syslog file from the syslog match string.

Syntax `admin-syslog-match-remove syslog-name` *`name-string`* `name` *`name-string`*

`syslog-name` *`name-string`*	The name of the syslog file to remove from the matching string
Specify the following match arguments:	
`name` *`name-string`*	Specify the name of the match.

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.

Usage Use this command to remove a syslog match parameter.

Examples To remove the syslog file, **june2012**, from the matching string, use the following command:

```
CLI network-admin@switch > admin-syslog-match-remove  june2012
```

admin-syslog-match-show

This command is used to display a syslog file for specific events logged to it.

Syntax `admin-syslog-match-show`

`syslog-name` *`name-string`*	Displays the name of the syslog file to use for matching an event or adding an event.
And the following match arguments:	
`msg-category event|audit|system|perror|container|os-logs`	Displays the category of the message to match or add in the systlog file.
`msg-program` *`program-string`*	Displays the name of the program used to generate log messages.
`msg-pid pid-number`	Displays the product ID generating log messages to match
`msg-name` *`name-string`*	Displays the type of message.
`msg-code` *`code-number`*	Displays the message code.
`msg-level critical|error| warn|note`	Displays the message level.
`msg-event-type systm|port|tcp|stp|igmp| lldp|lacp|vdp|ecp|evb|ptp| openflow|storage|tacacs|openstack|mld| mroute| vport|lacp-port-event`	Displays the type of event.
`msg-vnet` *`vnet-name`*	Displays the name of a VNET.
`msg-remote-switch node` *`name`*	Displays the name of a remote switch node.
`msg-user` *`user-name`*	Displays the user name.
`msg-client-pid client-pid-numbe`	Displays the product ID to match.
`msg-client-pid` *`client-pid-number`*	Displays the client product ID.

`msg-client-addr` *`ip-address`*	Displays the client IP address.
`msg-port` *`port-number`*	Displays the port.
`msg-vlan` *`vlan-id`*	Displays the VLAN ID.
`msg-bd bridge-domain name`	Displays the bridge domain to match.
`msg-vxlan` *`vxlan-name`*	Displays the VXLAN name.
`msg-start-time date/time:` *`yyyy-mm-ddThh:mm:ss`*	Displays the start time of the messages.
`msg-end-time date/time:` *`yyyy-mm-ddThh:mm:ss`*	Displays the end time of the messages.
`msg-duration duration:` *`#d#h#m#s`*	Displays the duration of the messages.
`msg-count` *`number`*	Displays the message count from 1 to 50000.
`msg-starting-point starting-point-number`	Displays the starting point of the messages.
`msg-length` *`length-number`*	Displays the length of the messages.
`msg-reverse|no-msg-reverse`	Displays if the messages are reversed or not.
`msg-since-last-reset|no-msg-since-last-reset ]`	Displays the messages since the log reset.
`name` *`name-string`*	Displays the name.
`set facility kern|user|mail|daemon| auth|syslog|lpr|news|uucp|clock| security|ftp|ntp|audit|alert|cron| local0|local1|local2|local3|local4| local5|local6|local7|0..23`	Displays the facility type.
`set severity emerg|alert|crit|err| warning|notice|info|debug|0..7`	Displays the severity of the event to match or add.

Defaults None

Access CLI

History

Version 1.2	Command introduced.

Version 2.3	The parameters, `mld` and `mroute`, added.
Version 2.3.3	The parameter, `vport`, added to message event type.

Usage Use this command to display search terms for a syslog file.

Examples To display the search terms for syslog file, **logevents-aug13**, use the following command:

```
CLI network-admin@switch > admin-syslog-match-show  syslog  logevents-aug13
```

api-install

This command is used to install Netvisor OS on a Linux platform and use the API associated features.

Syntax `api-install linux-host` *`linux-host-string`* `user` *`user-string`*

`linux-host` *`linux-host-string`*	Specify the name of the Linux host.
`user` *`user-string`*	Specify the user login for the Linux host.

Defaults None

Access CLI

History Command introduced in Version 2.2.

Usage Use this command to install the nvOS or ONVL API on a Linux platform.

Examples To install the nvOS or ONVL API on the Linux host, `centos-root`, and the user `root`, use the following syntax:

```
CLI network-admin@switch > api-install linux-host centos-server user root
```

alert-show

This command is used to display alerts for system issues

Syntax `alert-show [level critical]`

`level critical`	Specifies the alert level.

Defaults None

Access CLI

History Command introduced in Version 2.5.4

Usage Use this command to display alerts for system issues.

```
CLI network-admin@switch > alert-show
```

B Commands

bezel-portmap-show

This port is used to display physical to logical port mapping on the Dell platform. All port are 40G ports that can be split into 4 logical 10G ports.

Syntax `bexel-portmap-show port port bezel-intf number`

`port port`	Specify a logical port.
`bezel-intf number`	Specify an interface number.

Defaults None

Access network-admin

Usage Use this command to display the physical to logical port mapping on a Dell platform.

Examples To display port mapping on the Dell platform, use the following syntax:

```
CLI network-admin@switch > bezel-portmap-show

  switch   port  bezel-intf
  -------  ----  ----------
  s6000-2 1     1
  s6000-2 2     1.2
  s6000-2 3     1.3
  s6000-2 4     1.4
  s6000-2 5     2
  s6000-2 6     3
  s6000-2 7     3.2
  s6000-2 8     3.3
  s6000-2 9     3.4
  s6000-2 10    4
  s6000-2 11    5
  s6000-2 12    5.2
  s6000-2 13    5.3
  s6000-2 14    5.4
  s6000-2 15    6
  s6000-2 16    7
  s6000-2 17    7.2
  s6000-2 18    7.3
  s6000-2 19    7.4
```

From the output above, you can determine that port 1 has no cables connected to it. However port 2, has a 40G cable connected to another switch on the network. This is indicated by a single port number instead of 4 port numbers.

bootenv-activate-and-reboot

This command allows you to activate a boot environment and reboot it.

Syntax `bootenv-activate-and-reboot name` *`name-string g`* `apply-current-config|no-apply-current-confi`

`name` *`name-string`*	The name of the boot environment to activate.
`apply-current-config|no-apply-current-config`	Specify if you want to apply the current configuration after rebooting the switch.

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage Use this command to activate a boot environment.

Examples To activate an environment called, `backup`, and reboot it, use the following command:

```
CLI network-admin@switch > bootenv-activate-and-reboot name backup
```

bootenv-delete

This command is used to delete a boot environment from the switch.

Syntax `bootenv-delete name` *`name-string`*

`name` *`name-string`*	The name of the boot environment to delete.

Defaults None

Access CLI.

History Command introduced in nvOS Version 1.2.1.

Usage Use the command to remove stale boot environments from the platform.

Examples To delete the boot environment, **local-boot**, use the following command:

```
CLI network-admin@switch > bootenv-delete local-boot
```

bootenv-show

Display information about the boot environment.

Syntax `bootenv-show [name` *`name-string]`* `[version` *`version-string`* `] [current yes|no] [reboot yes|no]`

`name` *`name-string`*	Specifies the name of the boot environment.
`version` *`version-string`*	Specifies the version of the boot environment.
`current yes|no`	Specifies if the named boot environment is the current boot environment.

`reboot yes|no`	Specifies if the boot environment is set to reboot.
`apply-current-config|no-apply-current-config`	Specify if you want to apply the current configuration after rebooting the switch.

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage Used to display configured information about the boot environment.

Examples To display the boot environment, **local-copy**, in the format layout **horizontal**, use the following command:

```
CLI network-admin@switch > bootenv-show name local-copy layout horizontal

  name          version     current reboot space created
  ------------ ---------- ------- ------ ----- --------------
  ONVL-13 -                  no        no       17.6M 03-19,13:54:51
  ONVL-14 2.3.0-6795       yes       yes     19.8G 03-23,10:47:53
```

bridge-domain-create

bridge-domain-create

A bridge domain is a set of logical ports that share the same flooding or broadcast characteristics. This command creates a bridge domain.

Syntax `bridge-domain-create`

`name` *`name-string`*	Specify the name for the bridge domain.
`scope` *`local|cluster|fabric`*	Specify the bridge domain scope.
Specify any of the following options:	
`vxlan` *`0..16777215`*	Specify the VXLAN identifier for the tunnel.
`auto-vxlan|no-auto-vxlan`	Specify the options to automatically assign VXLAN and/or assign to VTEPs.
`description` *`description-string`*	Add a bridge domain description.
`rsvd-vlan` *`1..4093`*	Specify the fabric reserved VLAN for cluster switches for bridge domain.
`local-rsvd-vlan` *`1..4093`*	Specify the local reserved VLAN for cluster switches for bridge domain.

Defaults None

History Command introduced in nvOS version 5.2.0

Usage Use this command to create a bridge domain.

Examples To create a bridge domain with the name bd100 and cluster scope, use the command:

```
CLI network-admin@switch > bridge-domain-create name bd100 scope cluster
```

bridge-domain-modify

A bridge domain is a set of logical ports that share the same flooding or broadcast characteristics. This command modifies a bridge domain.

Syntax `bridge-domain-modify`

name *name-string*	Specify the name for the bridge domain.
Specify any of the following options:	
rsvd-vlan *1..4093*	Specify the fabric reserved VLAN for cluster switches for bridge domain.
local-rsvd-vlan *1..4093*	Specify the local reserved VLAN for cluster switches for bridge domain.
vnet *vnet-name*	Specify the vNET for this bridge domain.
description *description-string*	Modify the description for the bridge domain.

Defaults None

History Command introduced in nvOS version 5.2.0

Usage Use this command to modify a bridge domain.

Examples To modify the reserved vlan to 25 and the description to main for the bridge domain bd200, use the command:

```
CLI network-admin@switch > bridge-domain-modify name bd200 rsvd-vlan 25 description main
```

bridge-domain-delete

A bridge domain is a set of logical ports that share the same flooding or broadcast characteristics. This command deletes a bridge domain.

Syntax `bridge-domain-delete`

name *name-string*	Specify the name of the bridge domain.

Defaults None

History Command introduced in nvOS version 5.2.0

Usage Use this command to delete a bridge domain.

Examples The command below deletes the bridge domain bd200

```
CLI network-admin@switch > bridge-domain-delete name bd200
```

bridge-domain-show

A bridge domain is a set of logical ports that share the same flooding or broadcast characteristics. This command displays the bridge domain details.

Syntax `bridge-domain-show`

`name` *`name-string`*	Specify the name for the bridge domain.
`scope` *`local`*`|`*`cluster`*`|`*`fabric`*	Specify the bridge domain scope.
`vxlan` *`0..16777215`*	Specify the VXLAN identifier for the tunnel.
`auto-vxlan``|`*`no-auto-vxlan`*	Specify the options to automatically assign VXLAN and/or assign to VTEPs.
`hw-vpn` *`hw-vpn-number`*	Specify the hardware VPN number.
`hw-mcast-group` *`hw-mcast-group-number`*	Specify the hardware multicast group.
`description` *`description-string`*	Sepcify the bridge domain description.
`rsvd-vlan` *`1..4093`*	Specify the fabric reserved VLAN for cluster switches for bridge domain.
`local-rsvd-vlan` *`1..4093`*	Specify the local reserved VLAN for cluster switches for bridge domain.
`net-id` *`0..12287`*	Specify the bridge domain ID.
`peer-net-id` *`0..12287`*	Specify the peer network ID.
`active yes|no`	Specify the bridge domain active status.
`ports` *`port-list`*	Specify the ports assigned to the bridge domain.
`cluster-name` *`cluster-name-string`*	Specify the cluster that needs to use the internal VLANs.
`qinq_rsvd_vlan` *`0..4095`*	Specify the running reserved VLAN for cluster switches for bridge domain.

Defaults None

History Command introduced in nvOS version 5.2.0.

Usage Use this command to display the bridge domain details.

Examples

```
CLI network-admin@switch > bridge-domain-create name bd300
```

bridge-domain-port-add

A bridge domain is a set of logical ports that share the same flooding or broadcast characteristics. This command adds ports to a bridge domain.

Syntax `bridge-domain-port-add`

`name` *`name-string`*	Specify the name of the bridge domain to which the ports are to be added.

Specify any of the following options:	
switch *switch-name*	Specify the name of the switch.
port *port-list*	Specify the ports to be added to the bridge domain.
outer-vlan *1..4093*	Specify the outer VLANs for Q-in-Q.
vlans *vlan-list*	Specify the access VLANs for Q-in-Q.
qinq-untagged-port-vlan *1..4093*	Specify the VLAN for untagged port for Q-in-Q network.
inner-vlan *0..4095*	Specify the inner VLAN for ports assigned to a network.

Defaults None

History Command introduced in nvOS version 5.2.0

Usage Use this command to add ports to a bridge domain.

Examples To add the ports 17 and 18 to the bridge domain bd100, use the command:

```
CLI network-admin@switch > bridge-domain-port-add name bd100 port 17,18
```

bridge-domain-port-remove

A bridge domain is a set of logical ports that share the same flooding or broadcast characteristics. This command removes ports from a bridge domain.

Syntax bridge-domain-port-remove

name *name-string*	Specify the name of the bridge domain from which ports are to be removed.
Specify any of the following options:	
switch *switch-name*	Specify the name of the switch.
port *port-list*	Specify the ports to be removed from the bridge domain.

Defaults None

History Command introduced in nvOS version 5.2.0

Usage Use this command to remove ports from a bridge domain.

Examples To remove the ports 22 and 25 from the bridge domain bd400, use the command:

```
CLI network-admin@switch > bridge-domain-port-remove name bd400 port 22,25
```

bridge-domain-port-show

A bridge domain is a set of logical ports that share the same flooding or broadcast characteristics. This command displays the port information of a bridge domain.

Syntax `bridge-domain-port-show`

`name` *`name-string`*	Specify the name of the bridge domain.
Specify any of the following port arguments:	
`switch` *`switch-name`*	Specify the name of the switch.
`port` *`port-list`*	Specify the ports to be added to the bridge domain.
`active-ports` *`port-list`*	Specify the active ports.
`outer-vlan` *`1..4093`*	Specify the outer VLANs for Q-in-Q.
`vlans` *`vlan-list`*	Specify the access VLANs for Q-in-Q.
`qinq-untagged-port-vlan` *`1..4093`*	Specify the VLAN for untagged port for Q-in-Q network.
`inner-vlan` *`0..4095`*	Specify the inner VLAN for ports assigned to a network.

Defaults None

History Command introduced in nvOS version 5.2.0

Usage Use this command to display the port details of a bridge domain.

Examples To display the details of the bridge domain bd100, use the command:

```
CLI network-admin@switch > bridge-domain-port-show name bd100
```

bridge-domain-check-maps

A bridge domain is a set of logical ports that share the same flooding or broadcast characteristics. This command displays the bridge domain maps.

Syntax `bridge-domain-check-maps`

Defaults None

History Command introduced in nvOS version 5.2.0.

Usage Use this command to display the bridge domain maps.

Examples

```
CLI network-admin@switch > bridge-domain-check-maps
```

C Commands

cert-create

This command is used to create a self-signed server certificate

Syntax `cert-create name *name-string* country *country-string* state *state-string* city *city-string* organization *organization-string* organizational-unit *organizational-unit-string* common-name *common-name-string* container *zone*|*name*`

name *name-string*	Specify the name of the certificate.
country *country-string*	Specify the country name (2 letter code).
state *state-string*	Specify the state or province name.
city *city-string*	Specify the city name.
organization *organization-string*	Specify the organization name.
organizational-unit *organizational-unit-string*	Specify the organizational unit name.
common-name *common-name-string*	Specify the common name.
container *zone name*	Specify the certificate zone or name.

Defaults None

Access CLI

History Command introduced in Version 2.5.4.

Usage Use certificates to secure server connections.

Examples To create a self-signed server certificate named **cert1**, use the following command:

```
CLI network-admin@switch > CLI cert-create name cert1 country US state CA city PA organization
ovs organizational-unit ou common-name Pluribus


  Successfully generated self-signed certificate.
```

cert-delete

This command is used to delete certificates container *zone*|*name*

Syntax `cert-delete name *name-string*`

name *name-string*	Specify the name of the certificate to delete.
container *zone name*	Specify the certificate zone or container name.

Defaults None

Access CLI

History Command introduced in Version 2.5.4.

Usage Use this command to delete certificates.

Examples To successfully delete a certificate named cert1, use the following command:

```
CLI network-admin@switch > cert-delete name cert1


  Successfully deleted all certificate files.
```

If you try to delete a certificate currently in use by a service, the following message displays:

```
CLI network-admin@switch > cert-delete name cert1

  cert-delete: Certificate is being used by ovs service, cannot delete
  cert-delete
```

cert-import

This command is used to import CA certificate files from a Simple File Transfer Protocol (SFTP) directory

Syntax `cert-import`

name *name-string*	Specify a certificate name.
file-ca *file-ca-string*	Specify the name of CA certificate file.
file-server *file-server-string*	Specify the file server name.
container *zone name*	Specify a certificate zone name.
file-inter *file-inter-string*	Specify the name of intermediate CA certificate file.

Defaults None

Access CLI

History Command introduced in Version 2.5.4.

Usage You can create one common certificate for all Netvisor services or create multiple named certificates. Each service can use a different certificate identified by name or container name or zone.The Certificate facility keeps track of certificate use by using various applications. It notifies the applications when a certificate is updated and it also prevents a certificate from deletion if an application is using it.

Examples To import a CA certificate named **cert3** from file server **server.pem,** use the following command:

```
CLI network-admin@switch > cert-import name cert3 file-ca ca.pem file-server server.pem


  Successfully imported certificates.
```

cert-request-create

This command is used to create a certificate signing request from an existing server certificate

Syntax `cert-request-create container zone|name`

`name name-string`	Specify the certificate name.
`container zone name`	Specify the certificate zone or container name.

Defaults None

Access CLI

History Command introduced in Version 2.5.4.

Usage

Examples To generate a certificate signing request where the certificate name is **cert3**, use the following command:

```
CLI network-admin@switch > cert-request-create name cert3


  Certificate signing request successfully generated at /sftp/export/cert3-cert.csr.
```

cert-request-show

This command is used to display certificate signing request information.

Syntax `cert-show name`

`name name-string`	Specifies the certificate name.
`container zone name`	Specifies the certificate zone/container name.
`cert-request cert-request-string`	Specifies the certificate signing request.

Defaults None

Access CLI

History Command introduced in Version 2.5.4.

Usage You can display certificate signing request information.

Examples To display the certificate request for **cert3**, use the following command:

```
CLI network-admin@switch > cert-request-show name cert3

  ------------------------------------------------------------------
  -----BEGIN CERTIFICATE REQUEST-----
  MIICnDCCAYQCAQEwVzELMAkGA1UEBhMCdXMxCzAJBgNVBAgMAmNhMQswCQYDVQQH
  DAJtcDELMAkGA1UECgwCcGwxDTALBgNVBAsMBGVuZ2cxEjAQBgNVBAMMCXBsdXJp
  YnVzMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMrE6Jowg0VKUw2M
  NlL8vp1N8dYE/UL5pvu8FKYWgwG7tC2fjHunZCI0XmssFtZysQul/r9nk+edA5tt
  0zIWRmqTB60wnWmzl6uGymeAsC9OSm0ZHFc9zZfUxKjRM/n1dOri3Pw/rODbCjM9
  qwO5hsvZc/c1o3ajYFrj1yMlKDIiPW1td1VTpc5TL6wCwnDM697Yb9oQ0cbLKTDl
  w5AjQSgJK29rLUl8ptAZXIUkeendpE4MCYrl6Hd+ziOJHXncj65MJyfANTZMrtGD
```

```
IJD3m+JsKZt882vMw3AZ3C9WEuE0OZrbabGBHqVKARik2qFhu2bGjlbuj/M6TOf5
Jj1WROUCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4IBAQCh1YhXRNwkwmw3FVH4H0Xi
rczy0FkyHkdSbIUIf+6n3qroRpBpcEdrx8fREyiw8hLUks9OcUlT+nSshsWIitI7
R5dcFlyo5HUVjqQQVMlSq3j4fM9XE8y8KRMZ3mfLXRTmuFPxbBuE3ZGjlBSLnBgK
ODqHF1gVa4u7l9mO3TRXczLQiAPaw38/kxEwkh4erJp4jjXf8K0h9JMGvYONYWeI
1PbiZpjIWDLNbg6sKqqrPAxEAjzGNMgNPIMXRepmEmnC/BaLVA04noZran8LRLNp
Id41o3TnlXiAodF/Mc7H5fI1hYf0YzWDSfz3PNufn6Dusu5M2ma7jtWlEdBW8huH
-----END CERTIFICATE REQUEST----
```

cert-show

This command is used to display certificate information.

Syntax `cert-show`

`name` *`name-string`*	Specifies the certificate name.
`container zone name`	Specifies the certificate zone or container name.
`cert-type ca|intermediate|server`	Specifies the type of certificate: CA, intermediate or server.
`subject` *`subject-string`*	Specifies the certificate subject.
`issuer` *`issuer-string`*	Specifies the issuer of the certificate.
`serial-number` *`serial-number-number`*	Specifies the serial number of the certificate.
`valid-from` *`valid-from-string`*	Specifies the time from which the certificate is valid.
`valid-to` *`valid-to-string`*	Specifies the time at which the certificate expires and is no longer valid.
`country` *`country-string`*	Specifies the country name (2 letter code).
`state` *`state-string`*	Specifies the state or province name.
`city city-string`	Specifies the city name.
`organization` *`organization-strings`*	Specifies the organization name.
`organizational-unit` *`organizational-unit-string`*	Specifies the organization name.
`common-name` *`common-name-string`*	Specifies the common name.
`name` *`name-string`*	Specifies the certificate name.

Defaults None

Access CLI

History Command introduced in Version 2.5.4.

Usage You can display all or specific information for a particular certificate.

Examples To display certificate information, use the following command:

cert-show

```
switch:              switch1
name:                myswitch1
container:           vpod1-mgr
country:             US
state:               California
city:                Palo Alto
organization:        Pluribus Networks Inc
organizational-unit: Engineering
common-name:         myswitch1
cert-type:           server
subject:             /C=US/ST=California/L=Palo Alto/O=Pluribus Networks
Inc/OU=Engineering/CN=myswitch1
issuer:              /C=US/ST=California/L=Palo Alto/O=Pluribus Networks
Inc/OU=Engineering/CN=Pluribus Networks Test CA 2k-sha-
256/emailAddress=example@pluribusnetworks.com
serial-number:       2
valid-from:          Apr 20 18:28:45 2017 GMT
valid-to:            Apr 20 18:28:45 2018 GMT
```

client-server-stats-clear

This command is used to clear statistics generated between a client and server on the network.

Syntax `client-server-stats-clear`

Specify any of the following options:	
`time date/time: yyyy-mm-ddThh:mm:ss`	Clear statistics from a specific time period.
`start-time date/time: yyyy-mm-ddThh:mm:ss`	Clear statistics from a specific start time and date.
`end-time date/time: yyyy-mm-ddThh:mm:ss`	Clear statistic from a specific end time and date.
`duration: #d#h#m#s`	Clear statistics for a specific duration.
`interval duration: #d#h#m#s`	Clear statistics for a specific interval duration.
`since-start`	Clear statistics from the start of collection.
`older-than duration: #d#h#m#s`	Clear statistics older than a specified date and time.
`within-last duration: #d#h#m#s`	Clear statistics within a specified duration time.
`count count-number`	Clear the number of counters.
`vlan vlan-id`	Clear statistics for a specific VLAN.
`vxlan vxlan-id`	Clear statistics for a specific VXLAN.
`client-switch-port port-number`	Clear statistics for a specific port number on the client switch.
`server-switch-port port-number`	Clear statistics for a specific port number on the

	server switch.
`client-mac` *`mac-address`*	Clear statistics for a specific client MAC address.
`server-mac` *`mac-address`*	Clear statistics for a specific server MAC address.
`client-ip` *`ip-address`*	Clear statistics for a specific client IP address.
`server-ip` *`ip-address`*	Clear statistics for a specific client IP address.
`server-port`	Specifies the type of statistic to clear from the server port. This includes HDFS, Hive, Ganglia, Cassandra, Nutanix and other server types.
`syn` *`syn-number`*	Clear the statistics for SYN packets.
`est` *`est-number`*	Clear the statistics for established connections.
`fin` *`fin-number`*	Clear the statistics for the total number of closed connections.
`obytes` *`obytes-number`*	Specifis the number of outgoing bytes to clear statistics.
`ibytes` *`ibytes-number`*	Specifies the number of incoming bytes to clear statistics.
`total-bytes` *`total-bytes-number`*	Specifies the total bytes to clear statistics.
`avg-dur high resolution time:` *`#ns`*	Clear the average duration of high resolution statistics.
`avg-lat high resolution time:` *`#ns`*	Clear the average latency statistics.
`first-seen date/time:` *`yyyy-mm-ddThh:mm:ss`*	Clear the first-seen statistics only.
`last-seen date/time:` *`yyyy-mm-ddThh:mm`*	Clear the last-seen statistics only.

Defaults None

Access CLI

History

Version 2.0	Command introduced.
Version 2.1	The parameters, `timestamp`, `start-time`, `end-time`, `duration`, `interval`, `since-start`, `older-than`, and `within-last` added to the command. The options, `openstack-nova|openstack-keystone| openstack-metering| openstack-neutron |openstack-glance|openstack-cinder,` added to the parameter, `server-port`.
Version 2.2	The parameter, `no-since-start`, deprecated.
Version 2.2.5	The parameters, `HDFS-`, added.
Version 2.2.6	The parameters, `MR`, `HBase`, `Ganglia`, `Cassandra`,

	and Nutanix added to server-port.

Usage You can clear all statistics for a client server connection or you can use a filter to clear specific statistics.

Examples To clear statistics for VLAN12, use the following command:

```
CLI network-admin@switch > client-server-stats-clear  vlan  12
```

client-server-stats-clear-history

This command is used to clear the history of client and server statistics.

Syntax `client-server-stats-clear-history`

Defaults None

Access CLI

History Command introduced in Version 2.2.3.

client-server-stats-show

This command is used to show statistics generated between a client and server on the network.

Syntax `client-server-stats-show`

timestamp date/time:*yyyy-mm-ddThh:mm:ss*	Clear statistics from a specific timestamp period.
start-time date/time:*yyyy-mm-ddThh:mm:ss*	Clear statistics from a specific start time and date.
end-time date/time:*yyyy-mm-ddThh:mm:ss*	Clear statistic from a specific end time and date.
duration: *#d#h#m#s*	Clear statistics for a specific duration.
interval duration: *#d#h#m#s*	Clear statistics for a specific interval duration.
since-start	Clear statistics from the start of collection.
older-than duration: #d#h#m#s	Clear statistics older than a specified date and time.
within-last duration: #d#h#m#s	Clear statistics within a specified duration time.
count *count-number*	Specifies the number of counters.
vlan *vlan-id*	Specifies statistics for a specific VLAN.
vxlan *vxlan-id*	Specifies statistics for a specific VXLAN.
client-switch-port *port-number*	Specifies statistics for a specific port number on the client switch.
server-switch-port *port-number*	Specifies statistics for a specific port number on the server switch.
client-mac *mac-address*	Specifies statistics for a specific client MAC address.

`server-mac` *`mac-address`*	Specifies statistics for a specific server MAC address.
`client-ip` *`ip-address`*	Specifies statistics for a specific client IP address.
`server-ip` *`ip-address`*	Specifies statistics for a specific client IP address.
`server-port`	Specifies the type of protocol on the server port. This includes HDFS, Hive, Ganglia, Cassandra, Nutanix and other server types.
`syn` *`syn-number`*	Specifies the number of SYN packets.
`est` *`est-number`*	Specifies the number established connections.
`fin` *`fin-number`*	Specifies the total number of closed connections statistics.
`syn-resends` *`syn-resends-number`*	Specifies the number of SYN packet resends.
`syn-ack-resends` *`syn-ack-resends-number`*	Specifies the number of SYN-ACK packet resends.
`obytes` *`obytes-number`*	Specifis the number of outgoing bytes to clear statistics.
`ibytes` *`ibytes-number`*	Specifies the number of incoming bytes to clear statistics.
`total-bytes` *`total-bytes-number`*	Specifies the total bytes to clear statistics.
`avg-dur high resolution time:` *`#ns`*	Specifies the average duration of high resolution statistics.
`avg-lat high resolution time:` *`#ns`*	Specifies the average latency statistics.
`first-seen date/time:` *`yyyy-mm-ddThh:mm:ss`*	Specifies the first-seen statistics only.
`last-seen date/time:` *`yyyy-mm-ddThh:mm`*	Specifies the last-seen statistics only.
`last-seen-ago duration: #d#h#m#s`	Specifies a duration to clear statistics.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.4.1	The parameters, `syn-resends`, and `syn-ack-resends`, added.

Usage You can display all statistics for a client server connection or you can use a filter to display specific statistics.

Examples To display all statistics on switch pleiedes24, use the following command:

```
CLI network-admin@switch > client-server-stats-show  layout  vertical

  switch:              pleiades24
  vlan:                1
  vxlan:               0
  client-ip:            192.171.1.65
  server-ip:            192.171.2.60
  server-port:          ssh
  syn:                  4
  est:                  0
  fin:                  724
  obytes:               1.29M
  ibytes:               2.70M
  total-bytes:          3.99M
  avg-dur:              486ms
  avg-lat:              97.1us
  last-seen-ago:        51m4s
  switch:              pleiedes24
  vlan:                1
  vxlan:               0
  client-ip:            192.171.1.31
  server-ip:            192.171.2.60
  server-port:          ssh
  syn:                  10
  est:                  0
  fin:                  1.60K
  obytes:               2.92M
  ibytes:               6.09M
  total-bytes:          9.01M
  avg-dur:              490ms
  avg-lat:              86.3us
  last-seen-ago:        51m4s
```

cluster-create

To create a new cluster for high availability (HA) in a fabric, use the `cluster-create` command.

	**Informational Note:** You may configure multiple clusters of switches within a single fabric. However, a switch can participate in only one cluster configuration. For example, switch-1 and switch-2 can participate in cluster-1, and switch-3 and switch-4 can participate in cluster-2, but switch-1 and switch-2 cannot participate in cluster-2 or any other cluster.

Syntax `cluster-create name` *`name-string`* `cluster-node-1` *`cluster-node-1`*`cluster-node-2` *`cluster-node-2`* `[validate|no-validate]`

`cluster-name`	Specify the name of the cluster.
`cluster-node-1` *`fabric-node name`*	Specify the name of the first switch in the cluster.
`cluster-node-2` *`fabric-node name`*	Specify the name of the second switch in the cluster.
Any of the following options:	

`validate|no-validate`	Validate the inter-switch links and state of the switches in the cluster.
`cluster-sync-timeout` *`milliseconds`*	Specify the amount of time before a cluster times out during synchronization. Specify a time between 500 and 2000 ms.
`cluster-sync-offline-count` *`number`*	Specify the number of missed synchronizations before the cluster goes offline.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.1	The parameter, `private-link`, added.
Version 2.2	The parameter, `private-link`, deprecated.
Version 3.0.0	The parameters, `cluster-sync-timeout` and `cluster-sync-offline-count` added.

Usage A cluster allows two switches to cooperate in high-availability (HA) deployments. The nodes that form the cluster must be members of the same fabric. Clusters are typically used in conjunction with a virtual link aggregation group (VLAG) that allows links physically connected to two separate switches appear as a single trunk to a third device. The third device can be a switch, server, or any Ethernet device.

Examples To create a cluster named, `cluster_eng`, using an interswitch link or trunk between two cluster nodes, `switch_a` and `switch_b`, and available to other network traffic, use the following command:

```
CLI network-admin@switch > cluster-create name cluster_eng cluster-node-1 switch_a cluster-
node-2 validate
```

cluster-delete

To delete a cluster for high availability (HA) in a fabric, use the `cluster-delete` command.

Syntax `cluster-delete name` *`name-string`*

name *`name-string`*	Specify the name of the cluster.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.1	The parameter, `private-link`, added.
Version 2.2	The parameter, `private-link`, deprecated.

Usage A cluster allows two switches to cooperate in high-availability (HA) deployments. The nodes that form the cluster must be members of the same fabric. Clusters are typically used in conjunction with a virtual link aggregation group (VLAG) that allows links physically connected to two separate switches appear as a single trunk to a third device. The third device can be a switch, server, or any Ethernet device.

Examples To delete a cluster named, `cluster_eng`, use the following command:

```
CLI network-admin@switch > cluster-delete name cluster_eng
```

cluster-info

To view information about clusters in a fabric, use the `cluster-info` command.

> **Informational Note:** You may configure multiple clusters of switches within a single fabric. However, a switch can participate in only one cluster configuration. For example, switch-1 and switch-2 can participate in cluster-1, and switch-3 and switch-4 can participate in cluster-2, but switch-1 and switch-2 cannot participate in cluster-2 or any other cluster.

Syntax `cluster-info`

`cluster-name`	Displays the name of the cluster.
`cluster-node-1`	Displays the name of the first switch in the cluster.
`cluster-node-2`	Displays the name of the second switch in the cluster.
`tid`	Displays the transaction ID.
`ports`	Displays the port used to create the cluster configurarion.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.1	The parameter, `private-link`, added.
Version 2.2	The parameter, `private-link`, deprecated.

Usage A cluster allows two switches to cooperate in high-availability (HA) deployments. The nodes that form the cluster must be members of the same fabric. Clusters are typically used in conjunction with a virtual link aggregation group (VLAG) that allows links physically connected to two separate switches appear as a single trunk to a third device. The third device can be a switch, server, or any Ethernet device.

Examples To display information a cluster named, `vlag`, use the `cluster-info` command:

```
CLI network-admin@switch > cluster-info

  name:                 vlag
```

```
state:               online
cluster-node-1:  167772208
cluster-node-2:  167772196
tid:                 1
ports:               26
```

cluster-modify

To modify a cluster for high availability (HA) in a fabric, use the `cluster-modify` command.

Syntax `cluster-modify`

`name` *`name-string`*	Specify the name of the cluster.
`cluster-sync-timeout` *`milliseconds`*	Specify the amount of time before a cluster times out during synchronization. Specify a time between 500 and 2000 ms.
`cluster-sync-offline-count` *`number`*	Specify the number of missed synchronizations before the cluster goes offline.
`enable|disable`	Enable or disable the cluster configuration.
`stp-mode rstp|mstp`	Specify the STP mode for the cluster.
`bpdus-bridge-ports|bpdus-all-ports`	Specify sending BPDU packets to a specific bridge port.
`bridge-id` *`mac-address`*	Specify the MAC address as the bridge ID.
`bridge-priority` *`number`*	Specify the bridge priority as a multiple of 4096 with a default value of 32768.
`hello-time` *`seconds`*	Specify the hello-time in seconds with a default time of 2 seconds.
`forwarding-delay` *`seconds`*	Specify the forwarding-delay between 4 and 30 seconds with a default time of 15 seconds.
`max-age` *`seconds`*	Specify the maximum age time between 6 and 40 seconds with a default time of 20 seconds.
`mst-max-hops` *`number`*	Specify the maximum hop count for MSTP BPDU packets. The default value is 20 hops.
`mst-config-name` *`mst-config-name-string`*	Specify the name of the MST configuration instance.
`root-guard-wait-time` *`seconds`*	Specify the root guard wait time between 0 and 300 seconds with a default value of 20 seconds. If you set the time to 0, you disable the parameter.

Defaults None

Access CLI

History

Version 1.2	Command introduced.

Version 2.1	The parameter, **private link**, was added.
Version 2.2	Command deprecated.
Version 3.0.0	Command reintroduced with new parameters.

Usage A cluster allows two switches to cooperate in high-availability (HA) deployments. The nodes that form the cluster must be members of the same fabric. Clusters are typically used in conjunction with a virtual link aggregation group (VLAG) that allows links physically connected to two separate switches appear as a single trunk to a third device. The third device can be a switch, server, or any Ethernet device.

Examples To modify a cluster named, `cluster_eng`, , use the following command:

```
CLI network-admin@switch > cluster-modify name cluster_eng cluster-syn-timeout 500ms
```

cluster-show

To display a cluster configuration in a fabric, use the `cluster-show` command.

Syntax `cluster-show`

`name` *`name-string`*	Specifies the name of the cluster.
`cluster-id`	Specifies the ID assigned to the cluster configuration.
`state`	• `offline` • `unavailable` • `online` • `coming-online` • `slave-ready` • `going offline`
`cluster-node-1`	Specifies the name of the first switch in the cluster.
`cluster-node-2`	Specifies the name of the second switch in the cluster.
`tid` *`tid-number`*	Specifies the transaction ID number.
`mode none|master|slave`	Specifies the mode assigned to the cluster.
`ports` *`port-list`*	Specifies the list of ports.
`remote-ports` *`port-list`*	Specifies the list of remote ports.
`validate|no-validate`	Validate the inter-switch links and state of the switches in the cluster.
`cluster-sync-timeout` *`milliseconds`*	Specify the amount of time before a cluster times out during synchronization. Specify a time between 500 and 2000 ms.
`cluster-sync-offline-count` *`number`*	Specify the number of missed synchronizations before the cluster goes offline.
`enable|disable`	Displays if you enabled or disabled STP.

`stp-mode rstp|mstp`	Displays the STP mode.
`bpdus-bridge-ports|bpdus-all-ports`	Displays if the cluster sends BPDU packets to bridge specific ports.
`bridge-id` *`mac-address`*	Displays the MAC address of the bridge.
`bridge-priority` *`bridge-priority-number`*	Displays the bridge priority with a default value of 32768.
`hello-time` *`seconds`*	Displays the hello time in seconds
`forwarding-delay` *`seconds`*	Displays the forwarding time delay in seconds.
`max-age` *`seconds`*	Displays the maximum aging time in seconds.
`mst-max-hops` *`count`*	Displays the number of maximum hops for MSTP BPDUs.
`mst-config-name` *`mst-config-name-string`*	Displays the name of the MST configuration instance.
`mst-config-digest` *`mst-config-digest-string`*	Displays the MST configuration digest.
`cluster-mode none|master|slave`	Displays the STP cluster mode.
`root-guard-wait-time` *`seconds`*	Displays the root guard wait time.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.1	The parameter, `private-link`, added.
Version 2.2	The parameter, `private-link`, deprecated.
Version 2.4	The parameters, `mode` and `remote-ports`, added. The option, `synching`, deprecated. The option, `slave-ready`, and `going-offline` added.
Version 2.4.1	The parameters, `online`, and `unavailable` added.
Version 3.0.0	The parameters, `cluster-sync-timeout` and `cluster-sync-offline-count` added.

Usage Displays information about cluster configurations on the network.

Examples To show information about a cluster configuration, use the following command:

```
CLI network-admin@switch > cluster-show format all layout vertical

  name:                 vlag
  id:                      a000030:1
  state:                online
  cluster-node-1:  pubdev01
  cluster-node-2:  pubdev02
  tid:                  0
  mode:             master
  remote-port:     33,34
  ports:                26,128
```

cluster-membership-modify

To modify a cluster membership for high availability (HA) in a fabric, use the `cluster-membership-modify` command.

Syntax `cluster-membership-modify`

`name` *`name-string`*	Specify the name of the cluster membership.
`cluster-node-1 fabric-node` *`name`*	Specify the name of the first fabric node in the cluster.
`cluster-node-2 fabric-node` *`name`*	Specify the name of the second fabric node in the cluster.

Defaults None

Access CLI

History

Version 2.5.0	Command introduced.
Version 3.0.0	The parameter `validate|no-validate` deprecated.

Usage A cluster allows two switches to cooperate in high-availability (HA) deployments. The nodes that form the cluster must be members of the same fabric. Clusters are typically used in conjunction with a virtual link aggregation group (VLAG) that allows links physically connected to two separate switches appear as a single trunk to a third device. The third device can be a switch, server, or any Ethernet device.

Examples To modify a cluster membership, `cluster_eng`, using an interswitch link or trunk between two cluster nodes, `fabric_a` and `fabric_b`, and is available to other network traffic, use the following command:

```
CLI network-admin@switch > cluster-create name cluster_eng cluster-node-1 fabric_a cluster-
node-2 fabric_b
```

cluster-membership-show

To display a cluster membership for high availability (HA) in a fabric, use the `cluster-membership-show` command.

Syntax `cluster-membership-show`

`switch` *`fabric-node name`*	Displays the switch name.
`name` *`name-string`*	Displays the name of the cluster membership.
`id`	Displays the ID assigned to the cluster.
`state offline|online|unavailable| coming-online|slave-ready|going-offline`	Displays the state of the cluster.
`cluster-node-1` `fabric-node` *`name`*	Displays the name of the first fabric node in the cluster.
`cluster-node-2` `fabric-node` *`name`*	Displays the name of the second fabric node in the cluster.
`tid` *`tid-number`*	Displays the transaction ID assigned to the cluster.
`mode none|master|slave`	Displays the cluster mode.
`ports` *`port-list`*	Displays the list of ports.
`remote-ports` *`port-list`*	Displays the list of remote ports.
`validate|no-validate`	Displays if the cluster link validated.
`cluster-sync-timeout` *`mseconds`*	Displays the cluster synchronization timeout in ms.
`cluster-sync-offline-count` *`number`*	Displays the number of missed timeouts before the cluster goes offline.
`enable|disable`	Displays if you enabled or disabled STP.
`stp-mode rstp|mstp`	Displays the STP mode.
`bpdus-bridge-ports|bpdus-all-ports`	Displays if the cluster sends BPDU packets to bridge specific ports.
`bridge-id` *`mac-address`*	Displays the MAC address of the bridge.
`bridge-priority` *`bridge-priority-number`*	Displays the bridge priority with a default value of 32768.
`hello-time` *`seconds`*	Displays the hello time in seconds
`forwarding-delay` *`seconds`*	Displays the forwarding time delay in seconds.
`max-age` *`seconds`*	Displays the maximum aging time in seconds.
`mst-max-hops` *`count`*	Displays the number of maximum hops for MSTP BPDUs.
`mst-config-name` *`mst-config-name-string`*	Displays the name of the MST configuration instance.
`mst-config-digest` *`mst-config-digest-string`*	Displays the MST configuration digest.
`cluster-mode none|master|slave`	Displays the STP cluster mode.

`root-guard-wait-time` *`seconds`*	Displays the root guard wait time.

Defaults None

Access CLI

History

Version 2.5.0	Command introduced.
Version 3.0.0	The parameter `validate|no-validate` deprecated.

Usage A cluster allows two switches to cooperate in high-availability (HA) deployments. The nodes forming the cluster must be members of the same fabric. Clusters are typically used in conjunction with a virtual link aggregation group (VLAG) allowing links physically connected to two separate switches to appear as a single trunk to a third device. The third device can be a switch, server, or any Ethernet device.

Examples To display a cluster membership, use the following command:

```
CLI network-admin@switch > cluster-membership-show
```

connection-clear

To clear connection statistics for a switch, use the `connection-clear` command.

Syntax `connection-clear`

Specify any of the following options:	
`time date/time:` *`yyyy-mm-ddThh:mm:ss`*	Clear statistics from a specific timestamp period.
`start-time date/time:` *`yyyy-mm-ddThh:mm:ss`*	Clear statistics from a specific start time and date.
`end-time date/time:` *`yyyy-mm-ddThh:mm:ss`*	Clear statistic from a specific end time and date.
`duration:` *`#d#h#m#s`*	Clear statistics for a specific duration.
`interval duration:` *`#d#h#m#s`*	Clear statistics for a specific interval duration.
`since-start`	Clear statistics from the start of collection.
`older-than duration: #d#h#m#s`	Clear statistics older than a specified date and time.
`within-last duration: #d#h#m#s`	Clear statistics within a specified duration time.
`count` *`count-number`*	Clear the count number.
`vlan` *`vlan_id`*	Specifies the VLAN identifier.
`egress-vnet` *`vnet-name`*	Specifies the egress VNET.
`egress-bd` *`bridge-domain name`*	Specifies the bridge domain of the connection information.

egress-vlan *vlan_id*	Specifies the egress VLAN of the connection.
vxlan *vxlan-id*	Specifies the VXLAN identifier.
vnet *vnet-string*	Specifies the name of the virtual network (VNET).
src-switch-port	Specifies the physical port number on the switch where a client requested a connection.
dst-switch-port	Specifies the physical port number on the switch where a server responded to a connection.
ether_type	Specifies the EtherType value or keyword of the connection. The keywords can be arp, dot1X, fcoe, fcoe-init, ipv4, ipv6, jumbo, lldp, macsec, mpls-multi, mpls-uni, ptp, qing, rarp, vlan, and wake.
src-mac-addr	Specifies the MAC address of the client requesting a connection.
dst-mac-addr	Specifies the MAC address of the server responding to a connection.
src-ip	Specifies the IP address of the client requesting a connection.
dst-ip	Specifies the IP address of the server responding to a connection.
src-port	Specifies the type of port used by the client requesting a connection. This includes HDFS, Hive, Ganglia, Cassandra, Nutanix and other server types.
dst-port	Specifies the type of port used by the server responding to a connection. This includes HDFS, Hive, Ganglia, Cassandra, Nutanix and other server types.
dscp	Specifies the 6-bit Differentiated Services Code Point (DSCP).
protocol tcp|udp|icmp|igmp|ip	Specifies the protocol.
tunnel-vnet *vnet-name*	Specifies the tunnel VNET name.
tunnel-bd *bridge-domain name*	Specifies the tunnel bridge domain.
tunnel-vlan *vlan-id*	Specifies the VLAN ID.
tunnel-src-mac *mac-address*	Specifies the tunnel source MAC address.
tunnel-dst-mac *mac-address*	Specifies the tunnel destination MAC address.
tunnel-src-ip *ip-address*	Specifies the tunnel source IP address
tunnel-dst-ip *ip-address*	Specifies the tunnel destination IP address.
tunnel-src-port	Specifies the type of port used by the client

	requesting a connection. This includes HDFS, Hive, Ganglia, Cassandra, Nutanix and other server types.
`tunnel-dst-port`	Specifies the type of port used by the client requesting a connection. This includes HDFS, Hive, Ganglia, Cassandra, Nutanix and other server types.
`tunnel-proto tcp|udp|icmp|igmp|ip|icmpv6`	Specifies the protocol assigned to the tunnel.
`cur-state syn|est|fin|rst`	Specifies the current state of the connection.
`dur high resolution time:#ns`	Specifies the duration for high resolution time in nano seconds.
`latency high resolution time:#ns`	Specifies the latency for high resolution time in nano seconds
`latency(us)`	Specifies the network transmit time (latency) experienced by the connection in microseconds.
`obytes`	Specifies the number of bytes sent from the client side of the connection.
`ibytes`	Specifies the number of bytes received by the client side of the connection.
`total-bytes`	Specifies the total number of bytes for the connection.
`update-id high resolution time: #ns`	Specifies the last update to the connection in elapse time (nanoseconds).
`started-time-ns high resolution time: #ns`	Specifies the started time of the connection in nanoseconds.
`started-time date/time: yyyy-mm-ddThh:mm:ss`	Specifies the time and date of the initial connection.
`ended-time date/time: yyyy-mm-ddThh:mm:ss`	Specifies the time and date when the connection ended.
`transition-state any|started-and-ended |started|ended|ongoing`	Specifies the transition state of the connection.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 1.2.2	Command changed to connection-clear. bytes-sent and bytes-recvd changed to obytes and ibytes. older-than and within-last parameters added.

Version 2.1	The parameters, `client` and `server`, changed to `src` and `dst`. The parameter, `service`, is deprecated. The parameters, `started-time`, `ended-time`, and `transition-state` added.
Version 2.2	The parameter, `no-since-start`, deprecated.
Version 2.2.5	The parameters, `HDFS-`, added.
Version 2.4	The parameter, `egress-vlan`, added.
Version 2.4.1	The parameter, `egress-vnet`, added.
Version 2.6.2	The parameters, `tunnel-*`, added.
Version 5.1.1	The parameters, egress-bd, tunnel-bd, update-id `high resolution time, and started-time-ns high resolution time added.`

Usage Clears statistical information about the current connections on the switch.

connection-show

To display connection statistics for a switch, use the `connection-show` command.

Syntax `connection-show`

`start-time date/time:` *`yyyy-mm-ddThh:mm:ss`*	Specifies statistics from a specific start time and date.
`end-time date/time:` *`yyyy-mm-ddThh:mm:ss`*	Specifies statistic from a specific end time and date.
`duration:` *`#d#h#m#s`*	Specifies statistics for a specific duration.
`interval duration:` *`#d#h#m#s`*	Specifies statistics for a specific interval duration.
`since-start`	Specifies statistics from the start of collection. This is another way to specify the start time for the connection output.
`older-than duration: #d#h#m#s`	Specifies statistics older than a specified date and time. This is another way to specify the end time for the connection output.
`within-last duration: #d#h#m#s`	Specifies statistics within a specified duration time. This is another way to specify the start time for the connection output. Also, only the closed connections are displayed.
`vlan` *`vlan-id`*	Specifies the VLAN identifier.
`egress-vnet` *`vnet-name`*	Specifies the egress VNET.
`egress-vlan` *`vlan_id`*	Specifies the egress VLAN of the connection.
`vnet vnet-name`	Specifies the name of the virtual network (VNET).
`src-switch-port`	Specifies the physical port number on the

	switch where a client requested a connection.
dst-switch-port	Specifies the physical port number on the switch where a server responded to a connection.
ether_type	Specifies the EtherType value or keyword of the connection. The keywords can be arp, dot1X, fcoe, fcoe-init, ipv4, ipv6, jumbo, lldp, macsec, mpls-multi, mpls-uni, ptp, qing, rarp, vlan, and wake.
src-mac-addr	Specifies the MAC address of the client requesting a connection.
dst-mac-addr	Specifies the MAC address of the server responding to a connection.
src-ip	Specifies the IP address of the client requesting a connection.
dst-ip	Specifies the IP address of the server responding to a connection.
src-port	Specifies the type of data on the source port. HDFS indicates ports connected to Hadoop systems. Also includes HDFS, Hive, Ganglia, Cassandra, Nutanix and other server types.
dst-port	Specifies the type of data on the destination port. This includes HDFS, Hive, Ganglia, Cassandra, Nutanix and other server types.
dscp	Specifies the 6-bit Differentiated Services Code Point (DSCP).
tunnel-vnet *vnet-name*	Specifies the tunnel VNET name.
tunnel-vlan *vlan-id*	Specifies the VLAN ID.
tunnel-src-mac *mac-address*	Specifies the tunnel source MAC address.
tunnel-dst-mac *mac-address*	Specifies the tunnel destination MAC address.
tunnel-src-ip *ip-address*	Specifies the tunnel source IP address
tunnel-dst-ip *ip-address*	Specifies the tunnel destination IP address.
tunnel-src-port	Specifies the type of port used by the client requesting a connection. This includes HDFS, Hive, Ganglia, Cassandra, Nutanix and other server types.
tunnel-dst-port	Specifies the type of port used by the client requesting a connection. This includes HDFS, Hive, Ganglia, Cassandra, Nutanix and other server types.
tunnel-proto tcp|udp|icmp|igmp|ip|icmpv6	Specifies the protocol assigned to the tunnel.
proto [tcp|udp|icmp|igmp|ip	Specifies the protocol.

`cur-state syn|est|fin|rst`	Specifies the current state of the connection. syn — synchronized est — established fin — finished rst — reset
`dur high resolution time: #ns`	Specifies the duration of the connection.
`latency(us)high resolution time: #ns`	Specifies the network transmit time (latency) experienced by the connection in microseconds.
`obytes`	Specifies the number of bytes sent from the client side of the connection.
`ibytes`	Specifies the number of bytes received by the client side of the connection.
`active`	Specifies whether the connection is currently active or inactive.
`age duration:#d#h#m#s`	Specifies the duration of the connection in days, hours, minutes and seconds.
`transition-state any|started-and-ended |started| ended| ongoing`	Specifies the transition state of the connection.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 1.2.2	Command changed to connection-clear. bytes-sent and bytes-recvd changed to obytes and ibytes. older-than and within-last parameters added.
Version 2.1	The parameters, `client` and `server`, changed to `src` and `dst`. The parameter, `service`, is deprecated. The parameters, `started-time`, `ended-time`, and `transition-state` added.
Version 2.2	The parameter, `no-since-start`, deprecated.
Version 2.2.5	The parameters, `HDFS-`, added.
Version 2.4	The parameter, `egress-vlan`, added.
Version 2.4.1	The parameter, `egress-vnet`, added.
Version 2.6.2	The parameters, `tunnel-*`, added.
Version 5.1.1	The parameters, egress-bd, tunnel-bd, update-id `high resolution time`, and `started-time-ns high resolution time` added.

Usage Each switch maintains a set of standard flow-based statistics that are "always-on", meaning that they are continuously tracked and updated by the switch. This command displays the TCP connections transiting the local switch as identified through the SYN/FIN protocol handshake between the client and the server of the application.

Examples To show the connection statistics for vnet MyVNET, use the following command:

```
CLI network-admin@switch > connection-show vnet MyVNET layout vertical

  switch:                             pleiades24
  vlan:                               51
  vxlan:                              0
  vnet:
  src-ip:                             10.222.1.1
  dst-ip:                             10.222.1.2
  client-switch-port:                 8000
  server-switch-port:
  client-port:
  server-port:
  dscp:
  proto:
  service dur(s:
  latency(us):
  bytes-sent:
  bytes-recv:
  active:
```

connection-latency-show

This command is used to display latency information for connections on the switch. Comparing latency information for connections at various times can show whether the network performance has changed or stayed the same, and potentially eliminate the network as the cause of the problem

Syntax `connection-latency-show`

`min high resolution time: #ns`	Displays the minimum latency in nanoseconds.
`max high resolution time: #ns`	Displays the maximum latency in nanoseconds.
`num-bins num-bins-number`	Specify the number of bins to divide the latency range. Bins display the number of connections at each latency interval.

Defaults None

Access CLI

History Command introduced in Version 2.0.

Usage You can display all of the latency information about a connection or you can filter by the number of bins to display. Comparing latency information for connections at various times can show whether the network performance has changed or stayed the same, and potentially eliminate the network as the cause of the problem

Examples To display all latency information on pleiades24, use the following command:

```
CLI network-admin@switch > connection-latency-show

  switch     min    max   num-conns percent  avg-dur  obytes  ibytes  total-bytes
  --------    ------ ------ --------- ------- ------- ------ ------ -----------
  pleiades2   40.00ns 20.0us 13          0%                  0        0        0
  pleiades24 20.0us 40.0us 80          3%        1.28us   146K    305K    451K
  pleiades24 40.0us 60.0us 671         28%       14.9us   1.19M   2.50M   3.69M
  pleiades24 60.0us 80.0us 649         27%       19.2us   1.16M   2.42M   3.57M
  pleiades24 80.0us 100us   337        14%       12.9us   615K    1.25M   1.86M
  pleiades24 100us   120us   219        9%        10.2us   400K    835K    1.21M
  pleiades24 120us   140us   114        4%        6.33us   208K    434K    642K
  pleiades24 140us   160us   63         2%        4.01us   115K    241K    356K
  pleiades24 160us   180us   58         2%        4.19us   106K    222K    327K
  pleiades24 180us   200us   35         1%        2.85us   63.9K   134K    198K
  pleiades24 200us            94          4%        13.2us   172K    359K    530K
```

connection-stats-clear

This command clears statistics collected while connected to the host.

Syntax `connection-stats-clear`

`time date/time: yyyy-mm-ddThh:mm:ss`	Specify a time to clear the connection statistics.
`start-time date/time: yyyy-mm-ddThh:mm:ss`	Clear statistics from a specific start time and date.
`end-time date/time: yyyy-mm-ddThh:mm:ss`	Clear statistic from a specific end time and date.
`duration: #d#h#m#s`	Clear statistics for a specific duration.
`interval duration: #d#h#m#s`	Clear statistics for a specific interval duration.
`since-start`	Clear statistics from the start of collection.
`older-than duration: #d#h#m#s`	Clear statistics older than a specified date and time.
`within-last duration: #d#h#m#s`	Clear statistics within a specified duration time.
`count count-number`	Clear a specific number of statistics.
`mac mac-address`	Clear statistics for a MAC address.
`vnet vnet-name`	Clears statistics for a specific VNET.
`vlan vlan_id`	Clear the VLAN identifier.
`ip ip-address`	Clear the IP address of the connection.
`port port-number`	Clear the port number of the connection.

iconns *iconns-number*	Clear the number of incoming connections.
oconns *oconns-number*	Clear the number outgoing connections.
obytes	Clear the number of bytes sent from the client side of the connection.
ibytes	Clear the number of bytes received by the client side of the connection.
total-bytes *total-bytes-number*	Clear the total number of bytes.
first-seen date/time: yyyy-mm-ddThh:mm:ss	Clear statistics from the time a connection is first seen.
last-seen date/time: yyyy-mm-ddThh:mm:ss	Clear statistics from the time a connection was last seen.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 1.2.2	Command changed to connection-stats-show.
Version 2.2	The parameter, no-since-start, deprecated.
Version 2.4.1	The parameters, vnet and total-bytes, added.

Usage Used to clear statistics for a connection to a host.

Examples To clear the statistics from port 23, use the following command:

```
CLI network-admin@switch > connection-stats-clear port 23
```

connection-stats-show

This command displays statistics collected when connected to host.

Syntax connection-stats-show

time date/time: yyyy-mm-ddThh:mm:ss	Specify a time to display connection statistics.
start-time date/time: *yyyy-mm-ddThh:mm:ss*	Specifies statistics from a specific start time and date.
end-time date/time: *yyyy-mm-ddThh:mm:ss*	Specifies statistic from a specific end time and date.

duration: *#d#h#m#s*	Specifies statistics for a specific duration.
interval duration: *#d#h#m#s*	Specifies statistics for a specific interval duration.
since-start| no-since-start	Specifies statistics from the start of collection.
older-than duration: #d#h#m#s	Specifies statistics older than a specified date and time.
within-last duration: #d#h#m#s	Specifies statistics within a specified duration time.
count *count-number*	Clear a specific number of statistics.
mac *mac-address*	Clear statistics for a MAC address.
vnet *vnet-name*	Clears statistics for a specific VNET.
vlan *vlan_id*	Specifies the VLAN identifier.
ip *ip-address*	Specifies the IP address of the connection.
port *port-number*	Specifies the port number of the connection.
iconns *iconns-number*	Specifies the number of incoming connections.
oconns *oconns-number*	Specifies the number outgoing connections.
obytes	Specifies the number of bytes sent from the client side of the connection.
ibytes	Specifies the number of bytes received by the client side of the connection.
total-bytes total-bytes-number	Specifies the total number of bytes for the connection.
first-seen date/time: yyyy-mm-ddThh:mm:ss	Clear statistics from the time a connection is first seen.
last-seen date/time: yyyy-mm-ddThh:mm:ss	Clear statistics from the time a connection was last seen.

Access CLI

History

Version 1.2	Command introduced.

Version 1.2.2	Command changed to connection-stats-show.
Version 2.2	The parameter, `total-bytes`, added.
Version 2.4	The parameter, `age`, deprecated.
Version 2.4.1	The parameter, `vnet`, added.

Usage Used to clear statistics about a connection to a host.

Examples To display the statistics from port 23, use the following command:

```
CLI network-admin@switch > connection-stats-show format all layout vertical

  switch:             pubdev02
  mac:                   64:0e:94:28:03:56
  vnet:           vnet-global
  vlan:              1
  ip:                     192.168.42.30
  port:              41
  iconns:             184
  oconns:            0
  ibytes:            0
  obytes:            0
  total-bytes:     0
  first-seen:        01-14,10:33:44
  last-seen:          01-14,10:35:22
  last-seen-ago:  5d23h29m53s
  switch:             pubdev02
  mac:                   64:0e:94:28:00:5e
  vlan:              1
  ip:                     192.168.42.20
  port:              47
  iconns:            3
  oconns:            0
  ibytes:             1.47K
  obytes:             14.8K
  total-bytes:     16.3K
  first-seen:        01-13,13:59:35
  last-seen:          01-19,22:45:21
  last-seen-ago:  11h19m54s
```

connection-stats-clear-history

This command is used to clear the history of connection statistics.

Syntax `connection-stats-clear-history`

Defaults None

Access CLI

History Command introduced in Version 2.2.3.

connection-stats-settings-modify

This command allows you to modify the settings for collecting statistical data about connections.

Syntax `connection-settings-modify`

i

Specify one or more of the following options:	
`enable|disable`	Enable or disable collecting connections statistics.
`connection-max-memory` *`connection-max-memory-number`*	Specify the maximum memory allowed for connection statistics.
`connection-backup-enable| connection-backup-disable`	Enable backup for connection statistics collection.
`connection-backup-interval duration:` *`#d#h#m#s`*	Specify backup interval for connection statistics collection.
`client-server-stats-max-memory` *`client-server-stats-max-memory-numbe`*	Specify maximum memory for client server statistics.
`client-server-stats-log-enable| client-server-stats-log-disable`	Enable or disable statistics
`client-server-stats-log-interval duration:` *`#d#h#m#s`*	Specify the interval to collect statistics.
`client-server-stats-log-disk-space` *`disk-space-number`*	Specify the disk-space allocated for statistics.
`connection-stats-max-memory` *`connection-stats-max-memory-number`*	Specify the maximum memory allowed for connection statistics.
`connection-stats-log-enable| connection-stats-log-disable`	Enable or disable statistics.
`connection-stats-log-interval duration:` `#d#h#m#s`	Specify the interval to collect statistics.
`connection-stats-log-disk-space` *`disk-space-number`*	Specify the disk-space allocated for statistics.
`service-stat-max-memory` *`service-stat-max-memory-number`*	Specify tjhe maximum memory allowed for service statistics.

`fabric-connection-max-memory` *`fabric-connection-max-memory-number`*	Specify the maximum memory allowed for fabric connection statistics.
`fabric-connection-backup-enable|fabric-connection-backup-disable`	Enable backup for fabric connection statistics collection.
`fabric-connection-backup-interval duration:` *`#d#h#m#s`*	Specify the backup interval for fabric connection statistics collection.
`redirect-analytics-interface none|span1|span2|span3`	Specify if you want to redirect analytics flow to a rear-facing NIC.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to modify connection statistics collection.

Examples To disable statistics collection, use the following syntax:

```
CLI network-admin@switch > collection-stats-settings-modify  disable
```

connection-stats-settings-show

This command allows you to display the settings for collecting statistical data about connections.

Syntax `connection-stats-settings-show`

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to display connection statistics settings.

Examples To display connection statistics settings, use the following syntax:

```
CLI network-admin@switch > connection-stats-settings-show
```

control-stats-setting-modify

This command is used to modify the settings to collect statistics about packets sent from the CPU.

Syntax `control-stats-settings-modify enable|disable interval duration: #d#h#m#s disk-space disk-space-number`

`enable|disable`	Specify to enable or disable statistic collection.

`interval duration: #d#h#m#s`	Specify the intervals to collect statistics.
`disk-space` *`disk-space-number`*	Specify the disk space to allocate to the statistics.

Defaults None

Access CLI

History Introduced in Version 2.0.

Usage You can use this command to modify how packets statistics are collected.

Examples To disable statistic collection, use the following command:

```
CLI network-admin@switch > control-stats-settings-modify  disable
```

control-stats-setting-show

This command is used to display the settings for collecting statistics about packets sent from the CPU.

Syntax `control-stats-settings-show`

Defaults None

Access CLI

History Introduced in Version 2.0.

Usage You can use this command to display how packets statistics are collected.

Examples To disable statistic collection, use the following command:

```
CLI network-admin@switch > control-stats-settings-show
switch:     pubdev01
enable:     yes
interval:   1m
disk-space: 50M
switch:     pubdev03
enable:     yes
interval:   1m
disk-space: 50M
switch:     pubdev02
enable:     yes
interval:   1m
disk-space: 50M
```

control-stats-show

This command is used to display the packet counts sent from the CPU.

Syntax `control-stats-show`

`time` *`date/time: yyyy-mm-ddThh:mm:ss`*	Specify the timestamp of the statistics that you want to display.
`start-time date/time: yyyy-mm-ddThh:mm:ss`	Specify the start time for the statistics that you want to display.
`end-time date/time: yyyy-mm-ddThh:mm:ss`	Specify the end time for the statistics that you want to display.
`duration duration: #d#h#m#s`	Specify the duration of the statistics that you want to display.
`interval duration: #d#h#m#s`	Specify the interval between the statistics that you want to display.
`since-start`	Specify a start time for the statistics.
`older-than duration: #d#h#m#s`	Specify a duration that is older than a specified time.
`within-last duration: #d#h#m#s`	Specify a duration window for a specified time.
`caller Unknown|Total|Vxlan|Vle`	Specify the caller for the specific statistics. Total is displayed by default.

Defaults None

Access CLI

History

Version 2.0	Command introduced.
Version 2.1	The options, CPU-RX-TX|VLAG|BCAST|Flood, added to the parameter, caller.
Version 2.2	The parameters, older-than and within-last, added. The parameters, `|ARP|Vxlan-ARP| Vxlan-multicast|Vxlan-TCP|Vxlan-encap| Vxlan|Discovery|Keep-Alive|ECP| ICMP| IGMP|LLDP|LACP| Logical-switch|PTP|STP|PVST|nvOS-control|Local-subnet|Ipv6-mc|TCP-conn| RX-queue|NAT-Dynamic|CPU-RX-TX|VLAG| BCAST|Flood]` deprecated.
Version 2.4.0	The option, `Vxlan`, added to the parameter, `caller`.
Version 2.6.2	The option, `Vle`, added to the parameter, `caller`.

Usage You can use this command to display how many packets the operating system is sending out and how many packets were dropped. This can be helpful when debugging or troubleshooting problems on the network.

Examples To display control stats for a duration of three days and an interval of one day, use the following command:

```
CLI network-admin@switch > control-stats-show duration 03:00:00
interval 01:00:00 format all layout vertical
switch:             pubdev03
caller:             Total
ipkts:              1.80M
ibytes:             458M
idrops:             5
idrop-bytes:        300
idrops-err:         0
opkts:              1.87M
obytes:             395M
odrops:             29.7K
odrop-bytes:        1.51M
switch:             pubdev02
caller:             Total
ipkts:              978K
ibytes:             434M
idrops:             8
idrop-bytes:        490
idrops-err:         0
opkts:              1.53M
obytes:             399M
odrops:             53.4K
odrop-bytes:        15.2M
switch:             pubdev01
caller:             Total
ipkts:              1.86M
ibytes:             499M
idrops:             13
idrop-bytes:        780
idrops-err:         0
opkts:              2.33M
obytes:             454M
odrops:             89.0K
odrop-bytes:        15.0M
```

control-traffic-modify

This command is used to modify the control traffic on the switch.

Syntax `control-traffic-modify`

`type smac-miss|dmac-miss|l3-miss|l3-ttl`	Specify the type of control traffic.
`class` *`vflow-class-name`*	Specify the vFlow class name.
`cpu_class` *`cpu-class name`*	Specify the CPU class name.

Defaults None

Access CLI

History .

Version 2.4.0	Command introduced.

Version 2.6.0	The parameter, `smac-miss`, added.
Version 2.6.2	The parameter, `cpu_class`, added.

Usage You can use this command to update the control traffic configuration.

Examples To modify control traffic, use the following command:

```
CLI network-admin@switch > control-traffic-modify  type
```

control-traffic-show

This command is used to display the control traffic configuration on the switch.

Syntax `control-traffic-show`

`type smac-miss|dmac-miss|l3-miss|l3-ttl`	Specify the type of control traffic.
`class` *`vflow-class-name`*	Specify the start time for the statistics that you want to display.
`cpu_class` *`cpu-class name`*	Specify the CPU class name.

Defaults None

Access CLI

History .

Version 2.4.0	Command introduced.
Version 2.6.0	The parameter, `smac-miss`, added.
Version 2.6.2	The parameter, `cpu_class`, added.

Usage You can use this command to display the control traffic configuration.

Examples To display control traffic, use the following command:

```
CLI network-admin@switch > control-traffic-show
switch        type      class
------------- --------- ------
aquila-ext-43 smac-miss class1
aquila-ext-43 dmac-miss class0
aquila-ext-43 l3-miss   class0
aquila-ext-43 l3-ttl    class0
```

cpu-class-create

Netvisor’s CPU Control Packet Processing Protection feature allows the CPU control packet processing path be protected against misbehaving and malicious hosts or end-points that may flood control protocol

packets. This is also called “CPU hog protection”.

If a host floods a control protocol packet, it floods the to-cpu queue. This prevents lower-rate packets from valid senders from reaching Netvisor, resulting in traffic loss for those hosts. Typically a traffic loss occurs for other hosts on the network. Netvisor can process large streams of both valid and malformed protocol packets for various protocols.

Syntax `cpu-class-create`

`name` *`name-string`*	Specify a name for the CPU class.
`scope local|fabric`	Specify the scope as local or fabric.
`rate-limit` *`rate-limit-number`*	Specify the cap for the rate limit.
`hog-protect disable|enable|enable-and-drop`	Specify if you want to enable, enable and drop packets, or disable hog protection.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to create CPU protection.

Examples To create a CPU protection class for the local subnet, use the following syntax:

```
CLI network-admin@switch > cpu-class-create name local-subnet scope
local rate-limit 100 hog-protect enable-and-drop
```

cpu-class-delete

Netvisor’s CPU Control Packet Processing Protection feature allows the CPU control packet processing path be protected against misbehaving and malicious hosts or end-points that may flood control protocol packets. This is also called “CPU hog protection”.

If a host floods a control protocol packet, it floods the to-cpu queue. This prevents lower-rate packets from valid senders from reaching Netvisor, resulting in traffic loss for those hosts. Typically a traffic loss occurs for other hosts on the network. Netvisor can process large streams of both valid and malformed protocol packets for various protocols.

Syntax `cpu-class-delete`

`name` *`name-string`*	Specify a name for the CPU class.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to delete CPU protection.

Examples To delete a CPU protection class for the local subnet, use the following syntax:

```
CLI network-admin@switch > cpu-class-delete name local-subnet
```

cpu-class-modify

Netvisor's CPU Control Packet Processing Protection feature allows the CPU control packet processing path be protected against misbehaving and malicious hosts or end-points that may flood control protocol packets. This is also called "CPU hog protection".

If a host floods a control protocol packet, it floods the to-cpu queue. This prevents lower-rate packets from valid senders from reaching Netvisor, resulting in traffic loss for those hosts. Typically a traffic loss occurs for other hosts on the network. Netvisor can process large streams of both valid and malformed protocol packets for various protocols.

Syntax `cpu-class-modify`

`name` *`name-string`*	Specify a name for the CPU class.
`scope local|fabric`	Specify the scope as local or fabric.
`rate-limit` *`rate-limit-number`*	Specify the cap for the rate limit.
`hog-protect disable|enable|enable-and-drop`	Specify if you want to enable, enable and drop packets, or disable hog protection.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to modify CPU protection.

Examples To modify a CPU protection class for the local subnet to rate limit 1000, use the following syntax:

```
CLI network-admin@switch > cpu-class-modify name local-subnet rate-
limit 1000
```

cpu-class-show

Netvisor's CPU Control Packet Processing Protection feature allows the CPU control packet processing path be protected against misbehaving and malicious hosts or end-points that may flood control protocol packets. This is also called "CPU hog protection".

If a host floods a control protocol packet, it floods the to-cpu queue. This prevents lower-rate packets from valid senders from reaching Netvisor, resulting in traffic loss for those hosts. Typically a traffic loss occurs for other hosts on the network. Netvisor can process large streams of both valid and malformed protocol packets for various protocols.

Syntax `cpu-class-show`

`name` *`name-string`*	Displays the name for the CPU class.
`scope local|fabric`	Displays the scope as local or fabric.
`rate-limit` *`rate-limit-number`*	Displays the cap for the rate limit.
`hog-protect disable|enable|enable-and-drop`	Displays if you want to enable, enable and drop packets, or disable hog protection.
`hog-protect-support| no-hog-protect-support`	Displays if hog protection is supported or not.
`queue` *`queue-number`*	Displays the queue number.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to display information about CPU class configurations.

Examples To display CPU class configurations, use the following syntax:

```
CLI network-admin@switch > cpu-class-show

switch      name                scope  rate-limit  hog-protect  hog-protect-support  queue
----------  ---------------  -----  ----------  -----------  -------------------  -----
aquarius06  dmac-miss           local  1000         disable      none                    1
aquarius06  smac-miss           local  1000         disable      none                    2
aquarius06  l3-miss             local  1000         disable      none                    3
aquarius06  ttl1                local  1000         disable      none                    4
aquarius06  stp                 local  1000         disable      supported               5
aquarius06  lacp                local  1000         disable      supported               6
aquarius06  system-d            local  1000         disable      none                    7
aquarius06  dmac-miss           local  1000         disable      none                    8
aquarius06  smac-miss           local  1000         disable      none                    9
aquarius06  l3-miss             local  1000         disable      none                    10
aquarius06  ttl1                local  1000         disable      none                    11
```

```
aquarius06 stp                  local 1000        disable      supported             12
aquarius06 lacp                 local 1000        disable      supported             13
aquarius06 system-d             local 1000        disable      none                  14
aquarius06 igmp                 local 1000        disable      none                  15
aquarius06 bcast                local 1000        disable      none                  16
aquarius06 icmpv6               local 1000        disable      none                  17
aquarius06 tcp-analytics        local 1000        disable      none                  18
aquarius06 kpalv                local 1000        disable      none                  19
aquarius06 ecp                  local 1000        disable      none                  20
aquarius06 arp                  local 1000        disable      supported             21
aquarius06 lldp                 local 1000        disable      supported             22
aquarius06 vport-stats          local 1000        disable      none                  23
aquarius06 dhcp                 local 1000        disable      none                  24
aquarius06 pim                  local 1000        disable      none                  25
aquarius06 local-subnet         local 1000        disable      supported             26
aquarius06 bgp                  local 1000        disable      supported             27
aquarius06 ospf                 local 1000        disable      supported             28
aquarius06 bfd                  local 1000        disable      supported             29
aquarius06 vrrp                 local 1000        disable      supported             30
aquarius06 cluster-control      local 5000        disable      none                  31
aquarius06 control              local 5000        disable      none                  32
aquarius06 hog-arp              local 100         disable      none                  33
aquarius06 hog-ospf             local 100         disable      none                  34
aquarius06 hog-bgp              local 100         disable      none                  35
aquarius06 hog-bfd              local 100         disable      none                  36
aquarius06 hog-lacp             local 100         disable      none                  37
aquarius06 hog-stp              local 100         disable      none                  38
aquarius06 hog-vrrp             local 100         disable      none                  39
aquarius06 hog-lldp             local 100         disable      none                  40
aquarius06 hog-local-subnet     local 100         disable      none                  41
```

```
aquarius06 dhcp-log-drop     local 1000         disable      none                    42
```

cpu-class-settings-modify

Netvisor's CPU Control Packet Processing Protection feature allows the CPU control packet processing path be protected against misbehaving and malicious hosts or end-points that may flood control protocol packets. This is also called "CPU hog protection".

If a host floods a control protocol packet, it floods the to-cpu queue. This prevents lower-rate packets from valid senders from reaching Netvisor, resulting in traffic loss for those hosts. Typically a traffic loss occurs for other hosts on the network. Netvisor can process large streams of both valid and malformed protocol packets for various protocols.

Syntax *CLI network-admin@switch* >cpu-class-settings-show

hog-checker-interval *hog-checker-interval-number (ms)*	Specify the hog checking interval in milliseconds.
hog-max-hosts-per-class *hog-max-hosts-per-class-number*	Specify the maximum number of active hosts tracked per CPU class.
hog-max-violators-per-port *hog-max-violators-per-port-number*	Specify the maximum number of hog violators per port.
hog-max-violators-per-port *hog-max-violators-per-port-number*	Specify the hog warning threshold.
hog-violator-timeout *hog-violator-timeout-number (s)*	Specify the timeout before restoring the hog violator to normal queue after an idle state.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to modify statistics settings for CPU class.

Examples To modify CPU class settings for hog-checker-interval from 100 to 150, use the following syntax:

```
CLI network-admin@switch > cpu-clss-settings-modify  hog-checker-
interval 150
```

cpu-class-settings-show

The Netvisor OS CPU Control Packet Processing Protection feature allows the CPU control packet processing path be protected against misbehaving and malicious hosts or end-points that may flood control protocol packets. This is also called "CPU hog protection".

If a host floods a control protocol packet, it floods the to-cpu queue. This prevents lower-rate packets from valid senders from reaching Netvisor, resulting in traffic loss for those hosts. Typically a traffic loss occurs for other hosts on the network. Netvisor can process large streams of both valid and malformed protocol packets for various protocols.

Syntax `cpu-class-settings-show`

`hog-checker-interval` *`hog-checker-interval-number (ms)`*	Specify the hog checking interval in milliseconds.
`hog-max-hosts-per-class` *`hog-max-hosts-per-class-number`*	Specify the maximum number of active hosts tracked per CPU class.
`hog-max-violators-per-port` *`hog-max-violators-per-port-number`*	Specify the maximum number of hog violators per port.
`hog-max-violators-per-port` *`hog-max-violators-per-port-number`*	Specify the hog warning threshold.
`hog-violator-timeout` *`hog-violator-timeout-number (s)`*	Specify the timeout before restoring the hog violator to normal queue after an idle state.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to display statistic settings for CPU hog protection.

Examples To display statistic settings for CPU hog protection, use the following syntax:

```
CLI network-admin@switch > cpu-class-settings-show

switch:                                                Spine01
hog-checker-interval(ms):       100
hog-max-hosts-per-class:         500
hog-max-violators-per-port:  50
hog-warning-threshold:              5
hog-violator-timeout(s):         20
```

cpu-class-stats-clear

The Netvisor OS CPU Control Packet Processing Protection feature allows the CPU control packet processing path be protected against misbehaving and malicious hosts or end-points that may flood control protocol packets. This is also called "CPU hog protection".

If a host floods a control protocol packet, it floods the to-cpu queue. This prevents lower-rate packets from valid senders from reaching Netvisor, resulting in traffic loss for those hosts. Typically a traffic loss occurs for other hosts on the network. Netvisor can process large streams of both valid and malformed protocol packets for various protocols.

Syntax `cpu-class-stats-clear`

name *name-string*	Specify the name of the CPU class to clear statistics.
cos *cos-number*	Clear the CoS value for the CPU class.
hw-out-pkts *hw-out-pkts-number*	Clear the hardware transmitted packet count.
hw-drop-pkts *hw-drop-pkts-number*	Clear the number of hardware dropped packets.
sw-pkts *sw-pkts-number*	Clear the number of packets processed in software.
sw-drops-pkts *sw-drops-pkts-number*	Clear the number of packets dropped in software because the queue is full.
hog-violations *hog-violations-number*	Clear the number of hog protection host violations and moved to separate queue.
hog-warnings *hog-warnings-number*	Clear the number of hog protection delegated bandwidth warnings.
hog-hosts-in *hog-hosts-in-number*	Clear the number of added hosts for hog protection.
hog-hosts-out *hog-hosts-out-number*	Clear the number of hosts removed from hog protection.
hog-max-hosts-drops *hog-max-hosts-drops-number*	Clear the number of dropped hosts with hog protection because the maximum number of hosts is reached.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to clear statistics for CPU hog protection.

Examples To clear statistics for CPU hog protection, use the following syntax:

```
CLI network-admin@switch > cpu-class-stats-show
```

cpu-class-stats-show

The Netvisor OS CPU Control Packet Processing Protection feature allows the CPU control packet processing path be protected against misbehaving and malicious hosts or end-points that may flood control protocol packets. This is also called “CPU hog protection”.

If a host floods a control protocol packet, it floods the to-cpu queue. This prevents lower-rate packets from valid senders from reaching Netvisor, resulting in traffic loss for those hosts. Typically a traffic loss occurs for other hosts on the network. Netvisor can process large streams of both valid and malformed protocol packets for various protocols.

Syntax `cpu-class-stats-show`

`name` *`name-string`*	Specify the name of the CPU class to clear statistics.
`cos` *`cos-number`*	Displays the CoS value for the CPU class.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to display statistics for CPU hog protection.

Examples To display statistics for CPU hog protection, use the following syntax:

```
CLI network-admin@switch > cpu-class-stats-show
switch:                     Spine01
hog-checker-interval(ms):   100
hog-max-hosts-per-class:    500
hog-max-violators-per-port: 50
hog-warning-threshold:      5
hog-violator-timeout(s):    20
```

cpu-mgmt-class-modify

Informational Note: This feature is supported on the following platforms:

Freedom Series	Edge-Core Series	Dell Series
F9272-X	AS5512-54X	S6010-ON
F9232-C	AS6712-32X	Z9100-ON
F9372-T		

Control Plane Traffic Protection (CPTP) refers to a new feature that allows the user to impose rate limits on the flow of traffic that arrives on the CPU management port. When control plane traffic arrives out-of-band on the management NIC of the switch, there is currently no such protection. There is the possibility that excessive control plane traffic may saturate the 1G management port or starve the CPU of other critical traffic.

Syntax `cpu-mgmt-class-modify`

`name arp|icmp|ssh|snmp|fabric| bcast|nfs|web|web-ssl|net-api`	Select the class of traffic to modify.
Specify one or more of the following options:	
`rate-limit unlimited`	Specify the ingress rate limit on the management port in Bps or unlimited.
`burst-size default`	Specify the ingress traffic burst size in bytes or default.

Defaults Disabled by default.

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to modify management services to the CPU configuration.

Examples To modify the rate limit for ARP traffic to 100 Bps, use the following syntax:

```
CLI network-admin@switch > cpu-mgmt-class-modify name arp rate-limit
100 Bps
```

cpu-mgmt-class-show

Control Plane Traffic Protection (CPTP) refers to a new feature that allows the user to impose rate limits on the flow of traffic that arrives on the CPU management port. When control plane traffic arrives out-of-band on the management NIC of the switch, there is currently no such protection. There is the possibility that excessive control plane traffic may saturate the 1G management port or starve the CPU of other critical traffic.

Syntax `cpu-mgmt-class-show`

`name arp|icmp|ssh|snmp|fabric|bcast| nfs|web|web-ssl|net-api`	Displays the class of traffic.
one or more of the following options:	
`rate-limit unlimited`	Displays the ingress rate limit on the management port in Bps or unlimited.
`burst-size default`	Displays the ingress traffic burst size in bytes or default.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to display information about CPU traffic management.

Examples To display information about CPU management, use the following syntax:

```
CLI network-admin@switch > cpu-mgmt-class-show
switch  name    rate-limit
------- ------- ----------
draco07 arp     unlimited
draco07 icmp    unlimited
draco07 ssh     unlimited
draco07 snmp    unlimited
draco07 fabric  unlimited
draco07 bcast   unlimited
draco07 nfs     unlimited
draco07 web     unlimited
draco07 web-ssl unlimited
```

```
draco07 net-api unlimited
```

cpu-mgmt-class-stats-settings-modify

This command is used to modify the settings for statistics collection.

Syntax `cpu-mgmt-class-stats-settings-modify`

`enable|disable`	Specify if you want to enable statistics collection.
`interval duration: #d#h#m#s`	Specify the interval duration.
`disk-space` *`disk-space-number`*	Specify the amount of disk space for the statistics.

Defaults Disabled.

Access Network Administrator

History Command introduced in Version 3.0.0

Usage Use this command to modify a CPU management class statistics collection configuration.

Examples To enable statistics collection for the CPU management class configuration, use the following syntax:

```
CLI network-admin@switch > cpu=mgmt-class-settings-modify enable
```

cpu-mgmt-class-stats-settings-show

This command is used to display the settings for statistics collection.

Syntax `cpu-mgmt-class-stats-settings-show`

Defaults None.

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to display statistics collection settings.

Examples To display statistics collection settings, use the following syntax:

```
CLI network-admin@switch > cpu-mgmt-class-stats-settings-show
switch:     draco07
enable:     yes
interval:   30m
disk-space: 50M
```

cpu-mgmt-class-stats-show

This command is used to display CPU management class statistics.

Syntax `cpu-mgmt-class-stats-show`

`time date/time: yyyy-mm-ddTHH:mm:ss`	Displays the time to start collection.

start-time date/time: yyyy-mm-ddTHH:mm:ss	Displays the start time of collection.
end-time date/time: yyyy-mm-ddTHH:mm:ss	Displays the end time of collection.
duration duration: #d#h#m#s	Displays the duration of collection.
interval duration: #d#h#m#s	Displays the interval between collection.
since-start	Displays the statistics collected since the start time.
older-than duration: #d#h#m#s	Displays the statistics older than the specified time.
within-last duration: #d#h#m#s	Displays the statistics collected within last time.
name arp|icmp|ssh|snmp|fabric|bcast|nfs|web|web-ssl|net-api	Displays the CPU management class.
in-bytes in-bytes-number	Displays the ingress bytes processed.
in-pkts *in-pkts-number*	Displays the ingress packets processed.
drop-pkts *drop-pkts-number*	Displays the number of ingress packets dropped.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to display CPU management class statistics.

Examples To display statistics, use the following syntax:

```
CLI network-admin@switch > cpu-mgmt-class-stats-show
switch  name    in-bytes in-pkts drop-pkts
------- ------- -------- ------- ---------
draco07 arp     0        0       0
draco07 icmp    0        0       0
draco07 ssh     0        0       0
draco07 snmp    0        0       0
draco07 fabric  0        0       0
draco07 bcast   0        0       0
draco07 nfs     0        0       0
draco07 web     0        0       0
draco07 web-ssl 0        0       0
draco07 net-api 0        0       0
```

D Commands

dhcp-filter-create

DHCP snooping is a security feature which allows the network to avoid denial-of-service attacks from rogue DHCP servers. Trusted ports are defined to connect to the known DHCP servers. DHCP snooping also maintains a mapping table for current assignments.

In a DHCP packet flow, there are the following packet types:

- DHCPDISCOVER/DHCPREQUEST — Packets from the DHCP client to server (UDP dest-port = 67)
- DHCPOFFER/DHCPACK — Packets from the DHCP Server to client (UDP dest-port = 68)

  Netvisor must snoop the DHCP packets in order to implement this feature, and achieves this by installing a copy-to-cpu vFlow with the parameter, `bw-max`, to set packet rate limits.

- DHCP-client-vflow — Packets with UDP dest-port=67, copy-to-cpu
- DHCP-server-vflow — Packets with UDP dest-port=68, copy-to-cpu

  A trusted port is a port receiving the DHCP server messages from a trusted DHCP server. Any DHCP server message, such as OFFER/ACKNOWLEDGE, received from trusted ports are valid. Ports not configured as trusted are untrusted ports. Netvisor drops any DHCP server message received from untrusted ports, and ensures that a rogue DHCP server cannot assign IP addresses to devices on your network.

  This command is used to create a DHCP filter.

Syntax `dhcp—filter-create`

`name` *`name-string`*	Specify a name for the filter.
`trusted-ports` *`port-list`*	Specify a list of trusted ports.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to create a DHCP filter for trusted ports.

Examples To create a DHCP filter, trust-server-1 and port 13-17 , use the following syntax:

```
CLI network-admin@switch > dhcp-filter-create name trust-server-1 ports
13-17
```

dhcp-filter-delete

DHCP snooping is a security feature which allows the network to avoid denial-of-service attacks from rogue DHCP servers. Trusted ports are defined to connect to the known DHCP servers. DHCP snooping also maintains a mapping table for current assignments.

In a DHCP packet flow, there are the following packet types:

- DHCPDISCOVER/DHCPREQUEST — Packets from the DHCP client to server (UDP dest-port = 67)
- DHCPOFFER/DHCPACK — Packets from the DHCP Server to client (UDP dest-port = 68)

This command is used to delete a DHCP filter.

Syntax `dhcp—filter-add name name-string`

`name` *`name-string`*	Specify a name for the filter.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to create a DHCP filter for trusted ports.

Examples To delete a DHCP filter, **trust-server-1**, use the following syntax:

```
CLI network-admin@switch > dhcp-filter-delete name trust-server-1
```

dhcp-filter-modify

DHCP snooping is a security feature which allows the network to avoid denial-of-service attacks from rogue DHCP servers. Trusted ports are defined to connect to the known DHCP servers. DHCP snooping also maintains a mapping table for current assignments.

In a DHCP packet flow, there are the following packet types:

- DHCPDISCOVER/DHCPREQUEST — Packets from the DHCP client to server (UDP dest-port = 67)
- DHCPOFFER/DHCPACK — Packets from the DHCP Server to client (UDP dest-port = 68)

This command is used to modify a DHCP filter.

Syntax `dhcp—filter-modify name name-string trusted-ports port-list`

`name` *`name-string`*	Specify a name for the filter.
`trusted-ports` *`port-list`*	Specify a list of trusted ports.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to create a DHCP filter for trusted ports.

Examples To modify a DHCP filter, **trust-server-1** and change the ports to 33-35, use the following syntax:

```
CLI network-admin@switch > dhcp-filter-modify name trust-server-1 ports
33-35
```

dhcp-filter-show

DHCP snooping is a security feature which allows the network to avoid denial-of-service attacks from rogue DHCP servers. Trusted ports are defined to connect to the known DHCP servers. DHCP snooping also maintains a mapping table for current assignments.

In a DHCP packet flow, there are the following packet types:

- DHCPDISCOVER/DHCPREQUEST — Packets from the DHCP client to server (UDP dest-port = 67)
- DHCPOFFER/DHCPACK — Packets from the DHCP Server to client (UDP dest-port = 68)

This command is used to display DHCP filter information.

Syntax `dhcp-filter-show`

`name` *`name-string`*	Displays the name of the filter.
`trusted-ports` *`port-list`*	Displays a list of trusted ports.
`vlan` *`vlan-list`*	Displays a list of VLANs.

History Command introduced in Version 2.6.0.

Usage Use this command to display information about a DHCP filter configuration.

Examples To display DHCP filter information, use the following syntax:

```
CLI network-admin@switch > dhcp-filter-show
```

dhcp-lease-show

This command is used to display information about DHCP leases on the switch.

Syntax `dhcp-lease-show`

`ip` *`ip-address`*	Specifies the IP address of a DHCP client.
`mac` *`mac-address`*	Specifies the MAC address of a DHCP client.
`port` *`port-list`*	Specifies the port of a DHCP client.
`vlan` *`vlan-id`*	Specifies the VLAN for the DHCP client.
`vnet` *`vnet name`*	Specifies the vNET name.
`bd` *`bridge-domain name`*	Specifies the bridge domain name.
`db-state unknown|free|active| backup|abandoned| expired`	Specifies the state of a DHCP client's lease.
`start-time` *`yyyy-mm-ddThh:mm:ss`*	The beginning of the DHCP lease.

`end-time` *`yyyy-mm-ddThh:mm:ss`*	Specifies the end of the DHCP lease.
`server dhcp` *`name`*	Specifies the name of the DHCP server.
`server-ip` *`ip-address`*	Specifies the IP address of the DHCP server.
`server-port` *`server-port-number`*	Specifies the port number of the DHCP server.
`last-msg |discover|offer| request|decline|ack| nack|release|inform`	Specifies the last message received from the DHCP client.
`last-msg-time date/time:`*`yyyy-mm-ddThh:mm:ss`*	Specifies the time of the last message received from the DHCP client.
`trusted-server|no-trusted-server`	Specifies the trusted DHCP server.

Defaults None

Access CLI

History

Version 1.2.1	Command introduced.
Version 2.6	The parameter, `trusted-server`, added.
Version 5.1.1	The parameters, `vnet` and `bd`, added.

Usage Used to display information about DHCP leases on the switch.

Examples To display information about the DHCP leases on the switch, use the following command:

```
CLI network-admin@switch > dhcp-lease-show
switch:        pleiades25
ip:            172.16.23.2
mac:           66:0e:94:21:4a:7b
port:          none
vlan:          11
db-state:      active
start-time:    09:17:59
end-time:      10:17:59
server:        red-dhcp
server-ip:     172.16.23.1
switch:        pleiades25
ip:            172.16.23.3
mac:           00:25:90:63:8a:84
port:          10
vlan:          11
db-state:      active
start-time:    09:20:05
end-time:      10:20:05
server:        red-dhcp
server-ip:     172.16.23.1
server-port:   65
last-msg:      ack
```

```
last-msg-time: 09:20:06
```

dscp-map-create

Netvisor supports creating Quality of Service (QoS) maps to configure hardware based mapping of Differentiated Services Code Point (DSCP) value in a received IP header to a Cost of Service (CoS) priority. This helps with prioritizing traffic based on DSCP markings by using the appropriate egress CoS queues to send packets out.

Syntax `dscp-map-create name name-string`

name *name-string*	Create a name for the DSCP map.

Defaults

CoS Priority Value	Default DSCP Values
0	None
1	8,10,12,14
2	16,18,20,22
3	24,26,28,30
4	32,34,36,38
5	40
6	48
7	56

Access Network Administrator

History Command introduced in Version 2.5.3.

Usage Use this command to create a DSCP map with default DSCP to priority mappings.

Examples To create a DSCP map with the name DSCP-1, use the following syntax:

```
CLI network-admin@switch > dscp-map-create name DSCP-1
```

dscp-map-delete

Netvisor supports creating Quality of Service (QoS) maps that configure hardware based mapping of Differentiated Services Code Point (DSCP) value in a received IP header to a Cost of Service (CoS) priority. This helps in prioritizing traffic based on DSCP markings by using the appropriate egress CoS queues to send packets out.

Syntax `dscp-map-delete name name-string`

name *name-string*	Specify the name of the DSCP map.

Access Network Administrator

History Command introduced in Version 2.5.3.

Usage Use this command to delete a DSCP map.

Examples To delete a DSCP map with the name **DSCP-1**, use the following syntax:

```
CLI network-admin@switch > dscp-map-delete name DSCP-1
```

dscp-map-show

Netvisor supports creating Quality of Service (QoS) maps that configure hardware based mapping of Differentiated Services Code Point (DSCP) value in a received IP header to a Cost of Service (CoS) priority. This helps in prioritizing traffic based on DSCP markings by using the appropriate egress CoS queues to send packets out.

Syntax `dscp-map-show name` *`name-string`*

`name` *`name-string`*	Specify the name of the DSCP map.

Access Network Administrator

History Command introduced in Version 2.5.3.

Usage Use this command to display DSCP maps.

Examples To display a DSCP map with the name **DSCP-1**, use the following syntax:

```
CLI network-admin@switch > dscp-map-show name DSCP-1
```

dscp-map-pri-map-modify

Netvisor supports creating Quality of Service (QoS) maps that configure hardware based mapping of Differentiated Services Code Point (DSCP) value in a received IP header to a Cost of Service (CoS) priority. This helps in prioritizing traffic based on DSCP markings by using the appropriate egress CoS queues to send packets out.

Syntax `dscp-map-pri-map-modify name name-string`

`name` *`name-string`*	Specify the name of the DSCP map.
the following `pri-map` arguments:	
`pri` *`number`*	Specify a CoS priority from 0 to 7.
`dsmap` *`number-list`*	Specify a DSCP value(s)as a single value, comma separated list, or a number range.

Defaults

CoS Priority Value	Default DSCP Values
0	None

1	8,10,12,14
2	16,18,20,22
3	24,26,28,30
4	32,34,36,38
5	40
6	48
7	56

Access Network Administrator

History Command introduced in Version 2.5.3.

Usage Use this command to modify a DSCP map.

Examples To modify a DSCP map with the name DSCP-1, use the following syntax:

```
CLI network-admin@switch > dscp-map-pri-map-modify name DSCP-1 pri 5
dsmap 44
```

dscp-map-pri-map-show

Netvisor supports creating Quality of Service (QoS) maps that configure hardware based mapping of Differentiated Services Code Point (DSCP) value in a received IP header to a Cost of Service (CoS) priority. This helps in prioritizing traffic based on DSCP markings by using the appropriate egress CoS queues to send packets out.

Syntax `dscp-map-pri-map-show`

name *name-string*	Specify the name of the DSCP map.
the following pri-map arguments:	
pri *number*	Specify a CoS priority from 0 to 7.
dsmap *number-list*	Specify a DSCP value(s)as a single value, comma separated list, or a number range.

Defaults

CoS Priority Value	Default DSCP Values
0	None
1	8,10,12,14
2	16,18,20,22
3	24,26,28,30
4	32,34,36,38

5	40
6	48
7	56

Access Network Administrator

History Command introduced in Version 2.5.3.

Usage Use this command to display a DSCP map and values.

Examples To display a DSCP map with the name DSCP-1, use the following syntax:

> **Informational Note**: The `dscp-map-pri-map-show` displays output only if there are maps configured .

```
CLI network-admin@switch > dscp-map-pri-map-show name DSCP-1

  switch name pri dsmap
  ------- ---- --- -----------
  Spine1 ds2 0 none
  Spine1 ds2 1 8,10,12,14
  Spine1 ds2 2 16,18,20,22
  Spine1 ds2 3 24,26,28,30
  Spine1 ds2 4 32,34,36,38
  Spine1 ds2 5 40
  Spine1 ds2 6 48
  Spine1 ds2 7 56
```

E Commands

err-disable-clear-counters

Physical ports are automatically disabled by Netvisor due to certain violations. For example, if a port receives BPDU messages from an edge port, Netvisor disables the port because receiving BPDUs on a edge port is a security violation. However, there is no way to indicate that the port is shut down because of a violation and not because of physical link issues.

Syntax `err-disable-clear-counters`

`bpduguard|no-bpduguard`	Specify if you want BPDU guard enabled.
`macsecurity|no-macsecurity`	Specify if you want MAC recovery enabled.
`recovery-timer duration: #d#h#m#s`	Specify the recovery time value.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to reset port error counters.

Examples To clear port error counters, use the following syntax:

```
CLI network-admin@switch > err-disable-clear-counters
```

err-disable-modify

Physical ports are automatically disabled by Netvisor due to certain violations. For example, if a port receives BPDU messages from an edge port, Netvisor disables the port because receiving BPDUs on a edge port is a security violation. However, there is no way to indicate that the port is shut down because of a violation and not because of physical link issues.

Syntax `err-disable-modify`

`bpduguard|no-bpduguard`	Specify if you want BPDU guard enabled.
`macsecurity|no-macsecurity`	Specify if you want MAC recovery enabled.
`recovery-timer duration: #d#h#m#s`	Specify the recovery time value.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to modify port error counters.

Examples To clear port error counters, use the following syntax:

```
CLI network-admin@switch > err-disable-modify
```

err-disable-counters-clear

Physical ports are automatically disabled by Netvisor due to certain violations. For example, if a port receives BPDU messages from an edge port, Netvisor disables the port because receiving BPDUs on a edge port is a security violation. However, there is no way to indicate that the port is shut down because of a violation and not because of physical link issues.

Syntax `err-disable-counters-clear`

`bpduguard|no-bpduguard`	Specify if you want to clear BPDU guard counters.
`macsecurity|no-macsecurity`	Specify if you want to clear MAC recovery counters.
`recovery-timer duration: #d#h#m#s`	Specify the recovery time value.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to reset port error counters.

Examples To clear port error counters, use the following syntax:

```
CLI network-admin@switch > err-disable-counters-clear
```

eula-show

This command is used to display the End User License Agreement (EULA).

Syntax `eula-show`

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to display the End User License Agreement (EULA).

Examples To display End User License Agreement (EULA), use the following syntax:

```
CLI network-admin@switch > eula-show
```

exit

This command allows you to exit the CLI.

Defaults None

Access CLI.

Usage Use this command to exit the CLI.

F Commands

fabric-anycast-mac-modify

This command is used to modify the fabric anycast MAC address for the fabric.

Syntax `fabric-anycast-mac-modify`

mac *mac-address*	Modify the anycast MAC address for the fabric.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to modify the fabric anycast MAC address for the fabric.

Examples To modify the fabric anycast MAC address for the fabric, use the following syntax:

```
CLI network-admin@switch > fabric-anycast-mac-modify  mac
72:0e:94:40:00:02
```

fabric-anycast-mac-show

This command is used to display the anycast MAC address for the fabric.

Syntax `fabric-anycast-mac-show`

`mac` *`mac-address`*	Displays the anycast MAC address for the fabric. The default value is `64:0e:94:40:00:02`,

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to display the anycast MAC address for Virtual Routing and Forwarding (VRF).

Examples To display the anycast MAC address, use the following syntax:

```
CLI network-admin@switch > fabric-anycast-mac-show

  mac:       64:0e:94:40:00:02
```

fabric-comm-vrouter-bgp-create

This command is used to create a fabric over a Layer 3 network using a BGP vRouter.

Syntax `fabric-comm-vrouter-bgp-create`

`name` *`name-string`*	Specify the name of the fabric communication vRouter.
`bgp-as` *`number`*	Specify the BGP Autonomous System number from 1 to 4294967295.
`bgp-redistribute  static|connected|rip|ospf`	Specify the BGP route redistribution type.
`bgp-max-paths` *`integer`*	Specify the maximum BGP paths from 1 to 255.
`bgp-ibgp-multipath` *`integer`*	Specify the number of IBGP multipath connections from 1 to 255.
`router-id` *`ip-address`*	Specify the vRouter ID.

hw-vrrp-id *hw-vrrp-id-number*	Specify the VRRP ID assigned to the hardware router.
bgp-nic-ip *ip-address*	Specify the IP address.
bgp-nic-netmask netmask	Specify the netmask.
bgp-nic-linklocal *ip-address*	Specify the IPv6 link local address.
bgp-nic-vnet *vnet name*	Specify the VLAN interface.
bgp-nic-bd *bridge-domain name*	Specify the bridge domain interface.
bgp-nic-vlan *vlan-id*	Specify the VLAN ID.
bgp-nic-vlan-type public|private	Specify the VLAN type as public or private.
bgp-nic-l3-port *l3port-usable-port name*	Specify the Layer 3 port.
in-band-nic-ip *ip-address*	Specify the IP address of the in-band management interface.
in-band-nic-netmask *netmask*	Specify the netmask of the in-band management interface.
in-band-nic-linklocal *ip-address*	Specify the IPv6 link local address.
in-band-nic-vnet *vnet name*	Specify the VLAN interface.
in-band-nic-bd *bridge-domain name*	Specify the bridge domain interface.
in-band-nic-vlan *vlan-id*	Specify the VLAN interface.
in-band-nic-if-nat-realm internal| external	Specify the NAT interface realm.
neighbor *ip-address*	Specify the IP address of the BGP neighbor.
remote-as *integer*	Specify the BGP remote AS from 1 to 4294967295.
next-hop-self| no-next-hop-self	Specify the next hop as self or not.
password *password-string*	Specify the MD5 password for BGP.
ebgp-multihop *integer*	Specify the value for external BGP from 1 to 255.
override-capability| no-override-capability	Specify if you want override capability.

`soft-reconfig-inbound|no-soft-reconfig-inbound`	Specify if you want a soft reset to reconfigure inbound traffic.
`max-prefix` *`max-prefix-number`*	Specify the maximum number of prefixes.
`max-prefix-warn-only|no-max-prefix-warn-only`	Specify you want to receive a warning if the maximum number of prefixes is exceeded.
`bfd|no-bfd`	Specify if you want BFD protocol support for fault detection.
`weight none`	Specify the weight value between 0 and 65535 for the neighbor's routes. The default is none.
`default-originate|no-default-originate`	Specify to announce default routes to the neighbor or not.
`neighbor-keepalive-interval` *`seconds`*	Specify the keepalive interval in seconds. This is a value between 0 and 65535 seconds.
`neighbor-holdtime` *`seconds`*	Specify the neighbor hold time in seconds. This is a value between 0 and 65535 seconds
`allowas-in|no-allowas-in`	Specify if you want to reject routes with local AS in AS_PATH. Normally, when you do not set this option, nodes reject routes containing their own AS which helps prevent routing loops. However, in some cases nodes that belong to the same AS have no direct connectivity; for example when you form clusters and choose not to use the cluster link for iBGP communication. In this case the only way to direct routes through connected eBGP neighbors is to set this option so routes are not rejected routes from the cluster peer.
`interface vrouter interface` *`nic`*	Specify the interface to reach the neighbor.
`advertisement-interval 0..600`	Specify the minimum interval between sending BGP routing updates.
`no-route-map-in`	Specify if you want to remove an ingress route map.
`no-route-map-out`	Specify if you want to remove an egress route map.
`fabric-network` *`ip-address`*	Specify the in-band network IP address.
`fabric-netmask` *`netmask`*	Specify the in-band network mask.

Defaults None

Access Network administrator

History

Version 2.4.1	Command introduced.
Version 2.5.2	The parameter, allowas-in|no-allowas-in, added.
Version 3.0.0	The parameter, `interface`, added.
Version 3.1.0	The parameters, `advertisement-interval`, `no-route-map-in`, and `no-route-map-out`, added.

Usage This command is used to allow fabric communication over a Layer 3 network.

fabric-comm-ports-modify

This command is used to modify communication ports on a fabric.

Syntax `fabric-comm-ports-modify range-start port-number`

`range-start` *`port-number`*	Modify the communications port range. This is a value between 1024 and 65435 .

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to modify fabric communication ports.

Examples To modify fabric communication ports, use the following syntax:

```
CLI network-admin@switch > fabric-comm-ports-modify range-start 1050-
1060
```

fabric-comm-ports-show

This command is used to display communication ports on a fabric.

Syntax `fabric-comm-ports-show`

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to display fabric communication ports.

Examples To display fabric communication ports, use the following syntax:

```
CLI network-admin@switch > fabric-comm-ports-show

switch:                         Leaf-1
range-start:                    23300
```

```
fabric-port:                    23399
notify-port:                    23398
proxy-port:                     23397
fabric-keepalive-port:          23394
filesystem-replication-port:    23392
cluster-traffic-forwarding-port: 23391
vport-statistics-port:          23390
l2-encap-port:                  23389
igmp-encap-port:                23388
icmpv6-encap-port:              23387
arp-encap-port:                 23386
cluster-analytics-port:         23385
```

fabric-create

This command is used to create a fabric on the network.

Syntax `fabric-create`

`name` *`name-string`*	Specify the name of the fabric.
Specify any of the following options:	
`repeer-to-cluster-node` *`cluster-repeer-node name`*	Specify if you want to replace a dead cluster node by restoring the switch against the existing cluster node.
`vlan` *`vlan-id`*	Specify VLAN for the fabric.
`password` *`password-string`*	Specify the fabric password.
`fabric-network in-band|mgmt`	Specify the in-band interface or the management interface to send fabric communications over the fabric.
`control-network` `in-band|mgmt`	Specify the in-band interface or the management interface to send fabric communications over the control plane.
`delete-conflicts|` `abort-on-conflict`	Specify the action to take when there is a conflict with another fabric.
`fabric-advertisement-network inband-mgmt|inband-vmgmt|inband-only|mgmtonly`	Specify the network for fabric advertisement.

Defaults If the multicast address is not specified, a random IPv6 address in the range from ff95::239:4:10:1 to ff95::239:4:10:ff is used as the default fabric multicast address. Unless you specify a password, the default password for the fabric is blank.

Access CLI

History

Version 1.2	Command introduced.
Version 2.2	The parameter, `mcast-ip`, deprecated. The parameter, `vlan`, added.
Version 2.2.4	The parameter, `network-type`, added.
Version 2.4	The parameter, `network-type`, removed. Two parameters, `fabric-network` and `control-network` added. The parameter, `repeer-to-cluster-node`, added.
Version 2.4.1	The parameters, `fabric-advertisement-network inband-mgmt|inband-only` added.

Usage The fabric consists of one or more switches that share a fabric administrative domain. The fabric presents the abstraction of a big logical switch with a single point of management, hiding the complexity of the underlying collection of switch hardware and inter-switch links. This command creates the fabric abstraction, but not the switch membership.

Examples To create a fabric named `MyFabric` with the password `b0n3s123`

```
CLI network-admin@switch > fabric-create name MyFabric password
b0n3s123
```

fabric-info

This command is used to display information about a fabric on the switch.

Syntax `fabric-info`

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage The fabric consists of one or more switches that share an administrative domain. The fabric presents the abstraction of a big logical switch with a single point of management, hiding the complexity of the underlying collection of switch hardware and inter-switch links. Use this command to display information about the fabric on a local switch.

Examples To display information about a fabric, use the following command:

```
CLI network-admin@switch > fabric-info

  name:     pn-fab
  ident:    a1634:b
  mcastaddr:ff95::239:4:10:2c
  tid:      0
```

fabric-join

This command is used to join an existing fabric on the switch.

Syntax `fabric-join`

Specify one of the following options:	
`name` *`name-string`*	Specify the name of the fabric.
`password` *`password-string`*	Specify the fabric password if configured.
`switch-ip` *`ip-address`*	Specify the IP address of the switch joining the fabric.
Specify any of the following options:	
`vlan` *`vlan-id`*	Specify VLAN for the fabric.
`delete-conflicts|` `abort-on-conflict`	Specify the action to take when there is a conflict with another fabric.
`location-id` *`location-id-number`*	Specify the location ID to use for joining the fabric.
`repeer-to-cluster-node` *`cluster-repeer-node name`*	Replace a dead cluster node by restoring against the existing cluster node.

Defaults None.

Access CLI

History

Version 1.2	Command introduced.
Version 2.2	The parameter, `vlan`, added.
Version 2.3	The parameter, `repeer-to-cluster-node`, added.
Version 3.0.0	The parameter, `repeer-to-cluster-node`, deprecated. The parameter `location-id` added.
Version 5.1.1	The parameter, `repeer-to-cluster-node`, re-added.

Usage The fabric consists of one or more switches that share an administrative domain. The fabric presents the abstraction of a big logical switch with a single point of management, hiding the complexity of the underlying collection of switch hardware and inter-switch links. Use this command to join a fabric.

Examples To join the fabric, **network-1**, with the id, **admin**, and the password, **`pizzatime`**, use the following command:

```
CLI network-admin@switch > fabric-join name network-1 id admin password
pizzatime
```

fabric-local-modify

This command is used to modify a local fabric on the network.

Syntax `fabric-local-modify`

`vlan` *`vlan-id`*	Specify the VLAN to modify on the local fabric.
`control-network in-band|mgmt`	Specify the in-band interface or the management interface to send fabric communications over the control plane.
`fabric-network in-band|mgmt`	Specify the in-band interface or the management interface for fabric administrative network.
`fabric-advertisement-network inband-mgmt|inband-vmgmt|inband-only|mgmt-only`	Specify if you want to send fabric advertisement packets over the inband management interface or inband only.

Defaults The default VLAN for a fabric is VLAN 0.

Access CLI

History .

Version 2.2	Command introduced.
Version 2.2.4	The parameter, `network-type`, introduced.
Version 2.4	The parameter, `network-type`, removed. Two parameters, `fabric-network` and `control-network` added. The parameter, `repeer-to-cluster-node`, added.
Version 2.4.1	The parameter, `fabric-advertisement-network`, added.

Usage In some network configurations, you may want to assign a different VLAN to a local fabric.

Examples To modify a local fabric and assign it to VLAN 2, use the following syntax:

```
CLI network-admin@switch > fabric-local-modify vlan 2
```

fabric-stats-show

This command is used to display statistical information about the fabric configured on the network.

Syntax `fabric-stats-show`

`id` *`id-number`*	Specifies the ID number automatically assigned to the fabric.
`servers` *`servers-number`*	Specifies the number of servers in the fabric.
`storage` *`storage-number`*	Specifies the storage occupying the fabric.
`VM` *`VM-number`*	Specifies the number of VMs in the fabric.

vlan *vlan-number*	Specifies the number of VLANs in the fabric.
vxlan *vxlan-number*	Specifies the number of VXLANs in the fabric.
tcp-syn *tcp-syn-number*	Specifies the number of TCP packets synchronized by the fabric.
tcp-est *tcp-est-number*	Specifies the number of TCP packets estimated on the network.
tcp-completed *tcp-completed-number*	Specifies the number of completed TCP packets.
tcp-bytes *tcp-bytes-number*	Specifies the number of TCP bytes sent through the fabric.
udp-bytes *udp-bytes-number*	Specifies the number of UDP bytes sent through the fabric.
arp *arp-number*	Specifies the number of ARPs on the fabric.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.4	The parameter, VLAN, deprecated.
Version 2.4.1	The parameter, vlan, added.

Usage Use this command to display statistical information about the fabric configured on the network.

Examples To display the statistics about the fabric, use this command:

```
CLI network-admin@switch > fabric-stats-show layout vertical
switch:              pleiades25
id:                  0
servers:             0
storage:             0
VM:                  0
vxlan:               0
tcp-syn:             294
tcp-est:             51
tcp-completed:       67
tcp-bytes:           149
udp-bytes:           0
arp:                 0
vlan:                0
```

fabric-show

This command is used to display information about a fabric on the switch.

Syntax `fabric-show`

name *name-string*	Specifies the name of the fabric.
switch-ip *ip-address*	Specify the IP address of the switch joining the fabric.
id	Specifies the identifier for the fabric.
repeer-to-cluster-node *cluster-repeer-node name*	Specifies if the action is to replace a dead cluster node by restoring against the existing cluster node.
vlan *vlan-id*	Specifies the VLAN ID for the fabric.
fabric-network in-band|mgmt	Specifies the fabric network as in-band or management network.
control-network in-band|mgmt	Specifies the control network type as in-band or through the management interface.
tid *tid-number*	Specifies the transaction identifier.
fabric-advertisement-network inband-mgmt|inband-vmgmt|inband-only| mgmt-only	Specify if you want to send fabric advertisement packets over the inband management interface or inband only.

Defaults None.

Access CLI

History

Version 1.2	Command introduced.
Version 2.2	The parameters, `multicast-ip`, and `cid`, deprecated.
Version 2.2.8	The parameter, `network-type`, added.
Version 2.3	The parameter, `repeer-to-cluster-node`, added.
Version 2.4	The parameter, `network-type`, changed to `fabric-network` and `control-network`.

Usage The fabric consists of one or more switches that share an administrative domain. The fabric presents the abstraction of a big logical switch with a single point of management, hiding the complexity of the underlying collection of switch hardware and inter-switch links. Use this command to display information about the fabric.

Examples To display the fabric, network-1, use the following command:

```
CLI network-admin@switch > fabric-show name network-1

name:                           network-1
id:                 b0000dd:577a8c70
vlan:               0
fabric-network:     in-band
```

```
control-network:        in-band
tid:                    11
```

fabric-unjoin

This command is used to unjoin an existing fabric on the switch.

Syntax `fabric-unjoin [delete-conflicts|abort-on-conflict]`

`delete-conflicts|abort-on-conflict`	Specify the action to take when there is a conflict with another fabric.

Defaults None.

Access CLI

License SDF

History Command introduced in nvOS Version 1.2.1.

Usage The fabric consists of one or more switches that share an administrative domain. The fabric presents the abstraction of a big logical switch with a single point of management, hiding the complexity of the underlying collection of switch hardware and inter-switch links. Use this command to join a fabric.

Examples To join the fabric, `network-1`, with the id, `admin`, and the password, `pizzatime`, use the following command:

```
CLI network-admin@switch > fabric-unjoin name network-1 id admin
password pizzatime
```

fabric-stats-show

This command is used to display statistical information about the fabric configured on the network.

Syntax `fabric-stats-show`

`id` *`id-number`*	Specifies the ID number automatically assigned to the fabric.
`servers` *`servers-number`*	Specifies the number of servers in the fabric.
`storage` *`storage-number`*	Specifies the storage occupying the fabric.
`VM` *`VM-number`*	Specifies the number of VMs in the fabric.
`vlan` *`vlan-number`*	Specifies the number of VLANs in the fabric.
`vxlan` *`vxlan-number`*	Specifies the number of VXLANs in the fabric.
`tcp-syn` *`tcp-syn-number`*	Specifies the number of TCP packets synchronized by the fabric.
`tcp-est` *`tcp-est-number`*	Specifies the number of TCP packets estimated on the network.
`tcp-completed` *`tcp-completed-number`*	Specifies the number of completed TCP packets.

tcp-bytes *tcp-bytes-number*	Specifies the number of TCP bytes sent through the fabric.
udp-bytes *udp-bytes-number*	Specifies the number of UDP bytes sent through the fabric.
arp *arp-number*	Specifies the number of ARPs on the fabric.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.4	The parameter, VLAN, deprecated.
Version 2.4.1	The parameter, vlan, added.

Usage Use this command to display statistical information about the fabric configured on the network.

Examples To display the statistics about the fabric, use this command:

```
CLI network-admin@switch > fabric-stats-show layout vertical
switch:              pleiades25
id:                  0
servers:             0
storage:             0
VM:                  0
vxlan:               0
tcp-syn:             294
tcp-est:             51
tcp-completed:       67
tcp-bytes:           149
udp-bytes:           0
arp:                 0
vlan:                0
```

fabric-in-band-network-create

This command is used to create an in-band fabric network.

Syntax fabric-in-band-network-create network *ip-address* netmask *netmask*

network *ip-address*	Specify an in-band network IP address.
netmask *netmask*	Specify the netmask.

Defaults None

Access Network Admin

History Command introduced in Version 2.4.1.

Usage Use this command to create an in-band network for a fabric.

Examples To create an in-band network using the IP address 172.16.21.135, and netmask 255.255.255.0, use the following syntax:

```
CLI network-admin@switch > fabric-in-band-network-create network
172.16.21.135 netmask 255.255.255.0
```

fabric-in-band-network-delete

This command is used to delete an in-band fabric network.

Syntax `fabric-in-band-network-delete network` *`ip-address`* `netmask` *`netmask`*

`network` *`ip-address`*	Specify an in-band network IP address.
`netmask` *`netmask`*	Specify the netmask.

Defaults None

Access Network Admin

History Command introduced in Version 2.4.1.

Usage Use this command to delete an in-band network for a fabric.

Examples To delete an in-band network using the IP address 172.16.21.135, and netmask 255.255.255.0, use the following syntax:

```
CLI network-admin@switch > fabric-in-band-network-delete network
172.16.21.135 netmask 255.255.255.0
```

fabric-in-band-network-show

This command is used to display an in-band fabric network network.

Syntax `fabric-in-band-network-show network ip-address netmask netmask`

`network` *`ip-address`*	Specify an in-band network IP address.
`netmask` *`netmask`*	Specify the netmask.

Defaults None

Access Network Admin

History Command introduced in Version 2.4.1.

Usage Use this command to display an in-band network for a fabric .

Examples To display an in-band network, use the following syntax:

```
CLI network-admin@switch > fabric-in-band-network-show
```

fabric-node-evict

This command is used to remove a node from a fabric.

Syntax `fabric-node-evict name fabric-node-name id id-number`

`name fabric-node-name`	Specify the name of the fabric node to remove from the configuration.
`id id-number`	Specify the identifier of the fabric node.

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage The fabric consists of one or more switches sharing an administrative domain. The fabric presents the abstraction of a big logical switch with a single point of management, hiding the complexity of the underlying collection of switch hardware and inter-switch links. Use this command to remove a node.

Examples To remove the node, `ursa123`, use the following command:

```
CLI network-admin@switch > fabric-node-evict name switch123
```

fabric-node-location-mappings

Netvisor uses this command to generate location mappings for importing switch configurations.

Syntax `fabric-node-location-mappings`

`id id-number`	Displays the ID assigned to the node.
`location-id location-id-number`	Displays the location ID assigned to the fabric.
`serial serial-string`	Displays the serial number.
`name fabric-node name`	Displays the node name.
`fab-name fab-name-string`	Displays the fabric name.
`fab-id`	Displays the ID assigned to the fabric.
`cluster-id`	Displays the ID assigned to the cluster.
`local-mac mac-address`	Displays the local MAC address.
`fabric-network in-band|mgmt`	Displays the network fabric.

control-network *in-band|mgmt*	Displays the control plane network.
mgmt-ip *ip-address*	Displays the management IP address.
mgmt-netmask *netmask*	Displays the management netmask.
mgmt-ip2 *ip-address*	Displays the second management IP address.
mgmt-netmask2 *netmask*	Displays the second management netmask
mgmt-assignment2 none|dhcp|dhcpv6	Displays the type of IP address assignment.
mgmt-linklocal *ip-address*	Displays the IPv6 address of the link local.
mgmt-assignment-linklocal none|dhcp| dhcpv6	Displays the type of IP address assignment.
mgmt-mac *mac-address*	Displays the interface MAC address.
mgmt-vnet vnet *name*	Displays the interface VLAN VNET.
mgmt-public-vlan *vlan-id*	Displays the public VLAN ID.
mgmt-secondary-macs *secondary-macs-string*	Displays the secondary MAC addresses.
mgmt-if-nat-realm internal|external	Displays the NAT interface realm.
vmgmt-ip *ip-address*	Displays the IP address.
vmgmt-netmask *netmask*	Displays the netmask.
vmgmt-ip2 *ip-address*	Displays the second IP address.
vmgmt-netmask2 *netmask*	Displays the netmask.
vmgmt-assignment2 none|dhcp|dhcpv6	Displays the type of lPv6 address assignment.
vmgmt-linklocal *ip-address*	Displays the IPv6 linklocal address.
vmgmt-assignment-linklocal none|dhcp| dhcpv6	Displays the type of IPv6 address assignment.
vmgmt-mac *mac-address*	Displays the MAC address.
vmgmt-vnet vnet *name*	Displays the VNET name.
vmgmt-vlan *vlan-id*	Displays the VLAN ID.
vmgmt-public-vlan *vlan-id*	Displays the public VLAN ID.
vmgmt-secondary-macs *secondary-macs-string*	Displays the secondary MAC addresses.
in-band-ip *ip-address*	Displays the IP address.
in-band-netmask *netmask*	Displays the netmask.

in-band-ip2 *ip-address*	Displays the second IP address.
in-band-netmask2 *netmask*	Displays the netmask.
in-band-assignment2 none|dhcp|dhcpv6	Displays the type of lPv6 address assignment.
in-band-linklocal *ip-address*	Displays the IPv6 linklocal address.
in-band-assignment-linklocal none|dhcp|dhcpv6	Displays the type of IPv6 address assignment.
in-band-mac *mac-address*	Displays the MAC address.
in-band-vnet vnet name	Displays the VNET name.
in-band-bd *bridge-domain name*	Displays the interface bridge domain.
in-band-vlan *vlan-id*	Displays the VLAN ID.
in-band-vlan-type public|private	Displays the type of VLAN.
in-band-public-vlan *vlan-id*	Displays the public VLAN ID.
in-band-secondary-macs *secondary-macs-string*	Displays the secondary MAC addresses.
in-band-if-nat-realm internal|external	Displays the interface NAT realm.
fab-tid *fab-tid-number*	Displays the fabric transaction ID.
cluster-tid *cluster-tid-number*	Displays the cluster transaction ID.
out-port *out-port-number*	Displays the fabric outgoing port.
version *version-string*	Displays the Netvisor version.
state offline|online|in-band-only-online|vmgmt-only-online|mgmt-only-online|fabric-joined|eula-required|setup-required|fabric-required|fresh-install	Displays the fabric state.
firmware-upgrade	Displays the firmware upgrade status.
device-state	Displays the device state.
ports *ports-number*	Displays the ports.
keepalive-timeout high resolution time: #*ns*	Displays the keepalive timeout in nanoseconds.

Access Network Administrator

History Command introduced in Version 3.1.0.

Usage Use this command to generate location mappings for a node.

Examples To generate location mappings for a node, use the following syntax:

```
CLI network-admin@switch > fabric-node-locations-  mapping
```

fabric-node-show

This command is used to display information about a node from a fabric.

Syntax `fabric-node-show`

`name` *`fabric-node-name`*	Specifies the name of the fabric node to display information.
`id` *`id-string`*	Specifies the identifier for the fabric node
`location-id` *`location-id-number`*	Specifies the location ID assigned to the fabric node.
`serial` *`serial-string`*	Specifies the serial string for the fabric node
`fab-name` *`fab-name`*	Specifies the name of the fabric node
`fab-id`	Specifies the fabric identifier
`cluster-id`	Specifies the cluster identifier
`fabric-network in-band|mgmt|vmgmt`	Specifies the fabric network type.
`control-network in-band|mgmt||vmgmt`	Specifies the interface to send control plane communications.
`local-mac` *`mac-address`*	Specifies the local MAC address of the fabric
`mgmt-ip` *`ip-address`*	Specifies the IP address for the management NIC
`mgmt-netmask` *`netmask`*]	The netmask for the IP address
`mgmt-ip2` *`ip-address`*	Specifies the second IP address for the management NIC
`mgmt-netmask2` *`netmask`*]	Specifies the netmask for the second IP address.
`mgmt-assignment2 none|static|dhcp| dhcpv6|autov6`	Specifies the type of IP address assignment.
`mgmt-linklocal` *`ip-address`*	Specifies the IPv6 address for the link local address.
`mgmt-assignment-linklocal none| static|dhcp|dhcpv6|autov6`	Specifies the type of link local IP address assignment.
`mgmt-mac` *`mac-address`*	Specifies the MAC address for the management interface.
`mgmt-vnet` *`vnet-name`*	Specifies the management VNET.
`mgmt-public-vlan` *`vlan-id`*	Specifies the public VLAN ID.
`mgmt-secondary-mac` *`mac-address`*	Specifies the secondary MAC address of the management interface

vmgmt-ip *ip-address*	Specifies the IP address for the in-band interface to the switch control plane.
vmgmt-netmask *netmask*	Specifies the netmask for the in-band interface to the switch control plane.
vmgmt-ip2 *ip-address*	Specifies the second IP address for the in-band interface to the switch control plane.
vmgmt-netmask2 *netmask*	Specifies the second netmask for the in-band interface to the switch control plane.
vmgmt-mac *mac-address*	Specifies the MAC address for the in-band interface to the switch control plane.
vmgmt-vnet *vnet-name*	Specifies the inband VNET name.
vmgmt-vlan *vlan-id*	Specifies the inband VLAN ID.
vmgmt-band-vlan-type public|private	Specifies the type of inband VLAN as public or private.
vmgmt-public-vlan *vlan-id*	Specifies the inband public VLAN ID.
vmgmt-secondary-mac *mac-address*	Specifies the secondary MAC address of the in-band interface
vmgmt-sec-addresses *sec-addresses-number*	
in-band-ip *ip-address*	Specifies the IP address for the in-band interface to the switch control plane.
in-band-netmask *netmask*	Specifies the netmask for the in-band interface to the switch control plane.
in-band-ip2 *ip-address*	Specifies the second IP address for the in-band interface to the switch control plane.
in-band-netmask2 *netmask*	Specifies the second netmask for the in-band interface to the switch control plane.
in-band-mac *mac-address*	Specifies the MAC address for the in-band interface to the switch control plane.
in-band-vnet *vnet-name*	Specifies the inband VNET name.
in-band-vlan *vlan-id*	Specifies the inband VLAN ID.
in-band-vlan-type public|private	Specifies the type of inband VLAN as public or private.
in-band-public-vlan *vlan-id*	Specifies the inband public VLAN ID.
in-band-secondary-mac *mac-address*	Specifies the secondary MAC address of the in-band interface
fab-tid *fab-tid-number*	Specifies the fabric identifier.
cluster-tid *cluster-tid-number*]	Specifies the cluster identifier.

out-port *out-port-number*	Specifies the port number where the switch multicasts the fabric discovery messages to other Pluribus Networks switch.
version *version-string*	Specifies the current ONVL version.
state offline|online|inband-only-online|mgmt-only-online| fabric_joined|setup-required| eula-required|fabric-required| fresh-install]	Specifies the state of the fabric.
firmware_upgrade not-required|required|reboot-required	Specifies if a firmware upgrade is required.
device-state ok|error|simulator	Specifies the state of the switch.
ports *ports-number*	Specifies the port list used by the fabric.
keepalive-timeout high resolution time: #ns	Specifies the keepalive timeout in nanoseconds.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.3.2	The parameters, cluster-id, cluster-tid, mgmt-assignment, mgmt-vm-nic-type, mgmt-nic, mgmt-vxlan, mgmt-if, mgmt-alias-on, mgmt-vm-nic-type, mgmt-exclusive, mgmt-nic-enable, mgmt-nic-state, and corresponding in-band parameters deprecated.
Version 2.4.1	The parameters, mgmt-vnet, mgmt-public-vlan, in-band-vnet, in-band-vlan-type, and in-band-public-vlan added.
Version 5.1.1	The parameter, keepalive-timeout, added.

Usage The fabric consists of one or more switches sharing an administrative domain. The fabric presents the abstraction of a big logical switch with a single point of management, hiding the complexity of the underlying collection of switch hardware and inter-switch links. Use this command to display node information.

Examples To display a list of fabrics visible from the local switch, use the following command:

```
CLI network-admin@switch > fabric-node-show layout vertical
id:                         184551182
location-id:                2
```

```
serial:                         1714AC5700078
name:                           techpub-accton-2
fab-name:                       techpubs
fab-id:                         b00070c:5c562711
cluster-id:                     b00070c:0
local-mac:                      66:0e:94:0e:f7:9c
fabric-network:                 in-band
control-network:                in-band
mgmt-ip:                        10.13.22.47/23
mgmt-assignment2:               none
mgmt-assignment-linklocal:      none
mgmt-mac:                       64:0e:94:4c:10:34
mgmt-if-nat-realm:              internal
vmgmt-assignment2:              none
vmgmt-assignment-linklocal:     none
in-band-ip:                     5.5.5.9/24
in-band-assignment2:            none
in-band-assignment-linklocal: none
in-band-mac:                    66:0e:94:0e:f7:9c
in-band-vlan:                   1
in-band-vlan-type:              public
in-band-if-nat-realm:           internal
fab-tid:                        33
version:                        3.0.3000012772,#50~14.04.1-Ubuntu
state:                          online
firmware-upgrade:               not-required
device-state:                   ok
ports:                          72
```

fabric-upgrade-abort

This command is used to end a fabric-wide upgrade on the fabric.

Syntax `fabric-upgrade-abort {force|no-force]`

`force|no-force`	Specify if you want the upgrade to stop immediately or wait for a logical step in the upgrade process.

Defaults None.

Access CLI

History Command introduced in Version 2.2.6.

Usage The fabric consists of one or more switches that share an administrative domain. The fabric presents the abstraction of a big logical switch with a single point of management, hiding the complexity of the underlying collection of switch hardware and inter-switch links. Use this command to stop a fabric-wide upgrade.

Examples To stop the fabric upgrade and end the process immediately, use the following command:

```
CLI network-admin@switch > fabric-upgrade-abort force
```

fabric-upgrade-continue

This command is used to continue a rolling fabric upgrade that is paused due to a node failure.

Syntax `fabric-upgrade-continue`

Defaults None.

Access CLI

History Command introduced in Version 2.2.6.

Usage The fabric consists of one or more switches that share an administrative domain. The fabric presents the abstraction of a big logical switch with a single point of management, hiding the complexity of the underlying collection of switch hardware and inter-switch links. Use this command to continue a fabric-wide upgrade.

Examples To continue the fabric upgrade, use the following command:

```
CLI network-admin@switch > fabric-upgrade-continue
```

fabric-upgrade-finish

This command is used to reboot the fabric after a fabric-wide upgrade.

Syntax `fabric-upgrade-finish`

Defaults None.

Access CLI

History Command introduced in Version 2.2.6.

Usage The fabric consists of one or more switches that share an administrative domain. The fabric presents the abstraction of a big logical switch with a single point of management, hiding the complexity of the underlying collection of switch hardware and inter-switch links. Use this command to reboot the nodes after a fabric-wide upgrade.

Examples To finish the upgrade, use the following syntax:

```
CLI network-admin@switch > fabric-upgrade-finish
```

fabric-upgrade-start

This command is used to start a fabric-wide upgrade.

Syntax `fabric-upgrade-start packages sftp-files` *name* `[auto-finish|no-auto-finish]prepare|no-prepare reboot-parallel|reboot-single reboot-group` *number*

`packages sftp-files` *name*	Specify a comma delimited list of the offline packages to use for the upgrade process.
`auto-finish|no-auto-finish`	Specify if you want to automatically reboot the fabric after the upgrade.
`rolling|no-rolling`	Specify if you want to perform a rolling upgrade across the fabric.
`abort-on-failure|`	Specify if you want to stop the upgrade process if

`no-abort-on-failure`	the upgrade fails on a node.
`manual-reboot|no-manual-reboot`	Specify if you want to manually reboot the switches so that all switches do not reboot at the same time.
`prepare|no-prepare`	Specify if you want to perform setup steps for the actual upgrade.
`reboot-parallel|reboot-single`	Specify if you want to perform parallel rolling reboots or reboot each switch one at a time. The default is `reboot-parallel`.
`reboot-count` *number*	Specify the number of switches to reboot together in parallel mode. The default is the maximum number of switches in the fabric.
`upload-server` *upload-server-string*	Specify the upload server string.
`server-password` *server-password-string*	Specify the server password.

Defaults None.

Access CLI

History

Version 2.2.6	Command introduced.
Version 2.3	The parameters `prepare`, `reboot-parallel`, and `reboot-group` added.
Version 3.1.0	The paramters, `upload-server`, and `server-password`, added.

Usage The fabric consists of one or more switches that share an administrative domain. The fabric presents the abstraction of a big logical switch with a single point of management, hiding the complexity of the underlying collection of switch hardware and inter-switch links. Use this command to begin a fabric-wide upgrade.

Examples To force the upgrade to end immediately, use the following syntax:

```
CLI network-admin@switch > fabric-upgrade-start
```

fabric-upgrade-status-show

This command is used to display the status of a fabric-wide upgrade.

Syntax `fabric-upgrade-status-show`

Defaults None.

Access CLI

History Command introduced in Version 2.2.6.

Usage The fabric consists of one or more switches that share an administrative domain. The fabric presents

the abstraction of a big logical switch with a single point of management, hiding the complexity of the underlying collection of switch hardware and inter-switch links. Use this command to display the status of a fabric-wide upgrade.

Examples To force the upgrade to end immediately, use the following snyntax:

```
CLI network-admin@switch > fabric-upgrade-status-show
```

fabric-upgrade-prepare-cancel

Use this command to cancel a fabric upgrade prepared earlier.

Syntax `fabric-upgrade-prepare-cancel`

Defaults None

Access Network Administrator

History Command introduced in Version 5.1.1.

Usage If you prepared a switch for an upgrade and want to cancel it, use this command.

Examples To cancel a fabric upgrade, use the following syntax:

```
CLI network-admin@switch > fabric-upgrade-prepare-cancel
```

fabric-upgrade-prepare-resume

Use this command to resume a fabric upgrade prepared earlier.

Syntax `fabric-upgrade-prepare-resume`

Defaults None

Access Network Administrator

History Command introduced in Version 5.1.1.

Usage If you prepared a switch for an upgrade and want to resume it, use this command.

Examples To resume a fabric upgrade, use the following syntax:

```
CLI network-admin@switch > fabric-upgrade-prepare-resume
```

fabric-upgrade-prepare-show

Use this command to displays prepared fabric upgrades.

Syntax `fabric-upgrade-prepare-show`

Defaults None

Access Network Administrator

History Command introduced in Version 5.1.1.

Usage If you prepared a switches for an upgrade and want to display them, use this command.

Examples To display prepared fabric upgrades, use the following syntax:

```
CLI network-admin@switch > fabric-upgrade-prepare-show
```

fabric-vnic-create

Netvisor allows the creation of a management interface on a Virtual Network Interface Card (vNIC) for fabric communication. In the current fabric, Netvisor allows two subnets: one for out-of-band provisioning and fabric, and one for in-band fabric. This feature allows three subnets per fabric:

- An out-of-band provisioning subnet
- An out-of-band fabric subnet
- An in-band fabric subnet

Each subnets uses a separate VLAN for traffic isolation purposes. When a vNIC is created for the management interface, fabric communication automatically switches to this vNIC, without additional configuration.

Syntax `fabric-vnic-create`

`ip` *`ip-address`*	Specify the IP address of the vNIC.
`netmask` *`netmask`*	Specify the netmask for the IP address.
`vlan` *`vlan-id`*	Specify the VLAN ID for the vNIC. This must be unique to the vNIC.

Defaults None

Access Network Administrator

History Command introduced in Version 5.1.1.

Usage Use this command to create a vNIC for fabric management.

Examples To create a vNIC with IP address, 20.1.1.1/24 on VLAN 22, use the following syntax:

```
CLI network-admin@switch > fabric-vnic-create ip 20.1.1.1 netmask 255.255.255.0 vlan 22
```

fabric-vnic-delete

Netvisor allows the creation of a management interface on a Virtual Network Interface Card (vNIC) for fabric communication. In the current fabric, Netvisor allows two subnets: one for out-of-band provisioning and fabric, and one for in-band fabric. This feature allows three subnets per fabric:

- An out-of-band provisioning subnet

- An out-of-band fabric subnet
- An in-band fabric subnet

Each subnets uses a separate VLAN for traffic isolation purposes. When a vNIC is created for the management interface, fabric communication automatically switches to this vNIC, without additional configuration.

Syntax `fabric-vnic-delete`

Defaults None

Access Network Administrator

History Command introduced in Version 5.1.0.

Usage Use this command to delete a vNIC for fabric management.

Examples To modify a vNIC with IP address, 20.1.1.1/24 on VLAN 32, use the following syntax:

```
CLI network-admin@switch > fabric-vnic-delete
```

fabric-vnic-modify

Netvisor allows the creation of a management interface on a Virtual Network Interface Card (vNIC) for fabric communication. In the current fabric, Netvisor allows two subnets: one for out-of-band provisioning and fabric, and one for in-band fabric. This feature allows three subnets per fabric:

- An out-of-band provisioning subnet
- An out-of-band fabric subnet
- An in-band fabric subnet

Each subnets uses a separate VLAN for traffic isolation purposes. When a vNIC is created for the management interface, fabric communication automatically switches to this vNIC, without additional configuration.

Syntax `fabric-vnic-modify`

`ip` *`ip-address`*	Specify the IP address of the vNIC.
`netmask` *`netmask`*	Specify the netmask for the IP address.
`vlan` *`vlan-id`*	Specify the VLAN ID for the vNIC. This must be unique to the vNIC.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to modify a vNIC for fabric management.

Examples To modify a vNIC with IP address, 20.1.1.1/24 on VLAN 32, use the following syntax:

```
CLI network-admin@switch > fabric-vnic-modify ip 20.1.1.1 netmask 255.255.255.0 vlan 32
```

fabric-vnic-show

Netvisor allows the creation of a management interface on a Virtual Network Interface Card (vNIC) for fabric communication. In the current fabric, Netvisor allows two subnets: one for out-of-band provisioning and fabric, and one for in-band fabric. This feature allows three subnets per fabric:

- An out-of-band provisioning subnet
- An out-of-band fabric subnet
- An in-band fabric subnet

Each subnets uses a separate VLAN for traffic isolation purposes. When a vNIC is created for the management interface, fabric communication automatically switches to this vNIC, without additional configuration.

Syntax `fabric-vnic-show`

ip *ip-address*	Displays the IP address of the vNIC.
netmask *netmask*	Displays the netmask for the IP address.
vlan *vlan-id*	Displays the VLAN ID for the vNIC. This must be unique to the vNIC.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to display information about a fabric management vNIC.

Examples To display information about a fabric management vNI, use the following syntax:

```
CLI network-admin@switch > fabric-vnic-show
nic:            vmgmt0
ip:               20.1.1.1/24
mac:               66:0e:94:6a:2a:ad
vlan:          20
nic-config:  enable
nic-state:   up
```

From the output, you can see the status of the interface as enabled and up as well as the vNIC name, IP

address, MAC address, and VLAN.

factory-reset

This command is used to reset the switch to factory default settings.

Syntax `factory-reset`

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.1	Deprecated.
Version 2.6.2	Command re-introduced.

Usage This command restores all configuration and persistent state, including data on built-in storage devices, to factory default settings.

Examples To reset the switch use the following command:

```
factory-reset
```

flow-table-show

This command is used to display information about traffic flows on the switch.

Syntax `flow-table-show`

`name` *`name-string`*	Specifies the name of the traffic flow
`id` *`id-number`*	Specifies the identifier of the traffic flow
`hw-id` *`hw-id-number`*	Specifies the identifier of the hardware source
`flow-name` *`flow-name-string`*	Specifies the name of the traffic flow type
`flow-hw-id` *`flow-hw-id-number`*	Specifies the identifier of the hardware flow source

Defaults None

History

Version 1.2	Command introduced.
Version 2.0	The parameter, `flow-id` *`flow-id`*, deprecated.
Version 5.1.1	The parameter, `tbl-id`, deprecated.

Usage Each switch is built with a datapath ASIC inside and contains a set of hardware flow tables for traffic forwarding. Use this command to display flows as they are currently programmed in each of the hardware flow tables.

Examples To display the flows, use the following command:

```
CLI network-admin@switch > flow-table-show layout vertical

  switch:     pleaides24
  name:       Switch System Table - L2 to L4
  id:         2
  hw-id:      33
  flow-name:  Martian-L2-Check
  flow-id:    2
  flow-hw-id: 1048578
  switch:     pleaides24
  name:       Switch System Table - L2 to L4
  id:         2
  hw-id:      33
  flow-name:  Martian-IP4-L3-Check
  flow-id:    3
  flow-hw-id: 1048579
  switch:     pleaides24
  name:       Switch System Table - L2 to L4
  id:         2
  hw-id:      33
  flow-name:  Martian-IP6-L3-Check
  flow-id:    4
  flow-hw-id: 1048580
  switch:     pleaides24
  name:       Switch System Table - L2 to L4
  id:         2
  hw-id:      33
  flow-name:  STP-FLOW
  flow-id:    5
  flow-hw-id: 3145733
  switch:     pleaides24
  name:       Switch System Table - L2 to L4
  id:         2
  hw-id:      33
  flow-name:  PVST-FLOW
  flow-id:    6
  flow-hw-id: 1048582
  switch:     pleaides24
  name:       Switch System Table - L2 to L4
  id:         2
  hw-id:      33
  flow-name:  LLDP-NB-Flow
  flow-id:    7
  flow-hw-id: 1048583
  switch:     pleaides24
  name:       Switch System Table - L2 to L4
  id:         2
  hw-id:      33
  flow-name:  LLDP-NONTPMR-Flow
  flow-id:    8
```

```
flow-hw-id: 1048584
flow-hw-id: 1048585
```

H Commands

help

Displays usage information about commands.

Syntax `help`

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage Use this command to display usage information for all ONVL commands.

Examples To display usage information for fabric-create, use the following command:

```
CLI network-admin@switch > help fabric-create
name    name-string
any of the following options:
  mcast-ip ip-address
  password
  delete-conflicts|abort-on-conflict
```

hog-violator-show

The CPU Control Packet Processing Protection feature allows the CPU control packet processing path be protected against misbehaving and malicious hosts or end-points that may flood control protocol packets. This is also called “CPU hog protection”.

Netvisor provides three types of Control Plane Protection:

- Overall CPU Bandwidth
- Dedicated Queues for Critical Flows
- Protection from offending flows in Critical Queues (DDOS Protection) by using special CPU hog queues

Syntax `hog-violator-show`

`mac` *`mac-address`*	Displays the hog violator MAC address.
`vnet` *`vnet name`*	Displays the vNET name.
`bd` *`bridge-domain name`*	Displays the bridge domain name.
`vlan` *`vlan-id`*	Displays the hog violator VLAN ID.

`vxlan` *`vxlan-id`*	Displays the hog violator VXLAN ID.
`port` *`port-number`*	Displays the hog violator ingress port.
`cpu-class` *`cpu-class-string`*	Displays the hog violator original class.
`hog-cpu-class` *`hog-cpu-class-string`*	Displays the hog violator hog queue CPU class.
`created date/time:` *`yyyy-mm-ddTHH:mm:ss`*	Displays the time and date when hog violator is created.
`vflow` *`vflow-string`*	Displays the redirect vFlow.
`vflow2` *`vflow-string`*	Displays the redirect vFlow 2.
`vflow3` *`vflow-string`*	Displays the redirect vFlow 3.
`vflow4` *`vflow-string`*	Displays the redirect vFlow 4.
`vflow5` *`vflow-string`*	Displays the redirect vFlow 5.
`vflow6` *`vflow-string`*	Displays the redirect vFlow 6.
`idle-count` *`idle-count-number`*	Displays the current idle count.

Defaults None

Access Network Administrator

History

Version 2.6.0.	Command introduced.
Version 3.0.0	The parameter, `idle-count`, added.

Usage Use this command to display information about CPU hog violators.

Examples To display information about CPU hog violators, use the following syntax:

CLI network-admin@switch > hog-violator-show

```
mac               vlan vxlan  port cpu-class hog-cpu-class created
----------------- ---- ------ ---- --------- ------------- --------
66:0e:94:10:d8:4a 704         15   ospf      hog-ospf      13:13:58
66:0e:94:10:d8:4a 704         15   bfd       hog-bfd       13:14:02
06:c0:00:17:30:0f 16          15   lldp      hog-lldp      13:14:07
06:c0:00:17:30:0f 16          15   lacp      hog-lacp      13:14:10
66:0e:94:1d:09:58      101001 25   arp       hog-arp       13:14:19
00:00:5e:00:01:0b 2001        128  vrrp      hog-vrrp      13:14:22
```

```
06:c0:00:17:30:0e 16          15   stp       hog-stp       13:14:31
80:ac:ac:f0:aa:34 16          15   bgp       hog-bgp       13:14:35
00:00:33:33:33:33 2003        15   arp       hog-arp       13:14:46
```

hog-violator-stats-show

The CPU Control Packet Processing Protection feature allows the CPU control packet processing path be protected against misbehaving and malicious hosts or end-points that may flood control protocol packets. This is also called "CPU hog protection".

Netvisor provides three types of Control Plane Protection:

- Overall CPU Bandwidth
- Dedicated Queues for Critical Flows
- Protection from offending flows in Critical Queues (DDOS Protection) by using special CPU hog queues

Syntax `hog-violator-stats-show`

`time date/time: yyyy-mm-ddTHH:mm:ss`	Displays the time and date to start statistics collection.
`start-time date/time: yyyy-mm-ddTHH:mm:ss`	Displays the start time of the statistics collection.
`end-time date/time: yyyy-mm-ddTHH:mm:ss`	Displays the end time of the statistics collection.
`duration duration: #d#h#m#s`	Displays the duration of statistics collection.
`interval duration: #d#h#m#s`	Displays the interval between statistics collection.
`since-start`	Displays the statistics collection since the start time.
`older-than duration: #d#h#m#s`	Displays the statistics collection older than the time.
`within-last duration: #d#h#m#s`	Displays the statistics collection within a specified time period.
`name vflow-name`	Displays the name of the vFlow.
`vnet #d#h#m#s`	Displays the VNET name.
`id`	Displays the ID assigned by Netvisor.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to display settings for CPU hog violator statistics.

Examples To display settings for CPU hog violator statistics, use the following syntax:

```
CLI network-admin@switch > hog-violator-stats-settings-show

CLI network-admin@switch > show-diff-interval 1

name                                                    pkts  bytes cpu-pkts cpu-
bytes drops drop-bytes cpu-tx-pkts cpu-tx-bytes
------------------------------------------------------- ----- ----- --------
--------- ----- ---------- ---------- ------------
IP4-OSPF-hog-q20-66:0e:94:10:d8:4a-v704-vx0-p15         2.95M 372M  0        0
        0     0          0           0
BFD-Protocol-1Hop-hog-q21-66:0e:94:10:d8:4a-v704-vx0-p15 2.28M 233M  0        0
        0     0          0           0
BFD-Protocol-MHop-hog-q21-66:0e:94:10:d8:4a-v704-vx0-p15 0     0     0        0
        0     0          0           0
LLDP-NB-Flow-hog-q15-06:c0:00:17:30:0f-v16-vx0-p15      0     0     0        0
        0     0          0           0
LLDP-NONTPMR-Flow-hog-q15-06:c0:00:17:30:0f-v16-vx0-p15  5.48M 1.49G 11.2K
   3.03M     5.47M 1.49G      0           0
LLDP-NCB-Flow-hog-q15-06:c0:00:17:30:0f-v16-vx0-p15     0     0     0        0
        0     0          0           0
LACP-Local-hog-q6-06:c0:00:17:30:0f-v16-vx0-p15         6.39M 1022M 10.8K
   1.69M     6.38M 1021M      0           0
System-A-hog-q14-66:0e:94:1d:09:58-v0-vx101001-p25      201K  24.3M 7.23K    535K
     194K  23.8M      0           0
IP4-VRRP-hog-q22-00:00:5e:00:01:0b-v2001-vx0-p128       4.76M 391M  0        0
        0     0          0           0
IP6-VRRP-hog-q22-00:00:5e:00:01:0b-v2001-vx0-p128       0     0     0        0
        0     0          0           0
STP-Local-hog-q5-06:c0:00:17:30:0e-v16-vx0-p15          2.16M 363M  0        0
        0     0          0           0
PVST-Local-hog-q5-06:c0:00:17:30:0e-v16-vx0-p15         0     0     0        0
        0     0          0           0
IP4-BGP-Dst-Port-hog-q19-80:ac:ac:f0:aa:34-v16-vx0-p15  0     0     0        0
        0     0          0           0
IP4-BGP-Src-Port-hog-q19-80:ac:ac:f0:aa:34-v16-vx0-p15  4.11M 587M  0        0
        0     0          0           0
System-A-hog-q14-00:00:33:33:33:33-v2003-vx0-p15        1.44M 113M  6.32K    468K
     1.44M 112M       0           0
```

I Commands

id-led-modify

This command is used to locate the switch by blinking the LED on the front panel.

Syntax `id-led-modify enable|disable`

`enable|disable`	You can enable or disable this feature.

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage When you enable this feature, the LED on the switch blinks allowing you to physically locate it.

Examples To enable this feature, use the following command:

```
CLI network-admin@switch > id-led-modify  enable
```

id-led-show

This command is used to display LED parameters on the switch.

Syntax `id-led-show`

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage Use this command to display LED parameters on the switch.

Examples To display LED parameters, use the following command:

```
CLI network-admin@switch > id-led-show  layout  vertical
switch:    pleiades24
enable:    no
```

igmp-show

To show the Internet Group Management Protocol (IGMP) group membership information for a switch, use this command.

Syntax `igmp-show`

`group-ip` *`ip-address`*	Specifies the multicast group IP address.
`node-ip` *`ip-address`*	Specifies the node IP address
`vnet vnet-nam`	Specifies the name of the VNET.
`vlan` *`vlan-id`*	Specifies the VLAN identifier.
`port` *`port-number`*	Specifies the port number.
`source` *`ip-address`*	Specifies the multicast source traffic.
`node-type host|router|switch`	Specifies if the router is a host, router, or switch.

`expires` *`expires-number(s)`*	Specifies the ageout time on the IGMP router.

Defaults All IGMP group membership information for the local switch is displayed unless a single switch is specified.

Access CLI

History

Version 1.2	Commmand introduced.
Version 2.4	The parameters, `node-type`, and `expires`, added.
Version 2.4.1	The parameter, `host-ip`, changed to `node-ip`. The parameter, `vnet`, added.

Usage Use this command to display information about IGMP on the network.

Examples To display all IGMP group membership information for the local switch, use the following command:

```
CLI network-admin@switch > igmp-show
switch   group-ip  host-ip       vlan port source
-------- --------- ------------- ---- ---- -------
pubdev03 239.4.9.3 192.168.42.20 1    128  0.0.0.0
pubdev03 239.4.9.3 192.168.42.10 1    128  0.0.0.0
pubdev03 239.4.9.3 192.168.42.30 1    0    0.0.0.0
pubdev03 239.4.9.4 192.168.42.20 3    128  0.0.0.0
pubdev03 239.4.9.4 192.168.42.10 3    128  0.0.0.0
pubdev03 239.4.9.4 192.168.42.30 3    65   0.0.0.0
pubdev03 239.4.9.7 192.168.42.20 3    128  0.0.0.0
pubdev03 239.4.9.7 192.168.42.10 3    128  0.0.0.0
pubdev03 239.4.9.7 192.168.42.30 3    65   0.0.0.0
pubdev03 239.4.9.3 192.168.42.20 3    128  0.0.0.0
pubdev03 239.4.9.3 192.168.42.10 3    128  0.0.0.0
pubdev03 239.4.9.3 192.168.42.30 3    65   0.0.0.0
```

igmp-querier-ip-modify

You can configure an IGMP querier IP address for a VLAN or as a global IGMP querier. The IGMP querier sends IGMP General Query messages. on the network.

If you do not specify a querier IP address, then Netvisor uses 0.0.0.0 as the default value. There can be an unique querier IP for each VLAN, or you can configure the same Querier IP address for all the VLANs participating in IGMP snooping. The Querier IP address should have a local scope and every switch should have a unique Querier IP address.

With a valid source IP address on IGMP Query packets, the VLAN, where Query is received, is added to an IGMP Snoop switch list, and is now reflected in the `igmp-switches-show` output and the IGMP queries are sent to the peer Switch as well. This is to solicit a report from the hosts listening on the peer switch.

Syntax `igmp-querier-ip-modify`

`querier-ip` *`ip-address`*	Specify the Snooping Querier IP address.

`vlans-on-querier-ip` *`vlan-list`*	Specify the VLAN map for the querier IP address.

Defaults None

Access network-admin

History Command introduced in Version 2.5.

Usage Configure an IGMP querier IP address for a VLAN or as a global IGMP querier.

Examples To configure an IGMP querier IP address with a VLAN list of 12-15, use the following syntax:

```
CLI network-admin@switch > igmp-querier-ip-modify querier-ip 1.1.1.1
vlans-on-querier-ip 12-15
```

igmp-querier-ip-show

You can configure an IGMP querier IP address for a VLAN or as a global IGMP querier. The IGMP querier sends IGMP General Query messages. on the network.

If you do not specify a querier IP address, then Netvisor uses 0.0.0.0 as the default value. There can be an unique querier IP for each VLAN, or you can configure the same Querier IP address for all the VLANs participating in IGMP snooping. The Querier IP address should have a local scope and every switch should have a unique Querier IP address.

With a valid source IP address on IGMP Query packets, the VLAN, where Query is received, is added to an IGMP Snoop switch list, and is now reflected in the igmp-switches-show output and the IGMP queries are sent to the peer Switch as well. This is to solicit a report from the hosts listening on the peer switch.

Syntax `igmp-querier-ip-show`

`querier-ip` *`ip-address`*	Specify the Snooping Querier IP address.
`vlans-on-querier-ip` *`vlan-list`*	Specify the VLAN map for the querier IP address.

Defaults None

Access network-admin

History Command introduced in Version 2.5.

Usage Display an IGMP querier IP address for a VLAN or as a global IGMP querier.

Examples To display an IGMP querier IP address with a VLAN list of 12-15, use the following syntax:

```
CLI network-admin@switch > igmp-querier-ip-show querier-ip 1.1.1.1
vlans-on-querier-ip 12-15
```

igmp-router-show

This command is used to display IGMP routers on the network.

Syntax `igmp-router-show`

`node-ip` *`ip-address`*	Specifies the IP address of the host.
`vnet` *`vnet name`*	Specifies the host vNET.
`bd` *`bridge-domain name`*	Specifies the host bridge domain.
`vlan` *`vlan-id`*	Specifies the ID of the VLAN.
`port` *`port-number`*	Specifies the number of the port.

Defaults None

Access CLI

History

Version 2.2.2	Command introduced.
Version 5.1.1	The parameters, group-ip, `source`, `node-type`, and `expires`, deprecated. The parameters, vnet, and bd, added.

Usage Use this command to display information about IGMP routers on the network.

Examples To display information about IGMP routers on the network, use the following command:

```
CLI network-admin@switch > igmp-router-show
```

igmp-snooping-modify

This command enables or disables Internet Group Management Protocol (IGMP) snooping on the network.

Informational Note: Netvisor does not support IGMPv1. If you use IGMPv1, you must disable IGMP snooping on the Pluribus Networks switch

Syntax `igmp-snooping-modify`

Specify one or more of the following options:	
`scope local|fabric`	Specify if the scope is local or fabric.
`enable|disable`	Specify if IGMP snooping is enabled or disabled.
`vxlan|no-vxlan`	Specify to enable or disable IGMP snooping on VXLANs.
`enable-vlans` *`vlan-list`*	Specify a list of VLANs to enable for IGMP.
`snoop-linklocal-vlans` *`vlan-list`*	Specify if you allow snooping of link-local groups(224.0.0.0/24) on these VLANs.

`no-snoop-linklocal-vlans` *`vlan-list`*	Specify if you do not allow snooping of link-local groups(224.0.0.0/24) on these VLANs.
`igmpv3-vlans` *`vlan-list`*	Specify IGMP Version 3 VLAN list for sending queries.
`igmpv2-vlans` *`vlan-list`*	Specify IGMP Version 2 VLAN list for sending queries.
`query-interval` *`seconds`*	Specify the interval between queries in seconds.
`query-max-response-time` *`seconds`*	Specify the maximum response time for a query.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.1	The parameter, `scope`, added.
Version 2.4	The parameter, `version`, added.
Version 2.4.1	The parameter, `version`, changed to `igmpv2-vlans` and `igmpv3-vlans`. The parameter, `enable-vlans`, added.
Version 3.1.0	The parameters, `query-interval` and `query-max-response-time`, added.
Version 5.1.1	The parameters, VXLAN and `snoop-linklocal`, added.

Usage IGMP snooping allows the switch to listen in on IGMP traffic between hosts and routers, thus maintaining a map of the links that need IP multicast streams. Use this command to modify IGMP snooping on the switch.

Examples To enable IGMP snooping, use the following command:

```
CLI network-admin@switch > igmp-snooping-modify  enable
```

igmp-snooping-show

This command displays information about Internet Group Management Protocol (IGMP) snooping on the network.

Informational Note: Netvisor does not support IGMPv1. If you use IGMPv1, you must disable IGMP snooping on the Pluribus Networks switch

Syntax `igmp-snooping-show`

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage IGMP snooping allows the switch to listen in on IGMP traffic between hosts and routers, thus maintaining a map of the links that need IP multicast streams. Use this command to display IGMP snooping information on the switch.

Examples To display information about IGMP snooping, use the following command:

```
CLI network-admin@switch > igmp-snooping-show
switch: pubdev03
enable: yes
switch: pubdev02
enable: yes
switch: pubdev01
enable: yes
```

igmp-switches-show

This command is used to display switches with IGMP protocol enabled.

Syntax `igmp-switches-show`

`node-ip` *`ip-address`*	Displays the node IP address.
`vnet` *`vnet-name`*	Displays the name of the VNET assigned to the IGMP static source.
`bd` *`bridge-domain name`*	Displays the bridge domain name.
`vlan` *`vlan-id`*	Displays the VLAN identifier.
`port` *`port-number`*	Displays the port number.

Defaults None

Access CLI

History

Version 2.3.3	Command introduced.
Version 2.4.1	The parameters, `group-ip`, `node-type`, `expires`, and `source`, deprecated. The parameters, `vnet` and `vlan`, added.
Version 5.1.1	The parameter, `bd`, added.

Usage Displays information about IGMP switches.

Examples To display IGMP switches, use the following syntax:

```
CLI network-admin@switch > igmp-switches-show

  switch         node-ip vlan port
```

```
-------------- ------- ---- ----
spine-1        0.0.0.0 1    3
spine-1        0.0.0.0 1    57
spine-1        0.0.0.0 2    3
spine-1        0.0.0.0 3    3
```

igmp-static-group-create

This command creates a static IGMP group on the network.

Informational Note: IGMPv1 is not supported in nvOS. If you are using IGMPv1, you must disable IGMP snooping on the Pluribus Networks switch.

Syntax `igmp-static-group-create`

`group-ip` *`ip-address`*	Speicifies the group multicast IP address for IGMP.
`vlan` *`vlan-id`*	Specifies the VLAN identifier.
`ports` *`port-list`*	Specifies the list of ports.

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage Netvisor uses IGMP groups to determine the reception state for a specific multicast address. This allows the switch to determine if any switches need messages sent from a multicast group. Use this command to create an IGMP static group.

Examples To configure a static group for 239.4.9.3 on VLAN 202 and ports 55-57, use the following command:

```
CLI network-admin@switch > igmp-static-group-create group-ip 239.4.9.3
vlan 202 ports 55-57
```

igmp-static-group-delete

This command deletes information about IGMP snooping on the network.

Syntax `igmp-static-group-delete`

`group-ip` *`ip-address`*	Specify the group IP address for IGMP.
`vnet` *`vnet name`*	Specify the VNET to delete.
`l2-net` *`l2-net name`*	Specify the group Layer 2 network.
`vlan` *`vlan-id`*	Specify the VLAN identifier.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.1	The parameters, `ports`, is deprecated.
Version 3.0.0	The parameters, `vnet` and `l2-net`, added.

Usage IGMP groups are used to determine the reception state for a specific multicast address. This allows the switch to determine if any switches need messages sent from a multicast group. Use this command to remove an IGMP static group.

Examples To delete a static group for 239.4.9.3 on VLAN 202 and ports 55-57, use the following command:

```
CLI network-admin@switch > igmp-static-group-delete group-ip 239.4.9.3
vlan 202 ports 55-57
```

igmp-static-group-show

This command is used to display information about IGMP static groups configured on the switch.

Informational Note: IGMPv1 is not supported in nvOS. If you are using IGMPv1, you must disable IGMP snooping on the Pluribus Networks switch.

Syntax `igmp-static-group-show`

`group-ip` *`ip-address`*	Specifies the IP address of the IGMP static group.
`vnet` *`vnet-name`*	Specifies the VNET assigned to the IGMP static group.
`l2-net` *`l2-net name`*	Specify the group Layer 2 network.
`vlan` *`vlan-id`*	Specifies the VLAN assigned to the IGMP static group.
`ports` *`port-list`*	Specifies the ports assigned to the IGMP group.

Access CLI

History

Version 2.0	Command introduced.
Version 2.4.1	The parameter, `vnet`, added.
Version 3.0.0	The parameter `l2-net` added.

Usage IGMP groups are used to determine the reception state for a specific multicast address. This allows the switch to determine if any switches need messages sent from a multicast group. Use this command to display an IGMP static group.

Examples To display a static group for 239.4.9.3 on VLAN 202 and ports 55-57, use the following command:

```
CLI network-admin@switch > igmp-static-group-show group-ip 239.4.9.3
vnet global-fab vlan 202 ports 55-57
```

igmp-static-source-create

This command creates a static IP address as the IGMP source on the network.

Informational Note: IGMPv1 is not supported in nvOS. If you are using IGMPv1, you must disable IGMP snooping on the Pluribus Networks switch.

Syntax `igmp-static-source-create`

`source-ip` *`ip-address`*	Specify the source IP address. This is a unicast IP address.
`group-ip` *`ip-address`*	Specify the group IP address for IGMP.
`vlan` *`vlan-id`*	Specify the VLAN identifier.
Specify the following option:	
`vnet` *`vnet-name`*	Specify the name of the VNET assigned to the IGMP static source.
`bd` *`bridge-domain name`*	Specify the bridge domain name.
`ports` *`port-list`*	Specify the list of ports.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.4.1	The parameter, `vnet`, added.
Version 3.0.0	The parameter `l2-net` added.
Version 5.1.1	The parameter `l2-net` deprecated.

Usage IGMP groups are used to determine the reception state for a specific multicast address. This allows the switch to determine if any switches need messages sent from a multicast group. Use this command to create an IGMP static IP address as the source.

Examples To add the static source 12.0.0.1 as the static source, use the following command:

```
CLI network-admin@switch > igmp-static-source-create source-ip 12.0.0.1
group-ip vlan 202 ports 55-57
```

igmp-static-source-delete

This command deletes a static IGMP source on the netework.

Informational Note: IGMPv1 is not supported in nvOS. If you are using IGMPv1, you must disable IGMP snooping on the Pluribus Networks switch.

Syntax `igmp-static-source-delete`

`group-ip` *`ip-address`*	Specifies the group IP address for IGMP.
`source-ip` *`ip-address`*	Specifies the source IP address.
`bd` *`bridge-domain name`*	Specify the bridge domain name.
`vlan` *`vlan-id`*	Specifies the VLAN identifier.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.4.1	The parameter, `vnet`, added.
Version 3.0.0	The parameter `l2-net` added.
Version 5.1.1	The parameter `l2-net` deprecated.

Usage IGMP groups are used to determine the reception state for a specific multicast address. This allows the switch to determine if any switches need messages sent from a multicast group. Use this command to remove an IP address as the static source.

Examples To remove the static source 12.0.0.1 as the static source, use the following command:

```
CLI network-admin@switch > igmp-static-source-remove  source-ip  12.0.0.1
group-ip vlan 202 ports 55-57
```

igmp-static-source-show

This command displays a static IGMP source on the network.

Informational Note: IGMPv1 is not supported in nvOS. If you are using IGMPv1, you must disable IGMP snooping on the Pluribus Networks switch.

Syntax `igmp-static-source-show`

`group-ip` *`ip-address`*	Specifies the group IP address for IGMP.
`vnet` *`vnet-name`*	Specify the name of the VNET assigned to the IGMP static source.
`source-ip` *`ip-address`*	Specifies the source IP address.

bd *bridge-domain name*	Specifies the bridge domain name.
vlan *vlan-id*	Specifies the VLAN identifier.
ports *port-list*	Specifies the list of ports.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.4.1	The parameter, vnet, added.
Version 5.1.1	The parameter, host, deprecated, and the parameter, bd, added.

Usage IGMP groups are used to determine the reception state for a specific multicast address. This allows the switch to determine if any switches need messages sent from a multicast group. Use this command to remove an IGMP static source.

Examples To display information about all IGMP static source IP addresses, use the following command:

```
CLI network-admin@switch > igmp-static-source-show
```

igmp-stats-clear

Netvisor uses IGMP groups to determine the reception state for a specific multicast address. This allows the switch to determine if any switches need messages sent from a multicast group. Use this command to clear IGMP statistics:

Syntax igmp-stats-clear

vlan *vlan-id*	Specify the VLAN ID for which IGMP statistics are to be cleared. For multiple VLANs, specify VLAN IDs as a list separated by commas.

Defaults None

Access CLI

History

Usage This command clears IGMP statistics for the network. The command can be made specific to VLANs.

Examples To clear IGMP statistics for VLAN 1, use the command:

```
CLI (network-admin@Switch1) > igmp-stats-clear vlan 1
```

igmp-stats-show

This command displays IGMP statistics for a network on a per-VLAN basis.

Syntax `igmp-stats-show`

`vlan` *`vlan-id`*	Specify the VLAN ID for which IGMP statistics are to be displayed. For multiple VLANs, specify VLAN IDs as a list separated by commas.

Defaults None

Access CLI

History

Usage This command displays IGMP statistics for the network. The displayed information includes VLANs as well as the number of queries and number of member reports for IGMPv2 and IGMPv3, among other details.

Examples To display IGMP statistics for VLAN 1 in a vertical layout, use the command:

```
CLI (network-admin@switch1) > igmp-stats-show vlan 1 layout vertical
switch:            switch1
vlan:              1
v2-queries:        0
v3-queries:        581
v1-member-reports: 0
v2-member-reports: 0
v2-leave-group:    0
v3-member-reports: 2903
queries-sent:      577
drops:             0
ignored:           0
switch:            switch2
vlan:              1
v2-queries:        0
v3-queries:        116
v1-member-reports: 0
v2-member-reports: 0
v2-leave-group:    0
v3-member-reports: 2446
queries-sent:      1871
drops:             0
ignored:           0
```

inline-service-create

The Inline Service feature manages service chains for Layer 1 Virtual Wire switches. The term, Inline Services, refers to services attached to a Layer 1 Virtual Wire switch such as Next-Generation Firewall (NGFW), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and Distributed Denial of Service attack (DDoS) Prevention.

When an Inline Service fails, a policy determines if traffic is allowed to bypass the Inline Services or if the traffic is blocked until the Inline Services recovers.

This command creates an Inline Service configuration.

Syntax `inline-service-create`

`name` *`name-string`*	Specify a name for the Inline Service.
`tx-port` *`port-list`*	Specify the ports to send the Inline Service.
`rx-port` *`port-list`*	Specify the ports to receive the Inline Service.
`heartbeat service-heartbeat` *`name`* | `none`	Specify the service heartbeat.

Defaults None

Access Network Administrator

History .

Version 2.6.0	Command introduced.
Version 3.0.0	The parameter, `heartbeat service-heartbeat`, added.

Usage Use this command to create an Inline Service configuration.

Examples To create an Inline Service configuration for IDS on transmit port 1 and receive port 2, use the following syntax:

```
CLI network-admin@switch > inline-service-create name IDS tx-port 1 rx-port 2
```

inline-service-delete

The Inline Service feature manages service chains for Layer 1 Virtual Wire switches. The term, Inline Services, refers to services attached to a Layer 1 Virtual Wire switch such as Next-Generation Firewall (NGFW), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and Distributed Denial of Service attack (DDoS) Prevention.

When an Inline Service fails, a policy determines if traffic is allowed to bypass the Inline Services or if the traffic is blocked until the Inline Services recovers.

This command delete an Inline Service configuration.

Syntax `inline-service-delete`

`name` *`name-string`*	Specify a name for the Inline Service.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to delete an Inline Service configuration.

Examples To remove an Inline Service configuration named IDS, use the following syntax:

```
CLI network-admin@switch > inline-service-delete name IDS
```

inline-service-modify

The Inline Service feature manages service chains for Layer 1 Virtual Wire switches. The term, Inline Services, refers to services attached to a Layer 1 Virtual Wire switch such as Next-Generation Firewall (NGFW), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and Distributed Denial of Service attack (DDoS) Prevention.

When an Inline Service fails, a policy determines if traffic is allowed to bypass the Inline Services or if the traffic is blocked until the Inline Services recovers.

This command delete an Inline Service configuration.

Syntax `inline-service-modify`

`name` *`name-string`*	Specify a name for the Inline Service.
`heartbeat service-heartbeat` *`name`* `| none`	Specify the service heartbeat.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0

Usage Use this command to modify an Inline Service configuration.

Examples To remove an Inline Service configuration named IDS, use the following syntax:

```
CLI network-admin@switch > inline-service-modify name IDS
```

inline-service-show

The Inline Service feature manages service chains for Layer 1 Virtual Wire switches. The term, Inline Services, refers to services attached to a Layer 1 Virtual Wire switch such as Next-Generation Firewall (NGFW), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and Distributed Denial of Service attack (DDoS) Prevention.

When an Inline Service fails, a policy determines if traffic is allowed to bypass the Inline Services or if the traffic is blocked until the Inline Services recovers.

This command displays information about an inline service configuration.

Syntax `inline-service-show`

`name` *`name-string`*	Displays a name for the Inline Service.
`tx-port` *`port-list`*	Displays the ports to send the Inline Service.

`rx-port` *`port-list`*	Displays the ports to receive the Inline Service.
`status down|up`	Displays the status of the inline service.
`heartbeat service-heartbeat` *`name`* `| none`	Specify the service heartbeat.

Defaults None

Access Network Administrator

History

Version 2.6.0	Command introduced.
Version 3.0.0	The parameter, `heartbeat service-heartbeat`, added.

Usage Use this command to display information about an Inline Service configuration.

Examples To display an Inline Service configuration, use the following syntax:

```
CLI network-admin@switch > inline-service-show
switch      name tx-port      rx-port
---------- ---- ------------ -----------
Leaf1      IDS   1            2
Leaf1      FW    10           20
Leaf1      FW    40           40
```

ip-pool-create

This command creates a new IP address pool with a specific IP address range.

Syntax `ip-pool-create`

`name` *`ip-pool-name`*	Specify the name for the IP pool.
`vnet` *`vnet-name`*	Specify the VNET for the IP pool.
`start-ip` *`ip-address`*	Specify the first IP address in the pool. This address is included in the pool.
`end-ip` *`ip-address`*	Specify the end IP address of the pool and is included in the pool.
`netmask` *`netmask`*	Specify the subnet for the IP address pool.
Specify the following option:	
`bd` *`bridge-domain name`*	Specify the name of the bridge domain.
`vlan` *`vlan-id`*	Specify the VLAN identifier for an IP address pool that applies to a specific Layer 2 network segment.

Defaults Unless the netmask parameter is specified, the subnet for the IP address pool is assumed to be the

standard IP block for a given IP prefix. For example, if no netmask is specified and the IP address has a prefix of 192.168.0.x, the subnet is assumed as /24, 255.255.255.0.

Access CLI

History

Version 1.2.1	Command introduced.
Version 3.0.0	The parameter, `l2-net`, added.
Version 5.1.1	The parameter, l2-net, deprecated, and the parameter, bd, added.

Usage IP address pools help automate the management of IP addresses for hosts and virtual machines, including the management IP addresses of the switches in a fabric. Use this command to create a new IP pool.

Examples To create a fabric-wide IP address pool named `MyPublicIPv4Pool` to automate the allocation of IP addresses within a fabric for the IP address block `208.74.182.0 to 208.74.182.100/32`, use the following command:

```
CLI network-admin@switch > ip-pool-create name MyPublicIPv4Pool start-
ip 208.74.182.0 end-ip 208.74.182.100 netmask 255.255.255.0
```

ip-pool-delete

This command deletes an IP address pool with a specific IP address range.

Syntax `ip-pool-delete name ip-pool-name`

name *ip-pool-name*	Specify the name of the IP pool to delete.

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage IP address pools help automate the management of IP addresses for hosts and virtual machines, including the management IP addresses of the switches in a fabric. This command deletes an existing IP address pool.

Examples To delete the IP address pool name MyPublicIPv4Pool, use the following command:

```
CLI network-admin@switch > ip-pool-delete  MyPublicIPv4Pool
```

ip-pool-modify

This command modifies an IP address pool with a specific IP address range.

Syntax `ip-pool-modify`

name *ip-pool-name*	Specify the name of the IPpol.

Specify one or more of the following options:	
start-ip *ip-address*	Specify the first IP address in the pool. This address is included in the pool.
end-ip *ip-address*	Specify the end IP address of the pool and is included in the pool.
network ip-address	Specify the network for the IP address pool, for example, 192.168.1.0.
netmask *netmask*	Specify the subnet for the IP address pool.
vlan *vlan-id*	Specify the VLAN identifier for an IP address pool that applies to a specific Layer 2 network segment.
bd *bridge-domain name*	Specify the Bridge Domain assigned to IP pool.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.2	The parameter, vnet, deprecated.
Version 3.0.0	The parameter, l2-net, added.
Version 5.1.1	The parameter, l2-net, deprecated, and the parameter, bd, added.

Usage IP address pools help automate the management of IP addresses for hosts and virtual machines, including the management IP addresses of the switches in a fabric. Use this command to modify an existing IP pool.

Examples To modify a fabric-wide IP address pool named MyPublicIPv4Pool to automate the allocation of IP addresses within a fabric for the IP address block 208.74.182.0/24 to 208.74.182.201/24, use the following command:

```
CLI network-admin@switch > ip-pool-modify name MyPublicIPv4Pool start-ip 208.74.182.0 end-ip
208.74.182.200 netmask 255.255.255.0
```

ip-pool-show

This command displays information about an IP address pool with a specific IP address range.

Syntax ip-pool-show

name *ip-pool-name*	Specifies the name of the IP pool.

vnet *vnet-name*	Specifies the VNET for the IP pool.
scope local|fabric	Specifies the scope of the VNET.
start-ip *ip-address*	Specifies the first IP address in the pool. This address is included in the pool.
end-ip *ip-address*	Specifies the end IP address of the pool and is included in the pool.
network *ip-address*	Specify an IP address group such as 192.168.11.0.
netmask *netmask*	Specifies the subnet for the IP address pool.
l2-net *l2-net-name*	Specify the name of the Layer 2 network.
vlan *vlan-id*	Specifies the VLAN identifier for an IP address pool that applies to a specific Layer 2 network segment.
bd *bridge-domain name*	Specify the Bridge Domain assigned to IP pool.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.2	The parameter, vnet, deprecated.
Version 3.0.0	The parameter, l2-net, added.
Version 5.1.1	The parameter, l2-net, deprecated, and the parameter, bd, added.

Usage IP address pools help automate the management of IP addresses for hosts and virtual machines, including the management IP addresses of the switches in a fabric.

Examples To display information about a fabric-wide IP address pool named vPool, use the following command:

```
CLI network-admin@switch > ip-pool-show name vPool
Name   Owner   Scope   Range Start    Range End      Nemask   Gateway   DNS
-----  -----   -----   ----- -----    ----- ---      ------   -------   ---
vPool  None    local   192.168.240.1  192.168.240.254 24      10.9.40.1  0
```

ipv6security-raguard-create

Create a Router Advertisement (RA) IPv6 security policy for IPv6 addresses.

Syntax `ipv6security-raguard-create`

`name` *`name-string`*	Specify the RA policy name.
`device host|router`	Specify the type of device as host or router.
`router-priority low|medium|high`	Specify the router priority as low, medium, or high.
`access-list` *`name-string`*	Specify the access list name.
`prefix-list` *`name-string`*	Specify the prefix list name.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to create a RA Guard policy for IPv6 addresses.

Examples To create a RA Guard policy with the name **ra-guard-policy**, device router, router-priority low, access-list **ra-access-1**, and prefix-list **ra-prefix-1**, use the following syntax:

```
CLI network-admin@switch > ipv6security-raguard-create name ra-guard-
policy device router router-priority low access-list ra-access-1
prefix-list ra-prefix-1
```

ipv6security-raguard-delete

Delete a Router Advertisement (RA) IPv6 security policy for IPv6 addresses.

Syntax `ipv6security-raguard-delete`

`name` *`name-string`*	Specify the RA policy name.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to delete a RA Guard policy for IPv6 addresses.

Examples To delete a RA Guard policy with the name **ra-guard-policy**, device router, router-priority low, access-list **ra-access-1**, and prefix-list **ra-prefix-1**, use the following syntax:

```
CLI network-admin@switch > ipv6security-raguard-delete name ra-guard-policy
```

ipv6security-raguard-modify

Modify a Router Advertisement (RA) IPv6 security policy for IPv6 addresses.

Syntax `ipv6security-raguard-modify`

`name` *`name-string`*	Specify the RA policy name.
`device host|router`	Specify the type of device as host or router.
`router-priority low|medium|high`	Specify the router priority as low, medium, or high.
`access-list` *`name-string`*	Specify the access list name.
`prefix-list` *`name-string`*	Specify the prefix list name.
`attached-ports` *`port-list`*	Specify the ports attached to the RA Guard policy.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to modify a RA Guard policy for IPv6 addresses.

Examples To modify a RA Guard policy with the name **ra-guard-policy**, device router, router-priority low, access-list **ra-access-1**, and prefix-list **ra-prefix-1**, and add ports **11-13**, use the following syntax:

```
CLI network-admin@switch > ipv6security-raguard-modify name ra-guard-policy device router router-priority low access-list ra-access-1 prefix-list ra-prefix-1 attached-ports 11-13
```

ipv6security-raguard-remove

Remove ports from an IPv6 RA Guard policy.

Syntax `ipv6security-raguard-port-remove`

`name` *`name-string`*	Specify the name of the RA Guard policy to add ports.

ports *port-list*	Specify the list of ports to add to the policy.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to remove ports to a RA Guard policy.

Examples **To remove ports from a RA Guard policy, ra-guard-policy, use the following syntax:**

```
CLI network-admin@switch > ipv6security-raguard-port-remove name ra-guard-policy ports 11-13
```

ipv6security-raguard-show

Display information about a Router Advertisement (RA) IPv6 security policy configuration.

Syntax ipv6security-raguard-show

name *name-string*	Displays the RA policy name.
device host|router	Displays the type of device as host or router.
router-priority low|medium|high	Displays the router priority as low, medium, or high.
access-list *name-string*	Displays the access list name.
prefix-list *name-string*	Displays the prefix list name.
attached-ports *port-list*	Displays the ports attached to the policy.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0.

Usage Use this command to display information about a RA Guard policy configuration.

Examples To display information about a RA Guard policy configuration, NAT-1, use the following syntax:

```
CLI network-admin@switch > ipv6security-raguard-show
switch     name           device router-priority access-list prefix-list
attached-ports
---------- -------------- ------ -------------- ----------- -----------
--------------
leo-ext-22 ra-guard-policy router low            ra-access-1 ra-prefix-1 none
```

ipv6security-raguard-vlan-add

The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject

unwanted or rogue RA guard messages arriving at the network device platform.

Syntax `ipv6security-raguard-vlan-add`

`name` *`name-string`*	Specify the name of the RA Guard policy to add VLANs.
`vlans` *`vlan-id`*	Specify the VLANs to add to the policy.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0

Usage Use this command to add a VLAN to an RA Guard policy.

Examples To add VLAN 33 to RA Policy, **RA-Guard**, use the following syntax:

```
CLI network-admin@switch > ipv6security-raguard-vlan-add name RA-Guard
vlans 33
```

ipv6security-raguard-vlan-remove

The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue RA guard messages that arrive at the network device platform.

Syntax `ipv6security-raguard-vlan-remove`

`name` *`name-string`*	Specify the name of the RA Guard policy to add VLANs.
`vlans` *`vlan-id`*	Specify the VLANs to add to the policy.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0

Usage Use this command to remove a VLAN from an RA Guard policy.

Examples To remove VLAN 33 to RA Policy, **RA-Guard**, use the following syntax:

```
CLI network-admin@switch > ipv6security-raguard-vlan-remove name RA-
Guard vlans 33
```

ipv6security-raguard-vlan-show

The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue RA guard messages that arrive at the network device platform.

Syntax `ipv6security-raguard-vlan-show`

name *name-string*	Specify the name of the RA Guard policy to add VLANs.
vlans *vlan-id*	Specify the VLANs to add to the policy.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0

Usage Use this command to display a VLAN assigned to an RA Guard policy.

Examples To display for the RA Policy, **RA-Guard**, use the following syntax:

```
CLI network-admin@switch > ipv6security-raguard-vlan-show name RA-Guard
vlans 33
```

L Commands

l2-check-fix

It is possible for Layer 2 entries to go out of sync between what is present in the hardware and in software. This command checks the status of Layer 2 entries, logs the errors, and fixes them when possible.

Syntax l2-check-fix

mac *mac-address*	Specifies the virtual router ID from 0 to 15.
vnet vnet-name	Specifies the IP address of the entry.
l2-net *l2-net name*	Specifies the Layer 2 network.
vlan *vlan-id*	Specifies the VLAN ID.
public-vlan *vlan-id*	Specify the public VLAN assigned to the vPort.
vxlan *vxlan-id*	Specify if you want to check and fix out of synch VXLANs IDs of vPorts.
sw-port *port-number*	Specify the software port.
sw-state active|static|vrrp|tunnel| software|needs-peer-status|	Specify the software state to check.

port-mac|hit|ageout-check| moving|loop-probe|local-tunnel|igmp-mac|user-flush| vxlan-loopback|router|update-peer-only|active-state-mismatch|peer-port-missing| peer-port-not-vlag| peer-port-not-orphaned|peer-port-not-cluster-link|sw-active|hsrp| invalid-vlan|owner-lost| cluster-link-down|vxlan-router	
hw-port *port-number*	Specify the port number of the hardware.
hw-stateactive|static|vrrp| tunnel|software|needs-peer-status|port-mac| hit|ageout-check|moving|loop-probe|local-tunnel|igmp-mac|user-flush| vxlan-loopback|router|update-peer-only|active-state-mismatch|peer-port-missing| peer-port-not-vlag| peer-port-not-orphaned|peer-port-not-cluster-link|sw-active|hsrp| invalid-vlan|owner-lost| cluster-link-down| xlan-router	Specify the hardware state to check and fix.
fix-action none|add-to-hardware| removefrom-hardware|fix-port-in-hardware|fix-tunnel-in-hardware|FAILED-add-to-hardware|FAILED-remove-from-hardware|FAILED-fix-port-in-hardware|FAILED-fix-tunnel-in-hardware|delete-port-mac|mark-port-mac	Specifies the action used to fix the entry.

Defaults None

Access CLI

History

Version 2.4	Command introduced.
Version 2.4.1	The option, `igmp-mac`, `user-flush`, `vxlan-loopback`, `router` added to parameters `sw-state`

	and `hw-state`. The options, `delete-port-mac` and `mark-port-mac` added to the parameter `fix-action`. The parameter, `public-vlan`, also added.
Version 2.6.2	Additional parameters added to `sw-state` and `hw-state`.
Version 3.0.0	The parameter, `l2-net`, added.
Version 5.1.1	The options, `invalid-vlan|owner-lost|cluster-link-down|vxlan-router`, added to the parameters, sw-state, and hw-state.

Usage Use this command to verify and fix Layer 2 entries that are out of sync in the Layer 2 table.

Examples Use the following syntax to fix out of sync Layer 2 table entries.

```
CLI network-admin@switch > l2-check-fix vlan 25
```

l2-check-show

It is possible for Layer 2 entries to go out of sync between what is present in the hardware and in software. This command displays the status of Layer 2 entries.

Syntax `l2-check-show`

`mac` *`mac-address`*	Displays if you want to check and fix out of synch MAC addresses of vPorts.
`vnet` *`vnet-name`*	Specify the name of the VNET.
`vlan` *`vlan-id`*	Displays if you want to check and fix out of synch VLANs addresses of vPorts.
`l2-net` *`l2-net name`*	Specifies the Layer 2 network.
`public-vlan` *`vlan-id`*	Specify the public VLAN assigned to the vPort
`vxlan` *`vxlan-id`*	Displays if you want to check and fix out of synch VXLANs addresses of vPorts.
`sw-port` *`port-number`*	Displays the port number of the software.
`sw-state active|static|vrrp|tunnel|software|needs-peer-status|port-mac|hit|ageout-check|moving|loop-probe|local-tunnel|igmp-mac|user-flush|vxlan-loopback|router|update-peer-only| active-state-mismatch|peer-port-missing|peer-port-not-vlag| peer-port-not-orphaned|peer-port-not-cluster-link|sw-active|hsrp|invalid-vlan|owner-lost|cluster-link-down|vxlan-router`	Displays the software state to check.

hw-port *port-number*	Displays the port number of the hardware.
hw-state active|static|vrrp|tunnel| software|needs-peer-status|port-mac| hit|ageout-check|moving|loop-probe| local-tunnel|igmp-mac|user-flush|vxlan-loopback|router|update-peer-only| active-state-mismatch|peer-port-missing|peer-port-not-vlag| peer-port-not-orphaned|peer-port-not-cluster-link|sw-active|hsrp|invalid-vlan|owner-lost|cluster-link-down|vxlan-router	Displays the hardware state to check and fix.
tunnel-name *tunnel-name-string*	Displays the tunnel name.
fix-action none|add-to-hardware|remove-from-hardware|fix-port-in-hardware|fix-tunnel-in-hardware|FAILED-add-to-hardware|FAILED-remove-from-hardware| FAILED-fix-port-in-hardware|FAILED-fix-tunnel-in-hardware	Displays the type of fix action.

Defaults None.

Access CLI

History

Version 2.4	Command introduced.
Version 2.4.1	The option, igmp-mac, user-flush, vxlan-loopback, router added to parameters sw-state and hw-state. The options, delete-port-mac and mark-port-mac added to the parameter fix-action. The parameter, public-vlan, added.
Version 2.6.2	Additional parameters added to sw-state and hw-state.
Version 3.0.0	The parameter, l2-net, added.
Version 5.1.1	The options, invalid-vlan|owner-lost|cluster-link-down| vxlan-router, added to the parameters, sw-state, and hw-state.

Usage Use this command to display Layer 2 table entries.

Examples To display the Layer 2 entries and states, use the following command:

```
CLI network-admin@switch > l2-check-show vlan 25
```

l2-history-show

This command displays historical information about Layer 2 entries on the switch.

Syntax l2-history-show

time date/time: *yyyy-mm-ddThh:mm:ss*	Specifies a point in time for displaying historical information.
start-time date/time: *yyyy-mm-ddThh:mm:ss*	Specifies the start time for Layer 2 history collection.
end-time date/time: *yyyy-mm-ddThh:mm:ss*	Specifies the end time for Layer 2 history collection.
duration duration: *#d#h#m#s*	Specifies the duration to collect the Layer 2 history.
interval duration: *#d#h#m#s*	Specifies the intervals that data is collected Layer 2 history.
since-start	Specifies to display all of the Layer 2 history since collection began on the fabric.
older than duration: *yyyy-mm-ddThh:mm:ss*	Specifies a point in tjme for displaying historical information.
within-last duration: *yyyy-mm-ddThh:mm:ss*	Specifies the start time for Layer 2 history collection.
log-type l2-save|l3-save|restart |l2-modify|l2-delete|l3-modify|l3-delete	Filter output by the log type of each entry. The log-type column displays when a vPort is created, modified, saved, or deleted.
caller init|config|status|switch-cb| cluster|gre|ARP|router|flow-cb| vdp|vlag| port|inject|evict|vxlan|stats|vnm-vnic| adjacency|stp| trunk|intsw|ttl1|flood|flush| retire|loop|dhcp|fabric|table| l3-age-out| vlan|l2-checker|igmp| l2-age-out|port-mirror| mac-move|cluster-status|cluster-status-delete|vxlan-routing| subnet|ND	Specifies the feature making the change for this entry.
last-caller init|config|status|switch-cb| cluster|gre|ARP|router| flow-cb|vdp| vlag|port|inject|evict|vxlan|stats|vnm-vnic| adjacency|stp|trunk|intsw| ttl1|flood|flush|retire|loop|dhcp|fabric| table|l3-age-out|vlan|l2-checker|igmp|l2-age-out|port-mirror|mac-move|cluster-status| cluster-status-delete|vxlan-routing|subnet| ND	Specifies the most recent caller for this entry.
reason activate|deactivate|port-move| ip-move|ip-remove|batch-move|retire| break-loop|break-loop-timeout|create| modify|delete|policy|owner-status| remove-node|port-flags|check-owner| trunk-port-add|trunk-port-remove| move-router-if|age-out|hw-remove| restart|undo|flush|update-vxlan-vlan|	Specifies the reason for history entry.

needs-peer-status|owner-lost| owner-change|update-peer-only| user-delete|done|vm-metadata|ND	
last-reason activate|deactivate| port-move|ip-move|ip-remove| batch-move| retire|break-loop| break-loop-timeout|create|modify| delete| policy|owner-status| remove-node|port-flags|check-owner|trunk-port-add|trunk-port-remove|move-router-if| age-out| hw-remove|restart| undo|flush|update-vxlan-vlan|needs-peer-status|owner-lost|owner-change|update-peer-only| user-delete|done|vm-metadata|ND	Specifies the most recent reason for this entry.
changes owner|mac|ip|num-ips|config-intf| intf|ports|state|local-intf|local-ports| local-state|hostname|hypervisor|vm-id|vm-name|vm-flavor|vm-status |memory|cpus|disk|os|config| blocked-port|rem-switch|rem-intf| rem-ports|peer-intf|peer-state|status| tunnel|create-time|last-seen| vxlan-lru|hit|migrate|drops|hw-index|rt-if| hw-flags|ND	Specifies what changed in this entry.
count *count-number*	Filter output by the number of entries summed using the sum-by argument.
owner node *name*	
mac *mac-address*	Filter output by the Filter output by MAC address.
vnet *vnet-name*	Filter output by VNET name.
l2-net *l2-net name*	Specifies the Layer 2 network.
vlan *vlan-id*	Filter output by the VLAN ID.
public-vlan *vlan-id*	Filter output by public VLAN.
vxlan *vxlan-id*	Filter output by the VXLAN ID.
ip *ip-address*	Filter output by the IP address.
num-ips *num-ips-number*	Specify the number of IP addresses for the Layer 2 entry.
config-intf *config-intf-number*	Filter output by the configured interface of the Layer 2 entry.

`intf` *`intf-number`*	Filter output by the interface number. This is the port or trunk number of the Layer 2 entry.
`ports` *`port-list`*	Filter output by the list of ports.
`state active|static|vrrp|tunnel|software| needs-peer-status|port-mac|hit|ageout-check| moving|loop-probe|local-tunnel|igmp-mac| user-flush|vxlan-loopback| router|pdate-peer-only| active-state-mismatch|peer-port-missing|peer-port-not-vlag| peer-port-not-orphaned|peer-port-not-cluster-link|sw-active|anycast|hsrp|invalid-vlan|owner-lost|cluster-link-down| vxlan-router`	Filter output by the state of the Layer 2 entry.
`svc-name` *`svc-name-string`*	Filter output by service name.
`hostname` *`hostname-string`*	Filter output by the host name.
`entity` *`entity-string`*	Filter output by the VM or VM Kernel device name.
`power none|powered-off|powered-on|standby| suspended|unknown`	Filter by the vPort power status.
`portgroup` *`portgroup-string`*	Filter by the port group.
`pg-vlans` *`vlan-list`*	Filter by port group VLANs.
`vswitch` *`vswitch-string`*	Filter output by vSwitch name associated with VM MAC address.
`vs-type none|host-vs|distributed-vs|unknown`	Filter output by vSwitch type.
`vnic-type untagged|tagged|trunked|vm-mgmt| vm-kernel|vMotion|vSAN|FTL| rep|p-NFC|r-NFC|mgmt|unknown`	Filter output by VNIC type.
`memory memory-number`	Filter output by the amount of memory assigned to the VM.
`cpus cpus-number`	Filter output by the number of CPUs assigned to the VM.
`disk disk-number`	Filter output by the disk number where the VM is installed.
`os os-string`	Filter output by the OS installed on the VM.
`config none|owner|ip|port|hostname| hypervisor|vm-id|vm-name| vm-flavor|`	Filter output by the configuration of the VM.

memory|cpus|disk|os	
rem-switch *node name*	Filter output by the remote switch name.
rem-intf *rem-intf-number*	Filter output by the remote interface number.
rem-ports port-list	Filter output by the remote ports.
peer-intf *peer-intf-number*	Filter output by vPort peer interface.
peer-state active|static|vrrp|tunnel| software| needs-peer-status|port-mac|hit|ageout-check| moving|loop-probe|local-tunnel|igmp-mac| user-flush|vxlan-loopback| router|update-peer-only| active-state- mismatch|peer-port-missing|peer-port-not- vlag|peer-port-not-orphaned|peer-port-not- cluster-link|sw-active|anycast|hsrp|invalid- vlan|owner-lost|cluster-link-down| vxlan-router	Filter by the vPort peer state.
peer-owner-state active|static|vrrp|tunnel| software|needs-peer-status|port-mac|hit| ageout-check|moving|loop-probe| local- tunnel| igmp-mac|user-flush|vxlan-loopback| router||update-peer-only| active-state- mismatch|peer-port-missing|peer-port-not- vlag|peer-port-not-orphaned|peer-port-not- cluster-link|sw-active|anycast|hsrp|invalid- vlan|owner-lost|cluster-link-down| vxlan-router	Filter by the vPort peer owner state.
status phy-up|up|disabled|hw-nat-loop| mirror-loop|mirror-to|inuse| PN-switch|PN- fabric|PN-other| PN-cluster|PN-internal| PN-hypervisor|PN- guest|snmp-host|host|uplink|drop-pkts|no- pktin|no-fwd|no-flood|STP-BPDUs|LLDP|trunk| l3-port| remote-l3-port|vdp|dhcp|dhcpsvr| blocked|no-BPDU|LACP-PDUs| vlag-active|vlag- blocked|stp-edge-port|LACP-wait|LACP- fallback| adjacency-wait|adjacency-check| vlag-wait|multicast-router|host-disabled| loop|congested|vxlan-loopback|vlan-up|vm- kernel|vm|pnic|vle-wait|phy-down|down| enabled|err-disabled|err-bpdu-guard|mac- violation| stp-bpdu-guard|stp-root-guard	Filter output by the status of the Layer 2 entry.
vtep-ip *ip-address*	Specifies the IP address of the remote VTEP.

`tunnel` *`tunnel-string`*	Filter output by the tunnel name.
`create-time date/time:` *`yyyy-mm-ddTHH:mm:ss`*	Filter output by the time that the vPort was created.
`last-seen date/time:` *`yyyy-mm-ddTHH:mm:ss`*	Filter output by the time that the vPort was last seen on the fabric.
`vxlan-lru date/time:` *`yyyy-mm-ddTHH:mm:ss`*	Filter output by the number of received hits.
`hit` *`hit-number`*	Filter output by the number of times that the vPort migrated on the fabric.
`migrate` *`migrate-number`*	Filter output by the number of drops on the fabric.
`drops` *`drops-number`*	Filter output by the time that the vPort was created.
`hw-index` *`hw-index-number`*	Filter output by the hardware index number.
`rt-if` *`rt-if-string`*	Filter by the router interface.
`hw-flags invalid-vlan|invalid-port`	Filter by hardware flags.
`mc-index` *`mc-index-number`*	Specifies the multicast group index in hardware.

Defaults None

Access CLI

History

Version 2.3.2	Command introduced.
Version 2.4	The parameters, `peer-`, `hw-index`, and `rf-if` added.
Version 2.6.2	New parameters added. Some parameters removed, `vm-id`, `hypervisor`, `vm-name`, `vm-flavor`, and `vm-status`.
Version 3.1.0	The parameters, `ND` and `vtep-ip`, added.

Usage Use this command to display history of Layer 2 entries.

Examples To display Layer 2 information, use the following command:

```
CLI network-admin@switch > l2-history-show
time:                    09:02:33
log-type:                l2-modify
caller:                  router
reason:                  activate,create
owner:                   pleaides24
```

```
mac:                    66:0e:94:f4:ec:6e
vlan:                   1
ip:                     192.168.16.24
ports:                  65
state:                  active,static
hostname:               pleiades-tib
status:                 host
```

l2-net-port-add (deprecated)

l2-net-port-remove (deprecated)

l2-net-port-show (deprecated)

l2-setting-modify

This command modifies the Layer 2 settings in the configuration.

Syntax `l2-setting-modify`

`aging-time` *`seconds`*	Configures the aging time in Layer 2. You can configure a value from 1 to 2000000. The default value is 300 seconds.
`software-aging| no-software-aging`	Specify if you want to enable software aging or not. This is ON by default. This parameter controls how the aging of the L2 table entries is performed by Netvisor. When OFF, the aging is performed by the Ethernet switch ASIC. It is not recommended to change this setting.
`l2-max-count` *`l2-max-count-number`*	Specify the maximum count for Layer 2 entries.
`l2-checker|no-l2-checker`	Specify if you want to enable Layer 2 checker.
`l2-checker-interval duration:` *`#d#h#m#`*	Specify the interval between Layer 2 checks.
`l3-arp-max-count` *`l3-arp-max-count-number`*	Specify the number of maximum ARPs for Layer 3 entries.

Defaults None.

Access CLI

History

Version 1.2	Command introduced.
Version 2.4	The parameters, `software-aging`, `l2-checker` and `l2-checker-interval` added.
Version 5.1.1	The parameter, l2-max-count, added.

Usage Use this command to modify the Layer 2 aging time in seconds.

Examples To modify the aging time to 360 seconds, use the following command:

```
CLI network-admin@switch > l2-setting-modify aging-time 360
```

l2-setting-show

This commands displays the Layer 2 settings in the configuration.

Syntax `l2-setting-show`

Defaults None.

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage Use this command to display information about Layer 2 settings.

Examples To display the Layer 2 settings, use the following command:

```
CLI network-admin@switch > l2-setting-show
switch:           Pleiades24
aging-time(s):    300
l2-max-count:     1300000
l2-cur-count:     36
l2-active-count:  13
l2-max-mem:       1.81G
l2-cur-mem:       32.6K
l3-arp-max-count: 1300000
l3-arp-cur-count: 7
l3-arp-max-mem:   624M
l3-arp-cur-mem:   2.13K
switch:           Pleiades25
aging-time(s):    300
l2-max-count:     1300000
l2-cur-count:     36
l2-active-count:  14
l2-max-mem:       1.81G
l2-cur-mem:       32.6K
l3-arp-max-count: 1300000
l3-arp-cur-count: 7
l3-arp-max-mem:   624M
l3-arp-cur-mem:   2.13K
```

l2-static-multicast-group-create

This command is used to create a Layer 2 static multicast group. Hosts join multicast groups either by sending an unsolicited IGMP join message or by sending an IGMP join message in response to a general query from a multicast router (the switch forwards general queries from multicast routers to all ports in a VLAN). When you specify group membership for a multicast group address statically, the static setting supersedes any IGMP snooping learning. Multicast group membership lists can consist of both static and IGMP snooping-learned settings.

Syntax `l2-static-multicast-group-create`

`group-mac` *`mac-address`*	Specify a MAC address for the multicast group.

vlan *vlan-id*	Specify a VLAN ID for the multicast group.
ports *port-list*	Specify a list of ports for the multicast group.

Defaults None

Access network-admin

History Command introduced in Version 2.3.

Usage Use this command to create a Layer 2 static multicast group.

Examples To create a L2 static multicast group on MAC address, 0050.3e8d.6400, VLAN 25, and ports 10-12, use the following syntax:

```
CLI network-admin@switch > l2-static-multicast-group-create group-mac
0050.3e8d.6400 vlan 25 ports 10-12
```

l2-static-multicast-group-delete

This command is used to delete a Layer 2 static multicast group. Hosts join multicast groups either by sending an unsolicited IGMP join message or by sending an IGMP join message in response to a general query from a multicast router (the switch forwards general queries from multicast routers to all ports in a VLAN). When you specify group membership for a multicast group address statically, the static setting supersedes any IGMP snooping learning. Multicast group membership lists can consist of both static and IGMP snooping-learned settings.

Syntax `l2-static-multicast-group-create group-mac mac-address vlan vlan-id`

group-mac *mac-address*	Specify a MAC address for the multicast group.
vnet vnet-name	Specifies the IP address of the entry.
l2-net *l2-net name*	Specifies the Layer 2 network.
vlan *vlan-id*	Specify a VLAN ID for the multicast group.

Defaults None

Access network-admin

History

Version 2.3	Command introduced.
Version 3.0.0	The parameters, vnet and l2-net, added.

Usage Use this command to delete a Layer 2 static multicast group.

Examples To delete a L2 static multicast group on MAC address, 0050.3e8d.6400 and VLAN 25, use the following syntax:

```
CLI network-admin@switch > l2-static-multicast-group-delete group-mac
0050.3e8d.6400 vlan 25 ports 10-12
```

l2-static-multicast-group-show

This command is used to display information about a Layer 2 static multicast group. Hosts join multicast groups either by sending an unsolicited IGMP join message or by sending an IGMP join message in response to a general query from a multicast router (the switch forwards general queries from multicast routers to all ports in a VLAN). When you specify group membership for a multicast group address statically, the static setting supersedes any IGMP snooping learning. Multicast group membership lists can consist of both static and IGMP snooping-learned settings.

Syntax `l2-static-multicast-group-show`

`group-mac` *`mac-address`*	Specify a MAC address for the multicast group.
`vnet`	Specifies VNETs.
`l2-net` *`l2-net name`*	Specifies the Layer 2 network.
`vlan` *`vlan-id`*	Specify a VLAN ID for the multicast group.
`ports` *`port-list`*	Specify a list of ports for the multicast group.

Defaults None

Access network-admin

History

Version 2.3	Command introduced.
Version 3.0.0	The parameters, `vnet` and `l2-net`, added.

Usage Use this command to display a Layer 2 static multicast group.

Examples To display a L2 static multicast group on MAC address, 0050.3e8d.6400, VLAN 25, and ports 10-12, use the following syntax:

```
CLI network-admin@switch > l2-static-multicast-group-show group-mac
0050.3e8d.6400 vlan 25 ports 10-12
```

l2-table-flush

This command is used to clear information about the Layer 2 settings.

Syntax `l2-table-flush [vlan vlan-id] [port port-list]`

Specify either zero or both options:	
`mac` *`mac-address`*	Specifies the MAC address.
`vlan` *`vlan-id`*	Specifies the VLAN identifier.

ports *port-list*	Specifies the port list.

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage Used to flush the Layer 2 information.

Examples To flush the Layer 2 table information from VLAN 25, use the following command:

```
CLI network-admin@switch > l2-table-flush vlan 25
```

l2-table-show

To display Layer 2 flows in the forwarding table of the switch datapath, use this command.

Syntax l2-table-show

owner node *name*	Specifies the node name for the L2 table.
mac *mac-address*	Specifies the source MAC address for the flow.
ip *ip-address*	Specifies the source IP address for the flow.
vnet *vnet-name*	Specifies the VNET name.
bd *bridge-domain name*	Specify the bridge domain name assigned to vport.
l2-net *l2-net name*	Specifies the Layer 2 network.
vlan *vlan-id*	Specifies the VLAN identifier for the flow.
public-vlan *vlan-id*	Specifies the public VLAN.
vxlan *vxlan-id*	Specifies the ID for the VXLAN.
ip *ip-address*	Specifies the IP address.
num-ips *num-ips-number*	Specifies the number of IP addresses.
config-intf *config-intf-number*	Specifies a configured interface number.
intf intf-number	Specifies the interface number.
ports *port-list*	Specifies the source port number for the flow.
state active|static|vrrp|tunnel| software|needs-peer-status|port-mac| hit|ageout-check| moving|loop-probe|local-tunnel|igmp-mac|user-flush|vxlan-loopback|router| update-peer-only| active-state-mismatch|peer-port-missing|peer-port-	Specifies the state of the vPort.

not-vlag|peer-port-not-orphaned|peer-port-not-cluster-link|sw-active|hsrp|nvalid-vlan|owner-lost|cluster-link-down|vxlan-router	
svc-name *svc-name-string*	Specifies the service name.
hostname *hostname-string*	Specifies a hostname.
entity entity-string	Specifies theVM or VM Kernel device name.
power none|powered-off|powered-on|standby|suspended|unknown	Specifies the power status.
cpus *cpus-number*	Specifies the number of CPUs assigned to the VM.
disk *disk-number*	Specifies the number of disks assigned to the VM.
os *os-string*	Specifies the name of the operating system (OS) running on the VM.
portgroup portgroup-string	Specifies the port group associated with the VM MAC Address.
pg-vlans vlan-list	Specifies the VLANs associated with the port group.
vswitch vswitch-string	Specifies the vSwitch associated with the NIC.
vs-type none|host-vs|distributed-vs|unknown	Specifies the vSwitch type.
vnic-type untagged|tagged|trunked|vm-mgmt|vm-kernel|vMotion|vSAN|FTL| rep|p-NFC|r-NFC|mgmt|unknown	Specifies the vNIC type.
config none|switch|ip|port|hostname|hypervisor|vm-id|vm-name|vm-flavor|memory|cpus|disk|os	Displays the configuration on the host.
rem-switch *node-name*]	Specifies a remote switch.
rem-intf *rem-intf-number*	Specifies a remote switch interface.
rem-ports *port-list*	Specifies a remote switch port list.
peer-intf *peer-intf-number*	Filter output by vPort peer interface.
peer-state active|static|vrrp|tunnel|software|needs-peer-status| port-mac|hit|ageout-check|moving|loop-probe|local-tunnel|igmp-mac| update-peer-only|active-state-mismatch|peer-port-missing|peer-port-not-vlag|peer-port-not-orphaned| peer-port-not-cluster-link|sw-active|hsrp||nvalid-vlan|owner-	Filter by the vPort peer state.

lost|cluster-link-down|vxlan-router	
peer-owner-state active|static|vrrp| tunnel|software|needs-peer-status|port-mac|hit|ageout-check|moving|loop-probe| local-tunnel|igmp-mac|update-peer-only| active-state-mismatch|peer-port-missing|peer-port-not-vlag|peer-port-not-orphaned| peer-port-not-cluster-link|sw-active|hsrp|invalid-vlan|owner-lost|cluster-link-down|vxlan-router	Filter by the vPort peer owner state.
status phy-up|up|disabled|hw-nat-loop|mirror-loop| mirror-to|inuse| PN-switch|PN-fabric| PN-other|PN-cluster|PN-internal| PN-hypervisor|PN-guest| snmp-host|host|uplink| drop-pkts|no-pktin| no-fwd|no-flood| STP-BPDUs|LLDP|trunk| |l3-port|remote-l3-port|vdp|dhcp| dhcpsvr|blocked|no-BPDU| LACP-PDUs|vlag-active| vlag-blocked|stp-edge-port|LACP-wait| LACP-fallback| adjacency-wait |adjacency-check|vlag-wait|multicast-router|host-disabled|loop| congested| vxlan-loopback|vlan-up|vle|vle-wait| phy-down|down| enabled|err-disabled| err-bpdu-guard|mac-violation| stp-bpdu-guard|stp-root-guard||defer-bringup-wait	Specifies the status of the entry.
vtep-ip *ip-address*	Specifies the IP address of the remote VTEP.
tunnel *tunnel-string*	Specifies a tunnel name if configured.
create-time date/time: yyyy-mm-ddThh:mm:ss	Specifies the date and time that the flow was inserted into the Layer 2 table.
last-time date/time: yyyy-mm-ddThh:mm:ss	Specifies the most recent date and time that a packet matched the flow.
vxlan-lru date/time: yyyy-mm-ddThh:mm:ss	Specifies the last received update time for a VXLAN.
hit *number-of-hits*	Specifies the number of packets that matched the flow.
migrate *number-of-migrates*	Specifies the number of different ports that received packets matching the flow.
drops *number-of-drops*	Specifies the number of packets matching the flow that were dropped.

`hw-index` *`hw-index-number`*	Specifies the hardware index number.
`rt-if` *`rt-if-string`*	Specifies the router interface.
`hw-flags invalid-vlan|invalid-port`	Specifies any vPort hardware flags.
`mc-index` *`mc-index-number`*	Specifies the Layer 2 multicast group index in hardware.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.1	The parameter, `state`, added.
Version 2.2.4	The parameters, `config-intf`, `rem-switch`, `rem-intf`, and `rem-ports`, added.
Version 2.2.5	The parameters, `vlag-active`, `vlag-blocked`, `stp-edge-port`, deprecated. The parameters, `l3-port` and `remote-l3-port`, added.
Version 2.3	The parameters, `vlag-active`, `vlag-blocked`, `stp-edge-port`, added. The parameters `vm-status`, `tunnel`, and `vxlan-lru` added.
Version 2.4	The parameters, `peer-`, `hw-index`, and `rf-if` added.
Version 2.6.2	The parameters, `ip`, `num-ip`, `svc-name`, `entity`, `power`, `portgroup`, `pg-vlans`, `vswitch`, `vs-type`, `vnic-type`, and `hw-flags` added. The parameters, `hypervisor`, `vm-id`, `vm-name`, `vm-flavor`, `vm-status`, `memory`, and `blocked-port`, deprecated.
Version 3.1.0	The parameters, `ND` and `vtep-ip`, added.
Version 5.2.0	The parameter, `bd`, added

Usage Each switch has automatic safeguards to avoid forwarding loops in Layer 2 multipathing. This feature operates independently of Spanning Tree Protocol (STP) if STP is enabled. This command lists the Layer 2 flows in the forwarding table of the switch datapath. If there are ports in the blocked state may indicate the presence of loops in Layer 2 multipathing.

Examples To display the Layer 2 table, use the following command:

```
CLI network-admin@switch > l2-table-show format all layout vertical

switch:       pubdev02
mac:          02:08:20:38:00:c6
vlan:         4094
```

```
hostname:     pubdev02
create-time:  04-22,08:17:16
last-seen:    04-22,08:17:16
hit:          1
switch:       pubdev01
mac:          02:08:20:72:2d:ff
vlan:         4094
intf:         128
ports:        26,47-48
state:        active,static
hostname:     pubdev02
status:       PN-internal
last-seen:    05-19,15:10:12
switch:       pubdev02
mac:          02:08:20:72:2d:ff
vlan:         4094
intf:         65
ports:        65
state:        active
hostname:     pubdev02
status:       PN-internal
create-time:  04-22,08:53:08
last-seen:    05-19,15:03:08
hit:          1
switch:       pubdev03
mac:          02:08:20:72:2d:ff
vlan:         4094
intf:         128
ports:        45-48
state:        active,static
hostname:     pubdev02
status:       PN-internal
last-seen:    05-19,14:32:30
switch:       pubdev02
mac:          06:a0:00:03:00:1a
vlan:         1
intf:         26
ports:        26
state:        active
hostname:     pubdev01
status:       PN-switch,PN-fabric,PN-cluster
create-time:  04-22,08:42:19
last-seen:    11:17:47
hit:          4045
switch:       pubdev03
mac:          06:a0:00:03:00:2d
vlan:         1
intf:         45
ports:        45
state:        active
hostname:     pubdev01
status:       PN-switch,PN-fabric
create-time:  04-22,07:49:03
last-seen:    05-19,15:10:29
hit:          2
migrate:      10
```

l3-check-fix

Layer 3 entries can become unsynchronized between the software table and the hardware table. When routes are modified while the routes are updating on the network, this can occur. Use this command to fix any unsynchronized Layer 3 table entries.

Syntax `l3-check-fix`

`vrid ID`	Specifies the virtual router ID from 0 to 15.
`ip` *`ip-address`*	Specifies the IP address of the entry.
`prelen` *`length`*	Specifies the prefix length from 0 to 128.
`vlan` *`vlan-id`*	Specifies the VLAN ID.
`mac` *`mac-address`*	Specifies the MAC address.
`fix-action none|add-host-to-hardware| remove-host-from-hardware| re-add-host-to-hardware|add-route-to-hardware| remove-route-from-hardware|re-add-route-to-hardware| none-hardware-only-route|none-cached-route| FAILED-add-host-to-hardware|FAILED-remove-host-from-hardware|FAILED-add-route-to-hardware|FAILED-remove-route-from-hardware`	Specifies the action used to fix the entry.

Defaults None

Access CLI

History Command introduced in Version 2.5.

Usage Use this command to fix Layer 3 entries that are out of synch in the Layer 3 table.

Examples Use the following syntax to fix out of synch Layer 3 table entries.

```
CLI network-admin@switch > l3-check-fix
```

l3-check-show

Layer 3 entries can become unsynchronized between the software table and the hardware table. This is useful when routes are modified while the routes are updating on the network. Use this command to fix any unsynchronized Layer 3 table entries.

Syntax `l3-check-show`

`vrid ID`	Specifies the virtual router ID from 0 to 15.
`ip` *`ip-address`*	Specifies the IP address of the entry.
`prelen` *`length`*	Specifies the prefix length from 0 to 128.

vlan *vlan-id*	Specifies the VLAN ID.
mac *mac-address*	Specifies the MAC address.
fix-action none|add-host-to-hardware| remove-host-from-hardware| re-add-host-to-hardware|add-route-to-hardware| remove-route-from-hardware|re-add-route-to-hardware| none-hardware-only-route|none-cached-route| FAILED-add-host-to-hardware|FAILED-remove-host-from-hardware|FAILED-add-route-to-hardware|FAILED-remove-route-from-hardware	Specifies the action used to fix the entry.

Defaults None

Access CLI

History Command introduced in Version 2.5.

Usage Use this command to displays Layer 3 entries that are out of synch in the Layer 3 table.

Examples Use the following syntax to display out of synch Layer 3 table entries.

```
CLI network-admin@switch > l3-check-show
Spine-1:
Matched                    : 56
Fib host routes            : 14
Matched host routes        : 14
Fib only static routes     : 7
Rib local subnet routes    : 7
Fib local subnet routes    : 7
Spine-1: OK: 56
```

l3-history-show

This command displays historical information about Layer 3 entries on the switch.

Syntax l3-history-show

time date/time: *yyyy-mm-ddThh:mm:ss*	Specifies a point in tjme for displaying historical information.
start-time date/time: *yyyy-mm-ddThh:mm:ss*	Specifies the start time for Layer 3 history collection.
end-time date/time: *yyyy-mm-ddThh:mm:ss*	Specifies the end time for Layer 3 history collection.
duration duration: *#d#h#m#s*	Specifies the duration to collect the Layer 3 history.
interval duration: *#d#h#m#s*	Specifies the intervals that data is collected Layer 3 history.
since-start	Specifies to display all of the Layer 3 history since

	collection began on the fabric.
`time date/time: yyyy-mm-ddThh:mm:ss`	Specifies a point in tjme for displaying historical information.
`start-time date/time: yyyy-mm-ddThh:mm:ss`	Specifies the start time for Layer 3 history collection.
`log-type l2-save|l3-save|restart| l2-modify|l2-delete|l3-modify| l3-delete`	Filter output by the log type of each entry. The log-type column displays when a Layer 3 entry is created, modified, saved, or deleted.
`caller init|config|status|switch-cb|cluster| gre|ARP|router|flow-cb| vdp|vlag|port| inject|evict|vxlan|stats|vnm-vnic|adjacency| stp| trunk|intsw|ttl1|flood|flush|retire| loop|dhcp|fabric|table| l3-age-out|vlan|l2-checker|igmp|l2-age-out|port-mirror| mac-move|cluster-status| cluster-status-delete|vxlan-routing| subnet`	Specifies the feature that made the change for this entry.
`last-caller init|config|status|switch-cb| cluster|gre|ARP|router| flow-cb|vdp|vlag| port|inject |evict|vxlan|stats|vnm-vnic| adjacency|stp| trunk|intsw|ttl1|flood|flush|retire|loop| dhcp|fabric|table|l3-age-out|vlan|l2-checker|igmp|l2-age-out|port-mirror|mac-move|cluster-status| cluster-status-delete|vxlan-routing| subnet`	Specifies the most recent caller for this entry.
`reason activate|deactivate|port-move|ip-move|ip-remove| batch-move|retire|break-loop|break-loop-timeout|create|modify| delete| policy|owner-status| remove-node|port-flags| check-owner| trunk-port-add| trunk-port-remove|move-router-if|age-out|hw-remove|restart|undo|flush|update-vxlan-vlan| needs-peer-status|owner-lost| owner-change`	Specifies the reason for history entry.
`last-reason activate|deactivate| port-move|ip-move|ip-remove| batch-move| retire|break-loop| break-loop-timeout|create|modify| delete| policy|owner-status| remove-node|port-flags|check-owner| trunk-port-add| trunk-port-remove|move-router-if|age-out| hw-remove|restart|undo| flush|update-vxlan-vlan| needs-peer-status| owner-lost|owner-change|update-peer-only|`	Specifies the most recent reason for this entry.

user-delete|done|vm-metadata	
changes owner|mac|vnet|public-vlan|ip|num-ips|config-intf|intf|ports| state|local-intf|local-ports|local-state|alt-owner| alt-owner-port|alt-owner-ports|alt-owner-state| svc-name| hostname|entity|power|cpus|os| portgroup|pg-vlans|vswitch| vs-type|vnic-type|config|rem-switch|rem-intf|rem-ports| peer-intf|peer-state|peer-owner-state| status|tunnel|create-time|last-seen|vxlan-lru|hit|migrate|drops|hw-index|rt-if| hw-flags	Specifies what changed in this entry.
count *count-number*	Filter output by the number of entries summed using the sum-by argument.
owner node *name*	Filter output by the owner.
mac *mac-address*	Filter output by MAC address.
vnet *vnet-name*	Filter output by the VNET name.
l2-net *l2-net-name*	Filter output by the Layer 2 network name.
vlan *vlan-id*	Filter output by the VLAN ID.
public-vlan *vlan-id*	Filter output by the public VLAN ID.
vxlan *vxlan-id*	Filter output by the VXLAN ID.
ip *ip-address*	Filter output by the IP address.
num-ips *num-ips-number*	Specify the number of IP addresses for the Layer 3 entry.
config-intf *config-intf-number*	Filter output by the configured interface of the Layer 3 entry.
intf *intf-number*	Filter output by the interface number. This is the port or trunk number of the Layer 3 entry.
ports *port-list*	Filter output by the list of ports.
state active|static|vrrp| tunnel|software| needs-peer-status| port-mac|hit|ageout-check|moving|loop-probe| local-tunnel|igmp-mac| user-flush|vxlan-loopback|router|update-peer-only|active-state-mismatch|peer-port-missing|peer-port-	Filter output by the state of the Layer 3 entry.

not-vlag| peer-port-not-orphaned|peer-port-not-cluster-link|sw-active| hsrp	
svc-name *svc-name-string*	Filter output by service name.
hostname *hostname-string*	Filter output by the host name.
entity *entity-string*	Filter output by the VM or VM Kernel device name.
power none|powered-off|powered-on|standby|suspended|unknown	Filter by the vPort power status.
portgroup *portgroup-string*	Filter by the port group.
pg-vlans *vlan-list*	Filter by port group VLANs.
vswitch *vswitch-string*	Filter output by vSwitch name associated with VM MAC address.
vs-type none|host-vs|distributed-vs|unknown	Filter output by vSwitch type.
vnic-type untagged|tagged|trunked|vm-mgmt|vm-kernel|vMotion|vSAN|FTL| rep|p-NFC|r-NFC|mgmt|unknown	Filter output by VNIC type.
memory *memory-number*	Filter output by the amount of memory assigned to the VM.
cpus *cpus-number*	Filter output by the number of CPUs assigned to the VM.
disk *disk-number*	Filter output by the disk number where the VM is installed.
os *os-string*	Filter output by the OS installed on the VM.
config none|owner|ip|port|hostname|hypervisor|vm-id|vm-name| vm-flavor|memory|cpus|disk|os	Filter output by the configuration of the VM.
blocked-port *port-list*	Filter output by a list of ports to block for the VM.
rem-switch *node name*	Filter output by the remote switch name.
rem-intf *rem-intf-number*	Filter output by the remote interface number.
rem-ports port-list	Filter output by the remote ports.
peer-intf *peer-intf-number*	Filter output by the vPort peer interface.

peer-state active|static|vrrp|tunnel| software|needs-peer-status|port-mac|hit| ageout-check|moving|loop-probe|local-tunnel| igmp-mac|user-flush|vxlan-loopback|router| pdate-peer-only|active-state-mismatch|peer-port-missing|peer-port-not-vlag| peer-port-not-orphaned|peer-port-not-cluster-link|sw-active| hsrp	Filter output by the vPort peer state.
peer-owner-state active|static|vrrp|tunnel| software|needs-peer-status|port-mac|hit| ageout-check|moving|loop-probe|local-tunnel| igmp-mac|user-flush|vxlan-loopback|router| pdate-peer-only|active-state-mismatch|peer-port-missing|peer-port-not-vlag| peer-port-not-orphaned|peer-port-not-cluster-link|sw-active| hsrp	Filter output by the vPort peer owner state.
status phy-up|up|disabled|hw-nat-loop| mirror-loop|mirror-to|inuse| PN-switch|PN-fabric|PN-other|PN-cluster|PN-internal| PN-hypervisor|PN-guest|snmp-host|host|uplink| drop-pkts| no-pktin|no-fwd|no-flood|STP-BPDUs|LLDP|trunk|l3-port| remote-l3-port| vdp|dhcp|dhcpsvr|blocked|no-BPDU|LACP-PDUs| vlag-active|vlag-blocked|stp-edge-port|LACP-wait|LACP-fallback| adjacency-wait|adjacency-check| vlag-wait|multicast-router| host-disabled|loop|vxlan-loopback|vlan-up| vle|vle-wait|phy-down|down| enabled|err-disabled|err-bpdu-guard| mac-violation| stp-bpdu-guard|stp-root-guard	Filter output by the status of the Layer 3 entry.
vtep-ip *ip-address*	Specifies the IP address of the remote VTEP.
tunnel *tunnel-string*	Filter output by the tunnel name.
create-time date/time: yyyy-mm-ddTHH:mm:ss	Filter output by the time that the Layer 3 entry was created.
last-seen date/time: yyyy-mm-ddTHH:mm:ss	Filter output by the time that the Layer 3 entry was last seen on the fabric.
vxlan-lru date/time: yyyy-mm-ddTHH:mm:ss	Filter output by the number of received hits.
hit *hit-number*	Filter output by the number of times that the Layer 3 entry migrated on the fabric.
migrate *migrate-number*	Filter output by the number of drops on the fabric.
drops *drops-number*	Filter output by the time that the Layer 3 entry was created.
hw-index *hw-index-number*	Filter output by the hardware index number.

`rt-if` *`rt-if-string`*	Filter output by the router interface.
`hw-flags invalid-vlan|invalid-port`	Filter output by hardware flags.

Defaults None

Access CLI

History

Version 2.3.2	Command introduced.
Version 2.4	The parameters, `l2-checker|igmp|l2-age-out|port-mirror|mac-move` added. The parameters, `peer-`, `hw-index`, and `rt-if` added.
Version 2.4.1	The parameters, `vnet`, `public-vlan`, and `hw-flags` added. The options, `user-flush|vxlan-loopback|router`, added to `state`, `peer-state`, and `peer-owner-state`. The option, `cluster-status`, added to `caller` and `last-caller`. The options, `update-vxlan-vlan| needs-peer-status|owner-lost| owner-change` added to `reason` and `last-reason`.
Version 2.6.2	The parameters, `ip`, `num-ip`, `svc-name`, `entity`, `power`, `portgroup`, `pg-vlans`, `vswitch`, `vs-type`, `vnic-type`, and `hw-flags` added. The parameters, `hypervisor`, `vm-id`, `vm-name`, `vm-flavor`, `vm-status`, `memory`, and `blocked-port`, deprecated.
Version 3.1.0	The parameter, `vtep-ip`, added.

Usage Use this command to display history of Layer 3 entries.

Examples To display Layer 2 information, use the following command:

```
CLI network-admin@switch > l3-history-show
time:                   09:02:33
log-type:               l3-modify
caller:                 ARP
reason:                 activate,create
owner:                  pleaides24
mac:                    66:0e:94:f4:ec:6e
vlan:                   1
ip:                     192.168.16.24
state:                  active
```

l3-setting-modify

This command allows you to modify the Layer 3 settings.

Syntax `l3-setting-modify aging-time seconds`

Specify one or more of the following options:	
`aging-time`	Specifies the aging time between 0 to 2000000 seconds. Use 0 (zero) to disable aging time. The default aging time is 600 seconds.
`convergence-time` *`seconds`*	Specifies the unicast convergence time on bootup. This is a value from 0 to 3600 seconds.
`l3-checker|` `no-l3-checker`	Enable or disable Layer 3 checking.
`l3-checker-interval duration: #d#h#m#`	Specify the interval between Layer 3 checks.
`l3-checker-fix|` `no-l3-checker-fix`	Specify if after checking Layer 3 entries to fix the incorrect entries.

Defaults None

Access CLI

Usage Use this command to modify the Layer 3 setting.

Examples To modify the Layer 3 aging-time setting, use the following command:

```
CLI network-admin@switch > l3-setting-modify aging-time 1000

CLI network-admin@switch > l3-setting-show format all
switch:        spine-1
aging-time(s): 1000
```

l3-setting-show

This command allows you to display the Layer 3 settings.

Syntax `l3-setting-show`

Defaults None

Access CLI

Usage Use this command to show the Layer 3 setting.

Examples To display the Layer 3 setting, use the following command:

```
CLI network-admin@switch > l3-setting-show format all
switch:        spine-1
aging-time(s): 600
switch:        spine-2
aging-time(s): 600
```

From this output, you can see that the aging time is set to 600 seconds by default.

l3-table-show

This command allows you to display the Layer 3 table settings.

Syntax `l3-table-show`

Specify one or more of the following options:	
`mac` *`mac-address`*	Displays the MAC address.
`ip` *`ip-address`*	Displays the IP address.
`vnet` *`vnet-name`*	Displays the name of the VNET.
`l2-net` *`l2-net-name`*	Displays the name of the Layer 2 network.
`vlan id5`	Displays the VLAN ID.
`public-vlan` *`vlan-id`*	Specify the public VLAN assigned to the vPort
`vxlan id`	Displays the assigned VXLAN.
`intf intf-number`	Displays the interface.
`rt-if` *`rt-if-strin`*`g`	Displays the router interface.
`hw-intf` *`hw-intf-number`*	Displayss the interface programmed in hardware.
`state active|static|vrrp|tunnel| software|needs-peer-status|port-mac| hit|ageout-check| moving|loop-probe|local-tunnel|igmp-mac|user-flush|vxlan-loopback|router|update-peer-only| active-state-mismatch|peer-port-missing|peer-port-not-vlag| peer-port-not-orphaned|peer-port-not-cluster-link|sw-active| hsrp`	Displays the flags.
`owner-state active|static|vrrp|tunnel| software|needs-peer-status|port-mac| hit|ageout-check|moving|loop-probe| local-tunnel|igmp-mac| user-flush| vxlan-loopback| router|update-peer-only|active-state-mismatch|peer-port-missing|peer-port-not-vlag| peer-port-not-orphaned|peer-port-not-cluster-link|sw-active| hsrp`	Displays the owner-state flags.
`peer-state active|static|vrrp|tunnel| software|needs-peer-status|port-mac| hit|ageout-check| moving|loop-probe|local-tunnel|igmp-mac| user-flush| vxlan-loopback|router|update-peer-only| active-state-mismatch|peer-port-`	Displays the peer-state flags.

missing|peer-port-not-vlag|peer-port-not-orphaned|peer-port-not-cluster-link|sw-active| hsrp	
egress-id *egress-id-number*	Displays the hardware egress ID.
create-time date/time: yyyy-mm-ddThh:mm:ss	Displays the time entry created.
last-seen date/time: yyyy-mm-ddThh:mm:ss	Displays the last time seen on network.
hit *hit-number*	Displays the number of hits.
tunnel *tunnel-string*	Displays the tunnel name.

Defaults None

Access CLI

History

Version 2.4	Command introduced.
Version 2.4.1	The parameters, public-vlan, owner-state, peer-state and tunnel added. The options, user-flush|vxlan-loopback|router added to state, owner-state, and peer-state.
Version 2.6.2	The parameters, hw-intf and egress-id added. The options update-peer-only|active-state-mismatch|peer-port-missing|peer-port-not-vlag|peer-port-not-orphaned|peer-port-not-cluster-link|sw-active|hsrp added to state, owner-state, peer-state.
Version 3.0.0	The parameter, l2-net, added.

Usage Use this command to show the Layer 3 table setting.

Examples To display the Layer 3 table setting, use the following command:

```
CLI network-admin@switch > l3-table-show format all

 switch:                  spine1-1
 mac:                     c6:8f:66:55:fe:30
 ip:                      192.168.1.3
 vlan:                    1
 vxlan:                   0
 intf:                    128
```

```
rt-if:
state:                    active
create-time:              10-06,15:58:02
last-seen:                09:06:44
hit:                      1764
```

There is no routing interface (`rt-if`) value because there are no Layer 3 routes configured on the switch.

lacp-modify

This command is used to modify Link Aggregation Control Protocol (LACP) parameters on the switch.

Syntax `lacp-modify`

Specify one or more of the following options:	
`enable|disable`	Specify to enable or disable LACP on the switch.
`system-priority` *`priority`*	Specifies the priority for the configuration. The default value is 32768 with a range of 1 to 65535.

Defaults The default system-priority is 32768.

Access CLI

History Command introduced in Version 1.2.6

Usage Use this command to enable or disable LACP and set the priority.

Examples To enable LACP with a priority of 3567, use the following command:

```
CLI (network-admin@switch)> lacp-modify enable system-priority 3576
```

lacp-show

This command is used to display information about Link Aggregation Control Protocol (LACP) configurations on the switch.

Syntax `lacp-show`

`switch` *`switch-name`*	Specifies the name of the switch in the configuration.
`enable|disable`	Specifies if LACP is enabled or disabled.
`system-priority priority`	Specifies the priority for the configuration. The default value is 32768 with a range of 1 to 65535.

`system-id` *`id-string`*	Specifies the ID of the switch in the configuration. LACP uses the system priority with the MAC address to form the system ID and also during negotiation with other systems.

Defaults None

Access CLI

History Command introduced in Version 1.2

Usage Use this command to display information about the LACP configuration.

Examples To display LACP information, use the following syntax

```
CLI network-admin@switch > lacp-show
switch:              pleiades24
enable:              yes
system-priority:     32768
systemid:800640e942c007a
switch:              pleiades32
enable:              yes
system-priority:     32768
systemid:800640e942c0143
```

lacp-port-stats-settings-modify

This command is used to modify the settings for LACP port statistics.

Syntax `lacp-port-stats-settings-modify`

`enable|disable`	Specify if you want to enable or disable LACP port statistics.
`interval duration:` *`#d#h#m#s`*	Specify the interval between statistics collection.
`disk-space` *`disk-space-number`*	Specify the amount of disk space for the statistics.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to display settings for LACP port statistics collection.

Examples To modify settings for LACP port statistics and disable statistics collection, use the following syntax:

```
CLI network-admin@switch > lacp-port-stats-settings-modify   disable
```

lacp-port-stats-settings-show

Syntax `lacp-port-stats-settings-show`

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to display LACP port statistics settings.

Examples To display settings for LACP port statistics, use the following syntax:

```
CLI network-admin@switch > lacp-port-stats-settings-show
switch:     Leaf-1
enable:     yes
interval:   1m
disk-space: 50M
```

lldp-show

This command is used to display Link Layer Discovery Protocol (LLDP) information on the switch. Link Layer Discovery Protocol (LLDP) allows Ethernet network devices such as switches and routers to receive and transmit device-related information to directly connected devices on the network that are also using the protocols, and to store the information that is learned about other devices.

Syntax `lldp-show`

Specify any of the following options:	
`local-port` *`local-port-number`*	Specifies the local port where the LLDP packet is received.
`chassis-id` *`chassis-id-string`*	Specifies the chassis ID of the switch.
`port-id` *`port-id-string`*	Specifies the port of the switch sending the LLDP packet.

Defaults None

Access CLI

History Command introduced in Netvisor Version 2.0

Usage Use this command to display LLDP information on the switch.

Examples To display all LLDP information, use the following command:

```
CLI network-admin@switch > lldp-show

switch      local-port chassis-id port-id port-desc          sys-name
----------- ---------- ---------- ------- ------------------ -----------
Leaf2       41         0a0000c5   41      PN Switch Port(41) Spine1
Leaf2       42         0a0000c5   42      PN Switch Port(42) Spine1
Leaf2       63         0a0001ca   63      PN Switch Port(63) Spine2
```

```
Leaf2       64          0a0001ca   64      PN Switch Port(64) Spine2
Spine2      11          0c0000b3   11      PN Switch Port(11) Leaf1
Spine2      12          0c0000b3   12      PN Switch Port(12) Leaf1
Spine2      43          0a0000c5   43      PN Switch Port(43) Spine1
Spine2      44          0a0000c5   44      PN Switch Port(44) Spine1
Spine2      63          0a0001c8   63      PN Switch Port(63) Leaf2
Spine2      64          0a0001c8   64      PN Switch Port(64) Leaf2
Leaf1       11          0a0001ca   11      PN Switch Port(11) Spine2
Leaf1       12          0a0001ca   12      PN Switch Port(12) Spine2
Leaf1       31          0a0000c5   31      PN Switch Port(31) Spine1
Leaf1       32          0a0000c5   32      PN Switch Port(32) Spine1
Spine1      31          0c0000b3   31      PN Switch Port(31) Leaf1
Spine1      32          0c0000b3   32      PN Switch Port(32) Leaf1
Spine1      41          0a0001c8   41      PN Switch Port(41) Leaf2
Spine1      42          0a0001c8   42      PN Switch Port(42) Leaf2
Spine1      43          0a0001ca   43      PN Switch Port(43) Spine2
FSpine1     44          0a0001ca   44      PN Switch Port(44) Spine2
```

log-admin-audit-modify

This command is used to enable the collection of Netvisor auditing logs.

Syntax `log-admin-audit-modify  disable|enable`

Defaults Disabled

Access CLI

History

Version 2.5	Command introduced.
Version 3.1.0	Command deprecated.
Version 5.1.0	Command re-added.

Usage Use this command to enable the collection of Netvisor auditing logs.

Examples To enable the feature, use the following syntax:

```
CLI network-admin@switch > log-admin-audit-modify  enable
```

log-admin-audit-show

This command is used to display auditing functionality.

Syntax `log-admin-audit-show`

Defaults Disabled

Access CLI

History

Version 2.5	Command introduced.
Version 3.1.0	Command deprecated.

Usage Use this command to display auditing functionality.

Examples To display auditing functionality, use the following syntax:

```
CLI network-admin@switch > log-admin-audit-show
```

log-audit-exception-create

This command is used to control which CLI, `shell` and `vtysh` commands are subject to auditing. If a command is subject to auditing, the command is logged in the audit log and sent to the TACACS+ server as authorization and accounting messages.

Syntax `log-audit-exception-create`

`cli|shell|vtysh`	Specify the type of audit exception
`pattern` *`pattern-string`*	Specify a regular expression to match exceptions.
`any|read-only|read-write`	Specify the access type to match exceptions
`scope local|fabric`	Specify the scope of exceptions.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to create a log audit exception for TACACS+.

Examples To create a log audit exception, use the following syntax:

```
CLI network-admin@switch > log-audit-exception-create
```

log-audit-exception-delete

This command is used to control which CLI, shell and vtysh commands are subject to auditing. If a command is subject to auditing, the command is logged in the audit log and sent to the TACACS+ server as authorization and accounting messages.

Syntax `log-audit-exception-delete cli|shell|vtysh pattern` *`pattern-string`* `any|read-only|read-write`

`cli|shell|vtysh`	Specify the type of audit exception
`pattern` *`pattern-string`*	Specify a regular expression to match exceptions.
`any|read-only|read-write`	Specify the access type to match exceptions

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to delete a log audit exception..

Examples To delete a log audit exception, use the following syntax:

```
CLI network-admin@switch > log-audit-exception-delete
```

log-audit-exception-show

This command is used to control which CLI, `shell` and `vtysh` commands are subject to auditing. If a command is subject to auditing, the command is logged in the audit log and sent to the TACACS+ server as authorization and accounting messages.

Syntax `log-audit-exception-show cli|shell|vtysh pattern` *`pattern-string`* `any|read-only|read-write scope local|fabric`

`cli|shell|vtysh`	Specify the type of audit exception
`pattern` *`pattern-string`*	Specify a regular expression to match exceptions.
`any|read-only|read-write`	Specify the access type to match exceptions
`scope local|fabric`	Specify the scope of exceptions.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Usage Use this command to display information about log audit exceptions.

Examples To display information about log audit exceptions, use the following syntax:

```
CLI network-admin@switch > log-audit-exception-show
```

log-alert-show

This command displays information about the log alerts on the switch.

Syntax `log-alert-show`

`time date/time: yyyy-mm-ddThh:mm:ss]`	Displays the timestamp for the log file.
`start-time date/time: yyyy-mm-ddThh:mm:ss`	Displays the start time for the log file.
`end-time date/time: yyyy-mm-ddThh:mm:ss`	Displays the end time for the log file.
`duration duration: #d#h#m#s`	Displays the duration of the log file.
`interval duration: #d#h#m#s`	Displays the intervals that alerts occurred in the duration.
`since-start`	Displays alerts collected from the start.
`older-than duration: #d#h#m#s`	Displays alerts older than the duration.
`within-last duration: #d#h#m#s`	Displays alerts collected within the last duration.
`switch node name`	Displays the name of the switch collecting the alert data.
`code code-number`	Displays the code number of the alert.
`name name-string`	Displays the program name.

Defaults None

Access CLI

History Command introduced in Version 2.0.

Usage Use this command to display information about the alert log.

Examples To display information about log alerts, use the following command:

```
CLI network-admin@switch > log-alert-show
No problems found
```

log-audit-show

This command displays information about the log audit configuration.

Syntax `log-audit-show`

Specify between 0 and 2 of the following options:	
`start-time date/time: yyyy-mm-ddThh:mm:ss`	Specifies the start time for the audit log.
`end-time date/time: yyyy-mm-ddThh:mm:ss`	Specifies the end time for the audit log.
`duration duration: #d#h#m#s`	Specifies the duration of the audit log.
Specify any of the following options:	
`program program-string`	Specifies the program type.
`pid pid-number`	Specifies the product indentifiier.
`name name-string`	Specifies the name to match.
`code code-number`	Specifies the code number.
`vnet vnet-name`	Specifies the name of the virtual network.
`remote_switch node name`	Specifies the name of the remote switch.
`user user-name`	Spcifies the username.
`client-pid client-pid-number`	Specifies the client program identifier.
`client-addr ip-address`	Specifies the client IP address.
`port port-number`	Specifies the port number.
`vlan vlan-id`	Specifies the VLAN identifier.
`vxlan vxlan-name`	Specifies the VXLAN identifier.
`count number`	Displays the count between 1 and 50000.
`starting-point starting-point-number`	Specifies the starting point of the log audit.
`length length-number`	Specifies the length of the log audit.
`reverse|no-reverse`	Specifies if the log is displayed in reverse or not.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.2	The parameters, `starting-point`, `length` and `reverse` added.

Version 2.2.5	The IP address is logged as part of a user login event.

Usage Use this command to display information about the audit log.

Examples To display information about log audits, use the following command:

```
CLI network-admin@switch > log-audit-show
```

```
CLI (network-admin@pleiades25) > log-audit-show layout vertical
length:         1628527
category:       audit
time:           2015-04-22,07:59:08.947601-07:00
switch:         pubdev01
program:        nvOSd
pid:            1242
name:           xact_command
code:           11101
remote_switch:  pubdev03
user:           network-admin
client-addr:    10.9.10.24
message:        Transaction command "vlan-create id 25 scope fabric stats" result
success
starting-point: 8324
length:         1628813
category:       audit
time:           2015-04-22,08:08:32.577538-07:00
switch:         pubdev01
program:        nvOSd
pid:            1242
name:           user_command
code:           11001
user:           network-admin
client-pid:     5446
client-addr:    10.9.10.24
message:        Command "vlan-port-add vlan-id 25 ports 55 untagged" result
success
starting-point: 8324
length:         1629091
```

log-event-show

This command displays information about the log event configuration.

Syntax `log-event-show`

Specify between 0 and 2 of the following options:	
`start-time date/time: yyyy-mm-ddThh:mm:ss`	Displays the start time for the log file.
`end-time date/time: yyyy-mm-ddThh:mm:ss`	Displays the end time for the log file.
`duration duration: #d#h#m#s`	Displays the duration of the log file.
Specify any of the following options:	

program *program-string*	Specifies the program type.
pid *pid-number*	Specifies the program indentifiier.
name *name-string*	Specifies the program name.
code *code-number*	Specifies the code number.
event-type system|port|tcp| stp|igmp|lldp|lacp|vdp|ecp|evb|ptp| openflow|storage|tacacs| openstack|mld|mroute|vport|lacp-port| lacp-port-event	Specifies the type of event.
vnet *vnet-name*	Specifies the associated VNET.
remote_switch node *name*	Specifies the name of the remote switch.
user *user-name*	Specifies the username.
client-pid *client-pid-number*	Specifies the client program identifier.
client-addr *ip-address*	Specifies the client IP address.
port *port-number*	Specifies the port number.
vlan *vlan-id*	Specifies the VLAN identifier.
vxlan *vxlan-name*	Specifies the VXLAN identifier.
count *number*	Displays the count in a range from 1 to 50000.
starting-point *starting-point-number*	Specifies the starting point of the log audit.
length *length-number*	Specifies the length of the log audit.
reverse|no-reverse	Specifies if the log is reverse or not reverse.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.1	The event type, TACACS, added.
Version 2.2	The parameters, starting-point, length and reverse added.
Version 2.3.2.1	The options, mld|mroute|vport, added to event type.
Version 3.0.0	The options, lacp-port and lacp-port-event, added.

Usage Use this command to display information about the event log.

Examples To display information about log events, use the following command:

```
CLI network-admin@switch > log-event-show
category:      event
time:          2014-06-24,15:01:08.094640-07:00
switch:        pleiades24
program:       nvOSd
pid:           1384
name:          mac_ip_add
code:          11022
event-type:    port
port:          10
vlan:          11
message:       mac/ip address added mac=50:73:9f:e0:7f:fd ip=172.16.23.3
category:      event
time:          2014-06-24,15:03:24.063484-07:00
switch:        pleiades24
program:       nvOSd
pid:           1384
name:          mac_ip_add
code:          11022
event-type:    port
port:          65
vlan:          11
message:       mac/ip address added mac=50:73:9f:e0:7f:fd ip=172.16.23.2
category:      event
time:          2014-06-24,15:26:04.863472-07:00
switch:        pleaides
program:       nvOSd
pid:           1384
name:          mac_ip_add
code:          11022
```

log-event-settings-modify

This command allows you to modify the log event settings.

Syntax `log-event-settings-modify`

Specify one or more of the following options:	
`system|no-system`	Specifies system events.
`port|no-port`	Specifies the port event.
`tcp|no-tcp`	Specifies TCP events
`stp|no-stp`	Specifies the STP events.
`igmp|no-igmp`	Specifies IGMP events.
`lldp|no-lldp`	Specifies LLDP events.

lacp|no-lacp	Specifies LACP events.
vdp|no-vdp	Specifies VDP events.
ecp|no-ecp	Specifies ECP events.
evb|no-evb	Specifies EVB events.
ptp|no-ptp	Specifies PTP events.
openflow|no-openflow	Specifies Openflow events.
storage|no-storage	Specifies storage events.
tacacs|no-tacacs	Specifies TACACS events.
mld|no-mld	Specifies MLD events.
openstack|no-openstack	Specifies OpenStack events.
mroute|no-mroute	Specifies multicast routing events.
vport|no-vport	Specifies vPort events.
lacp-port-event|no-lacp-port-event	Specifies to log LACP port events.

Defaults None

Access CLI

History

Version 1.2	Command introduced.
Version 2.1	The parameter, TACACS, added.
Version 2.2	The parameter, openstack, added.
Version 2.2.5	The parameter, LACP, added.
Version 2.3	The parameters, mld and mroute, added.
Version 2.3.1	The parameter, vport, added.
Version 2.6.2	The parameter, lacp-port-event, added.

Usage Use this command to modify log event settings including the type of event.

Examples To modify the log event settings to exclude vdp events, use the following command:

```
CLI network-admin@switch > log-event-settings-modify  no-vdp
```

log-event-settings-show

This command allows you to display the log event settings.

Syntax log-event-settings-show

Defaults None

Access CLI

History Command introduced in nvOS Version 1.2.1.

Usage Use this command to display log event settings including the type of event.

Examples To display the log event settings, use the following command:

```
CLI network-admin@switch > log-event-settings-show
switch:    Pleiades24
system:    on
port:      on
tcp:       off
stp:       off
igmp:      off
lldp:      off
lacp:      off
vdp:       off
ecp:       off
evb:       off
ptp:       off
openflow:  off
storage:   on
tacacs:    on
openstack: on
switch:    Pleiades25
system:    on
port:      on
tcp:       off
stp:       off
igmp:      off
lldp:      off
lacp:      off
vdp:       off
ecp:       off
evb:       off
ptp:       off
openflow:  off
storage:   on
tacacs:    on
openstack: on
```

log-system-show

This command displays information about the log system configuration.

Syntax `log-system-show`

Specify between 0 and 2 of the following options:	
`start-time date/time:` *yyyy-mm-*	Specify the start time for the log file.

ddThh:mm:ss	
end-time date/time: *yyyy-mm-ddThh:mm:ss*	Specify the end time for the log file.
duration duration: #d#h#m#s	Specify the duration of the log file.
Specify any of the following options:	
program *program-string*	Specifies the program type.
pid *pid-number*	Specifies the program identifiier.
name *name-string*	Specifies the program name.
code *code-number*	Specifies the code number.
level critical|error|warn| note	Specifies the type of event.
vnet *vnet-name*	Specifies the VNET name.
remote_switch node *name*	Specifies the name of the remote switch.
user *user-name*	Spcifies the username.
client-pid *client-pid-number*	Specifies the client program identifier.
client-addr *ip-address*	Specifies the client IP address.
port *port-number*	Specifies the port number.
vlan *vlan-id*	Specifies the VLAN identifier.
vxlan *vxlan-name*	Specifies the VXLAN identifier.
count *number*	Displays the count from 1 to 50000.
starting-point *starting-point-number*	Specifies the starting point of the log audit.
length *length-number*	Specifies the length of the log audit.
reverse| no-reverse	Specifies if the log is reverse or not reverse.

Defaults None

Access CLI

History Command introduced in Version 1.2.

Usage Use this command to display information about the audit log.

Examples To display information about system logging, use the following command:

```
CLI network-admin@switch > log-system-show
```

```
CLI (network-admin@pleiades25) > log-system-show format all layout vertical
category:      system
```

```
time:          2014-06-16,10:33:54.425701-07:00
switch:        pleiades25
program:       nvOSd
pid:           1431
name:          fan_initial_status
code:          11303
level:         warn
message:       Fan 4 initial status ok
category:      system
time:          2014-06-16,10:33:54.425839-07:00
switch:        pleiades25
program:       nvOSd
pid:           1431
name:          ps_initial_status
code:          11302
level:         warn
message:       Power supply 1 initial status ok
category:      system
time:          2014-06-16,10:34:51.479611-07:00
switch:        pleiades25
program:       sh
pid:           3873
name:          smf_nvOSd_stop
code:          30108
level:         note
message:       SMF Service stopping nvOSd
category:      system
time:          2014-06-16,10:36:57.144770-07:00
switch:        pleiades25
program:       sh
pid:           871
name:          smf_nvOSd_start
code:          30107
level:         note
message:       SMF Service starting nvOSd
category:      system
time:          2014-06-16,10:36:58.543972-07:00
switch:        pleiades25
program:       nvOSd
pid:           1014
name:          nvOSd_start
code:          11008
level:         note
message:       ===== nvOSd start: version=2.1.201005777,pn-ONVL-2.0.2-2000212193
changeset=ceb01f7ff168 branch=default
category:      system
time:          2014-06-16,10:37:07.796715-07:00
switch:        pleiades25
program:       perl
pid:           1506
name:          fanmon_fan_status
code:          30100
level:         note
message:       Controller 1 fan 1 speed 7050 RPM
```

log-system-counters-reset

This command resets the log counters on the switch.

Syntax `log-system-counters-reset reset-time reset-time-string`

`reset-time` *`reset-time-string`*	Specify the reset time.

Defaults None

Access CLI

History Command introduced in Version 1.2.

Usage Use this command to reset log counters.

Examples To reset log counters, use the following commands:

```
CLI network-admin@switch > log-system-counters-reset
```

log-system-counters-show

This command displays the log counters on the switch.

Syntax `log-system-counters-show`

Defaults None

Access CLI

History Command introduced in Version 1.2.

Usage Use this command to display log counters.

Examples To display log counters, use the following command:

```
CLI network-admin@switch > log-system-counters-show
switch           critical error warn note
---------------- -------- ----- ---- ----
pleiades24       0        0     390  494
pleiades25       26       0     546  843
```

M Commands

mac-limit-modify

You can now limit the number of MAC addresses per port. You can configure port security only on ports. Details about port security for ports are as follows:

- **Access ports**—You can configure port security on interfaces that you have configured as Layer 2 access ports. On an access port, port security applies only to the access VLAN.
- **Trunk ports**—You can configure port security on interfaces that you have configured as Layer 2 trunk ports.

Syntax `mac-limit-modify`

`port` *`port-list`*	Specify the port or port list.
`mac-limit` *`mac-limit-number`*	Specify the number of MAC addresses to limit on the port.
`mac-limit-action log|disable`	Specify the action to take if the MAC address limit is exceeded.

Defaults None

Access Network Administrator

History Command introduced in Version 2.6.0.

Version 2.6.0	Command introduced.
Version 5.2.0	The parameter, `drop`, deprecated.

Usage Use this command to modify the MAC address limits on ports.

Examples To modify the number of MAC addresses on ports, use the following syntax:

```
CLI network-admin@switch > mac-limit-modify
```

mac-limit-show

You can now limit the number of MAC addresses per port. You can configure port security only on ports. Details about port security for ports are as follows:

- **Access ports**—You can configure port security on interfaces that you have configured as Layer 2 access ports. On an access port, port security applies only to the access VLAN.
- **Trunk ports**—You can configure port security on interfaces that you have configured as Layer 2 trunk ports.

Syntax `mac-limit-show`

`port` *`port-list`*	Displays the port or port list.
`mac-limit` *`mac-limit-number`*	Displays the number of MAC addresses to limit on the port.
`mac-limit-action log|disable`	Displays the action to take if the MAC address limit is exceeded.
`num-macs` *`num-macs-number`*	Displays the number of MAC addresses learned on the port.

Access Network Administrator

History Command introduced in Version 2.6.0.

Version 2.6.0	Command introduced.

Version 5.2.0	The parameter, `drop`, deprecated.

Usage Use this command to display information about MAC address limits on ports.

Examples To display information about MAC address limits on ports, use the following syntax:

```
CLI network-admin@switch > mac-limit-show
```

mcast-show

This command displays multicast group information for a switch.

Syntax `mcast-show`

`group-ip` *`muticast-ip-address`*	Specifies the IP address for the multicast group.
`vnet` *`vnet-name`*	Specifies the VNET name.
`l2-net` *`l2-net-name`*	Specifies the Layer 2 network name.

Defaults Unless otherwise specified, all multicast group membership information for the local switch is displayed.

Access CLI

History

Version 1.2	Command introduced.
Version 3.0.0	The parameter, `l2-net`, added.

Usage Hosts and adjacent switches on IPv4 networks can establish multicast group memberships.

Examples To display all multicast group memberships for the local switch, use the following command:

```
CLI network-admin@switch > mcast-show
group-ip         vlan      group-id       group-ports
--------         -----     --------       -----------
239.4.10.122     1         28             43
239.4.10.70      1         27             43
239.4.10.190     1         26             17
239.4.10.222     1         25             17
239.4.10.187     1         24             17
239.4.10.32      1         23             17
239.4.10.115     1         22             17
```

mgmt-session-show

In earlier versions of Netvisor, Netvisor did not support viewing current user sessions using the CLI. This can be very useful for security and troubleshooting. Netvisor now lists all currently logged-in users along with the IP they are connecting from and the login time when you execute the command, `mgt-session-show`.

Syntax `mgmt-session-show`

user *user-string*	Displays the user name.
cli-user *cli-user-string*	Displays the name used to log into the switch.
pid *pid-number*	Displays the process ID.
terminal *terminal-string*	Displays the terminal.
from-ip *ip-address*	Displays the IP address for the user.
login-time date/time: *yyyy-mm-ddTHH:mm:ss*	Displays the time and date that the user logged into the switch.
remote-node *remote-node-string*	Displays the name of the remote node.
vnet *vnet-string*	Displays the VNET assigned to the user.
type cli|api|shell	Displays the type of login session.

Defaults None

Access Network Administrator

History Command introduced in Version 3.0.0

Usage Use this command to display users logged into the switch.

Examples To display users logged into the switch, NAT-1, use the following syntax:

```
CLI network-admin@switch > mgmt-session-show
switch        user  cli-user      pid   terminal from-ip      login-time     type
------------- ----- ------------- ----- -------- ------------ ------------   -------
Spine-ext-41  admin network-admin 13805 pts/3    10.60.1.216  11:20:52        cli
Spine-ext-41  root  network-admin 8589  pts/2    10.14.20.109 11-15,17:16:17  cli
```

mirror-create

This command is used to create mirror ports and flows. Network engineers or administrators use port mirroring to analyze and debug data or diagnose errors on a network. It helps administrators keep a close eye on network performance and alerts them when problems occur. It can be used to mirror either inbound or outbound traffic (or both) on single or multiple interfaces.

Syntax mirror-create

name *name-string*	Specify a name for the mirror configuration.
direction ingress|egress| bidirection	Specify a direction for the mirrored traffic.
out-port *port-list*	Specify the port for outgoing traffic.
out-trunk *trunk name*	Specify the name of the outgoing trunk configuration.
in-port *port-list*	Specify the port for incoming traffic. Supported ports are 1-64 on the F64 platform. The parameter,

	`all`, is not supported.
`filtering port|vflow-and-port|vflow-or-port`	Specify the filter type for the configuration.
`enable|disable`	Enable or disable the configuration.
`other-egress-out allow|prevent`	Specify if other outgoing traffic is allowed or prevented. The default value is `prevent`.
`span-encap none|over-ip|over-vlan`	Specify the mirror span type. The default type is none.
`span-local-ip` *`ip-address`*	Specify the local IPv4 address for the mirror span.
`span-remote-ip` *`ip-address`*	Specify the remote IPv4 address fpr the mirror span.
`span-src-mac` *`mac-address`*	Specify the source MAC address for the mirror span.
`span-dst-mac` *`mac-address`*	Specify the destination MAC address for the mirror span.
`span-tagging-vlan` *`vlan-id`*	Specify the mirror span VLAN tagging ID. The default value is none.
`span-tos` *`integer`*	Specify the mirror span ToS from 0 to 255. The default value is 0.
`nvie-mirror|no-nvie-mirror`	Specify to mark this mirroring as an NVIE mirror and mirror traffic to NVIE VM.

Defaults None

Access CLI

History

Version 2.2	Command introduced.
Version 2.4	The parameter, `span-`, introduced.
Version 2.6.2	The parameter, `nvie-mirror`, added.

Usage Use this command to create mirrored traffic or ports for analyzing traffic.

Examples To create a mirror configuration, mirror-port, with the direction egress, port 73, inbound port 33, filtering by port, and allow other egress traffic, use the following syntax:

```
CLI network-admin@switch > mirror-create name mirror-port direction
egress out-port 73 in-port 33 enable other-egress-out allow
```

mirror-delete

This command is used to delete a mirror configuration.

Syntax `mirror-delete name name-string`

name *name-string*	Specify a name for the mirror configuration.

Defaults None

Access CLI

History Command introduced in Version 2.2.

Usage Use this command to delete a mirror configuration.

Examples To delete a mirror configuration, **mirror-port**, use the following syntax:

```
CLI network-admin@switch > mirror-delete name mirror-port
```

mirror-modify

This command allows you to modify a port mirror configuration.

Syntax `mirror-modify`

name *name-string*	Specify the name of the mirror configuration to modify.
Specify any of the following options:	
direction disabled|ingress| egress|bidirection	Specify the direction of the traffic that you want to mirror on the port.
out-port *port-list*	Specify the list of ports for outgoing network traffic.
out-trunk *trunk-name*	Specify the trunk name for the outgoing trunk.
in-port *port-list*	Specify the list of ports for incoming network traffic.
filtering port|vflow-and-port| vflow-or-port	Specify the type of traffic to filter.
enable|disable	Enable or disable port mirroring on the network.
other-egress-out allow|prevent	Specify if other outgoing traffic is allowed or prevented.
span-encap none|over-ip|over-vlan	Specify the mirror span type. The default type is none.
span-local-ip *ip-address*	Specify the local IPv4 address for the mirror span.
span-remote-ip *ip-address*	Specify the remote IPv4 address fpr the mirror span.
span-src-mac *mac-address*	Specify the source MAC address for the mirror span.
span-dst-mac *mac-address*	Specify the destination MAC address for the mirror span.
span-tagging-vlan *vlan-id*	Specify the mirror span VLAN tagging ID. The default value is none.

span-tos *integer*	Specify the mirror span ToS from 0 to 255. The default value is 0.
nvie-mirror|no-nvie-mirror	Specify to mark this mirroring as an NVIE mirror and mirror traffic to NVIE VM.

Defaults None.

Access CLI

History

Version 1.2	port-mirror-modify introduced.
Version 2.0	Command changed to mirror-modify.
Version 2.1	The parameter, out-trunk, added.
Version 2.2.2	The parameter, direction, added.
Version 2.2.3	The parameter, policy, changed to filtering. The parameter other-egress-out added. j
Version 2.4	The parameter, span-, introduced.
Version 2.6.2	The parameter, nvie-mirror, added.

Usage Port mirroring is used to send copies of network traffic on one port to a network monitoring connection on another port. You can use this command to enable or disable port mirroring as well as designate the ports to use for it.

Examples To enable port mirroring on outbound ports 3-5 and inbound ports 8-9, use the following command:

```
CLI network-admin@switch > mirror-modify out-port 3-5 in-port 8-9
mirroring
```

mirror-show

This command is used to display information about port mirroring on the switch.

Syntax mirror-show

name *name-string*	Specifies a name for the mirror configuration.
id	Specifies the mirror ID assigned by nvOS.
direction ingress|egress| bidirection	Specifies a direction for the mirrored traffic.
out-port *port-list*	Specifies the port for outgoing traffic.
out-trunk *trunk name*	Specifies the name of the outgoing trunk configuration.
loopback-port *loopback-port-number*	Specifies the loopback port for mirrored traffic.

in-port *port-list*	Specifies the port for incoming traffic.
filtering port| vflow-and-port|vflow-or-port	Specifies the filter type for the configuration.
enable|disable	Enable or disable the configuration.
other-egress-out allow|prevent	Specifies if other outgoing traffic is allowed or prevented.
span-encap none|over-ip|over-vlan	Specify the mirror span type. The default type is none.
span-local-ip *ip-address*	Specify the local IPv4 address for the mirror span.
span-remote-ip *ip-address*	Specify the remote IPv4 address fpr the mirror span.
span-src-mac *mac-address*	Specify the source MAC address for the mirror span.
span-dst-mac *mac-address*	Specify the destination MAC address for the mirror span.
span-tagging-vlan *vlan-id*	Specify the mirror span VLAN tagging ID. The default value is none.
span-tos *integer*	Specify the mirror span ToS from 0 to 255. The default value is 0.
nvie-mirror|no-nvie-mirror	Specify to mark this mirroring as an NVIE mirror and mirror traffic to NVIE VM.

Defaults None.

Access CLI

History

Version 1.2	Command introduced.
Version 2.0	Command changed to `mirror-show`.
Version 2.4	The parameter, `span-`, introduced.
Version 2.6.2	The parameter, `nvie-mirror`, added.

Usage Use this command to display port mirroring information.

Examples To display information about port mirroring, use the following command:

```
CLI (network-admin@pleiades25) > mirror-show
switch:        pleiades25
mirroring:     disable
```

mld-router-show

Multicast Listener Discovery (MLD) is a Layer 3 multicast protocol used between IPv6 hosts and routers similar to how IGMP is used for IPv4. MLD snooping allows a switch to examine MLD packets and make

forwarding decisions based on their content.

MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv6 multicast traffic only to those ports that want to receive it.

If MLD Snooping is not configured, Netvisor forwards multicast traffic to all the switch ports, impacting switch performance.

Syntax `mld-router-show`

`node-ip` *`ip-address`*	Specifies the name of the IP node for the MLD configuration.
`vnet` *`vnet-name`*	Specifies the name of the VNET assigned to the MLD configuration.
`l2-net` *`l2-net-name`*	Specifies the name of the Layer 2 network.
`vlan` *`vlan-id`*	Specifies the ID of the VLAN for the MLD configuration.
`port` *`port-number`*	Specifies the number of the port for the MLD configuration.

Defaults None.

Access CLI

History

Version 2.3	Command introduced.
Version 2.4.1	The parameters, `group-ip`, `source-ip`, `node-type`, `and expires`, `deprecated`. The parameter, `vnet`, added.
Version 3.0.0	The parameter, `l2-net`, added.

Usage Default behavior, when MLD Snooping is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance.

Examples To display MLD router parameters for the local switch, use the following command:

```
CLI network-admin@switch > mld-router-show
```

mld-show

Multicast Listener Discovery (MLD) is a Layer 3 multicast protocol used between IPv6 hosts and routers similar to how IGMP is used for IPv4. MLD snooping allows a switch to examine MLD packets and make forwarding decisions based on their content.

MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv6 multicast traffic only to those ports that want to receive it.

The default behavior, when MLD Snooping is not configured, multicast traffic will be forwarded to all the switch ports, impacting switch performance.

Syntax `mld-show`

`group-ip` *`ip-address`*	Specifies the name of the IP group for the MLD configuration.
`node-ip` *`ip-address`*	Specifies the name of the IP host for the MLD configuration.
`vnet` *`vnet-name`*	Specifies the name of the VNET assigned to the MLD configuration.
`l2-net` *`l2-net-name`*	Specifies the name of the Layer 2 network.
`vlan` *`vlan-id`*	Specifies the ID of the VLAN for the MLD configuration.
`port` *`port-number`*	Specifies the number of the port for the MLD configuration.
`source-ip` *`ip-address`*	Specifies the IP source name for the MLD configuration.
`node-type host|router|switch`	Specifies the node type as host or router.
`expires` *`expires-number(s)`*	Specifies the ageout time.

Defaults None.

Access CLI

History

Version 2.3	Command introduced.
Version 2.4.1	The parameter, `switch`, deprecated. The parameter, `vnet`, added.
Version 3.0.0	The parameter, `l2-net`, added.

Usage Default behavior, when MLD is not configured, forwards multicast traffic to all the switch ports, impacting switch performance.

Examples To display MLD parameters for the local switch, use the following command:

```
CLI network-admin@switch > mld-show

    switch:           spine01
    group-ipv6:       ff02::1:ff11:1111
    host-ipv6:        fe80::3636:3bff:fece:44f2
    vlan:             100
    port:             8,69
    source-ipv6:      2001:db8::2:1
```

mld-router-show

Multicast Listener Discovery (MLD) is a Layer 3 multicast protocol used between IPv6 hosts and routers similar to how IGMP is used for IPv4. MLD snooping allows a switch to examine MLD packets and make forwarding decisions based on their content.

MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv6 multicast traffic only to those ports that want to receive it.

The default behavior, when MLD Snooping is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance.

Syntax `mld-router-show`

`node-ip` *`ip-address`*	Specifies the name of the IP node for the MLD configuration.
`vnet` *`vnet-name`*	Specifies the name of the VNET assigned to the MLD configuration.
`l2-net` *`l2-net-name`*	Specifies the name of the Layer 2 network.
`vlan` *`vlan-id`*	Specifies the ID of the VLAN for the MLD configuration.
`port` *`port-number`*	Specifies the number of the port for the MLD configuration.

Defaults None.

Access CLI

History

Version 2.3	Command introduced.
Version 2.4.1	The parameters, `group-ip`, `source-ip`, `node-type`, `and expires`, `deprecated`. The parameter, `vnet`, added.
Version 3.0.0	The parameter, `l2-net`, added.

Usage Default behavior, when MLD Snooping is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance.

Examples To display MLD router parameters for the local switch, use the following command:

```
CLI network-admin@switch > mld-router-show
```

mld-snooping-modify

Multicast Listener Discovery (MLD) is a Layer 3 multicast protocol used between IPv6 hosts and routers similar to how IGMP is used for IPv4. MLD snooping allows a switch to examine MLD packets and make forwarding decisions based on their content.

MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to

forward IPv6 multicast traffic only to those ports that want to receive it.

The default behavior, when you do not configure MLD Snooping, Netvisor forwards multicast traffic to all the switch ports, impacting switch performance.

Syntax `mld-snooping-modify`

`scope local|fabric`	Modify the scope of MLD Snooping to local or fabric.
`enable|disable`	Enable, disable MLD Snooping. Default: disable
`mldv1-vlans` *`vlan-list`*	VLANs on which to enable snooping and use MLDv1 protocol. Default: none
`mldv2-vlans` *`vlan-list`*	VLANs on which to enable snooping and use MLDv2 protocol. Default 1 - 4092
`snoop-linklocal-vlans` *`vlan-list`*	Allow snooping of link-local groups (ff02::/16) on these vlans. Default 1 - 4092
`snoop-nd-vlans` *`vlan-list`*	Allow snooping of ND SN Multicast addresses (ff02::1:ff/104) on these vlans. Default 1 - 4092
`query-interval` *`seconds`*	Specify the interval between queries in seconds.
`query-max-response-time` *`seconds`*	Specify the maximum response time for a query.

Defaults See above description

Access CLI

History

Version 2.3	Command introduced.
Version 2.4	The parameters, `version` and `snoop-link`, introduced.
Version 2.5.2	The parameters, `version`, `snoop-linklocal`, and `snoop-nd` deprecated. The parameters, `mldv1-vlans`, `mldv2-vlans`, `snoop-linklocal-vlans`, and `snoop-nd-vlans` introduced.
Version 3.1.0	The parameters, `query-interval` and `query-max-response-time`, added.

Usage When MLD Snooping is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance. Use this command to modify the scope of MLD Snooping, enable snooping on specific VLANs, link-local groups, or ND SN multicast addresses, or to disable snooping.

Examples To modify the scope from local to fabric use the following syntax:

```
CLI network-admin@switch > mld-snooping-modify scope fabric
```

mld-snooping-show

Multicast Listener Discovery (MLD) is a Layer 3 multicast protocol used between IPv6 hosts and routers similar to how IGMP is used for IPv4. MLD snooping allows a switch to examine MLD packets and make forwarding decisions based on their content.

MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv6 multicast traffic only to those ports that want to receive it.

When MLD Snooping is not configured multicast traffic, by default, is forwarded to all the switch ports thus impacting switch performance.

Syntax `mld-snooping-show`

Defaults None.

Access CLI

History

Version 2.3	Command introduced.
Version 2.4	The parameters, `version` and `snoop-link`, introduced.
Version 2.5.2	The parameters, `version`, `snoop-linklocal`, and `snoop-nd` deprecated. The parameters, `mldv1-vlans`, `mldv2-vlans`, `snoop-linklocal-vlans`, and `snoop-nd-vlans` introduced.
Version 3.1.0	The parameters, `query-interval` and `query-max-response-time`, added.

Usage The default behavior, when MLD Snooping is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance.

Examples To display the format for all options for the local switch, use the following command:

```
CLI network-admin@switch > mld-snooping-show format all

switch:                 switch name
enable:                 yes
mlvdv1-vlans            none
mldv2-vlans             1-4092
snoop-linklocal-vlans   1-4092
snoop-nd-vlans          1-4092
nvOS-managed-vlans      100
interop-v1-vlans        none
vlans                   1-99,101-4092
```

mld-static-group-create

Multicast Listener Discovery (MLD) is a Layer 3 multicast protocol used between IPv6 hosts and routers similar to how IGMP is used for IPv4. MLD snooping allows a switch to examine MLD packets and make forwarding decisions based on their content.

MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv6 multicast traffic only to those ports that want to receive it.

The default behavior, when MLD Snooping is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance.

Syntax `mld-static-group-create`

`group-ip` *`ip-address`*	Specifies the name of the IP group for the MLD configuration.
`vlan` *`vlan-id`*	Specifies the ID of the VLAN for the MLD configuration.
`ports` *`port-list`*	Specifies the list of the ports for the MLD configuration

Defaults None.

Access CLI

History Command introduced in Version 2.3.

Usage The default behavior, when MLD Snooping is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance.

Examples To create a multicast group memberships for the local switch, use the following command:

```
CLI network-admin@switch > mld-static-group-create
```

mld-static-group-delete

Multicast Listener Discovery (MLD) is a Layer 3 multicast protocol used between IPv6 hosts and routers similar to how IGMP is used for IPv4. MLD snooping allows a switch to examine MLD packets and make forwarding decisions based on their content.

MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv6 multicast traffic only to those ports that want to receive it.

The default behavior, when MLD Snooping is not configured, multicast traffic will be forwarded to all the switch ports, impacting switch performance.

Syntax `mld-static-group-delete`

`group-ip` *`ip-address`*	Specifies the name of the IP group for the MLD configuration to be deleted.
`vlan` *`vlan-id`*	Specifies the ID of the VLAN for the MLD configuration to be deleted.

Defaults None.

Access CLI

History Command introduced in Version 2.3.

Usage The default behavior, when MLD Snooping is not configured, multicast traffic will be forwarded to all the switch ports, impacting switch performance.

Examples To display all multicast group memberships for the local switch, use the following command:

```
CLI network-admin@switch > mld-static-group-delete
```

mld-static-group-show

Multicast Listener Discovery (MLD) is a Layer 3 multicast protocol used between IPv6 hosts and routers similar to how IGMP is used for IPv4. MLD snooping allows a switch to examine MLD packets and make forwarding decisions based on their content.

MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv6 multicast traffic only to those ports that want to receive it.

The default behavior, when MLD Snooping is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance.

Syntax `mld-static-group-show`

`group-ipv6` *`ip-address`*	Specifies the name of the IP group for the MLD configuration.
`vnet` *`vnet-name`*	Specifies the name of the VNET.
`vlan` *`vlan-id`*	Specifies the ID of the VLAN for the MLD configuration.
`ports` *`port-list`*	Specifies the number of the port for the MLD configuration.

Defaults None.

Access CLI

History

Version 2.3	Command introduced.
Version 2.4.1	The parameter, `vnet`, added.

Usage When MLD Snooping is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance.

Examples To display MLD parameters for the local switch, use the following command:

```
CLI network-admin@switch > mld-static-group-show

switch:            aquila-ext-01
group-ipv6:        ff02::1:ff11:1111
```

```
vlan:              100
port:              8,69, 129
```

mld-static-source-create

Multicast Listener Discovery (MLD) is a Layer 3 multicast protocol used between IPv6 hosts and routers similar to how IGMP is used for IPv4. MLD snooping allows a switch to examine MLD packets and make forwarding decisions based on their content.

MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv6 multicast traffic only to those ports that want to receive it.

The default behavior, when MLD Snooping is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance.

Syntax `mld-static-source-create`

`source-ip` *`ip-address`*	Specifies the source IPv6 address for the MLD configuration.
`group-ip` *`ip-address`*	Specifies the source of the IP group for the MLD configuration.
`vlan` *`vlan-id`*	Specifies the ID of the VLAN for the MLD configuration.
`vnet` *`vnet-name`*	Specifies the name of the VNET.
`l2-net` *`l2-net-name`*	Specifies the name of the Layer 2 network.
`ports` *`port-list`*	Specifies the list of the ports for the MLD configuration.

Defaults None.

Access CLI

History

Version 2.3	Command introduced.
Version 2.4.1	The parameter, `vnet`, added.
Version 3.0.0	The parameter, `l2-net`, added.

Usage The default behavior, when MLD is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance.

Examples To display all multicast group memberships for the local switch, use the following command:

```
CLI network-admin@switch > mld-static-source-create
```

mld-static-source-delete

Multicast Listener Discovery (MLD) is a Layer 3 multicast protocol used between IPv6 hosts and routers similar to how IGMP is used for IPv4. MLD snooping allows a switch to examine MLD packets and make forwarding decisions based on their content.

MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv6 multicast traffic only to those ports that want to receive it.

The default behavior, when MLD Snooping is not configured, multicast traffic will be forwarded to all the switch ports, impacting switch performance.

Syntax `mld-static-source-delete`

`source-ip` *`ip-address`*	Specifies the source IPv6 address for the MLD configuration to be deleted.
`l2-net` *`l2-net-name`*	Specifies the name of the Layer 2 network.
`group-ip` *`ip-address`*	Specifies the source of the IP group for the MLD configuration to be deleted.
`vlan` *`vlan-id`*	Specifies the ID of the VLAN for the MLD configuration to be deleted.

Defaults None.

Access CLI

History .

Version 2.3.0	Command introduced.
Version 3.0.0	The parameter, `l2-net`, added.

Usage The default behavior, when MLD Snooping is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance. For this CLI, the group has to be seated statically already.

Examples To display all multicast group memberships for the local switch, use the following command:

```
CLI network-admin@switch > mld-static-source-delete
```

mld-static-source-show

Multicast Listener Discovery (MLD) is a Layer 3 multicast protocol used between IPv6 hosts and routers similar to how IGMP is used for IPv4. MLD snooping allows a switch to examine MLD packets and make forwarding decisions based on their content.

MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv6 multicast traffic only to those ports that want to receive it.

The default behavior, when MLD Snooping is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance.

Syntax `mld-static-source-show`

`group-ip` *`ip-address`*	Specifies the IP address of the group.

vnet *vnet-name*	Specifies the name of the VNET.
l2-net *l2-net-name*	Specifies the name of the Layer 2 network.
vlan *vlan-id*	Specifies the name of the VLAN.
source-ip *ip-address*	Specifies the IP address of the source.
host-ip *ip-address*	Specifies the IP address of the host.
ports *port-list*	Specifies the list of ports.

Defaults None.

Access CLI

History Command introduced in Version 2.3.

Version 2.3	Command introduced.
Version 2.4.1	The parameter, `switch`, deprecated. The parameter, `vnet`, added.
Version 3.0.0	The parameter, `l2-net`, added.

Usage The default behavior, when MLD Snooping is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance.

Examples To display all multicast group memberships for the local switch, use the following command:

```
CLI network-admin@switch > mld-static-source-show
```

```
switch:          aquila-ext-01
group-ip:        ff02::1:ff11:1111
vlan:            100
source-ip:       2001:db8::2:1
host-ip:         fe80::3636:3bff:fece:44f2
ports:           8,69,129
```

mld-stats-show

Multicast Listener Discovery (MLD) is a Layer 3 multicast protocol used between IPv6 hosts and routers similar to how IGMP is used for IPv4. MLD snooping allows a switch to examine MLD packets and make forwarding decisions based on their content.

MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv6 multicast traffic only to those ports that want to receive it.

The default behavior, when MLD Snooping is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance.

Syntax `mld-stats-show vlan` *vlan-id*

Defaults None.

Access

History Command introduced in Version 2.3.0.

Usage The default behavior, when MLD Snooping is not configured, multicast traffic is forwarded to all the switch ports, impacting switch performance.

Examples To display all multicast group memberships for the local switch, use the following command:

```
CLI network-admin@switch > mld-stats-show
```

mld-switches-show

This command is used to display switches with MLD protocol enabled.

Syntax `mld-switches-show`

`node-ip` *`ip-address`*	Specifies the node IP address.
`vnet` *`vnet-name`*	Specifies the name of the VNET assigned to the MLD configuration.
`l2-net` *`l2-net-name`*	Specifies the name of the Layer 2 network.
`vlan` *`vlan-id`*	Specifies the ID of the VLAN for the MLD configuration.
`port` *`port-number`*	Specifies the port number.

Defaults None

Access CLI

History

Version 2.3.3	Command introduced.
Version 2.4.1	The parameters, `group-ip`, `source-ip`, `node-type`, and `expires`, deprecated. The parameter, `vnet`,`vlan` added.
Version 3.0.0	The parameter, `l2-net`, added.

Usage Displays information about MLD switches.

Examples To display MLD switches, use the following syntax:

```
CLI network-admin@switch > mld-switches-show
```

```
switch:       spine-1
node-ip:     ::
vlan:        1
```

```
port:       3
switch:     leaf-1
node-ip:    ::
vlan:       2
port:       3
switch:     leaf-2
node-ip:    ::
vlan:       3
port:       3
```

mst-config-create

Multiple Spanning Tree Protocol as defined in IEEE802.1s or IEEE802.1Q-2005 provides the ability to manage multiple VLANs from a single MST instance. MST allows the formation of MST regions that can run multiple MST instances (MSTIs). Multiple regions and other STP bridges are interconnected using one single Common Spanning Tree (CST).

Syntax `mst-config-create`

`instance-id` *`id`*	Specify an ID for the MST configuration.
`vlans` *`vlan-list`*	Specify the list of VLANs associated with the MST configuration.
`bridge-priority` *`bridge-priority-number`*	Specify the bridge priority for the MST configuration. The bridge priority is a value from 0 to 65536, with a default value of 0. The value increments by 4096 each time. So for example, values can be 0, 4096, 8192, up to 65536.

Defaults None

Access CLI

History Command introduced in Version 2.4.

Usage This command is used to create a MST configuration on the switch.

Examples To create a MST configuration with the ID 10, VLANs 12-15, and bridge-priority of 4096, use the following syntax:

```
CLI network-admin@switch > mst-config-create instance-id 10 vlans 12-15
bridge-priority  4096
```

mst-config-delete

Multiple Spanning Tree Protocol as defined in IEEE802.1s or IEEE802.1Q-2005 provides the ability to manage multiple VLANs from a single MST instance. MST allows the formation of MST regions that can run multiple MST instances (MSTIs). Multiple regions and other STP bridges are interconnected using one single Common Spanning Tree (CST).

Syntax `mst-config-delete`

`instance-id` *`id`*	Displays an ID for the MST configuration. This is a number between 0 and 63.

Defaults None

Access CLI

History Command introduced in Version 2.4.

Usage This command is used to delete a MST configuration on the switch.

Examples To delete a MST configuration with the ID 10, use the following syntax:

```
CLI network-admin@switch > mst-config-delete instance-id 10
```

mst-config-modify

Multiple Spanning Tree Protocol as defined in IEEE802.1s or IEEE802.1Q-2005 provides the ability to manage multiple VLANs from a single MST instance. MST allows the formation of MST regions that can run multiple MST instances (MSTIs). Multiple regions and other STP bridges are interconnected using one single Common Spanning Tree (CST).

Syntax `mst-config-modify`

`instance-id` *`id`*	Specify an ID for the MST configuration. This is a number between 0 and 63.
`vlans` *`vlan-list`*	Specify the list of VLANs associated with the MST configuration.
`bridge-priority` *`bridge-priority-number`*	Specify the bridge priority for the MST configuration. The bridge priority is a value from 0 to 65536, with a default value of 0. The value increments by 4096 each time. So for example, values can be 0, 4096, 8192, up to 65536.

Defaults None

Access CLI

History Command introduced in Version 2.4.

Usage This command is used to modify information about a MST configuration on the switch.

Examples To modify a MST configuration with the ID 10, VLANs 13-16, and bridge-priority of 4096, use the following syntax:

```
CLI network-admin@switch > mst-config-modify instance-id 10 vlans 13-16
bridge-priority 4096
```

mst-config-show

Multiple Spanning Tree Protocol as defined in IEEE802.1s or IEEE802.1Q-2005 provides the ability to manage multiple VLANs from a single MST instance. MST allows the formation of MST regions that can run multiple MST instances (MSTIs). Multiple regions and other STP bridges are interconnected using one single Common Spanning Tree (CST).

Syntax `mst-config-show`

`instance-id` *`id`*	Specify an ID for the MST configuration. This is a number between 0 and 63.
`vlans` *`vlan-list`*	Specify the list of VLANs associated with the MST configuration.
`bridge-priority` *`bridge-priority-number`*	Specify the bridge priority for the MST configuration. The bridge priority is a value from 0 to 65536, with a default value of 0. The value increments by 4096 each time. So for example, values can be 0, 4096, 8192, up to 65536.

Defaults None

Access CLI

History Command introduced in Version 2.4.

Usage This command is used to display a MST configuration on the switch.

Examples To display a MST configuration with the ID 10, VLANs 13-16, and bridge-priority of 4096, use the following syntax:

```
CLI network-admin@switch > mst-config-show instance-id 10 vlans 13-16
```

N Commands

node-info

This command displays information about the local node switch in the fabric.

Syntax `node-info`

Defaults None.

Access CLI

History Command introduced in Version 1.2.

Usage To show information about a local switch node in the fabric, use this command.

Examples Use the following command to display node information:

```
CLI network-admin@switch > node-info
```

```
CLI (network-admin@pubdev03) > node-info
name:              pubdev03
fab-name:          TAC
mgmt-ip:           10.9.100.50/16
mgmt-vnet:
in-band-ip:        192.168.42.30/24
in-band-vnet:
in-band-vlan-type: public
```

```
fab-tid:           66
cluster-tid:       8
out-port:          0
version:           2.4.204019818,pn-nvOS-2.4.1-2040112371
state:             online
firmware-upgrade:  not-required
device-state:      ok
```

node-show

This command displays information about all nodes in the fabric. This command can only be invoked at the network-administrator access level.

Syntax `node-show`

`name` *`fabric-node-name`*	Specifies the name of the fabric node to display information.
`id` *`id-string`*	Specifies the identifier for the fabric node
`serial` *`serial-string`*	Specifies the serial string for the fabric node
`fab-name` *`fab-name`*	Specifies the name of the fabric node
`fab-id`	Specifies the fabric identifier
`cluster-id`	Specifies the cluster identifier.
`local-mac` *`mac-address`*	Specifies the local MAC address of the fabric
`fabric-network in-band|mgmt|vmgmt`	Specifies the interface for sending fabric packets.
`mgmt-vnet` *`vnet-name`*	Specifies the management VNET.
`mgmt-public-vlan` *`vlan-id`*	Specifies the management public VLAN ID.
`mgmt-ip` *`ip-address`*	Specifies the IP address for the management NIC
`mgmt-netmask` *`netmask`*]	The netmask for the IP address
`mgmt-mac` *`mac-address`*	Specifies the MAC address for the management interface.
`vmgmt-ip ip-address`	Specifies the IP address of the virtual management interface.
`vmgmt-netmask netmask`	Specifies the netmask of the virtual management interface.
`vmgmt-mac mac-address`	Specifies the MAC address of the virtual management interface.
`vmgmt-vnet vnet name`	Specifies the VNET name for the virtual management interface.
`vmgmt-vlan` *`vlan-id`*	Specifies the VLAN ID of the virtual management interface.

vmgmt-public-vlan *vlan-id*	Specifies the public VLAN for the virtual management interface.
vmgmt-secondary-macs secondary-macs-string	Specifies the secondary MAC address of the virtual management interface.
mgmt-secondary-macs secondary-mac-string	Specifies the secondary MAC address for the management interface.
in-band-ip *ip-address*	Specifies the IP address for the in-band interface to the switch control plane.
in-band-netmask *netmask*	Specifies the netmask for the in-band interface to the switch control plane.
in-band-mac *mac-address*	Specifies the MAC address for the in-band interface to the switch control plane.
in-band-vnet *vnet-name*	Specifies the in-band VNET.
in-band-vlan *vlan-id*	Specifies the VLAN identifier for the in-band interface to the switch control plane can be reached on Layer 2.
in-band-vlan-type public|private	Specifies the in-band VLAN type as public or private.
in-band-public-vlan vlan-id	Specifies the public VLAN ID.
in-band-secondary-macs secondary-mac-string	Specifies the secondary MAC address for the in-band interface.
fab-tid *fab-tid-number*	Specifies the fabric identifier.
cluster-tid *cluster-tid-number*]	Specifies the cluster identifier.
out-port *out-port-number*	Specifies the port number where the switch multicasts the fabric discovery messages to other Pluribus Networks switch.
version *version-string*	Specifies the current OS version.
state offline|online|in-band-only-online|mgmt-only-online|fabric_joined|setup-required| fabric-required| fresh-install]	Specifies the state of the fabric.
firmware_upgrade not-required|required| reboot-required	Specifies if a firmware upgrade is required.
device_state ok|error|simulator	Specifies the state of the switch.
ports *ports-number*	Specifies the port list used by the fabric.
keepalive-timeout high resolution time: #n	Specifies the keepalive timeout.

Defaults None.

Access network-admin

History .

Version 1.2	Command introduced.
Version 2.3	The parameter, `fab-mcast`, deprecated.
Version 2.4.1	The parameters, `mgmt-vnet`, `mgmt-public-vlan`, `in-band-vnet`, `in-band-vlan-type`, and `in-band-public-vlan` added. The options, `in-band-only-online` and `mgmt-only-online`, added to the parameter, `state`.
Version 2.6.2	The parameters, `vmgmt-*` and `keepalive`, added.

Usage To show information about all switch nodes on the network, use this command. This command is useful if you have a node that hasn't joined a fabric and you want to view all nodes on the network. This command is not available at the VNET manager access level.

Examples Use the following command to display node information:

```
CLI network-admin@switch > node-show
id:                     167772387
name:                   pubdev03
fab-name:               TAC
fab-id:                 a0000e3:57c0c0ea
cluster-id:             a000024:1
local-mac:              64:0e:94:28:03:56
fabric-network:         in-band
control-network:        in-band
mgmt-ip:                10.9.100.50/16
mgmt-mac:               64:0e:94:28:03:58
mgmt-vnet:
mgmt-public-vlan:       0
mgmt-secondary-macs:
in-band-ip:             192.168.42.30/24
in-band-mac:            64:0e:94:28:03:56
in-band-vnet:
in-band-vlan:           0
in-band-vlan-type:      public
in-band-public-vlan:    0
in-band-secondary-macs:
fab-tid:                66
cluster-tid:            8
out-port:               0
version:                2.4.204019818,pn-nvOS-2.4.1-2040112371
state:                  online
firmware-upgrade:       not-required
device-state:           ok
ports:                  72
```

nv-queue-stats-clear

This command is used to clear high priority packets such as LACP, LLDP, ARP, and STP. This is useful when you want to see how the packet queues are used and troubleshoot the operating system based on this information.

Syntax `nv-queue-stats-clear`

`name` *`nv-queue-stats-list name`*	Specify the name of the queue.

Defaults None

Access CLI

History Command introduced in Version 2.4

Usage Use this command to clear the statistics collection settings for packet queues.

Examples To clear statistics collection for packet queues, use the following syntax:

```
CLI network-admin@switch > nv-queue-stats-clear name nv-queue-stats-list name
```

nv-queue-stats-show

This command is used to display ONVL high priority packets such as LACP, LLDP, ARP, and STP. This is useful when you want to see how the packet queues are used and troubleshoot ONVL based on this information.

Syntax `nv-queue-stats-show`

`time date/time: yyyy-mm-ddThh:mm:ss`	Specify the time to start the statistic collection.
`start-time date/time: yyyy-mm-ddThh:mm:ss`	Specify the start time of to statistic collection.
`end-time date/time: yyyy-mm-ddThh:mm:ss`	Specify the end time of statistic collection.
`duration duration: #d#h#m#s`	Specify the duration of statistic collection.
`interval duration: #d#h#m#s`	Specify the interval between statistic collection.
`since-start`	Specify the statistics collected since the start time.
`older-than duration: #d#h#m#s`	Specify the statistics older than the initial time.
`within-last duration: #d#h#m#s`	Specify the statistics collected within the last time.
`name` *`nv-queue-stats-list name`*	Specify the name of the queue.
`q-high` *`q-high-number`*	Specify to display the highest count in queue.
`q-low` *`q-low-number`*	Specify to display the lowest count in queue.
`q-max` *`q-max-number`*	Specify to display the maximum queue size.
`q-in` *`q-in-number`*	Specify to display the number of items inserted into

	queue
q-out *q-out-number*	Specify to display the number of items removed from queue.
q-delay-high *high resolution time: #ns*	Specify to display the highest delay from insertion to removal from the queue.
q-delay-samples *q-delay-samples-number*	Specifies number of delay samples queue.
q-delay-avg high *resolution time: #ns*	Specifies average sampled delay from insertion to removal.
q-overflow *q-overflow-number*	Specifies if insertion failed because queue was full.
q-underflow *q-underflow-number*	Specifies that the allocation failed because queue was empty.

Defaults None

Access CLI

History

Version 2.2.5	Command introduced.
Version 2.3.1	The parameters, q-delay-avg, q-overflow, and q-underflow added.

Usage Use this command to modify the statistics collection settings for packet queues.

Examples To disable statistics collection for ONVL packet queues, use the following syntax:

```
CLI network-admin@switch > nv-queue-stats-show since-start format all
layout vertical
switch:       pubdev01
time:         12-07,10:08:00
name:         eventq-guaranteed-0
q-high:       1
q-low:        0
q-max:        0
q-in:         1
q-out:        1
switch:       pubdev01
time:         12-07,10:08:00
name:         eventq-guaranteed-1
q-high:       1
q-low:        0
q-max:        0
q-in:         23
q-out:        23
q-delay-high: 63.1us
switch:       pubdev01
time:         12-07,10:08:00
name:         eventq-guaranteed-cache
q-high:       512
```

```
q-low:        503
q-max:        8192
q-in:         63
q-out:        63
```

nv-queue-stats-settings-modify

This command is used to modify the parameters to collect high priority packets such as LACP, LLDP, ARP, and STP into a receiving queue on the CPU. This is useful when you want to see how the packet queues are used and troubleshoot the operating system based on this information.

Syntax `nv-queue-stats-settings-modify`

`enable|disable`	Enable or disable statistics collection.
`interval duration: #d#h#m#s`	Modify the interval to collect statistics.
`disk-space` *`disk-space-number`*	Modify the disk-space allocated for statistics.

Defaults None

Access CLI

History Command introduced in Version 2.2.5.

Usage Use this command to modify the statistics collection settings for the operating system packet queues.

Examples To disable statistics collection for nvOS packet queues, use the following syntax:

```
CLI network-admin@switch > nv-queue-stats-settings-modify  disable
```

nv-queue-stats-settings-show

This command is used to display the parameters used to collect high priority packets such as LACP, LLDP, ARP, and STP into a receiving queue on the CPU. This is useful when you want to see how the packet queues are used and troubleshoot nvOS based on this information.

Syntax `nv-queue-stats-settings-show`

Defaults None

Access CLI

History Command introduced in Version 2.2.5.

Usage Use this command to display the statistics collection settings for nvOS packet queues.

Examples To display statistics collection for nvOS packet queues, use the following syntax:

```
CLI network-admin@switch > nv-queue-stats-settings-show
switch:     pubdev01
enable:     yes
interval:   1m
```

```
disk-space: 50M
```

O Commands

object-location-modify

The command displays any objects with a location field, and the current locations. The modify commands allows you to batch move objects from one location to another.

Syntax `object-location-modify`

`location fabric-node` *`name`*	Specify the current location of the object.
`new-location node` *`name`*	Specify the new location of the object.

Defaults None

Access CLI

History

Version 2.5.0	Command introduced.
Version 2.6.2	The parameters, `type` and `name`, deprecated.

Usage Use this command to migrate objects to new locations in the fabric.

Examples To modify a location use the following syntax:

```
CLI network-admin@switch > object-location-modify location Spine16 new-
location Leaf1
```

object-location-show

The command displays any objects with a location field, and the current locations. The modify commands allows you to batch move objects from one location to another.

Syntax `object-location-show`

`location fabric-node` *`name`*	Specify the current location of the object.
`type` *`type-string`*	Specify the type of object.
`name` *`name-string`*	Specify the name of the object.

Defaults None

Access CLI

History Command introduced in Version 2.5.

Usage Use this command to migrate objects to new locations in the fabric.

Examples To display an object location use the following syntax:

```
CLI network-admin@switch > object-location-show
type         name         location
------------ ------------ --------
openstack    opens        Spine16
dhcp         pxedhcp      Leaf2
vrouter      vr2          Leaf1
vrouter      vr1          aquila16
vnet-manager pxevnet-mgr  Leaf2
nat          global-nat   Spine16
vrouter-hw-if eth0.12     Spine16
```

openstack-config-create (deprecated)

Informational Note: The Netvisor feature, Openstack, is deprecated for Version 5.1.0.

openvswitch-create

Open vSwitch is a multilayer virtual switch licensed by Apache 2.0. It is designed to enable massive network automation through programmable extensions. This command creates an Open vSwitch instance on the switch.

Syntax `openvswitch-create name`

`name` *`name-string`*	Specify a name for the Open vSwitch instance.
`vnet` *`vnet-name`*	Specify the name of the VNET for Open vSwitch.
Specify any of the following options:	
`dedicated-vnet-service|shared-vnet-service`	Specify if Open vSwitch is a dedicated or shared VNET service.
`shared-vnet-mgr` *`vnet-manager name`*	Specify the VNET manager to share with if this is a shared service.
`location fabric-node name`	Specify the location of the service.
`storage-pool` *`storage-pool-name`*	Specify a storage pool to apply to the VNET.
`cert-name` *`cert-name-string`*	Specify the certificate name for SSL connections

ca-cert-name *ca-cert-name-string*	Specify the CA Certificate name for SSL connections
cert-location none|global| container	Specify the Certificate location - global or within container.
global-vtep|local-vtep	Specify the hardware VTEP associated with Open vSwitch.
tunnel-ip *ip-address*	Specify the IP address for the tunnel.
bfd|no-bfd	Specify if you want to enable BFD for OVSDB created tunnels.

Defaults None

Access CLI

History

Version 2.4	Command introduced.
Version 2.4.1	The parameters, `tunnel` and `vtep`, added.
Version 2.5	The parameters, `gateway`, `db-conn-type`, `db-port`, `db-socket`, and `db-ip` are deprecated.
Version 2.5.4	The parameter, `shared-vnet-mgr`, `cert-name`, `ca-cert-name`, and `cert-location` added.
Version 2.6.2	The parameter, `gateway`, deprecated.
Version 3.0.0	The parameter, `bfd`, added.

Usage Use this command to create an Open vSwitch instance on a VNET.

Examples To create an OpenStack instance, **Open-One**, on VNET, **opvnet**, as a dedicated service, with storage pool, **vry-lrg-str**, use the following command:

```
CLI network-admin@switch > openvswitch-create name Open-One vnet opvnet
dedicated-vnet-service storage-pool vry-lrg-str
```

openvswitch-delete

Open vSwitch is a multilayer virtual switch licensed by Apache 2.0. It is designed to enable massive network automation through programmable extensions. This command removes an Open vSwitch instance on the switch.

Syntax `openvswitch-delete name name-string`

name *name-string*	Specify a name for the Open vSwitch instance.

Defaults None

Access CLI

History Command introduced in Version 2.4.

Usage Use this command to delete an Open vSwitch instance on a VNET.

Examples To delete an Open vSwitch instance, **Open-One**, on VNET, **opvnet**, use the following command:

```
CLI network-admin@switch > openvswitch-delete name Open-One vnet opvnet
db-ip 10.9.31.141
```

openvswitch-modify

Open vSwitch is a multilayer virtual switch licensed by Apache 2.0. It is designed to enable massive network automation through programmable extensions. This command modifies an Open vSwitch instance on the switch.

Syntax `openvswitch-modify`

`name` *`name-string`*	Specify a name for the Open vSwitch instance.
Specify between 0 and 7 of the following options:	
`gateway` *`ip-address`*	Specify the gateway IP address.
`tunnel-ip` *`ip-address`*	Specify the IP address for the tunnel.
`global-vtep|local-vtep`	Specify the hardware VTEP associated with Open vSwitch.
`cert-name` *`cert-name-string`*	Specify the certificate name for SSL connections
`ca-cert-name` *`ca-cert-name-string`*	Specify the CA Certificate name for SSL connections
`cert-location none|global|container`	Specify the Certificate location - global or within container
`location` *`fabric-node name`*	Specify the location of the service.
`storage-pool` *`storage-pool-name`*	Specify a storage pool to apply to the VNET.
`bfd|no-bfd`	Specify if you want to enable BFD for OVSDB created tunnels.

Defaults None

Access CLI

History

Version 2.4	Command introduced.
Version 2.4.1	The parameters `vnet, dedicated-vnet-service|shared-vnet-service disable|enable, storage-pool, gateway db-conn-type, db-ip, db-port, db-socket` deprecated.
Version 2.5.4	The parameters, `cert-name, ca-cert-name,and cert-location` added.
Version 3.0.0	The parameter, `bfd`, added.

Usage Use this command to modify an Open vSwitch instance on a VNET and to accept TLS certificates.

Examples To modify an Open vSwitch instance, **Open-One**, on VNET, **opvnet**, and add the database IP address, 10.9.31.141, use the following command:

```
CLI network-admin@switch > openvswitch-modify name Open-One vnet opvnet
db-ip 10.9.31.141
```

openvswitch-show

Open vSwitch is a multilayer virtual switch licensed by Apache 2.0. It is designed to enable massive network automation through programmable extensions. This command displays an Open vSwitch instance on the switch.

Syntax `openvswitch-show`

`name` *`name-string`*	Specify a name for the Open vSwitch instance.
Specify any of the following options:	
`type vnet-mgr|vrouter|vlb|dhcp|dns|netzone|ofpd|orphaned|netvm|nat| openstack|netvmm|ovs`	Specify the type of VNET.
`scope local|fabric`	Specify the scope for Open vSwitch.
`vnet` *`vnet-name`*	Specify the name of the VNET for Open vSwitch.
`is-global true|false`	Specify if service is global.
`location fabric-node` *`name`*	Specify the location of the Open vSwitch instance.
`cert-name` *`cert-name-string`*	Specify the certificate name for SSL connections.
`ca-cert-name` *`ca-cert-name-string`*	Specify the CA Certificate name for SSL connections.
`cert-location none|global|container`	Specify the Certificate location - global or within container.
`db-conn-type unix-socket|tcp|punix-socket-listen|tcp-`	Specify the type of database connection.

`listen|ssl|default`	
`db-ip` *`ip-address`*	Specify the IP address of the database.
`db-port` *`db-port-number`*	Specify the port number to listen on for the database.
`db-socket` *`db-socket-string`*	Specify the socket for the database.
`mode standalone|master|slave`	
`tunnel-ip` *`ip-address`*	Specify the IP address for the tunnel.
`global-vtep|local-vtep`	Specify the hardware VTEP associated with Open vSwitch.
`bfd|no-bfd`	Specify if you want to enable BFD for OVSDB created tunnels.

Defaults None

Access CLI

History .

Version 2.4	Command introduced.
Version 2.4.1	The parameters, `tunnel` and `vtep`, added.
Version 2.5.4	The parameter, `shared-vnet-mgr`, `cert-name`, `ca-cert-name`, and `cert-location` added.
Version 2.6.2	The parameter, `mode`, added.
Version 3.0.0	The parameter, `bfd`, added.

Usage Use this command to display Open vSwitch instance information on a VNET.

Examples To display an Open vSwitch instance, **Open-One**, use the following command:

```
CLI network-admin@switch > openvswitch-show name Open-One
```

openvswitch-hwvtep-manager-add

Open vSwitch is a multilayer virtual switch licensed by Apache 2.0. It is designed to enable massive network automation through programmable extensions. This command adds an Open vSwitch interface to the switch.

Syntax `openvswitch-hwvtep-manager-add`

`name` *`name-string`*	This parameter is not configurable. It defaults to the name that you used to create the Open vSwitch service.
Specify one or both of the following options:	

`manager-type odl|nsx`	Specify the type of HWVTEP manager.
`connection-method unix-socket| tcp|unix-socket-listen|tcp-listen|ssl|default`	Specify the connection method for the HWVTEP manager interface.
`ip` *`ip-address`*	Specify the IP address of the database.
`username` *`username-string`*	Specify the username.
`password` *`password-string`*	Specify the password.
`port` *`port-number`*	Specify the port number of the database.
`auto-service-binding| no-auto-service-binding`	Specify if you want a VTEP automatically or manually added as a hardware device to NSX.

Defaults None

Access CLI

History .

Version 2.4.0	Command introduced.
Version 2.6.0	The parameters, `manager-type`, `username`, and `password`, added.
Version 3.0.0	The parameter, `auto-service-binding| no-auto-service-binding`, added.

Usage Use this command to add an HWVTEP manager interface.

Examples To add an HWVTEP manager interface, **hwvtep-1**, use the following command:

```
CLI network-admin@switch > openvswitch-hwvtep-manager-add name hwvtep-1
```

openvswitch-hwvtep-manager-remove

Open vSwitch is a multilayer virtual switch licensed by Apache 2.0. It is designed to enable massive network automation through programmable extensions. This command removes a HWVTEP manager interface to the switch.

Syntax `openvswitch-hwvtep-manager-remove name name-string [ip ip-address]`

`name` *`name-string`*	This parameter is not configurable. It defaults to the name that you used to create the Open vSwitch service.

ip *ip-address*	Specify the IP address of the database.

Defaults None

Access CLI

History Command introduced in Version 2.4.

Usage Use this command to remove an HWVTEP manager interface.

Examples To remove an Open vSwitch controller, **hwvtep-1**, use the following command:

```
CLI network-admin@switch > openvswitch-hwvtep-manager-remove name
hwvtep-1
```

openvswitch-hwvtep-manager-show

Open vSwitch is a multilayer virtual switch licensed by Apache 2.0. It is designed to enable massive network automation through programmable extensions. This command displays information about a HWVTEP interface to the switch.

Syntax openvswitch-hwvtep-manager-show

name *name-string*	This parameter is not configurable. It defaults to the name that you used to create the Open vSwitch service.
Specify one or both of the following options:	
manager-type odl|nsx	Displays the type of HWVTEP manager.
ip *ip-address*	Displays the IP address of the database.
controller-ip *ip-address*	Displays the IP address of the controller.
connection-method unix-socket|tcp|unix-socket-listen|tcp-listen| ssl|default	Displays the connection method for the HWVTEP manager interface.
username *username-string*	Displays the username.
password *password-string*	Specify the password.
port *port-number*	Displays the port number of the database.
status *status*	Displays the controller status.

`auto-service-binding| no-auto-service-binding`	Displays if a VTEP is automatically or manually added as a hardware device to NSX.

Defaults None

Access CLI

History .

Version 2.4.0	Command introduced.
Version 2.6.0	The parameters, `manager-type`, `username`, and `controller-ip`, added.
Version 3.0.0	The parameter, `auto-service-binding| no-auto-service-binding`, added.

Usage Use this command to display an Open vSwitch interface.

Examples To display a HWVTEP manager, **hwvtep-1**, use the following command:

```
CLI network-admin@switch > openvswitch-hwvtep-manager-show name hwvtep-1
```

openvswitch-interface-add

Open vSwitch is a multilayer virtual switch licensed by Apache 2.0. It is designed to enable massive network automation through programmable extensions. This command adds an Open vSwitch interface to the switch.

Syntax `openvswitch-interface-add`

`name` *`name-string`*	This parameter is not configurable. It defaults to the name that you used to create the Open vSwitch service.
Specify one or both of the following options:	
`ipaddr` *`ip-address`*	Specify the IP address for the interface.
`netmask netmask`	Specify the netmask.
`assignment none|static|dhcp| dhcpv6|autov6`	Specify the method of IP address assignment.
`scope local|fabric`	Specify the VLAN assigned to the interface.
`vlan` *`vlan-id`*	Optionally, specify the VXLAN assigned to

	the interface.
`vlan-type public|private`	Specify the type of VLAN for the interface.
`if mgmt|data|span`	Specify an alias if desired.
`alias-on alias-on-string`	Specify if the interface is exclusive or not.
`exclusive|no-exclusive`	Specify if the NIC is enabled or disabled.
`nic-enable|nic-disable`	Specify the ID assigned by VRRP.
`vrrp-id` *`id`*	Specify the primary interface for VRRP.
`vrrp-primary vrrp-primary-string`	Specify the VRRP priority for the interface.
`vrrp-adv-int` *`milliseconds`*	Specify the VRRP advertisement interval in milliseconds. The range is 10 to 40950 with a default value of 1000.
`secondary-macs secondary-macs-string`	Specify a secondary MAC address for the interface.
`if-nat-realm internal|external`	Specify the NAT interface realm.
`priority-tag| no-priority-tag`	Specify the VLAN 0 priority tag on forwarded traffic.

Defaults None

Access CLI

History .

Version 2.4	Command introduced.
Version 2.4.1	The parameter, `vxlan`, deprecated. The parameter, `vlan-type`, added.
Version 2.6.2	The parameter, `if-nat-realm`, added.
Version 3.1.0	The parameter, `priority-tag|no-priority-tag`, added.

Usage Use this command to add an Open vSwitch interface.

Examples To add an Open vSwitch controller, **openvswitch-1**, use the following command:

```
CLI network-admin@switch > openvswitch-controller-add name openvswitch-
1
```

openvswitch-interface-modify

Open vSwitch is a multilayer virtual switch licensed by Apache 2.0. It is designed to enable massive network automation through programmable extensions. This command modifies an Open vSwitch interface to the switch.

Syntax `openvswitch-interface-modify`

`name` *`name-string`*	This parameter is not configurable. It defaults to the name that you used to create the Open vSwitch service.
Specify one or both of the following options:	
`ipaddr` *`ip-address`*	Specify the IP address for the interface.
`netmask netmask`	Specify the netmask.
`assignment none|static|dhcp| dhcpv6|autov6`	Specify the method of IP address assignment.
`scope local|fabric`	Specify the VLAN assigned to the interface.
`vlan` *`vlan-id`*	Optionally, specify the VXLAN assigned to the interface.
`vlan-type public|private`	Specify the type of VLAN for the interface.
`if mgmt|data|span`	Specify an alias if desired.
`alias-on alias-on-string`	Specify if the interface is exclusive or not.
`exclusive|no-exclusive`	Specify if the NIC is enabled or disabled.
`nic-enable|nic-disable`	Specify the ID assigned by VRRP.
`vrrp-id` *`id`*	Specify the primary interface for VRRP.
`vrrp-primary vrrp-primary-string`	Specify the VRRP priority for the interface.
`vrrp-adv-int` *`milliseconds`*	Specify the VRRP advertisement interval in milliseconds. The range is 10 to 40950 with a default value of 1000.
`secondary-macs secondary-macs-string`	Specify a secondary MAC address for the interface.
`if-nat-realm internal|external`	Specify the NAT interface realm.
`priority-tag| no-priority-tag`	Specify the VLAN 0 priority tag on forwarded traffic.

Defaults None

Access CLI

History .

Version 2.4	Command introduced.
Version 2.4.1	The parameter, `vxlan`, deprecated. The parameter, `vlan-type`, added.
Version 2.6.2	The parameter, `if-nat-realm`, added.
Version 3.1.0	The parameter, `priority-tag|no-priority-tag`, added.

Usage Use this command to modify an Open vSwitch interface.

Examples To modify an Open vSwitch interface and enable the NIC, **openvswitch-1**, use the following command:

```
CLI network-admin@switch > openvswitch-controller-modify name
openvswitch-1 nic-enable
```

openvswitch-interface-remove

Open vSwitch is a multilayer virtual switch licensed by Apache 2.0. It is designed to enable massive network automation through programmable extensions. This command removes an Open vSwitch interface to the switch.

Syntax `openvswitch-interface-remove ovs-name name-string nic nic-string`

name *name-string*	This parameter is not configurable. It defaults to the name that you used to create the Open vSwitch service.
Specifythe following interface option:	
nic *nic-string*	Specify the NIC to remove from the interface.

Defaults None

Access CLI

History Command introduced in Version 2.4.

Usage Use this command to remove an Open vSwitch interface.

Examples To add an Open vSwitch controller, **openvswitch-1**, use the following command:

```
CLI network-admin@switch > openvswitch-controller-remove name
openvswitch-1
```

openvswitch-interface-show

Open vSwitch is a multilayer virtual switch licensed by Apache 2.0. It is designed to enable massive network automation through programmable extensions. This command displays information about an Open vSwitch interface to the switch.

Syntax openvswitch-interface-show

name *name-string*	This parameter is not configurable. It defaults to the name that you used to create the Open vSwitch service.
Specify one or more of the following options:	
ipaddr *ip-address*	Specifies the IP address for the interface.
netmask netmask	Specifies the netmask.
assignment none|static|dhcp| dhcpv6|autov6	Specifies the method of IP address assignment.
scope local|fabric	Specifies the VLAN assigned to the interface.
vlan *vlan-id*	Specifies the VXLAN assigned to the interface.
vlan-type public|private	Specifies the type of VLAN for the interface.
public-vlan *vlan-id*	Specifies the public VLAN ID.
if mgmt|data|span	Specifies an alias if desired.
alias-on alias-on-string	Specifies if the interface is exclusive or not.
exclusive|no-exclusive	Specifies if the NIC is enabled or disabled.
nic-enable|nic-disable	Specifies the ID assigned by VRRP.
vrrp-id *id*	Specifies the primary interface for VRRP.
vrrp-primary vrrp-primary-string	Specifies the VRRP priority for the interface.
vrrp-adv-int *milliseconds*	Specifies the VRRP advertisement interval in milliseconds. The range is 10 to 40950 with a default value of 1000.
secondary-macs secondary-macs-string	Specifies a secondary MAC address for the interface.
if-nat-realm internal|external	Specify the NAT interface realm.
priority-tag| no-priority-tag	Specify the VLAN 0 priority tag on forwarded traffic.

Defaults None

Access CLI

History .

Version 2.4	Command introduced.
Version 2.4.1	The parameter, `vxlan`, deprecated. The parameter, `vlan-type`, added.
Version 2.6.2	The parameter, `if-nat-realm`, added.
Version 3.1.0	The parameter, `priority-tag|no-priority-tag`, added.

Usage Use this command to display interface information about an Open vSwitch interface.

Examples To display information about an Open vSwitch interface, **openvswitch-1**, use the following command:

```
CLI network-admin@switch > openvswitch-controller-show  name
openvswitch-1
```

openvswitch-interface-modify

Open vSwitch is a multilayer virtual switch licensed by Apache 2.0. It is designed to enable massive network automation through programmable extensions. This command modifies an Open vSwitch interface to the switch.

Syntax `openvswitch-interface-modify`

`name` *`name-string`*	This parameter is not configurable. It defaults to the name that you used to create the Open vSwitch service.
Specify one or more of the following options:	
`ipaddr` *`ip-address`*	Specify the IP address for the interface.
`netmask netmask`	Specify the netmask.
`assignment none|static|dhcp|dhcpv6|autov6`	Specify the method of IP address assignment.
`scope local|fabric`	Specify the VLAN assigned to the interface.
`vlan` *`vlan-id`*	Optionally, specify the VXLAN assigned to the interface.
`vlan-type public|private`	Specify the type of VLAN for the interface.

`if mgmt|data|span`	Specify an alias if desired.
`alias-on alias-on-string`	Specify if the interface is exclusive or not.
`exclusive|no-exclusive`	Specify if the NIC is enabled or disabled.
`nic-enable|nic-disable`	Specify the ID assigned by VRRP.
`vrrp-id` *`id`*	Specify the primary interface for VRRP.
`vrrp-primary vrrp-primary-string`	Specify the VRRP priority for the interface.
`vrrp-adv-int` *`milliseconds`*	Specify the VRRP advertisement interval in milliseconds. The range is 10 to 40950 with a default value of 1000.
`secondary-macs secondary-macs-string`	Specify a secondary MAC address for the interface.
`if-nat-realm internal|external`	Specify the NAT interface realm.
`priority-tag| no-priority-tag`	Specify the VLAN 0 priority tag on forwarded traffic.

Defaults None

Access CLI

History

Version 2.4	Command introduced.
Version 2.4.1	The parameter, `vxlan`, deprecated. The parameter, `vlan-type`, added.
Version 2.6.2	The parameter, `if-nat-realm`, added.
Version 3.1.0	The parameter, `priority-tag|no-priority-tag`, added.

Usage Use this command to modify an Open vSwitch interface.

Examples To modify an Open vSwitch interface and enable the NIC, **openvswitch-1**, use the following command:

```
CLI network-admin@switch > openvswitch-controller-modify  name
openvswitch-1  nic-enable
```

openvswitch-interface-remove

Open vSwitch is a multilayer virtual switch licensed by Apache 2.0. It is designed to enable massive network automation through programmable extensions. This command removes an Open vSwitch interface to the switch.

Syntax `openvswitch-interface-remove ovs-name name-string nic nic-string`

name *name-string*	This parameter is not configurable. It defaults to the name that you used to create the Open vSwitch service.
Specifythe following interface option:	
nic *nic-string*	Specify the NIC to remove from the interface.

Defaults None

Access CLI

History Command introduced in Version 2.4.

Usage Use this command to remove an Open vSwitch interface.

Examples To add an Open vSwitch controller, **openvswitch-1**, use the following command:

```
CLI network-admin@switch > openvswitch-controller-remove name
openvswitch-1
```

openvswitch-interface-show

Open vSwitch is a multilayer virtual switch licensed by Apache 2.0. It is designed to enable massive network automation through programmable extensions. This command displays information about an Open vSwitch interface to the switch.

Syntax `openvswitch-interface-show`

name *name-string*	This parameter is not configurable. It defaults to the name that you used to create the Open vSwitch service.
Specify one or more of the following options:	
ipaddr *ip-address*	Specifies the IP address for the interface.
netmask netmask	Specifies the netmask.
assignment none|static|dhcp| dhcpv6|autov6	Specifies the method of IP address assignment.
scope local|fabric	Specifies the VLAN assigned to the interface.
vlan *vlan-id*	Specifies the VXLAN assigned to the interface.
vlan-type public|private	Specifies the type of VLAN for the interface.
public-vlan *vlan-id*	Specifies the public VLAN ID.
if mgmt|data|span	Specifies an alias if desired.

`alias-on alias-on-string`	Specifies if the interface is exclusive or not.
`exclusive|no-exclusive`	Specifies if the NIC is enabled or disabled.
`nic-enable|nic-disable`	Specifies the ID assigned by VRRP.
`vrrp-id` *`id`*	Specifies the primary interface for VRRP.
`vrrp-primary vrrp-primary-string`	Specifies the VRRP priority for the interface.
`vrrp-adv-int` *`milliseconds`*	Specifies the VRRP advertisement interval in milliseconds. The range is 10 to 40950 with a default value of 1000.
`secondary-macs secondary-macs-string`	Specifies a secondary MAC address for the interface.
`if-nat-realm internal|external`	Specify the NAT interface realm.
`priority-tag| no-priority-tag`	Specify the VLAN 0 priority tag on forwarded traffic.

Defaults None

Access CLI

History .

Version 2.4	Command introduced.
Version 2.4.1	The parameter, `vxlan`, deprecated. The parameter, `vlan-type`, added.
Version 2.6.2	The parameter, `if-nat-realm`, added.
Version 3.1.0	The parameter, `priority-tag|no-priority-tag`, added.

Usage Use this command to display interface information about an Open vSwitch interface.

Examples To display information about an Open vSwitch interface, **openvswitch-1**, use the following command:

```
CLI network-admin@switch > openvswitch-controller-show  name
openvswitch-1
```

Acknowledgments for Open Source Software

The Pluribus Networks Command Line Interface (CLI) used the following Open Source Software:

bean.js

(bean.js):

bean.js - copyright Jacob Thornton 2011

https://github.com/fat/bean

MIT License

special thanks to:

dean edwards: http://dean.edwards.name/

dperini: https://github.com/dperini/nwevents

the entire mootools team: github.com/mootools/mootools-core

Bonzo: DOM Utility (c) Dustin Diaz 2011

https://github.com/ded/bonzo

License MIT

d3v2

(d3v2):

Copyright (c) 2012, Michael Bostock

All rights reserved.

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name Michael Bostock may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL MICHAEL BOSTOCK BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

d3v2

(d3v2):

TERMS OF USE - EASING EQUATIONS

Open source under the BSD License.

Copyright 2001 Robert Penner

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation * and/or other materials provided with the distribution.

Neither the name of the author nor the names of contributors may be used to endorse or promote products derived from this software without specific * prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"* AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

DataTables

(DataTables):

@summary DataTables

@description Paginate, search and sort HTML tables

@version 1.9.4

@file jquery.dataTables.js

@author Allan Jardine (www.sprymedia.co.uk)

@contact www.sprymedia.co.uk/contact

@copyright Copyright 2008-2012 Allan Jardine, all rights reserved.

This source file is free software, under either the GPL v2 license or a BSD style license, available at: http://datatables.net/license_gpl2

http://datatables.net/license_bsd

This source file is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the license files for details.

For details please refer to: http://www.datatables.net

(Envision)

Envision.js

(c) 2012 Carl Sutherland, Humble Software

Distributed under the MIT License

Source: http://www.github.com/HumbleSoftware/envisionjs

Homepage: http://www.humblesoftware.com/envision

excanvas

(excanvas.js):

Filament Group modification note:

This version of excanvas is modified to support lazy loading of this file. More info here: http://pipwerks.com/2009/03/12/lazy-loading-excanvasjs/

Copyright 2006 Google Inc.

Licensed under the Apache License, Version 2.0 (the "License");

you may not use this file except in compliance with the License.

You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

FloodLight

Copyright 2012, Big Switch Networks, Inc.

Originally created by David Erickson, Stanford University

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License

Flotr2

Flotr2 (c) 2012 Carl Sutherland

MIT License

Special thanks to:

Flotr: http://code.google.com/p/flotr/ (fork)

Flot: https://github.com/flot/flot (original fork)

g.Raphael

g.Raphael 0.5 - Charting library, based on RaphaÃ«l

Copyright (c) 2009 Dmitry Baranovskiy (http://g.raphaeljs.com)

Licensed under the MIT (http://www.opensource.org/licenses/mit-license.php) license.

GRUB

GRUB -- GRand Unified Bootloader

Copyright (C) 1999,2000,2001,2002,2004 Free Software Foundation, Inc.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or

(at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the

implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the

GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

GSON

Copyright (C) 2008 Google Inc.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

DNS/DHCP

Copyright (c) 2004-2013 by Internet Systems Consortium, Inc. ("ISC")

Copyright (c) 1995-2003 by Internet Software Consortium

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Internet Systems Consortium, Inc.

950 Charter Street

Redwood City, CA 94063

<info@isc.org>

https://www.isc.org

JIT

Copyright (c) 2011 Sencha Inc. - Author: Nicolas Garcia Belmonte (http://philogb.github.com/)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

jquery.js

jQuery JavaScript Library v1.4.3

http://jquery.com/

Copyright 2010, John Resig

Dual licensed under the MIT or GPL Version 2 licenses.

http://jquery.org/license

Includes Sizzle.js

http://sizzlejs.com/

Copyright 2010, The Dojo Foundation

Released under the MIT, BSD, and GPL Licenses.

Date: Thu Oct 14 23:10:06 2010 -0400

jQuery UI

Copyright (c) 2011 Paul Bakaus, http://jqueryui.com/

This software consists of voluntary contributions made by many individuals (AUTHORS.txt, http://jqueryui.com/about) For exact contribution history, see the revision history and logs, available at http://jquery-ui.googlecode.com/svn/

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

jquery.cookie.js

jQuery Cookie plugin

Copyright (c) 2010 Klaus Hartl (stilbuero.de)

Dual licensed under the MIT and GPL licenses:

http://www.opensource.org/licenses/mit-license.php

http://www.gnu.org/licenses/gpl.html

jquery.hotkeys.js

jQuery Hotkeys Plugin

Copyright 2010, John Resig

Dual licensed under the MIT or GPL Version 2 licenses.

Based upon the plugin by Tzury Bar Yochay:

http://github.com/tzuryby/hotkeys

Original idea by:

Binny V A, http://www.openjs.com/scripts/events/keyboard_shortcuts/

jquery.validate.min.js

Query Validation Plugin 1.8.1

http://bassistance.de/jquery-plugins/jquery-plugin-validation/

http://docs.jquery.com/Plugins/Validation

Copyright (c) 2006 - 2011 JÃ¶rn Zaefferer

Dual licensed under the MIT and GPL licenses:

http://www.opensource.org/licenses/mit-license.php

http://www.gnu.org/licenses/gpl.html

JSTL

DO NOT ALTER OR REMOVE COPYRIGHT NOTICES OR THIS HEADER.

Copyright (c) 1997-2010 Oracle and/or its affiliates. All rights reserved.

The contents of this file are subject to the terms of either the GNU General Public License Version 2 only ("GPL") or the Common Development and Distribution License("CDDL") (collectively, the "License"). You

may not use this file except in compliance with the License. You can obtain a copy of the License at

https://glassfish.dev.java.net/public/CDDL+GPL_1_1.html or packager/legal/LICENSE.txt. See the License for the specific language governing permissions and limitations under the License.

When distributing the software, include this License Header Notice in each file and include the License file at packager/legal/LICENSE.txt.

GPL Classpath Exception:

Oracle designates this particular file as subject to the "Classpath" exception as provided by Oracle in the GPL Version 2 section of the License file that accompanied this code.

Modifications:

If applicable, add the following below the License Header, with the fields enclosed by brackets [] replaced by your own identifying information:

"Portions Copyright [year] [name of copyright owner]"

Contributor(s):

If you wish your version of this file to be governed by only the CDDL or only the GPL Version 2, indicate your decision by adding "[Contributor] elects to include this software in this distribution under the [CDDL or GPL Version 2] license." If you don't indicate a single choice of license, a recipient has the option to distribute your version of this file under either the CDDL, the GPL Version 2 or to extend the choice of license to its licensees as provided above. However, if you add GPL Version 2 code and therefore, elected the GPL Version 2 license, then the option applies only if the new code is made subject to such option by the copyright holder.

This file incorporates work covered by the following copyright and permission notice:

Copyright 2004 The Apache Software Foundation

Licensed under the Apache License, Version 2.0 (the "License");

you may not use this file except in compliance with the License.

You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

jstree

jsTree 1.0-rc3

http://jstree.com/

Copyright (c) 2010 Ivan Bozhanov (vakata.com)

Licensed same as jquery - under the terms of either the MIT License or the GPL Version 2 License

http://www.opensource.org/licenses/mit-license.php

http://www.gnu.org/licenses/gpl.html

$Date: 2011-02-09 01:17:14 +0200 (ср, 09 февр 2011) $

$Revision: 236 $

Start Copyright text (libedit 3.0)

Copyright (c) 1992, 1993

The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Christos Zoulas of Cornell University.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

(log4j

Licensed to the Apache Software Foundation (ASF) under one or more contributor license agreements. See the NOTICE file distributed with this work for additional information regarding copyright ownership.

The ASF licenses this file to You under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

(pciutils-3.1.10):

The PCI Utilities -- Declarations

Copyright (c) 1997--2008 Martin Mares <mj@ucw.cz>

Can be freely distributed and used under the terms of the GNU GPL.

qtip 2.0

qTip2 - Pretty powerful tooltips - v2.0.0 - 2012-10-03

http://craigsworks.com/projects/qtip2/

Copyright (c) 2012 Craig Michael Thompson; Licensed MIT, GPL

raphael 2.1.0

Raphaël 2.1.0 - JavaScript Vector Library

Copyright © 2008-2012 Dmitry Baranovskiy (http://raphaeljs.com)

Copyright © 2008-2012 Sencha Labs (http://sencha.com)

Licensed under the MIT (http://raphaeljs.com/license.html) license.

Copyright (c) 2013 Adobe Systems Incorporated. All rights reserved.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at //

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

Eve 0.4.2 - JavaScript Events Library

Author Dmitry Baranovskiy (http://dmitry.baranovskiy.com/)

Rickshaw v1.1.2

Adapted from https://github.com/Jakobo/PTClass */

Copyright (c) 2005-2010 Sam Stephenson

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Based on Alex Arnell's inheritance implementation.

section: Language

class Class

Manages Prototype's class-based OOP system.

Refer to Prototype's web site for a [tutorial on classes and inheritance](http://prototypejs.org/learn/class-inheritance).

science.js 1.7.0

Copyright (c) 2011, Jason Davies

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name Jason Davies may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JASON DAVIES BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

sizzle

Copyright (c) 2009, John Resig

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the <organization> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY John Resig ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL <copyright holder> BE LIABLE FOR ANY

DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

tcl 8.5.9

This software is copyrighted by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, ActiveState Corporation and other parties. The following terms apply to all files associated with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that existing copyright notices are retained in all copies and that this

notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the U.S. government, the Government shall have only "Restricted Rights" in the software and related documentation as defined in the Federal Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you are acquiring the software on behalf of the Department of Defense, the software shall be classified as "Commercial Computer Software" and the Government shall have only "Restricted Rights" as defined in Clause 252.227-7013 (b) (3) of DFARs. Notwithstanding the foregoing, the authors grant the U.S. Government and others acting in its behalf permission to use and distribute the software in accordance with the terms specified in this license.

tcllib 1.13

This software is copyrighted by Ajuba Solutions and other parties.

The following terms apply to all files associated with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses.

Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the U.S. government, the Government shall have only "Restricted Rights" in the software and related documentation as defined in the Federal Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you are acquiring the software on behalf of the Department of Defense, the software shall be classified as "Commercial Computer Software" and the Government shall have only "Restricted Rights" as defined in Clause 252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the authors grant the U.S. Government and others acting in its behalf permission to use and distribute the software in accordance with the terms specified in this license.

tclreadline 2.1.0

Copyright (c) 1998 - 2000, Johannes Zellner <johannes@zellner.org>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Johannes Zellner nor the names of contributors to this software may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

UI Widgets

The MIT License

Copyright (c) 2010 Filament Group, Inc

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell

copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Underscore.js v1.1.7

Underscore.js 1.1.7

(c) 2011 Jeremy Ashkenas, DocumentCloud Inc.

Underscore is freely distributable under the MIT license.

Portions of Underscore are inspired or borrowed from Prototype,

Oliver Steele's Functional, and John Resig's Micro-Templating.

For all details and documentation:

http://documentcloud.github.com/underscore

Underscore.js v1.1.7

Xelerated version (hxps 2.5.3 and earlier):

Copyright 2008-2012 (c) Xelerated AB.

This program may be used and/or copied only with the written permission from Xelerated AB, or in accordance

with the terms and conditions stipulated in the agreement/contract under which the program has been supplied.

All rights reserved.

Underscore.js v1.1.7

Marvell version (hxps 2.6 and above):

(c), Copyright 2008-2013, Marvell International Ltd. (Marvell)

This code contains confidential information of Marvell.

No rights are granted herein under any patent, mask work right or copyright of Marvell or any third party. Marvell reserves the right at its sole discretion to request that this code be immediately returned to Marvell.

This code is provided "as is". Marvell makes no warranties, expressed, implied or otherwise, regarding its accuracy, completeness or performance.

Oracle Solaris Open Source Projects

http://solaris.java.net/license.html

About Pluribus Networks

Pluribus Networks delivers an open, controllerless software-defined network fabric for modern data centers, multi-site data centers and distributed cloud edge environments.

The Linux-based Netvisor® ONE operating system and the Adaptive Cloud Fabric™ have been purpose-built to deliver radically simplified networking and comprehensive visibility along with white box economics by leveraging hardware from our partners Celestica, Dell EMC, and Edgecore, as well as Pluribus' own Freedom™ Series of switches.

The Adaptive Cloud Fabric provides a fully automated underlay and virtualized overlay with comprehensive visibility and brownfield interoperability and is optimized to deliver rich and highly secure per-tenant services across data center sites with simple operations having no single point of failure.

Further simplifying network operations is Pluribus UNUM™, an agile, multi-functional web management portal that provides a rich graphical user interface to manage the Adaptive Cloud Fabric. UNUM has two key modules - UNUM Fabric Manager for provisioning and management of the fabric and UNUM Insight Analytics to quickly examine billions of flows traversing the fabric to ensure quality and performance.

Pluribus is deployed in more than 275 customers worldwide, including the 4G and 5G mobile cores of more than 75 Tier 1 service providers delivering mission-critical traffic across the data center for hundreds of millions of connected devices. Pluribus is networking, simplified.

For additional information contact Pluribus Networks at info@pluribusnetworks.com, or visit www.pluribusnetworks.com.

Follow us on Twitter @pluribusnet or on LinkedIn at https://www.linkedin.com/company/pluribus-networks/.

Corporate Headquarters

Pluribus Networks, Inc.
5201 Great America Parkway, Suite 422
Santa Clara, CA 95054
1-855-438-8638 / +1-650-289-4717

India Office

Pluribus Networks India Private Limited
Indiqube Brigade Square, 4th Floor
21, Cambridge Road
Bangalore 560008

Document Version - June 2020