PVTD Command Reference

Version 1.0

www.marathon-networks.com

Table of Contents

Text Conventions

Command descriptions use these text conventions:

- Commands and commands keywords are in a **boldface**.
- Arguments for which values supplied by the user are in *italic*.
- Square brackets ([ ]) means optional elements, which are not mandatory.
- Braces ({}) group required, non-optional choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen font`.
- Information you enter is in **`boldface screen font`**.
- Nonprinting characters, such as hidden passwords or tab presses, are in angle brackets (< >).

ADD commands

Add commands are used to add configuration.

add ntp_host

Add a NTP server.

add ntp_host *ipv4_address*

Elements description

ipv4_address	A NTP server IP address

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to add a NTP server to the NTP server list.

Use *show ntp_status* to show if there are errors syncing with the new server. If there are errors, use *show log* to see what is the fault.

Adding or deleting a NTP host will restart the NTP process.

Example

Add a NTP server at 192.115.25.212 to the NTP server list:

```
   PVTD#add ntp_host 192.115.25.212
```

Show the NTP status for the NTP process:

```
   pvtd_d#show ntp_status
   NTP is enabled
   : bad peer 192.115.25.212 (192.115.25.212)
```

Show log entries related to NTP:

```
   pvtd_d#show log | match ntp
   Apr 28 08:33:15 pvtd_d pvtsh.py: PVTSH001-CMD_LOG-I: A-add ntp_host 192.115.25.212
   Apr 28 08:33:15 pvtd_d ntpd[30620]: ntp engine exiting
   Apr 28 08:33:15 pvtd_d ntpd[21250]: dispatch_imsg in main: pipe closed
   Apr 28 08:33:15 pvtd_d ntpd[20575]: Terminating
   Apr 28 08:33:15 pvtd_d ntpd[26605]: ntp engine ready
   Apr 28 08:33:15 pvtd_d ntpd[26605]: recvmsg 192.115.25.212: Connection refused
   Apr 28 08:33:22 pvtd_d pvtsh.py: PVTSH001-CMD_LOG-I: A-show ntp_status
   Apr 28 08:33:22 pvtd_d ntpd[26605]: 0 out of 2 peers valid
   Apr 28 08:33:22 pvtd_d ntpd[26605]: bad peer 192.114.71.34 (192.114.71.34)
   Apr 28 08:33:22 pvtd_d ntpd[26605]: bad peer 192.115.25.212 (192.115.25.212)
   Apr 28 08:33:32 pvtd_d pvtsh.py: PVTSH001-CMD_LOG-I: A-show log | match ntp
   Apr 28 08:33:34 pvtd_d ntpd[26605]: peer 192.114.71.34 now valid
   Apr 28 08:35:27 pvtd_d pvtsh.py: PVTSH001-CMD_LOG-I: A-show ntp_status
   Apr 28 08:35:27 pvtd_d ntpd[26605]: 1 out of 2 peers valid
   Apr 28 08:35:27 pvtd_d ntpd[26605]: bad peer 192.115.25.212 (192.115.25.212)
   Apr 28 08:36:30 pvtd_d pvtsh.py: PVTSH001-CMD_LOG-I: A-show log | match ntp
```

add pvlan

Add Primary VLAN.

add pvlan *primary_vlan*

Elements description

primary_vlan	A Primary VLAN number

Permissions

Minimal permission group is OPER

History

1.0	Command first appearance

Guide

Use this command to add a Primary VLAN to the Private VLAN table.

Primary VLAN number, as any VLAN number should be between 1 to 4095.

Adding a Primary VLAN won’t make it active. To make a Private VLAN active, it’s IPv4 address, IPv4 mask and it’s gateway IPv4 address must be set.

Example

Add Primary VLAN 99 to the Private VLAN table::

```
PVTD#add pvlan 99
```

add radius_host

Add a RADIUS server.

add radius_host *ipv4_address*

Elements description

ipv4_address	A RADIUS server IPv4 address

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to add a RADIUS server to the RADIUS servers list.

The order of RADIUS servers selection for authentication is the order of which RADIUS servers are added.

The added RADIUS server will not be used until a password for it will be set using the *set radius_password* or *set radius_obscure* commands.

Examples

Add a RADIUS with IPv4 address of 10.0.123.204:

```
PVTD#add radius_host 10.0.123.204
```

Add a RADIUS server with address of 10.0.123.205:

```
PVTD#add radius_host 10.0.123.205
```

Show RADIUS servers list:

```
pvtd_d#show conf_radius
!
! Radius Config
!
add radius_host 10.0.123.204
set radius_obscure 10.0.123.204 PASS_NOT_SET
add radius_host 10.0.123.205
set radius_obscure 10.0.123.205 PASS_NOT_SET
set radius_disable
```

To make RADIUS server at 10.0.123.205 to be the first RADIUS server to be used for authentication, first delete 10.0.123.204 from the RADIUS server list and re-add it:

```
pvtd_d#del radius_host 10.0.123.204
pvtd_d#add radius_host 10.0.123.204
pvtd_d#show conf_radius
!
! Radius Config
!
add radius_host 10.0.123.205
set radius_obscure 10.0.123.205 PASS_NOT_SET
add radius_host 10.0.123.204
set radius_obscure 10.0.123.204 PASS_NOT_SET
set radius_disable
```

add snmp_allowedv4:

Add a SNMP manager.

add snmp_allowedv4 *ipv4_address network_mask*

Elements description

ipv4_address	A network address
network_mask	A network mask

Permissions
Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to add a SNMP manager or a network of SNMP managers to the list of allowed SNMP managers.

A server in the allowed SNMP managers list of networks is allowed to query PVTD using SNMP.

No SNMP ‘write’ are allowed.

A network address can’t be 0.0.0.0 with mask 0.0.0.0. It is highly recommended not to allow any host with access to PVTD. However, if one wishes to allow all hosts to access PVTD using SNMP it is possible to add the following two networks: 0.0.0.0/128.0.0.0 and 128.0.0.0/128.0.0.0.

Examples

Add a specific SNMP manager at 10.0.123.2 to the list of allowed SNMP managers:

```
    PVTD#add snmp_allowedv4 10.0.123.2 255.255.255.255
```

Add a network of SNMP managers at 10.0.123.0/24 to the list of allowed SNMP managers:

```
    PVTD#add snmp_allowedv4 10.0.123.0 255.255.255.0
```

Allow any SNMP manager to access PVTD using SNMP:

```
    PVTD#add snmp_allowedv4 0.0.0.0 128.0.0.0
    PVTD#add snmp_allowedv4 128.0.0.0 128.0.0.0
```

add ssh_allowedv4:

Add a SSH client.

add ssh_allowedv4 *ipv4_address network_mask*

Elements description

ipv4_address	A network address
network_mask	A network mask

Permissions
Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to add a SSH client or a network of SSH clients to the list of allowed SSH clients.

A client in the allowed SSH client list of networks is allowed to SSH into PVTD.

A network address can’t be 0.0.0.0 with mask 0.0.0.0. It is highly recommended not to allow any host with access to PVTD. However, if one wishes to allow all hosts to access PVTD using SSH it is possible to add the following two networks: 0.0.0.0/128.0.0.0 and 128.0.0.0/128.0.0.0.

Examples

Add a specific SSH client at 10.0.123.2 to the list of allowed SSH clients list:

```
    PVTD#add ssh_allowedv4 10.0.123.2 255.255.255.255
```

Add a network of SSH clientsat 10.0.123.0/24 to the list of allowed SSH clients list:

```
    PVTD#add ssh_allowedv4 10.0.123.0 255.255.255.0
```

Allow any SSH client to access PVTD using SSH:

```
    PVTD#add ssh_allowedv4 0.0.0.0 128.0.0.0
    PVTD#add ssh_allowedv4 128.0.0.0 128.0.0.0
```

add svlan

Add a Secondary VLAN.

add svlan vlan *vlan_range*

Elements description

vlan_range	Secondary VLAN number, or numbers separated by commas

Permissions

Minimal permission group is OPER

History

1.0	Command first appearance

Guide

Use this command add a Secondary VLAN to the Private VLAN table.

The vlan range can be a single VLAN number or a list of VLAN numbers. Hyphen can be used to define a range of consecutive vlans.

No spaces are allowed in the VLAN range.

Adding a Secondary VLAN won't make it active. To activate a Secondary VLAN the type and association must be configured.

Example

Add Seconadry VLAN #101:

```
    PVTD#add svlan vlan 101
```

Add Secondary VLANs #102 and #104:

```
    PVTD#add svlan vlan 102,104
```

Add Secondary VLANs #105,#106 and #107:

```
    PVTD#add svlan vlan 105-107
```

Add Secondary VANs #101,#103,#105,#106 and #107

```
    PVTD#add svlan vlan 101,103,105-107
```

add syslog_host

Add a SYSLOG server.

add syslog_host *ipv4_address*

Elements description

ipv4_address	A SYSLOG server IP address

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to add a SYSLOG server to the SYSLOG server list.

Adding or deleting a SYSLOG host will restart the SYSLOG process. Which means that for few seconds new messages won't be sent to the SYSLOG servers on the least.

Example

Add SYSLOG server at 10.0.123.204 to the SYSLOG server list:

```
   PVTD#add ntp_host 10.0.123.204
```

add user

Add a user.
add user *user_name*

Elements description

user_name	A local user_name

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command add a user to the local users table.

The default permission group for a new user is VIEWER.

Example

Add pvtd_oper to the local users table

```
   PVTD#add user_pvtd_oper
```

add web_allowedv4:

Add a web client .

add web_allowedv4 *ipv4_address network_mask*

Elements description

ipv4_address	A network address
network_mask	A network mask

Permissions
Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to add a web client Ipv4 address or a network of web clients to the list of allowed web clients.

Web clients are allowed to access PVTD using HTTPS.

Add web clients to the allowed web clients list is not enough. The internal web server must be enabled using the *set web_enable* command.

Examples

Add a specific web client at 10.0.123.2 to the list of allowed web clients:

```
PVTD#add web_allowedv4 10.0.123.2 255.255.255.255
```

Add a network of web clients at 10.0.123.0/24 to the list of allowed web clients:

```
PVTD#add web_allowedv4 10.0.123.0 255.255.255.0
```

Allow any web client to access PVTD using HTTPS:

```
PVTD#add web_allowedv4 0.0.0.0 128.0.0.0
PVTD#add web_allowedv4 128.0.0.0 128.0.0.0
```

CLEAR commands

Clear commands are used to delete entries from various tables, such as the host and track tables. Clear command are also used to clear the log.

clear host_ipv4

Clears a host or hosts from IPv4 host table.

clear host_ipv4 *ipv4_pattern*

Elements description

ipv4_pattern	IP address or parts of IP address such as 10.* or 10.*.2*

Permissions

Minimal permission group is OPER

History

1.0	Command first appearance

Guide

Use this command to clear/remove hosts from IPv4 host table based on their IP address.

Cleared hosts will also be removed from IPv4 tracking table.

Example

Clear all hosts with IPv4 addresses starting with 172.19.

```
   PVTD#clear host_ipv4 172.19.*
```

clear host_mac

Clears a host or hosts from IPv4 host table.
clear host_mac *mac_pattern*

Elements description

mac_pattern	MAC address or parts of MAC address, such as 0001.34* or *.1*

Permissions

Minimal permission group is OPER

History

1.0	Command first appearance

Guide

Use this command to clear/remove hosts from IPv4 host table based on their MAC address.

Cleared hosts will also be removed from IPv4 tracking table.

Examples

Clear all VMWare hosts

```
   PVTD#clear host_mac 0050.56*
```

Clear a host with a specific MAC address

```
   PVTD#clear host_mac 0034.a24f.112d
```

clear host_vlan

Clears a host or hosts from IPv4 host table.
clear host_vlan *secondary_vlan*

Elements description

secondary_vlan	Secondary VLAN number

Permissions

Minimal permission group is OPER

History

1.0	Command first appearance

Guide

Use this command to clear/remove hosts from IPv4 host table based on their Secondary VLAN assignment.

Cleared hosts will also be removed from IPv4 tracking table.

Example

Clear all hosts in secondary VLAN number 101

```
   PVTD#clear host_vlan 101
```

clear lock_config

Clears a for stale configuration locks.
clear lock_config

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to clear/remove the config lock.

To prevent two admins from changing configuration in the same time, the first admin automatically acquires a configuration lock and automatically release the lock when his set/add/del commands are finished.

Under certain circumstances, it is possible for the admin to not automatically release the configuration lock. This command can force the configuration lock removal.

Notice: Make sure no other admin is in the middle of configuration

Example

Clear the config lock:

```
   PVTD#clear lock_config
```

clear log

Clear the log file

clear log

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to delete all the log entries. After deleting the log, the log will contain a duplicate user command logging to indicate when and by whom the log was cleared.

When the log reaches 3MB it will be automatically cleared.

Last 4 cleared logs are kept. Use *show log_old* command to view them.

COPY commands

Copy commands are used to copy files from and to disk0.

copy disk0_disk0

Copy a file from disk0 to disk0.

copy disk0_disk0 *source destination*

Elements description

source	A source file name
destination	A destination file name

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to copy a file from disk0 to disk0.

Notice: If the destination file already exists, it will be overwritten without any warning.

Example

Copy a file named myconf to old_conf

```
   PVTD#copy disk0_disk0 myconf old_conf
```

copy disk0_ftp

Copy a file from disk0 to a FTP server.

copy disk0_ftp *source FTP_server*

Elements description

source	A source file name
FTP_server	A FTP server IPv4 address

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to copy a file from disk0 to a FTP server.

Notice: If the destination file already exists, it will be overwritten without any warning.

Example

Copy a file named myconf to a FTP server 10.0.123.204

```
pvtd_d#copy disk0_ftp myconf 10.0.123.204
Username[anonymous]: ↵
Destination [myconf]:↵
#
File copied succesfully
```

copy ftp_disk0

Copy a file from a FTP server to disk0.

copy ftp_disk0 *FTP_server destination*

Elements description

FTP_server	A FTP server IPv4 address
destination	A destination file name

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to copy a file from a FTP server to disk0.

Notice: If the destination file already exists, it will be overwritten without any warning.

Example

Copy a file named myconf from FTP server at 10.0.123.204 to disk0:

```
pvtd_d#copy ftp_disk0 10.0.123.204 myconf
Username[anonymous]: ↵
Source file name [myconf]:↵
##
File copied succesfully
```

DEL commands

Del commands are used to delete configuration from PVTD.

del conf_all

Delete all configuration
del conf_all

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to delete all configuration except for the following configurations:

- Hostname and domain name
- Time Zone
- System IP address, network mask and default gateway
- ARP timeout

The Fixup MAC address will be changed to a random value starting with 404c.6fXX.XXX

del file_disk0

Delete a file from disk0
del file_disk0 *file_name*

Elements description

file_name	A filename on disk0

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command delete a file from disk0.

Notice: you will not be prompted for confirmation.

Example

Delete a file called old_config

```
   PVTD#del file_disk0 old_config
```

del ntp_host

Delete a NTP server.
del ntp_host *ipv4_address*

Elements description

ipv4_address	A NTP IPv4 address

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command delete a NTP server from the list of NTP servers used for NTP time/date synchronization.

Example

Delete 192.114.71.34 from the NTP server list:

```
   PVTD#del ntp_host 192.114.71.34
```

del pvlan

Delete a Primary VLAN.
del pvlan *primary_vlan*

Elements description

primary_vlan	Primary VLAN number

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command delete a Primary VLAN from the Private VLAN table.

Notice: The Primary VLAN should not have Secondary VLANs assigned to it.

Example

Delete Primary VLAN #10:

```
   PVTD#del pvlan 10
```

del radius_host

Delete a RADIUS server.
del radius_host *ipv4_address*

Elements description

ipv4_address	A RADIUS server IPv4 address

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command delete a RADIUS server from the list of RADIUS servers used for authentication.

When all RADIUS servers are deleted

Example

Delete 10.0.123.204 from the RADIUS server list:

```
   PVTD#del radius_host 10.0.123.204
```

del snmp_allowedv4

Delete a SNMP manager.
del snmp_allowedv4 *ipv4_address*

Elements description

ipv4_address	A SNMP manager server IP address or network address

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to delete a SNMP manager server from the list of allowed SNMP managers.

Servers in list of allowed SNMP managers are allowed to query PVTD using SNMP requests.

The *ipv4_address* can be either a specific host address or a network address. In case of a network address, there is no need to specify the network mask.

Example

Delete 10.0.123.204 from the allowed SNMP manager server list:

```
   PVTD#del snmp_allowedv4 10.0.123.204
```

del ssh_allowedv4

Delete a SSH client.
del ssh_allowedv4 *ipv4_address*

Elements description

ipv4_address	A SSH clientIP address or network address

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to delete a SSH client from the list of allowed SSH client list.

Clients in the SSH list are allowed to SSH to PVTD.

The *ipv4_address* can be either a specific host address or a network address. In case of a network address, there is no need to specify the network mask.

Example

Delete 10.0.123.204 from the allowed SSH clientlist:

```
    PVTD#del ssh_allowedv4 10.0.123.204
```

del svlan

Delete a Secondary VLAN.
del svlan vlan *vlan_range*

Elements description

vlan_range	Secondary VLAN number, or numbers separated by commas

Permissions

Minimal permission group is OPER

History

1.0	Command first appearance

Guide

Use this command delete a Secondary VLAN from the Private VLAN table.

The vlan range can be a single VLAN number or a list of VLAN numbers. Hyphen can be used to define a range of consecutive vlans.

No spaces are allowed in the VLAN range

Example

Delete Seconadry VLAN #101:
```
   PVTD#del svlan vlan 101
```
Delete Secondary VLANs #102 and #104:
```
   PVTD#del svlan vlan 102,104
```
Delete Secondary VLANs #105,#106 and #107:
```
   PVTD#del svlan vlan 105-107
```
Delete Secondary VANs #101,#103,#105,#106 and #107
```
   PVTD#del svlan vlan 101,103,105-107
```

del syslog_host

Delete a SYSLOG server.
del syslog_host *ipv4_address*

Elements description

ipv4_address	A SYSLOG IPv4 address

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command delete a SYSLOG server from the list of SYSLOG servers used as a SYSLOG destinations.

Example

Delete 192.114.71.34 from the SYSLOG server list:
```
   PVTD#del SYSLOG_host 192.114.71.34
```

del user

Delete a user.
del user *user_name*

Elements description

user_name	A local user_name

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command delete a user from the local users table.

Example

Delete pvtd_oper from the local users table

```
   PVTD#del user_pvtd_oper
```

del web_allowedv4

Delete a web client.
del web_allowedv4 *ipv4_address*

Elements description

ipv4_address	A web client IPv4 address or network address

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to delete a web client from the list of allowed web client list.

Clients in the web list are allowed to HTTPS to PVTD.

The *ipv4_address* can be either a specific host address or a network address. In case of a network address, there is no need to specify the network mask.

Example

Delete 10.0.123.204 from the allowed web client list:

```
   PVTD#del web_allowedv4 10.0.123.204
```

SET commands

Set commands are used to change configuration parameters.

set arp_timeout

Change the ARP timeout.

set arp_timeout *seconds*

Elements description

seconds	Seconds until idle host entry is removed. The range is 5 to 3600 seconds.

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change the ARP Timeout for hosts.

ARP Timeout is the time since the a host was last seen sending an ARP frame. The timeout should be little larger than the maximal ARP Timeout of all hosts and gateways/firewalls in the network.

Setting the timer too low will result in excess of ARP requests sent by PVTD, and high CPU utilization.

Setting the time too high, will result in hosts table bloating and it will take longer to detect ig a host silently changed its MAC address.

3 seconds before the ARP Timeout expires, PVTD will send an ARP request to the host.

Notice: Changing the ARP Timeout will not affect the current entries in the host table. The new ARP Timeout value will be used when an ARP frame is received from a host.

It is recommended to use ARP timeout of 360 seconds, which are 6 minutes.

Example

Set ARP timeout to 6 minutes, which are 360 seconds:

```
   PVTD#set arp_timeout 360
```

set fixup_disable

Disable fixup.

set fixup_disable

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to disable Private VLAN ARP Fixup.

When ARP Fixup is disabled, PVTD will just learn about hosts in the Private VLAN network, but will not use ARP Fixup to force traffic going through the gateway or firewall.

set fixup_enable

Enable fixup.

set fixup_enable

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to enable Private VLAN ARP Fixup.

When ARP Fixup is enabled, PVTD will learn about hosts in the Private VLAN network, and will use ARP Fixup to force traffic going through the gateway or firewall.

The ARP Fixup will be used in the following conditions:

- When a Host in an Isolated VLAN is sending ARP request for any other host.
- When a Host in a Community VLAN is sending ARP request for a host on a different Community VLAN.
- When a Host in a Community VLAN is sending ARP request for a host on any Isolated VLAN.

ARP Fixup will not be used when a host is looking for a host not in the same Primary VLAN.

set interface_duplex

Change Private VLAN interface duplex.

set interface_duplex *duplex*

Elements description

duplex	full,half

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change Private VLAN interface duplex.

When interface speed is set to auto, duplex is ignored and it will be negotiated.

When interface speed set to 1000, duplex is ignored as 1000baseT will only support full duplex.

To show the actual interface speed and duplex use the *show stat_interface* command.

Example

Set Private VLAN interface duplex to half:

```
   PVTD#set interface_duplex half
```

set interface_speed

Change Private VLAN interface speed.

set interface_speed *speed*

Elements description

speed	auto,10,100 or 1000

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change Private VLAN interface speed.

When interface speed is set to auto, duplex is ignored and it will be negotiated.

When interface speed set to 1000, duplex is ignored as 1000baseT will only support full duplex.

To show the actual interface speed and duplex use the *show stat_interface* command.

Example

Set Private VLAN interface speed to auto:

```
   PVTD#set interface_speed auto
```

Set Private VLAN interface speed to 100:

```
   PVTD#set interface_speed 100
```

set license

Change the device license.

set license *<number_of_hosts> <hash>*

Elements description

number_of_hosts	Number of hosts licensed to the device
hash	A hash string received from Marathon-Networks to authenticate the license

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Contact support@marathon-networks.com to get a license for the device.

Notice: Restart the *pvtd* process to enable license. Use the *restart pvtd* command to restart the *pvtd* process.

set lldp_disable

Disable discovery protocols.

set lldp_disable

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to disable discovery protocols.

The following protocols will be disabled:

- LLDP - IETF
- CDP - Cisco
- EDP - Extreme
- FDP - Foundry
- NDP - Nortel

set lldp_enable

Enable discovery protocols.

set lldp_enable

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to enable discovery protocols.

When discovery protocols are enabled, PVTD will do the following:

- At first PVTD will send LLDP on all of its interface.
- If PVTD receives any discovery protocol, that protocol will be considered as an active protocol
- PVTD will send discovery packets to all active protocols

For example: PVTD is always sending LLDP packets. If PVTD receives CDP packets, then it will also send CDP packets.

set mac_address

Change PVTD MAC address.

set mac_address *mac_address*

Elements description

mac_address	A MAC address in the following format: 404c.6fxx.xxxxx or the keyword RANDOM

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Unless there is a specific reason, it is advised to use the RANDOM keyword

The MAC address should always start with 404c.6f

The MAC address is used for sending ARP requests and ARP fixups.

Notice: Two PVTDs on the same L2 network should not have the same MAC address. Use the RANDOM keyword to generate a random MAC address wich starts with 404c.6f

Example

Set MAC address to 404c.6f00.0001:

```
   PVTD#set mac_address 404c6f00.0001
```

Set MAC address to a random MAC address

```
PVTD#set mac_address RANDOM
PVTD#show conf_global | match mac
set mac_address 404c.6fb0.b972
```

set ntp_disable

Disable NTP.

set ntp_disable

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to disable time synchronization using NTP.

set ntp_enable

Enable NTP.

set ntp_disable

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to enable time synchronization using NTP.

Notice: To speed up synchronization, it is recommended to first set the local time/date manually using *set system_time and system_date.* The more the local time is far from the NTP time, them more it takes to synchronize the time.

set pvlan_gwv4

Change gateway/firewall IPv4 address.

set pvlan_fwv4 *pvlan ipv4_address*

Elements description

pvlan	Primary VLAN number
ipv4_address	The IP address of the gateway or firewall for the Primary VLAN

Permissions

Minimal permission group is OPER

History

1.0	Command first appearance

Guide

Use this command to change the IPv4 address of a gateway or firewall for the given Primary VLAN.

Every second, PVTD sends ARP request for each gateway/Firewall and stores the results in the gateway/Firewall table. Use the *show gwv4_mac* to see the returned MAC address of the gateway/Firewall.

PVTD is using the MAC address returned by the gateway/Firewall for ARP Fixup.

If the gateway/Firewall MAC changes, PVTD will send notifications to ARP Fixuped hosts to update them with the new MAC address.

The IPv4 gateway/Firewall address is usually the VIP of the Firewall on the specific Primary VLAN. It is also usually the default gateway IPv4 address configured on the host on the specific Primary VLAN.

The IPv4 address should be in the subnet of PVTD IPv4 address.

Example

Set Firewall IPv4 address on Primary VLAN 10 to 10.10.0.254:

```
   PVTD#set pvlan_gwv4 10 10.10.0.254
```

set pvlan_ipv4

Change PVTD IPv4 address.

set pvlan_ipv4 *pvlan ipv4_address*

Elements description

pvlan	Primary VLAN number
ipv4_address	The IP address of PVTD for the Primary VLAN

Permissions

Minimal permission group is OPER

History

1.0	Command first appearance

Guide

Use this command to change the IPv4 address of PVTD for the given Primary VLAN.

This address will be used as the ARP Source Protocol Address (SPA) for non ARP Fixup ARP packets.

This address should be unique on the specific Primary VLAN.

Notice: It is recommended not to use the network address or the broadcast address, as some OS will not reply to ARP requests with SPA of network address or broadcast address such as 10.10.1.0/24 or 10.10.1.255/24.

Example

Set PVTD IPv4 address on Primary VLAN 10 to 10.10.0.200:

```
   PVTD#set pvlan_ipv4 10 10.10.0.200
```

set pvlan_maskv4

Change PVTD IPv4 network mask.

set pvlan_maskv4 *pvlan network_mask*

Elements description

pvlan	Primary VLAN number
network_mask	The IP address of PVTD for the Primary VLAN

Permissions

Minimal permission group is OPER

History

1.0	Command first appearance

Guide

Use this command to change the network mask of PVTD for the given Primary VLAN.

Together with PVTD IPv4 address, PVTD will validate every ARP request to be in the network of the specific Primary VLAN it belongs to.

Example

Set PVTD network mask on Primary VLAN 10 to 255.255.255.0:

```
   PVTD#set pvlan_maskv4 10 255.255.255.0
```

set radius_disable

Disable RADIUS.

set radius_disable

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to disable RADIUS authentication.

Local users, configured with *add user* command will be used for authentication.

set radius_enable

Enable RADIUS.

set ntp_disable

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to enable RADIUS for authentiaction.

If all the RADIUS servers failed to respond, or are not configured with a password then local users will be used for authentication.

set radius_obscure

Change a radius password.

set radius_obscure *host obscured_password*

Elements description

host	A RADIUS server
obscured_password	A hex string of an obscured password

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change the obscured RADIUS password for the specified RADIUS server.

This command is used for copy pasting configuration, as *show conf_radius* will only show the obscured password.

Notice: The password is not hashed or encrypted. It is just obscured to avoid over the shoulder glance. Keep this obscured password private.

Example

Set the obscured password for RADIUS server at 10.0.123.204:

```
PVTD#set radius_obscure 10.0.123.204 5a5f455f425e595c
```

set radius_password

Change a radius password.

set radius_obscure *host password*

Elements description

host	A RADIUS server
password	A clear text password, with no blanks.

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change the RADIUS password for the specified RADIUS server.

This password is shared between PVTD and the RADIUS server for request validation and password envryption.

Notice: *show conf_radius* will only show the obscured password.

Example

Set the password for RADIUS server at 10.0.123.204:

```
   PVTD#set radius_password MyClearTextPassword
```

set snmp_community

Change the SNMP community.

set snmp_community *community*

Elements description

community	A community string with no spaces

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

The community string is used for SNMPv1 read only access. There is no read-write access to PVTD.

Notice that a SNMP manager server should also be listed in the allowed IPv4 SNMP networks. Use the *set allowed_snmpv4* command.

Example

Set the SNMP community to my_com

```
   PVTD#set snmp_community my_com
```

set snmp_contact

Change the SNMP contact.

set snmp_contact *contact*

Elements description

contact	A contact string with no spaces

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change the SNMP contact string.

Example

Set the SNMP contact string to my_contact

```
   PVTD#set snmp_contact my_contact
```

set snmp_description

Change the SNMP description.

set snmp_description *description*

Elements description

description	A description string with no spaces

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change the SNMP description string.

Example

Set the SNMP description string to my_desc

```
   PVTD#set snmp_description my_description
```

set snmp_disable

Disable SNMP.

set snmp_disable

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Local users, configured with *add user* command will be used for authentication.

set snmp_enable

Enable SNMP.

set snmp_disable

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to enable the SNMP agent.

set snmp_location

Change the SNMP location.

set snmp_contact *contact*

Elements description

location	A location string with no spaces

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change the SNMP location string.

Example

Set the SNMP location string to mars

```
   PVTD#set snmp_location mars
```

set svlan_desc

Change a Secondary VLAN description.

set svlan_desk *vlan [description]*

Elements description

vlan	The Secondary VLAN number
description	Description string

Permissions

Minimal permission group is OPER

History

1.0	Command first appearance

Guide

Use this command to change the Secondary VLAN description string.

The VLAN description string is only for display, and it does not alter the behaviour of PVTD in any way.

If the *description* parameter is missing, then the description will be set to empty string and not shown on *show conf** commands.

Example

Set a description of Secondary VLAN 101 to “Exchange_Servers_VLAN”

```
   PVTD#set svlan_desc 101 Exchange_Servers_VLAN
```

set svlan_pvlan

Change a Secondary VLAN association to a Primary VLAN.

set svlan_pvlan *pvlan* **vlan** *svlan_range*

Elements description

pvlan	The Primary VLAN number
svlan_range	A single Secondary VLAN, or a range of secondary VLANs

Permissions

Minimal permission group is OPER

History

1.0	Command first appearance

Guide

Use this command to change the Secondary VLAN association to a Primary VLAN.

The vlan range can be a single VLAN number or a list of VLAN numbers. Hyphen can be used to define a range of consecutive vlans.

No spaces are allowed in the VLAN range.

Notice: When a Secondary VLAN is first added using the *add svlan* command, it is not associated to any Primary VLAN. To see the list of unassociated Secondary VLANs, use the *show conf_pvlan 0* or *show conf_all* commands.

Examples

Set a secondary VLAN 101 association to Primary VLAN 10

```
    PVTD#set svlan pvlan 10 vlan 101
```

Set a secondary VLANs 101,103 association to Primary VLAN 10

```
    PVTD#set svlan pvlan 10 vlan 101,103
```

Set a secondary VLANs 101,103,105,106,107,109 association to Primary VLAN 10

```
    PVTD#set svlan pvlan 10 vlan 101,103,105-107,109
```

set svlan_type

Change a Secondary VLAN type..

set svlan_pvlan *type* **vlan** *svlan_range*

Elements description

type	One letter indicating then Secondary VLAN type. C - Community I - Isolated U - Undefined
svlan_range	A single Secondary VLAN, or a range of secondary VLANs

Permissions

Minimal permission group is OPER

History

1.0	Command first appearance

Guide

Use this command to change the Secondary VLAN type.

The vlan range can be a single VLAN number or a list of VLAN numbers. Hyphen can be used to define a range of consecutive vlans.

No spaces are allowed in the VLAN range.

Notice: When a Secondary VLAN is first added using the *add svlan* command, its type is Undefined. Undefined Seocndary VLAN is not active and will not be used by PVTD. You can use Undefined type to temporarily disable a Secondary VLAN.

Examples

Set a secondary VLAN 101 type to Isolated:

```
   PVTD#set svlan type C vlan 101
```

Set a secondary VLANs 103,105,106,107,109 type to Community

```
   PVTD#set svlan type C vlan 103,105-107,109
```

Disable VLAN 103 by setting its type to Undefined:

```
   PVTD#set svlan type U vlan 103
```

set sys_date

Change the system date.

set sys_date *date*

Elements description

date	Date format is YYYYMMDD Y - Year M - Month. 01 for january D - Day. 02 for the second day of the month.

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change the system date.

To show the current system date, use the *show sys_date* command.

Example

Set system date to 29 AUG 1958:

```
   PVTD#set sys_date 19580829
```

set sys_domain

Change the system domain name.

set sys_domain *domain_name*

Elements description

domain	A domain name string

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change the system domain name.

set sys_host_name

Change the system hostname.

set sys_host_name *host_name*

Elements description

host_name	A hostname string

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change the system hostname.

Notice: Changing the hostname will also change the prompt to that hostname.

set sys_interface_duplex

Change system interface duplex.

set sys_interface_duplex *duplex*

Elements description

duplex	full,half

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change system interface duplex.

The system interface, is the interface connected to the management network.

When interface speed is set to auto, duplex is ignored and it will be negotiated.

When interface speed set to 1000, duplex is ignored as 1000baseT will only support full duplex.

To show the actual interface speed and duplex use the *show stat_sys_interface* command.

Example

Set system interface duplex to half:

```
PVTD#set sys_interface_duplex half
```

set interface_speed

Change system interface speed.

set sys_interface_speed *speed*

Elements description

speed	auto,10,100 or 1000

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change the system interface speed.

When interface speed is set to auto, duplex is ignored and it will be negotiated.

When interface speed set to 1000, duplex is ignored as 1000baseT will only support full duplex.

To show the actual interface speed and duplex use the *show stat_sys_interface* command.

Example

Set system interface speed to auto:

```
PVTD#set sys_interface_speed auto
```

Set system interface speed to 100:

```
PVTD#set sys_interface_speed 100
```

set sys_ipv4

Change the system IPv4 address.

set sys_ipv4 *ipv4_address network_mask*

Elements description

ipv4_address	System interface IPv4 address.
network_mask	A network mask, using full IPv4 string, such as 255.255.255.0

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

The IPv4 address is used for:

- SSH
- SYSLOG
- SNMP
- ICMP

Notice: It is recommended to configure the system IPv4 address using the console and not using SSH.

Use the *ping* and *traceroute* command to verify connectivity.

Example

Change the system IPv4 address to 10.0.99.100/24

```
PVTD#set sys_ipv4 10.0.99.100 255.255.255.0
```

set sys_ipv4_gw

Set the system IPv4 gateway.

set sys_ipv4_gw *ipv4_address*

Elements description

ipv4_address	Default gateway IPv4 address

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

The default gateway should be directly reachable on the system interface. Otherwise, the default gateway will be deleted.

Example

Set gateway to 10.0.123.1:

```
PVTD#set sys_ipv4_gw 10.0.123.1
```

set sys_time

Change the system time.

set sys_time *time*

Elements description

time	Time format is HHMM H - Hours in 24 hours format. 1AM = 01. 1PM = 13. M - Minutes. 1 minutes = 01. 10 minutes = 10

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change the system time.

To show the current system time, use the *show sys_time* command.

Example

Set system time to 09:00 / 9pm

```
   PVTD#set sys_time 0900
```

set sys_time_zone

Change the system time zone.

set sys_time_zone *time_zone*

Elements description

time_zone	Time zone string. Use TAB completion to list the available time zones.

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change the system time zone.

Time zone is important when using NTP, as NTP updates are in UTM time.

Time zone is also important for *show host** commands, as timestamps are stored internally in UTC.

Example

Set system time zone to Vostok in Antarctica:

```
   PVTD#set sys_time_zone Antarctica_Vostok
```

set tracking_disable

Disable host tracking.

set tracking_disable

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to disable host tracking.

set tracking_enable

Enable host tracking.

set ntp_disable

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to enable host tracking.

Host tracking will log the following events:

- A New host has been seen on the Private VLAN network.
- Host changed VLAN number
- Host changed its MAC address
- Host deleted due to idle timeout. It usually means that the host is down.

set user_group

Change a user’s group.

set user_group *user group*

Elements description

user	A username for which a new group will be assigned
group	The new group name. Can be one of the following: ADMIN - Can do anything OPER - Can change Private VLAN configurations, but can not change any security related features or any system settings. VIEWER - Can only view statistics and configurations.

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to change a user’s group association..

Notice: You should be careful to have at least one ADMIN user.

Example

Sets john’s group to allow changing Primary VLANs settings:

```
   PVTD#set user_group john OPER
```

set user_hash

Change a user’s hash.

set user_group *user password salt*

Elements description

user	A username for which a new password be assigned
password	A hash of the password
salt	A random value used to protect the hash

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

This command is for configuration copy paste operations.

set user_password

Change a user's pssword.

set user_group *user group*

Elements description

user	A username for which a new password will be assigned
password	A clear text password. The password should be without spaces.

Permissions

Minimal permission group is VIEWER/OPER/ADMIN

History

1.0	Command first appearance

Guide

Use this command to change a user's password.

Users in the VIEWER and OPER groups can only change their own address.

ADMIN users can change any user's password.

set web_disable

Disable the internal web server.

set web_disable

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Use this command to disable the internal web server.

set web_enable

Enable the internal web server.

set web_enable

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Remember to use the *add web_allowed* command to allow clients to connect to the internal web server.

Use HTTPS to connect to the internal web server.

Notice: For new install or RMA please regenerate the SSL self signed certificate using the *regen ssl* command.

SHOW commands

Show commands are used to view current configuration and status.

show conf_*

Show various configuration commands.

show conf_all	Show all configuration elements
show conf_general	Show general configuration items
show conf_ntp	Show NTP configurations
show conf_pvlan *pvlan_number*	Show Primary VLAN Configurations
show conf_radius	Show RADIUS configurations
show conf_snmp	Show SNMP configurations
show conf_ssh	Show SSH configurations
show conf_svlan *svlan_number*	Show specific Secondary VLAN configurations
show conf_svlan_desc *desc_pattern*	Show Secondary VLANs matching the description pattern
show conf_syslog	Show SYSLOG configurations
show conf_users	Show local users Configurations
show conf_web	Show the internal web server configuration

Elements description

pvlan_number	Primary VLAN number
svlan_number	Secondary VLAN number
desc_pattern	Description string pattern. Use * for wildcard

Permissions

Minimal permission group is VIEWER
For the following configurations commands the ADMIN permission group us required:

- show conf_radius
- show conf_ssh
- show conf_snmp
- show conf_ssh
- show conf_users
- show conf_web

History

1.0	Command first appearance

Guide

The show conf_all command will show only partial configurations for non-admin users.

The add/set commands displayed by the show conf_* commands can be used for configuration copy and paste.

show dir_disk0

Show disk0 directory listing.

show dir_disk0

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

For each file the filename, the file size in bytes and the file's last modification date.

The list of file is sorted by name.

The Total bytes on the device is not the sum of all file sizes. Due to padding and metadata, file sizes are more than the actual number of data bytes.

Example:

```
pvtd_d#show dir_disk0
File Name                                          Size          Date
-------------------------------------------------- ------------- ------------------
conf.txt                                                       0 2012.04.06 13:03
myconf                                                      2341 2012.04.28 23:06
myconf2                                                     2264 2012.04.10 22:23
myconf3                                                     2341 2012.05.10 23:23
support                                                    17826 2012.04.22 07:21
upgrade01.tar.gz                                           82834 2012.04.11 23:39
upgrade02.tar.gz                                           82833 2012.04.11 23:39
upgrade03.tar.gz                                           82837 2012.04.11 23:39

Total bytes on the device: 4224907264
Available bytes on the device: 4013373440
```

show fixup_status

Show whether ARP Fixup is enabled.

show fixup_status

Elements description

None

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

None

Example:

Disable ARP Fixup and show status:

```
   pvtd_d#set fixup_disable
   pvtd_d#show fixup_status
   PVTD is in learning mode
```

Enable ARP Fixup and show status:

```
   pvtd_d#set fixup_enable
   pvtd_d#show fixup_status
   PVTD is in ARP fixup mode
```

show gwv4_mac

Show MAC address of an IPv4 gateway/Firewall

show gwv4_mac *pvlan*

Elements description

pvlan	Primary VLAN number

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

None

Example

Show the resolved MAC address for Primary VLAN 10:

```
   pvtd_d#show gwv4_mac 10
   CMD003-GWV4_MAC_RPL-I PVLAN 10 GWIPv4 10.10.255.254 MAC 000a.1010.fffe
```

Show the unresolced MAC address for Primary VLAN 99:

```
   pvtd_d#show gwv4_mac 99
   CMD004-GWV4_UNRESOLVED-E GW unresolved
```

show host_*

Show active hosts on the Private VLAN network.

show host_ipv4 *ipv4_pattern*	Show IPv4 hosts by IPv4 address pattern
show host_macv4 *mac_pattern*	Show IPv4 hosts by MAC address pattern
show conf_svlan *svlan_pattern*	Show IPv4 hosts by Secondary VLAN pattern

Elements description

ipv4_pattern	Host’s IPv4 Address or pattern. Use * for wildcard
mac_pattern	Host’s MAC address or pattern. Use * for wildcard
svlan_pattern	Host’s Secondary VLAN or pattern. Use * for wildcard

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

For each host, the IPv4 address, MAC address, Secondary VLAN, when it was first seen on the network, when it was last seen on the network, and when & what was the last operation.

Operation can be one of the following:

- ADDED - The host was added
- MAC_UPD - Host’s MAC address was changed
- VLAN_UPD - Host’s VLAN was changed

Notice: The host table is updated every 5 seconds.

Example:

Show data for 10.10.0.2:

```
pvtd_d#show host_ipv4 10.10.0.2
IP              VLAN MAC            FIRST SEEN        LAST SEEN         LAST CHANGE       LAST ACT
--------------- ---- -------------- ----------------- ----------------- ----------------- ----------
10.10.0.2       1000 000b.1010.0002 20120511 00:14:57 20120511 00:14:57 20120511 00:14:57 ADDED
```

Show data for all hosts starting with 10.10:

```
pvtd_d#show host_ipv4 10.10.*
IP              VLAN MAC            FIRST SEEN        LAST SEEN         LAST CHANGE       LAST ACT
--------------- ---- -------------- ----------------- ----------------- ----------------- ----------
10.10.0.2       1000 000b.1010.0002 20120511 00:14:57 20120511 00:14:57 20120511 00:14:57 ADDED
10.10.0.3       1000 000b.1010.0003 20120511 00:11:23 20120511 00:16:15 20120511 00:11:23 ADDED
10.10.0.4       1000 000b.1010.0004 20120511 00:15:08 20120511 00:15:08 20120511 00:15:08 ADDED
10.10.0.6       1000 000b.1010.0006 20120511 00:14:45 20120511 00:16:16 20120511 00:14:45 ADDED
10.10.1.4       1001 000b.1010.0104 20120511 00:10:46 20120511 00:16:07 20120511 00:10:46 ADDED
10.10.1.6       1001 000b.1010.0106 20120511 00:11:42 20120511 00:16:17 20120511 00:11:42 ADDED
10.10.8.2       1008 000b.1010.0802 20120510 23:58:17 20120511 00:16:18 20120510 23:58:17 ADDED
10.10.9.4       1009 000b.1010.0904 20120510 23:43:19 20120511 00:16:19 20120510 23:43:19 ADDED
```

Show data for all hosts with MAC address ending with 1002:

```
pvtd_d#show host_macv4 *1002
IP              VLAN MAC            FIRST SEEN        LAST SEEN         LAST CHANGE       LAST ACT
--------------- ---- -------------- ----------------- ----------------- ----------------- ----------
10.11.10.2      1110 000b.1011.1002 20120511 00:04:58 20120511 00:17:43 20120511 00:04:58 ADDED
10.12.10.2      1210 000b.1012.1002 20120510 23:52:44 20120511 00:17:37 20120510 23:52:44 ADDED
```

Show data for all hosts in Secondary VLAN 1109:

```
pvtd_d#show host_svlanv4 1109
IP              VLAN MAC            FIRST SEEN        LAST SEEN         LAST CHANGE       LAST ACT
--------------- ---- -------------- ----------------- ----------------- ----------------- ----------
10.11.9.1       1109 000b.1011.0901 20120510 23:51:05 20120511 00:18:37 20120510 23:51:05 ADDED
```

```
10.11.9.3       1109 000b.1011.0903 20120510 23:32:51 20120511 00:18:38 20120510 23:32:51 ADDED
10.11.9.5       1109 000b.1011.0905 20120511 00:12:46 20120511 00:18:39 20120511 00:12:46 ADDED
```

show lldp

Show LLDP/CDP and EDP/FDP/NDP table.

show show_lldp

Elements description

None

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

See the commands reference for the *set lldp_enable* command for what discovery protocols are expected to be seen.

The following table describe the role of local interface to their function by model number:

Model	Interface	Interface function
PVTD-5K01R	em0	System interface. Used for management.
	em1	Private VLAN interface. Connected to the Private VLAN network.

Example:

```
pvtd_d#show lldp
Capability Codes:
        r - Repeater, B - Bridge, H - Host, R - Router, S - Switch,
        W - WLAN Access Point, C - DOCSIS Device, T - Telephone, O - Other

Device ID           Local Intf    Proto   Hold-time    Capability    Port ID
SW1                 em1           CDP     145          RS            Gi0/1
SW1                 em1           LLDP    102          BR            Gi0/1
```

show lldp_status

Show whether LLDP is enabled

show lldp_status

Elements description

None

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

None

Examples:

Disable LLDP and show status:

```
pvtd_d#set lldp_disable
pvtd_d#show lldp_status
LLDP is disabled
pvtd_d#show lldp
LLDP/CDP is disabled
```

Enable LLDP and show status:

```
pvtd_d#set lldp_enable
pvtd_d#show lldp_status
LLDP is enabled
pvtd_d#show lldp
Capability Codes:
        r - Repeater, B - Bridge, H - Host, R - Router, S - Switch,
        W - WLAN Access Point, C - DOCSIS Device, T - Telephone, O - Other

Device ID           Local Intf    Proto   Hold-time    Capability    Port ID
SW1                 em1           LLDP    117          BR            Gi0/1
```

show log

Print the current log

show log

Elements description

None

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

Notice: Every hour the log will be cleared if its over 3MB long. To show previous log files, use the *show log_old* command.

Use pipe command to filter the log. See PIPE Commands section

Example:

Show log entries for 11 MAY 14:09:

```
   pvtd_d#show log | match May 11 14:09
   May 11 14:09:01 pvtd_d ladvd: new peer SW1.dans-net.com (LLDP) on interface em1
   May 11 14:09:01 pvtd_d ladvd: enabling LLDP on interface em1
   May 11 14:09:01 pvtd_d pvtsh.py: PVTSH001-CMD_LOG-I: A-show lldp_status
   May 11 14:09:04 pvtd_d pvtsh.py: PVTSH001-CMD_LOG-I: A-show lldp
   May 11 14:09:08 pvtd_d ladvd: new peer SW1.dans-net.com (CDP) on interface em1
   May 11 14:09:08 pvtd_d ladvd: enabling CDP on interface em1
   May 11 14:09:10 pvtd_d ladvd: new peer SW1.dans-net.com (LLDP) on interface em0
   May 11 14:09:10 pvtd_d ladvd: enabling LLDP on interface em0
   May 11 14:09:19 pvtd_d ladvd: new peer SW1.dans-net.com (CDP) on interface em0
   May 11 14:09:19 pvtd_d ladvd: enabling CDP on interface em0
   May 11 14:13:16 pvtd_d pvtsh.py: PVTSH001-CMD_LOG-I: A-show log | match May 11 14:09
```

show log_old

Show cleared log entries.

show log_old *revision*

Elements description

revision	0 to 4. 0 is the most recent. 4 is the oldest.

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

Every hour the log will be cleared if its over 3MB long, or PVTD will clear the log file whenever *clear log* command is issued. However PVTD stores revisions of cleared log files.

Example

Show the last log before it was cleared:

```
pvtd_d#show log_old 0
May  7 06:24:03 pvtd_d newsyslog[14889]: logfile turned over
May  7 06:24:03 pvtd_d syslogd: restart
May  7 06:24:08 pvtd_d pvtsh.py: PVTSH001-CMD_LOG-I: A-clear log
May  7 06:24:10 pvtd_d pvtsh.py: PVTSH001-CMD_LOG-I: A-show log
May  7 06:24:26 pvtd_d pvtsh.py: PVTSH001-CMD_LOG-I: A-show log
May  7 06:24:30 pvtd_d pvtsh.py: PVTSH001-CMD_LOG-I: A-clear log
May  7 06:24:30 pvtd_d newsyslog[16313]: logfile turned over
```

show md5_disk0

Show MD5 sum for a file on disk0.

show md5_disk0 *filename*

Elements description

filename	A filename of a file on disk0

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

None

Example

```
pvtd_d#show md5_disk0 upgrade01.tar.gz
MD5 sum: 4445e65c4dec4a08d48e95d72719d054
```

show ntp_host

Show a list of NTP servers

show ntp_host

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

None

Examples:

Show a list of NTP hosts:

```
pvtd_d#show ntp_host
NTP Host
---------------
192.115.25.212
192.114.71.34
```

show ntp_status

Show a the status of NTP communication

show ntp_status

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

The command will show if NTP is enabled, and if there are errors.

If there are errors you can see more details in the log, using the *show log* **|** *match <ntp server ip address>* command.

Examples:

Show a NTP status where 192.115.15.212 is not responding:

```
pvtd_d#show ntp_status
NTP is enabled
: bad peer 192.115.25.212 (192.115.25.212)
```

Show log entries for the erroneous NTP server:

```
pvtd_d#show log | match 192.115.25.212
May  7 10:36:41 pvtd_d ntpd[7485]: bad peer 192.115.25.212 (192.115.25.212)
May  8 10:38:51 pvtd_d ntpd[7485]: bad peer 192.115.25.212 (192.115.25.212)
Jun  9 10:40:23 pvtd_d ntpd[7485]: bad peer 192.115.25.212 (192.115.25.212)
Jun 10 10:48:18 pvtd_d ntpd[6787]: recvmsg 192.115.25.212: No route to host
Jun 10 11:38:27 pvtd_d ntpd[6787]: bad peer 192.115.25.212 (192.115.25.212)
Jun 10 11:40:37 pvtd_d ntpd[6787]: recvmsg 192.115.25.212: Connection refused
Jun 10 11:42:47 pvtd_d ntpd[6787]: bad peer 192.115.25.212 (192.115.25.212)
Jun 10 11:43:01 pvtd_d ntpd[6787]: bad peer 192.115.25.212 (192.115.25.212)
Jun 10 11:50:36 pvtd_d ntpd[6787]: bad peer 192.115.25.212 (192.115.25.212)
```

show print_disk0

Show the content of a file on disk0.

show print_disk0 *filename*

Elements description

filename	A filename of a file on disk0

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

None

Example

Create file on disk0 by redirecting a show command output to a file on disk0:

```
pvtd_d#show conf_pvlan 10 | disk0 pvlan_10
```

Show the content of disk0:

```
pvtd_d#show dir_disk0
File Name                                          Size          Date
-------------------------------------------------- ------------- ------------------
conf.txt                                                       0 2012.04.06 13:03
myconf                                                      2341 2012.04.28 23:06
myconf2                                                     2264 2012.04.10 22:23
myconf3                                                     2341 2012.05.10 23:23
pvlan_10                                                     247 2012.05.17 08:49
support                                                    17826 2012.04.22 07:21
upgrade01.tar.gz                                           82834 2012.04.11 23:39
upgrade02.tar.gz                                           82833 2012.04.11 23:39
upgrade03.tar.gz                                           82837 2012.04.11 23:39

Total bytes on the device: 4224907264
Available bytes on the device: 4013371392
```

Print the file we have created with the *show conf_pvlan 10* | *disk0 pvlan_10* command:

```
pvtd_d#show print_disk0 pvlan_10
!
! PVLAN 10
!
add pvlan 10
set pvlan_ipv4 10 10.10.255.220
set pvlan_maskv4 10 255.255.0.0
set pvlan_gwv4 10 10.10.255.254
add svlan vlan 1000-1020
set svlan_pvlan 10 vlan 1000-1020
set svlan_type C vlan 1002-1020
set svlan_type I vlan 1000-1001
```

show radius_host

Show a list of RADIUS servers

show radius_host

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

If RADIUS is enabled, then the order of the displayed RADIUS servers is also the order in which PVTD will contact the RADIUS servers for authentication.

Examples:

Show a list of RADIUS servers:

```
pvtd_d#show radius_host
Radius Host
---------------
10.0.123.205
10.0.123.204
```

show radius_status

Show if RADIUS authentication is enabled or disabled

show radius_status

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

If RADIUS authentication is disabled, then only locally configured users table will be used for authentication

Examples:

Enable RADIUS authentication and show status:

```
pvtd_d#set radius_enable
pvtd_d#show radius_status
RADIUS is enabled
```

Disable RADIUS authentication and show status:

```
pvtd_d#set radius_disable
pvtd_d#show radius_status
RADIUS is disabled
```

show radius_test

Test radius configuration

show radius_test *user password*

Elements description

user	A username to be tested
password	A clear text password. The password should be without spaces.

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

If you can successfully authenticate to a RADIUS server then:

- Connectivity to the radius server is OK
- Radius server password is OK
- Username and password are OK

Examples

Test RADIUS with wrong RADIUS server password:

```
   pvtd_d#set radius_password 10.0.123.204 wrong_password
   pvtd_d#show radius_test myview myviewpass
   RADIUS test timeout or not RADIUS hosts configured. Check RADIUS configuration and RADIUS
      server's log
```

Correct the RADIUS password:

```
   pvtd_d#set radius_password 10.0.123.204 RADPVTD
```

Test RADIUS with wrong user password:

```
   pvtd_d#show radius_test myview mywrongpassword
   User rejected by RADIUS server
```

Test RADIUS server with a user which does not return priv-lvl attribute, needed for group association (1-VIEWER,7-OPER,15-ADMIN):

```
   pvtd_d#show radius_test myview myviewpass
   User was accepted by didn't returned any valid priv-lvl attribute
```

After correcting the error at the RADIUS server, try again to Test the user:

```
   pvtd_d#show radius_test myview myviewpass
   User accepted. Group is VIEWER
```

show snmp_allowed

Show a list of IPv4 network from where SNMP managers can send SNMP queries to PVTD

show snmp_allowed

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

The command will show both the IPv4 network and network mask.

Examples:

Show a list of allowed SNMP managers. Notice 0.0.0.0/128.0.0.0 and 128.0.0.0/128.0.0.0 which results in allowing any host to send SNMP queries to PVTD:

```
   pvtd_d#show snmp_allowedv4
   IPv4            MASKv4
   --------------- ---------------
   0.0.0.0         128.0.0.0
   10.0.123.0      255.255.255.0
   128.0.0.0       128.0.0.0
```

show snmp_status

Show if SNMP agent (SNMP server) is enabled or disabled

show snmp_status

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

None

Examples:

Disable SNMP agent and show status:

```
   pvtd_d#set snmp_disable
   pvtd_d#show snmp_status
   SNMP is disabled
```

Enable SNMP agent and show status:

```
   pvtd_d#set snmp_enable
   pvtd_d#show snmp_status
   SNMP is enabled
```

show ssh_allowed

Show a list of IPv4 network from where SSH clients can to connect to PVTD.

show ssh_allowed

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

The command will show both the IPv4 network and network mask.

Examples:

Show a list of allowed SSH clients. Notice 0.0.0.0/128.0.0.0 and 128.0.0.0/128.0.0.0 which results in allowing any host to SSH to PVTD:

```
pvtd_d#show ssh_allowedv4
IPv4            MASKv4
--------------- ---------------
0.0.0.0         128.0.0.0
1.2.3.0         255.255.255.0
10.0.123.0      255.255.255.0
128.0.0.0       128.0.0.0
```

show stat_*

Show various component's status and statistics.

show stat_interface	Show Private VLAN interface status and counters
show stat_interface_live	Show Private VLAN interface statistics updated every 1 second.
show stat_pvtd	Show PVTD statistics
show stat_sys	Show system counters. Updated every 1 second.
show stat_sys_interface	Show system interface status and counters
show stat_sys_interface_live	Show system interface statistics updated every 1 second
show stat_top	Show CPU/Memory and top 20 processes

Elements description

None

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

show stat_interface command will show the following information for the interface connected to the Private VLAN network:

- OS interface name
- Speed and duplex settings, and result of auto negotiation if it was configured so.
- Link status
- Packets counters

show stat_interface_live command will show the following information for the interface connected to the Private VLAN network:

- Packets counters for the interface connected to the Private VLAN network
- Total packet counters for all interfaces on PVTD.
- Notice: The first line and every 20 lines, total count will be displayed. For other rows, only the delta from the previous row will be displayed.
- Notice: Use CTRL+C to stop the scrolling display.

show stat_pvtd command will show the following statistics:

- Number of of times PVTD send buffers were empty. This can happen during interface link errors or during very heavy system load.
- Number of times packets were dropped due to empty send buffers. This can happen if the system is under a very heavy load for long time periods.
- Number of ARP received on the Private VLAN interface.
- Number of time the gateway's MAC address were changed. This can happen if the firewall/HSRP/VRRP cluster is not stable, or if ARP Spoofing attack in underway.
- Number of ARP Fixups sent by PVTD to the Private VLAN network.
- Number of invalid ARP received. This can sometime indicate an ARP attack, or just a bug is some host's OS.
- Number of BPF dropps. This can happen due to L2 loop in the network, bug in a host's OS or ARP attacks.

show stat_sys will display live system counters such as CPU/Memory and IO usage. Use CTRL+C to stop the display.

show stat_sys_interface command will show the following information for the system interface connected management network:

- OS interface name
- Speed and duplex settings, and result of auto negotiation if it was configured so.
- Link status
- Packets counters

show stat_sys_interface_live command will show the following information for the system interface connected to the management network:

- Packets counters for the interface connected to the Private VLAN network

- Total packet counters for all interfaces on PVTD.
- Notice: The first line and every 20 lines, total count will be displayed. For other rows, only the delta from the previous row will be displayed.
- Notice: Use CTRL+C to stop the scrolling display.

show stat_top command will show the system CPU/Memory and top 20 processes sorted by CPU usage

show support

Show most of the available data in one command.

show support

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

It is advised to redirect the show support output to disk0, using the *show support* **|** *disk0 <file name>* command

Examples:

Show support and redirect it to a file named *mysupport2.txt* on disk0:

```
   pvtd_d#show support | disk0 mysupport2.txt
```

show sys_*

Show various system information.

show sys_date	Show date and time in local timezone.
show sys_host_domain	Show the system domain name
show sys_host_name	Show the system host name
show sys_ipv4	Show system IPv4 address for management.
show sys_ipv4_gateway	Show system IPv4 default gateway.

Elements description

None

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

None

show ntp_host

Show a list of NTP servers

show ntp_host

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

None

Examples:

Show a list of NTP hosts:

```
pvtd_d#show ntp_host
NTP Host
---------------
192.115.25.212
192.114.71.34
```

show syslog_host

Show a list of SYSLOG servers, which log entries are sent to them using SYSLOG

show syslog_host

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

None

Examples:

Show SYSLOG host list with two entries:

```
pvtd_d#show syslog_host
Syslog Host
---------------
10.0.123.204
10.0.123.1
```

show track_*

Show the tracking table.

show track_sipv4 *ipv4_pattern*	Show IPv4 track table by IPv4 source address pattern
show track_tipv4 *mac_pattern*	Show IPv4 track table by IPv4 target address pattern

Elements description

ipv4_pattern	Host’s IPv4 Address or pattern. Use * for wildcard

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

Track table is a table of all host pairs which were helped by ARP FIxup to communicate with each other.

Example:

Show data for source 10.10.0.2:

```
pvtd_d#show track_sipv4 10.10.0.5
SIP             SVLAN TIP             TVLAN
--------------- ----- --------------- -----
10.10.0.5        1000 10.10.8.5        1008
10.10.0.5        1000 10.10.10.5       1010
```

Show data for all hosts target starting with 10.10:

```
pvtd_d#show track_tipv4 10.10.*
SIP             SVLAN TIP             TVLAN
--------------- ----- --------------- -----
10.10.0.5        1000 10.10.8.5        1008
10.10.10.5       1010 10.10.9.6        1009
10.10.0.5        1000 10.10.10.5       1010
```

show users

Show a list of local users and their groups

show users

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

None

Examples:

Show the local users

```
pvtd_d#show users
User                             Group
-------------------------------- ------
A                                ADMIN
O                                OPER
sysadmin                         ADMIN
V                                VIEWER
```

show version

Show version info

show version

Elements description

None

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

The command will show:

- PVTD version
- PVTSH (CLI) version
- Serial number, which is the mac address of the system interface
- Device model

Examples:

Show version:

```
pvtd_d#show version
PVTD Version is 01.01
PVTSH version is 01.01
Serial number is 0000.24ce.9748
Device model is PVTD-5K01R
```

show whoami

Show current user and group

show whoami

Elements description

None

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

None

TRACK commands

Track commands are used for troubleshooting

track ipv4

Show ARP frames on the Private VLAN interface, filtered by the IP address requested or replied in ARP frames.

track ipv4 *ipv4_address*

Elements description

ipv4_address	IPv4 Address to track

Permissions

Minimal permission group is VIEWER

Notice: When running the command from the console, the tracking will stop after 100 packets.

History

1.0	Command first appearance

Guide

Use CTRL+C to stop tracking

Example

Track default gateway 10.10.0.254:

```
pvtd_d#track ipv4 10.10.255.254
tcpdump: listening on em1, link-type EN10MB
19:59:02.835832 40:4c:6f:00:00:01 ff:ff:ff:ff:ff:ff 8100 46: 802.1Q vid 10 pri 0 arp who-has 10.10.255.254 tell
    10.10.255.220
19:59:03.283496 00:0b:10:10:11:06 ff:ff:ff:ff:ff:ff 8100 64: 802.1Q vid 1011 pri 0 arp who-has 10.10.255.254
    tell 10.10.11.6
19:59:03.885678 40:4c:6f:00:00:01 ff:ff:ff:ff:ff:ff 8100 46: 802.1Q vid 10 pri 0 arp who-has 10.10.255.254 tell
    10.10.255.220
^C
21 packets received by filter
0 packets dropped by kernel
```

track mac

Show ARP frames on the Private VLAN interface, filtered by the source MAC address of ARP frames.

track mac *mac_address*

Elements description

mac_address	MAC address. Format: xxxx.xxxx.xxxx

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

Use CTRL+C to stop tracking

Notice: When running the command from the console, the tracking will stop after 100 packets.

Example

Track default gateway ARPs:

```
pvtd_d#track mac 000a.1010.fffe
tcpdump: listening on em1, link-type EN10MB
00:26:23.791700 00:0a:10:10:ff:fe 40:4c:6f:00:00:01 8100 64: 802.1Q vid 10 pri 0 arp reply 10.10.255.254 is-at
    00:0a:10:10:ff:fe
```

track netv4

Show ARP frames on the Private VLAN interface, filtered by the IP address requested or replied in ARP frames.

track netv4 *network_address mask*

Elements description

network_address	IPv4 network address
mask	Network mask

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

Use CTRL+C to stop tracking.

Notice: When running the command from the console, the tracking will stop after 100 packets.

Examples

Show ARP frames requesting or replying for network 10.10.0.0/16:

```
pvtd_d#track netv4 10.10.0.0 255.255.0.0
tcpdump: listening on em1, link-type EN10MB
00:33:41.612411 40:4c:6f:00:00:01 ff:ff:ff:ff:ff:ff 8100 46: 802.1Q vid 10 pri 0 arp who-has 10.10.255.254 tell
10.10.255.220
00:33:42.612456 40:4c:6f:00:00:01 ff:ff:ff:ff:ff:ff 8100 46: 802.1Q vid 10 pri 0 arp who-has 10.10.255.254 tell
10.10.255.220
00:33:42.883833 00:0a:10:10:ff:fe 40:4c:6f:00:00:01 8100 64: 802.1Q vid 10 pri 0 arp reply 10.10.255.254 is-at
00:0a:10:10:ff:fe
00:33:43.447902 00:0b:10:10:00:01 ff:ff:ff:ff:ff:ff 8100 64: 802.1Q vid 1000 pri 0 arp who-has 10.10.8.3 tell
10.10.0.1
00:33:43.465724 40:4c:6f:00:00:01 00:0b:10:10:00:01 8100 46: 802.1Q vid 10 pri 0 arp who-has 10.10.8.3
(00:0a:10:10:ff:fe) tell 10.10.8.3 (00:0a:10:10:ff:fe)
00:33:43.612488 40:4c:6f:00:00:01 ff:ff:ff:ff:ff:ff 8100 46: 802.1Q vid 10 pri 0 arp who-has 10.10.255.254 tell
10.10.255.220
00:33:44.220645 00:0b:10:10:08:03 ff:ff:ff:ff:ff:ff 8100 64: 802.1Q vid 1008 pri 0 arp who-has 10.10.8.5 tell
10.10.8.3
^C
26 packets received by filter
0 packets dropped by kernel
```

MISC commands

Other commands

escape

Goto appliance’s OS shell.

escape

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

This command is used to do advanced debugging by Marathon Networks support team.

Both the user and the Marathon Networks support team need to agree in order to “escape” to shell.

To ensure that neither the user nor the Marathon Networks support team can escape to shell on their own, both need to provide keys to “escape” to shell:

- The user generated a random number
- The Marathon Networks support team provide a hash which takes the user’s provided random number and other elements into the hashing function

Notice: Escaping to shell can be destructive and its not allowed without direct permission from the Marathon Network support team.

ping

Send ICMP echo request to a destination. A.K.A. ping.

ping *destination*

Elements description

destination	IPv4 address of the destination

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

The ping output packets are coming from the system interface to test connectivity to the management network.

regen ssh

Create new SSH host keys.

regen ssh

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

It is always recommended to re-generate new SSH keys for every new PVTD install.

The length of keys are:
- DSA - 1024
- RSA - 2048

regen ssl

Create new SSL self signed certificate.

regen ssh

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

It is always recommended to re-generate new SSL keys for every new PVTD install or RMA.

The RSA key length is 2048.

restart *

Restart the whole device or a process in a device.

restart device	Restart the whole device. Notice: Under abnormal conditions, it can take upto 25 minutes to boot a device. Usually it takes upto 5 minutes to restart.
restart lldp	Restart the LLDP process (Also restart CDP and other discovery protocols)
restart monitor	Restart internal monitor process
restart ntp	Restart the NTP process
restart pvtd	Restart the PVTD process
restart snmp	Restart the SNMP process
restart ssh	Restart the SSH process. Notice: It will close all remotely connected administrators.
restart syslog	Restart the SYSLOG process
restart web	Restart the internal web server

Elements description

None

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Notice: After restarting pvtd process, it is recommended to restart the web service and logout from all active SSH or console sessions

traceroute

Send ICMP traceroute to destination.

traceroute *destination*

Elements description

destination	IPv4 address of the destination

Permissions

Minimal permission group is VIEWER

History

1.0	Command first appearance

Guide

The traceroute output packets are coming from the system interface to test connectivity to the management network.

Traceroute is using ICMP echo request for traceroute. It does not use UDP traceroute.

upgrade

Upgrade PVTD with a new software version.

upgrade disk0 *filename*

Elements description

filename	An upgrade package file name

Permissions

Minimal permission group is ADMIN

History

1.0	Command first appearance

Guide

Notice: It is only possible to upgrade. Downgrading is currently not supported.

Notice: Upgrading might require restarting the PVTD process or completely restarting the device, which might take 25 minutes.