PVTD Quick Start Guide

www.marathon-networks.com

Table of Contents

Preface

This quick start guide will help the PVTD administrator with the installation, the operation and the troubleshooting of the PVTD device.

This guide does not include all the command options. Please refer to the “PVTD command reference” for the complete documentation of each and every command.

Assumptions

It is assumed that the reader knows how to configure switches, knows basic routing and that you know what Private VLANs are and how to use them.

It is also assumed that the reader knows how to work with CLI, such as Cisco’s or Juniper’s CLIs.

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:

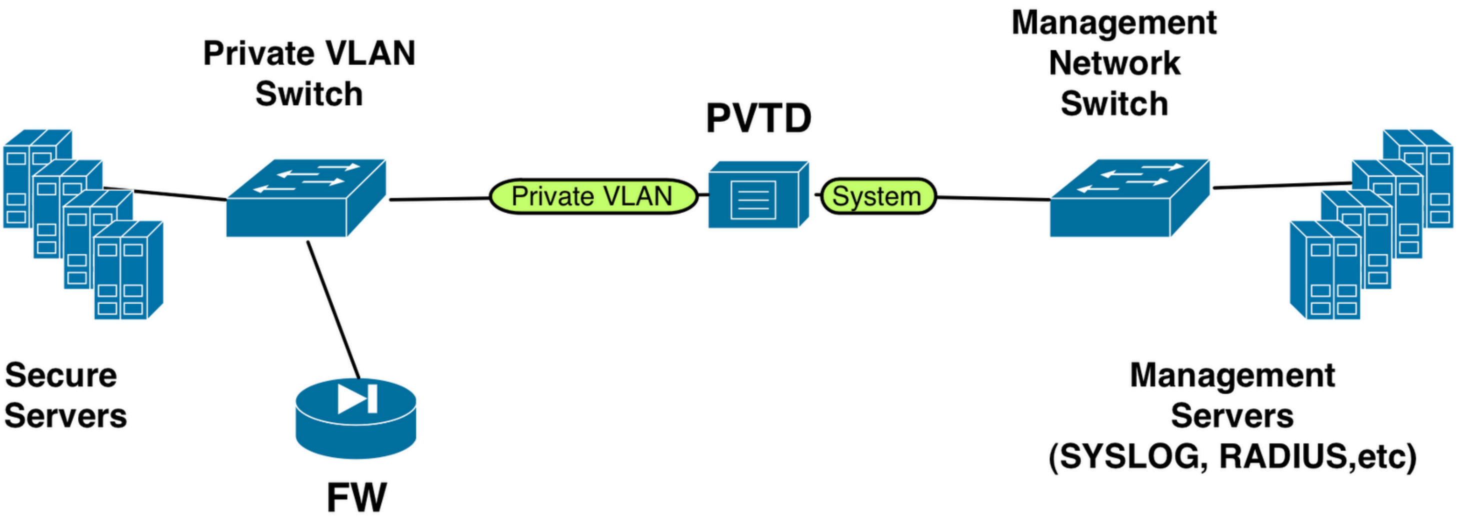
- Terminal sessions and system displays are in `screen font`.
- Information you enter is in **`boldface screen font`**.
- Nonprinting characters, such as hidden passwords or tab presses, are in angle brackets (< >).

Reference Network

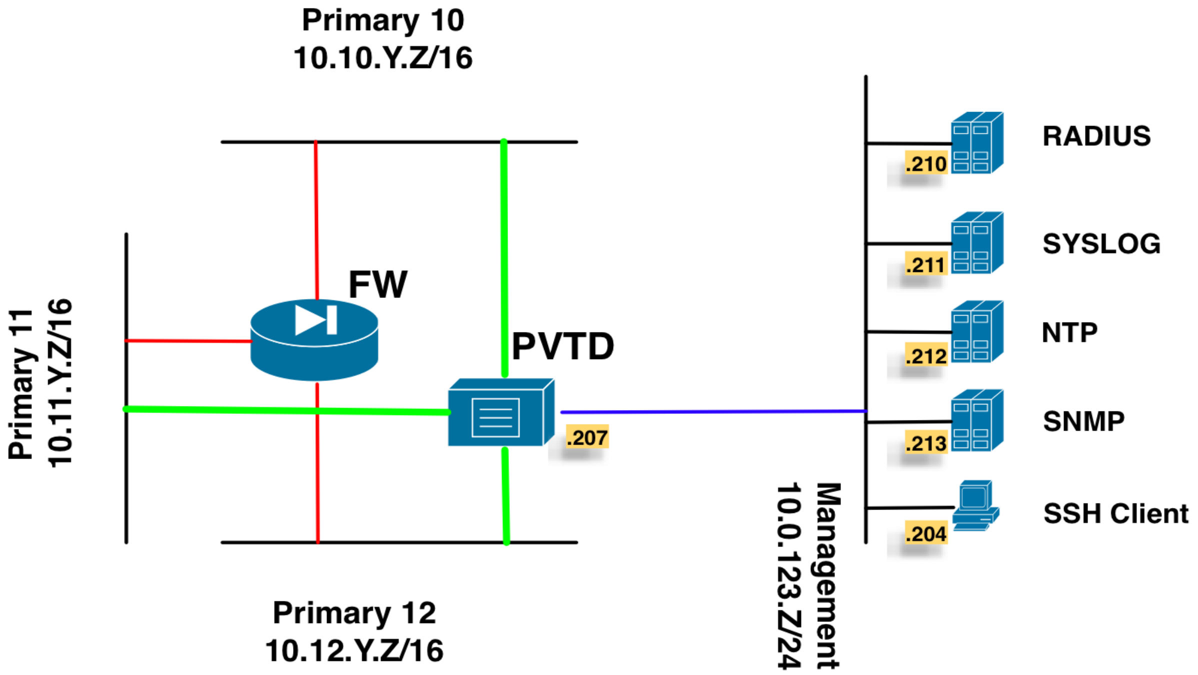
Throughout of this guide, the following sample reference network is used.

Diagram

Physical diagram


Private VLAN Switch
PVTD
Management Network Switch
Private VLAN
System
Secure Servers
FW
Management Servers (SYSLOG, RADIUS,etc)

Logical diagram



Description

There are two networks: Management network and Private VLAN network. Management network can be any network, even a part of the Private VLAN network. Usually its a dedicated management VLAN, where all of the system infrastructure servers reside.

The management network has several auxiliary servers such as RADIUS and NTP servers.

The Private VLAN network is where the secured servers are connected to, which is the target of the PVTD device. The Private VLAN network has 3 Primary networks: 10,11 and 12.

In the heart of the Private VLAN network, there is a Firewall connected to each Primary VLAN.

The PVTD device is connected to the management network as a host on that network, just like a server or a PC.

The PVTD device is connected to the private VLAN network using a 802.11Q trunk. On the switch side of the connection, all the VLANs should be enabled.

The connection to the management interface is called System Interface and the connection to the Private VLAN network is called Private VLAN Interface

Interface Type Table

The following table describes how to locate each interface type on the PVTD device.

Model	System Interface	Private VLAN Interface
PVTD-5K01R	Labeled eth0	Labeled eth1
PVTD-5K02R	Labeled eth0	Rightmost SFP port
PVTD-5H01R	Rightmost ethernet port (Near Console port)	Leftmost ethernet port (Near USB ports)
PVTD-DEMO	Rightmost ethernet port (Near Console port)	Leftmost ethernet port (Near USB ports)
PVTD-VR	First Network interface	Second Network interface

Notice: All other ports are currently unused and they are for future use.

Configuration Tables

Management network

Server purpose	IPv4 Address
RADIUS	10.0.123.210
SYSLOG	10.0.123.211
NTP	10.0.123.212
SNMP	10.0.123.213
Default Gateway	10.0.123.1
PVTD’s Management interface	10.0.123.207
SSH/web Client	10.0.123.204

Private VLAN network structure

Primary VLAN	Secondary VLAN	Type
10	1000	Isolated
10	1001-1004	Community
11	1100	Isolated
11	1101-1104	Community
12	1200	Isolated
12	1201-1204	Community

Firewall and PVTD IPv4 addresses

Private VLAN	Firewall IPv4 address	PVTD IPv4 address
10	10.10.255.254	10.10.255.220/24
11	10.11.255.254	10.11.255.220/24
12	10.12.255.254	10.23.255.220/24

Quick Start

Preface

This chapter will describe how to setup a PVTD device to operate in the reference network described in the Preface->Reference network chapter.

There are 3 configuration steps for the PVTD configuration process:

1. System setup
2. Private VLAN setup
3. Services setup

Connecting the device

Connect the Management interface to the management network.

Connect the Private VLAN interface to the Private VLAN network using a 802.11Q trunk, where all VLANs are enabled.

Connecting Virtual Appliance

The order of the configured interfaces in the VM is very important!

The first interface is the Management/System interface, which can be connected to any port-group. Connect it to the management network.

The second interface is the Private VLAN interface, which should be connected to a vDS/Nexus1000V port-group with the following attributes:

- The port-group should belong to the vDS/Nexus1000V which is connected to the Private VLAN network.
- The port-group should be VLAN Trunking type with full range of VLANs (1-4095)
- The port-group should allow Promiscuous Mode in the Security Policy settings.

Connecting to the device

Two phase login

The login to the device is a two phase process. First you need to login to the device, then you need to login to the CLI (Command Line Interface).

The credentials for the device login are:
User: marathon
Password: networks

The credentials for the device login is always the same, and can not be changed.

Default CLI user

The default credentials for the CLI are:
Username: sysadmin
Password: sysadmin

It is highly recommended to change the password right after the first login.

Console

You can connect to the console using the provided DB9 cable. Any standard DB9 Null Modem cable will do.
The speed is 9600 baud, 8 bit, no parity, 1 stop bit, no flow control, A.K.A, 9600/8-N-1.
You can use any terminal software to connect to the console port, such as Putty, SecureCRT, cu and minicom.

For the Virtual Appliance, open the VM's Console from the vShpere Client.

SSH

The default IP address of PVTD is 192.168.1.100/24. The initial config will not allow any user to connect to PVTD, and the command *add ssh_allowedv4* should be used to allow SSH clients to connect to the PVTD device.

WEB

The default IP address of PVTD is 192.168.1.100/24. The initial config will not allow any user to connect to PVTD, and the command *add web_allowedv4* and *set web_enable* should be used to allow WEB clients to connect to the PVTD device.

System setup

This section demonstrates a basic device setup to allow remote management.

First connect to the serial port and login to the device. Use username *marathon* and password *networks.* Then login to the CLI using the default credentials: *sysadmin/sysadmin*:

```
OpenBSD/i386 (PVTD.marathon-networks.com) (tty00)

login: marathon
Password: <networks>
Last login: Wed Jun 20 05:56:52 on tty00
OpenBSD 5.1 (GENERIC) #160: Sun Feb 12 09:46:33 MST 2012

***********************************************************
*       Marathon Networks Command Line Interface (CLI)    *
*       for PVTD                                          *
*                                                         *
*       Copyright (c) 2012 by Marathon Networks, Inc.     *
*                                                         *
*             Restricted Rights Legend                    *
*                                                         *
* Use,  duplication,  or disclosure by the Government is  *
* subject  to  restrictions as set forth in subparagraph  *
* (c)  of  the Commercial Computer Software - Restricted  *
* Rights  clause at FAR  sec. 52.227-19 and subparagraph  *
* (c)(1)(ii) of the Rights in Technical Data and Computer *
* Software clause at DFARS sec. 252.227-7013.             *
*                                                         *
*        Marathon Netowrks, Inc.                          *
*        www.marathonnetworks.com                         *
*        e-mail: support@marathon-networks.com            *
*                                                         *
***********************************************************

Username: sysadmin
Password: <sysadmin>
PVTD#
```

Configure IP addressing and test it:

```
PVTD#set sys_ipv4 10.0.123.207/24
Missing parameters. set sys_ipv4 <ipv4> <netmask>
PVTD#set sys_ipv4 10.0.123.207 255.255.255.0
PVTD#set sys_ipv4_gw 10.0.123.1
PVTD#ping 10.0.123.1
PING 10.0.123.1 (10.0.123.1): 56 data bytes
64 bytes from 10.0.123.1: icmp_seq=0 ttl=255 time=7.725 ms
64 bytes from 10.0.123.1: icmp_seq=1 ttl=255 time=4.467 ms
--- 10.0.123.1 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.467/6.096/7.725/1.629 ms
```

```
PVTD#ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=41 time=104.830 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=41 time=97.512 ms
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 97.512/101.171/104.830/3.659 ms
```

Notice that the CLI can help you with missing or wrong parameters. You can also use *help set* command to see help about the command, or use the TAB key to show completion options.

Configure the hostname and domain, and regenerate the SSH keys and SSL keys:

```
PVTD#set sys_host_name PVTD-Demo
PVTD-Demo#set sys_host_domain mydomain.com
PVTD-Demo#regen ssh
Are you sure?[yes|NO]yes
This will take few minutes. Hang on...
PVTD-Demo#regen ssl
Are you sure?[yes|NO]yes
This will take few minutes. Hang on...
```

Notice that the command prompt changed to “PVTD-Demo”

Change the sysadmin password to *my_secure_password*, and add a new administrative user *pvt_admin* with password *pvt_p@ssw0rd*:

```
PVTD-Demo#set user_password sysadmin my_secure_password
PVTD-Demo#add user pvt_admin
PVTD-Demo#set user_password pvt_admin pvt_p@ssw0rd
PVTD-Demo#set user_group pvt_admin ADMIN
```

Add two more users, one for operators and the other for viewers. Operators can change Private VLAN settings, Viewers can issue *show* commands:

```
PVTD-Demo#add user pvt_operator
PVTD-Demo#set user_password pvt_operator op_pa$$
PVTD-Demo#set user_group pvt_operator OPER
PVTD-Demo#add user pvt_viewer
PVTD-Demo#set user_password pvt_viewer v1ew_p@55
```

Notice that there is no need to configure the group for the *pvt_viewer* users as the default group is VIEWER.

Check configuration using the *show users* command:

```
PVTD-Demo#show conf_users
!
! Users Config
!
add user pvt_admin
set user_group pvt_admin ADMIN
set user_hash pvt_admin 28d432130cb4be....4e15001e031904eb6ee6640920bd3214 b9df595d
add user pvt_operator
set user_group pvt_operator OPER
set user_hash pvt_operator 6ae403894817f2489f4c1bcd8e090f....30c02b8896e15f719 bdfe95b4
add user pvt_viewer
set user_group pvt_viewer VIEWER
set user_hash pvt_viewer 5f19842151c814.....00ff1bbf2b15b3c563a1f8550 c238196c
add user sysadmin
set user_group sysadmin ADMIN
set user_hash sysadmin 69a6e40c5fdedc9d...e6bd85a9d00850c8a86a8ccbb9c 8e0763d9
```

Notice that the passwords are not shown. Users' passwords are not stored anywhere, just a hash and a salt is stored. You can safely copy and paste this configuration to another PVTD device.

Configure SSH to allow hosts from the 10.0.123.0/24 network to access the device using SSH:

```
PVTD-Demo#add ssh_allowedv4 10.0.123.0 255.255.255.0
PVTD-Demo#show conf_ssh
!
! SSH Config
!
add ssh_allowedv4 10.0.123.0 255.255.255.0
PVTD-Demo#show ssh_allowedv4
IPv4            MASKv4
--------------- ---------------
10.0.123.0      255.255.255.0
```

Notice: More than one network can be configured to be allowed to access the device using SSH.

Notice: There are several ways to see the configuration. Both *show conf_ssh* and *show ssh_allowedv4* will show you the allowed SSH table.

SSH to the device from any computer on the 10.0.123.0/24 network. Remember the two phase login. First login with username *marathon* with password *networks*, then login using the users created by the CLI:

```
$ ssh marathon@10.0.123.207
The authenticity of host '10.0.123.207 (10.0.123.207)' can't be established.
ECDSA key fingerprint is 91:50:8e:81:fd:cd:e8:02:30:22:eb:9a:97:07:77:21.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.123.207' (ECDSA) to the list of known hosts.
marathon@10.0.123.207's password: <networks>
Last login: Wed Jun 20 22:04:35 2012 from 10.0.123.204
OpenBSD 5.1 (GENERIC) #160: Sun Feb 12 09:46:33 MST 2012

***********************************************************
*       Marathon Networks Command Line Interface (CLI)    *
*       for PVTD                                          *
*                                                         *
*       Copyright (c) 2012 by Marathon Networks, Inc.     *
*                                                         *
*             Restricted Rights Legend                    *
*                                                         *
* Use,  duplication,  or disclosure by the Government is  *
* subject  to  restrictions as set forth in subparagraph  *
* (c)  of  the Commercial Computer Software - Restricted  *
* Rights  clause at FAR  sec. 52.227-19 and subparagraph  *
* (c)(1)(ii) of the Rights in Technical Data and Computer *
* Software clause at DFARS sec. 252.227-7013.             *
*                                                         *
*        Marathon Netowrks, Inc.                          *
*        www.marathonnetworks.com                         *
*        e-mail: support@marathon-networks.com            *
*                                                         *
***********************************************************

Username: sysadmin
Password: <my_secure_password>
PVTD-Demo#Timeout. Exiting
Connection to 10.0.123.207 closed.
```

Notice that the sessions timed out due to 5 minutes of inactivity.

Configure the internal web server to allow hosts from the 10.0.123.0/24 network to access the device using HTTPS:

```
PVTD-Demo#add web_allowedv4 10.0.123.0 255.255.255.0
PVTD-Demo#set web_enable
PVTD-Demo#show conf_web
!
! Web Config
!
add web_allowedv4 10.0.123.0 255.255.255.0
set web_enable

PVTD-Demo#show web_allowedv4
IPv4            MASKv4
--------------- ---------------
10.0.123.0      255.255.255.0
```

Notice: More than one network can be configured to be allowed to access the device using HTTPS.

Notice: There are several ways to see the configuration. Both *show conf_web* and *show web_allowedv4* will show you the allowed HTTPS table.

To connect to the internal web server, use the following URL https://10.0.123.207.

Notice: The web interface for PVTD is read only.

Private VLAN setup

This section demonstrates Private VLAN setup, which is the core operation of the PVTD device.

PVTD is usually deployed in a redundant setup, where there are two or more PVTDs operating in the same Private VLAN network. Each PVTD should have a unique MAC address for its Private VLAN interface. It is recommended to use the *set mac_address RANDOM* command to set the Private VLAN interface MAC address:

```
PVTD-Demo#set mac_address RANDOM
PVTD-Demo#show conf_global | match mac
set mac_address 404c.6f37.7ad0
```

Configure the Private VLAN tables. Here is a copy of the Private VLAN network to be configured:

Private VLAN network structure

Primary VLAN	Secondary VLAN	Type
10	1000	Isolated
10	1001-1004	Community
11	1100	Isolated
11	1101-1104	Community
12	1200	Isolated
12	1201-1204	Community

Firewall and PVTD IPv4 addresses

Private VLAN	Firewall IPv4 address	PVTD IPv4 address
10	10.10.255.254	10.10.255.220/16
11	10.11.255.254	10.11.255.220/16
12	10.12.255.254	10.23.255.220/16

For each Primary VLAN the following configuration steps are needed:

1. Add the Primary VLAN.
2. Configure PVTD’s IPv4 address and mask.
3. Configure the Firewall’s IPv4 address on that Primary VLAN.
4. Add Secondary VLANs.
5. Configure the Secondary VLANs type.
6. Associate the Secondary VLANs to the Primary VLAN.

Configure the Private VLAN section:

```
PVTD-Demo#add pvlan 10
PVTD-Demo#set pvlan_ipv4 10 10.10.255.220
CMD015-PVLAN_ICM_MASKV4-E Config changed but incomplete. Missing valid IPv4 network mask
PVTD-Demo#set pvlan_maskv4 10 255.255.0.0
CMD008-GWV4_NMASK-E GW IPv4 0.0.0.0 is not in same subnet as PVTD 10.10.255.220. Reconfigure GW IPv4
PVTD-Demo#set pvlan_gwv4 10 10.10.255.254
PVTD-Demo#add svlan vlan 1000-1004
PVTD-Demo#set svlan_type I vlan 1000
PVTD-Demo#set svlan_type C vlan 1001-1004
PVTD-Demo#set svlan_pvlan 10 vlan 1000-1004
PVTD-Demo#add pvlan 11
PVTD-Demo#set pvlan_ipv4 11 10.11.255.220
CMD015-PVLAN_ICM_MASKV4-E Config changed but incomplete. Missing valid IPv4 network mask
PVTD-Demo#set pvlan_maskv4 11 255.255.0.0
CMD008-GWV4_NMASK-E GW IPv4 0.0.0.0 is not in same subnet as PVTD 10.11.255.220. Reconfigure GW IPv4
PVTD-Demo#set pvlan_gwv4 11 10.11.255.254
PVTD-Demo#add svlan vlan 1100-1104
PVTD-Demo#set svlan_type I vlan 1100
PVTD-Demo#set svlan_type C vlan 1101-1104
PVTD-Demo#set svlan_pvlan 11 vlan 1100-1104
PVTD-Demo#add pvlan 12
PVTD-Demo#set pvlan_ipv4 12 10.12.255.220
CMD015-PVLAN_ICM_MASKV4-E Config changed but incomplete. Missing valid IPv4 network mask
PVTD-Demo#set pvlan_maskv4 12 255.255.0.0
CMD008-GWV4_NMASK-E GW IPv4 0.0.0.0 is not in same subnet as PVTD 10.12.255.220. Reconfigure GW IPv4
PVTD-Demo#set pvlan_gwv4 12 10.12.255.254
PVTD-Demo#add svlan vlan 1200-1204
PVTD-Demo#set svlan_type I vlan 1200
PVTD-Demo#set svlan_type C vlan 1201-1204
PVTD-Demo#set svlan_pvlan 12 vlan 1200-1204
```

Notice the error messages. They are generated as a warning that the Primary VLAN configuration is incomplete. For a Primary VLAN configuration to be complete the following 3 parameters are needed to be in sync:

- PVTD’s IPv4 address.
- Network mask.
- Gateway address (usually the Firewall address on that Primary VLAN).

Verify configuration for each Primary VLAN. For example:

```
PVTD-Demo#show conf_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 1000-1004
set svlan_pvlan 10 vlan 1000-1004
set svlan_type C vlan 1001-1004
set svlan_type I vlan 1000
```

Verify that PVTD can reach the Firewall on each and every Primary VLAN:

```
PVTD-Demo#show gwv4_mac 10
CMD003-GWV4_MAC_RPL-I PVLAN 10 GWIPv4 10.10.255.254 MAC 000a.1010.fffe
PVTD-Demo#show gwv4_mac 11
CMD003-GWV4_MAC_RPL-I PVLAN 11 GWIPv4 10.11.255.254 MAC 000a.1011.fffe
PVTD-Demo#show gwv4_mac 12
CMD003-GWV4_MAC_RPL-I PVLAN 12 GWIPv4 10.12.255.254 MAC 000a.1012.fffe
```

Verify that hosts are seen on the network using the *show host* commands:

```
PVTD-Demo#show host_ipv4 *
IP              VLAN MAC            FIRST SEEN        LAST SEEN         LAST CHANGE       LAST ACT
--------------- ---- -------------- ----------------- ----------------- ----------------- ----------
10.10.0.2       1000 000b.1010.0002 20120625 07:00:58 20120625 07:24:45 20120625 07:00:58 ADDED
10.10.1.1       1001 000b.1010.0101 20120625 05:57:27 20120625 07:24:46 20120625 05:57:27 ADDED
10.11.0.5       1100 000b.1011.0005 20120625 07:11:09 20120625 07:25:04 20120625 07:11:09 ADDED
10.11.0.6       1100 000b.1011.0006 20120625 07:16:00 20120625 07:19:49 20120625 07:16:00 ADDED
10.11.1.3       1101 000b.1011.0103 20120625 07:21:20 20120625 07:21:22 20120625 07:21:20 ADDED
10.11.1.4       1101 000b.1011.0104 20120625 05:56:09 20120625 07:15:44 20120625 05:56:09 ADDED
10.11.2.2       1102 000b.1011.0202 20120625 06:13:58 20120625 07:24:22 20120625 06:13:58 ADDED
10.11.2.4       1102 000b.1011.0204 20120625 07:25:04 20120625 07:25:04 20120625 07:25:04 ADDED
10.11.2.5       1102 000b.1011.0205 20120625 07:23:39 20120625 07:24:23 20120625 07:23:39 ADDED
10.11.2.6       1102 000b.1011.0206 20120625 07:17:20 20120625 07:21:36 20120625 07:17:20 ADDED
10.11.3.3       1103 000b.1011.0303 20120625 06:33:33 20120625 07:24:24 20120625 06:33:33 ADDED
10.11.3.6       1103 000b.1011.0306 20120625 06:02:45 20120625 07:24:26 20120625 06:02:45 ADDED
10.11.4.1       1104 000b.1011.0401 20120625 07:16:46 20120625 07:20:43 20120625 07:16:46 ADDED
10.11.4.4       1104 000b.1011.0404 20120625 06:31:32 20120625 07:24:29 20120625 06:31:32 ADDED
10.11.4.6       1104 000b.1011.0406 20120625 07:16:32 20120625 07:20:28 20120625 07:16:32 ADDED
10.12.1.3       1201 000b.1012.0103 20120625 07:10:15 20120625 07:21:57 20120625 07:10:15 ADDED
10.12.1.5       1201 000b.1012.0105 20120625 07:03:11 20120625 07:24:30 20120625 07:03:11 ADDED
10.12.2.1       1202 000b.1012.0201 20120625 06:36:37 20120625 07:24:34 20120625 06:36:37 ADDED
10.12.2.4       1202 000b.1012.0204 20120625 06:56:44 20120625 07:24:35 20120625 06:56:44 ADDED
10.12.3.6       1203 000b.1012.0306 20120625 06:05:06 20120625 07:23:53 20120625 06:05:06 ADDED
10.12.4.4       1204 000b.1012.0404 20120625 06:54:17 20120625 07:24:38 20120625 06:54:17 ADDED
10.12.4.5       1204 000b.1012.0405 20120625 06:59:33 20120625 07:24:39 20120625 06:59:33 ADDED
10.12.4.6       1204 000b.1012.0406 20120625 07:10:31 20120625 07:22:54 20120625 07:13:11 MAC_UPD
```

Notice the last line, where it is indicated by MAC_UPD that the MAC address for 10.12.4.6 was changed on 25JUN2012 07:13:11.

You can view parts of the host table using different *show host* commands and using wildcards. Here are some examples:

```
PVTD-Demo#show host_ipv4 10.11.0.*
IP              VLAN MAC            FIRST SEEN        LAST SEEN         LAST CHANGE       LAST ACT
--------------- ---- -------------- ----------------- ----------------- ----------------- ----------
10.11.0.5       1100 000b.1011.0005 20120625 07:11:09 20120625 07:27:59 20120625 07:11:09 ADDED
10.11.0.6       1100 000b.1011.0006 20120625 07:16:00 20120625 07:28:13 20120625 07:16:00 ADDED
PVTD-Demo#show host_  <tab><tab>
host_ipv4     host_macv4    host_svlanv4
PVTD-Demo#show host_svlanv4 1201
IP              VLAN MAC            FIRST SEEN        LAST SEEN         LAST CHANGE       LAST ACT
--------------- ---- -------------- ----------------- ----------------- ----------------- ----------
10.12.1.3       1201 000b.1012.0103 20120625 07:10:15 20120625 07:21:57 20120625 07:10:15 ADDED
10.12.1.5       1201 000b.1012.0105 20120625 07:03:11 20120625 07:28:07 20120625 07:03:11 ADDED
PVTD-Demo#show host_ipv4 * | match 1104
10.11.4.1       1104 000b.1011.0401 20120625 07:16:46 20120625 07:29:05 20120625 07:16:46 ADDED
10.11.4.4       1104 000b.1011.0404 20120625 06:31:32 20120625 07:29:37 20120625 06:31:32 ADDED
10.11.4.6       1104 000b.1011.0406 20120625 07:16:32 20120625 07:28:51 20120625 07:16:32 ADDED
```

Notice that at this point the PVTD will not send ARP Fixups and its just monitoring the network. To enable ARP Fixup you need to enable it using the *set fixup_enable* command:

```
PVTD-Demo#set fixup_enable
```

It is advised to enable tracking to log all changes in the Private VLAN network. Enable tracking using the *set tracking_enable* command:

```
PVTD-Demo#set tracking_enable
```

You can see the log entries using the *show log* command. It is recommended to filter the *show log* command to show only messages starting with PVTD0:

```
PVTD-Demo#show log | match PVTD0
Jun 20 05:56:22 PVTD pvtd[9976]: PVTD009-PVTD_STARTED-I: PVTD was started
Jun 20 05:56:23 PVTD ifstated: PVTD010-SYS_INTERFACE_UP-I: System interface is up
Jun 25 05:50:57 PVTD ifstated: PVTD012-PVLAN_INTERFACE_UP-I: Private VLAN interface is up
Jun 25 05:53:13 PVTD pvtd[9976]: PVTD001-SUPPRESSED-W: Message ARP002-GW_MAC_CHG-W was suppressed 2
times in the last 8 seconds. Next interval in 16 seconds
Jun 25 07:37:09 PVTD pvtsh.py: PVTSH001-CMD_LOG-I: sysadmin-show log | match PVTD0
Jun 25 07:44:58 PVTD pvtd[9976]: PVTD008-PVTD_TERMINATED-I: PVTD was terminated by SIGTERM
Jun 25 07:44:59 PVTD pvtd[3637]: PVTD009-PVTD_STARTED-I: PVTD was started
Jun 25 07:44:59 PVTD pvtd[3637]: PVTD002-NEW_HOST-I: New host found. SVLAN 1000 MAC 000b.1010.0005 IPv4
10.10.0.5
Jun 25 07:45:08 PVTD pvtd[3637]: PVTD001-SUPPRESSED-W: Message ARP002-GW_MAC_CHG-W was suppressed 2
times in the last 8 seconds. Next interval in 16 seconds
Jun 25 07:45:19 PVTD pvtd[3637]: PVTD002-NEW_HOST-I: New host found. SVLAN 1101 MAC 000b.1011.0104 IPv4
10.11.1.4
Jun 25 07:51:01 PVTD pvtd[3637]: PVTD002-NEW_HOST-I: New host found. SVLAN 1101 MAC 000b.1011.0103 IPv4
10.11.1.3
Jun 25 07:55:06 PVTD pvtd[3637]: PVTD003-DEL_HOST-I: Host deleted due to timeout. SVLAN 1204 MAC
10.12.4.1 IPv4 000b.1012.0401
Jun 25 07:56:25 PVTD pvtd[3637]: PVTD003-DEL_HOST-I: Host deleted due to timeout. SVLAN 1000 MAC
10.10.0.2 IPv4 000b.1010.0002
Jun 25 07:56:51 PVTD pvtd[3637]: PVTD002-NEW_HOST-I: New host found. SVLAN 1204 MAC 000b.1012.0401 IPv4
10.12.4.1
Jun 25 08:00:52 PVTD pvtd[3637]: PVTD002-NEW_HOST-I: New host found. SVLAN 1100 MAC 000b.1011.0003 IPv4
10.11.0.3
Jun 25 08:01:03 PVTD pvtd[3637]: PVTD003-DEL_HOST-I: Host deleted due to timeout. SVLAN 1101 MAC
10.11.1.3 IPv4 000b.1011.0103
Jun 25 08:01:11 PVTD pvtd[3637]: PVTD005-HOST_CHG_MAC-W: Host IPv4 10.12.4.6 has changed its MAC
address. Old MAC 000b.1012.0406 New MAC 000f.1012.0406
Jun 25 08:01:30 PVTD pvtd[3637]: PVTD002-NEW_HOST-I: New host found. SVLAN 1104 MAC 000b.1011.0402 IPv4
10.11.4.2
Jun 25 08:01:51 PVTD pvtd[3637]: PVTD003-DEL_HOST-I: Host deleted due to timeout. SVLAN 1001 MAC
10.10.1.3 IPv4 000b.1010.0103
```

Notice that that the output shown here is truncated to show example entries.

To monitor the Private VLAN interface use the following examples:

```
PVTD-Demo#show stat_interface
interface vr1
 media:   Ethernet autoselect (100baseTX full-duplex)
 status:  active
 stats:   In PKTS: 23881     In ERR: 0         Out PKTS: 23362     Out ERR 0
PVTD-Demo#show stat_top | match CPU states|Memory:
CPU states:  0.1% user,  0.0% nice,  0.1% system,  0.2% interrupt, 99.6% idle
Memory: Real: 26M/206M act/tot Free: 36M Cache: 154M Swap: 0K/65M
PVTD-Demo#show stat_pvtd
Send buffer empty:        0
Send drops:               0
ARP received:             94432
GW Changed:               3
ARP requests sent:        23324
ARP fixup sent:           12
Invalid ARP received:     0
BPF drops:                0
```

Service setup

This section demonstrates configuring the following services:

- SYSLOG
- LLDP
- SNMP
- NTP
- RADIUS

SYSLOG

Add a SYSLOG server to which log messages are sent using the *add syslog_host* command:

```
PVTD-Demo#add syslog_host 10.0.123.211
PVTD-Demo#show syslog_host
Syslog Host
---------------
10.0.123.211
PVTD-Demo#show conf_syslog
!
! Syslog Config
!
add syslog_host 10.0.123.211
```

Notice: SYSLOG messages are sent with LOCAL6 facility.

Notice: All CLI commands are also logged and sent to the configured SYSLOG servers. Passwords are sent stared (*).

Notice: More than one server can be configured.

LLDP

PVTD support both LLDP and CDP. By default LLDP and CDP are not enabled. To enable it use the *set lldp_enable* command:

```
PVTD-Demo#set lldp_enable
PVTD-Demo#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
SW0                 vr0           LLDP    96           BR            Fa0/7
SW0                 vr0           CDP     176          RS            Fa0/7
SW1                 vr1           LLDP    100          BR            Fa0/6
SW1                 vr1           CDP     176          RS            Fa0/6
```

Notice: PVTD sends and receives LLDP messages. Only when PVTD receives a CDP frame on one of its interfaces, it will send CDP advertisements out of the interface.

SNMP

SNMP management stations can query PVTD using standard MIB-2 object, using SNMPv1. PVTD does not support SNMP SET.

There are 3 minimal steps required to configure SNMP:

1. Enable SNMP using the *set snmp_enable* command
2. Configure who is allowed to send SNMP queries using *add snmp_allowedv4* command
3. Configure Read Only community string using the *set snmp_community* command

Configure SNMP:

```
PVTD-Demo#set snmp_enable
PVTD-Demo#add snmp_allowedv4 10.0.123.0 255.255.255.0
PVTD-Demo#set snmp_community mycommunity
PVTD-Demo#show snmp_status
SNMP is enabled
PVTD-Demo#show snmp_allowedv4
IPv4            MASKv4
--------------- ---------------
10.0.123.0      255.255.255.0

PVTD-Demo#show conf_snmp
!
! SNMP Config
!
add snmp_allowedv4 10.0.123.0 255.255.255.0
set snmp_contact
set snmp_description
set snmp_location
set snmp_community mycommunity
set snmp_enable
```

Notice: More than one management servers network can be confgiured.

NTP

Enable NTP using the *set ntp_enable* command and use the *add ntp_host* command:

```
PVTD-Demo#show sys_time
Tue Jun 26 10:02:13 IDT 2012
PVTD-Demo#set ntp_enable
PVTD-Demo#add ntp_host 10.0.123.212
PVTD-Demo#show sys_time
Tue Jun 26 15:25:43 IDT 2012
PVTD-Demo#show ntp_status
NTP is enabled
: 1 out of 1 peers valid
PVTD-Demo#show log | match ntp
Jun 26 10:02:30 PVTD-Demo pvtsh.py: PVTSH001-CMD_LOG-I: sysadmin-set ntp_enable
Jun 26 10:02:37 PVTD-Demo pvtsh.py: PVTSH001-CMD_LOG-I: sysadmin-add ntp_host 10.0.123.212
Jun 26 10:02:37 PVTD-Demo ntpd[9342]: ntp engine exiting
Jun 26 10:02:37 PVTD-Demo ntpd[9306]: dispatch_imsg in main: pipe closed
Jun 26 10:02:37 PVTD-Demo ntpd[26215]: Terminating
Jun 26 10:02:37 PVTD-Demo ntpd[21334]: ntp engine ready
Jun 26 10:02:58 PVTD-Demo ntpd[21334]: peer 10.0.123.212 now valid
Jun 26 10:03:52 PVTD-Demo ntpd[17331]: adjusting local clock by 18384.818727s
Jun 26 15:26:18 PVTD-Demo pvtsh.py: PVTSH001-CMD_LOG-I: sysadmin-show ntp_status
Jun 26 15:26:18 PVTD-Demo ntpd[10077]: 1 out of 1 peers valid
Jun 26 15:26:22 PVTD-Demo pvtsh.py: PVTSH001-CMD_LOG-I: sysadmin-show log | match ntp
```

Notice: It is best to first set the time and date manually using the *set sys_date / set sys_time* commands and then add NTP servers.

Notice: More than one NTP server can be configured.

RADIUS

PVTD can use RADIUS to authenticate users. If PVTD fail to communicate with all the RADIUS servers, it will use the locally configured users to authenticate.

PVTD expects the shell:*priv-lvl*= Cisco AV-Pair to be returned to PVTD to indicate the group the user belong to. Priv 15 is for ADMIN group. Priv 7 is for OPERATOR group. Priv 1 is for VIEWER group.

Enable RADIUS using the *set radius_enable* command and add RADIUS servers using the *add radius_host* command:

```
PVTD-Demo#set radius_enable
PVTD-Demo#add radius_host 10.0.123.210
PVTD-Demo#set radius_password 10.0.123.210 RADPVTD
PVTD-Demo#show conf_radius
!
! Radius Config
!
add radius_host 10.0.123.210
set radius_obscure 10.0.123.210 63716a60786576
set radius_enable
```

Notice that the *set radius_password* command is translated into *set radius_obscure* command, to hide the RADIUS password from over the shoulder glance. It is not encrypted. Keep it safe and secret.

Example for FreeRadius configurations:

```
client PVTD_DEMO {
        ipaddr = 10.0.123.207
        secret = RADPVTD
        require_message_authenticator = no
        nastype = other
}
myadmin   Cleartext-Password := "myadminpass"
      Service-Type = NAS-Prompt-User,
      cisco-avpair = "shell:priv-lvl=15"
myoper   Cleartext-Password := "myoperpass"
      Service-Type = NAS-Prompt-User,
      cisco-avpair = "shell:priv-lvl=7"
myview   Cleartext-Password := "myviewpass"
      Service-Type = NAS-Prompt-User,
      cisco-avpair = "shell:priv-lvl=1"
```

Login example:

```
Last login: Tue Jun 26 21:19:46 2012 from 10.0.123.2
OpenBSD 5.1 (GENERIC) #160: Sun Feb 12 09:46:33 MST 2012

***********************************************************
*       Marathon Networks Command Line Interface (CLI)    *
*       for PVTD                                          *
*                                                         *
*       Copyright (c) 2012 by Marathon Networks, Inc.     *
*                                                         *
*             Restricted Rights Legend                    *
*                                                         *
* Use,  duplication,  or disclosure by the Government is  *
* subject  to  restrictions as set forth in subparagraph  *
* (c)  of  the Commercial Computer Software - Restricted  *
* Rights  clause at FAR  sec. 52.227-19 and subparagraph  *
* (c)(1)(ii) of the Rights in Technical Data and Computer *
* Software clause at DFARS sec. 252.227-7013.             *
*                                                         *
*        Marathon Netowrks, Inc.                          *
*        www.marathonnetworks.com                         *
*        e-mail: support@marathon-networks.com            *
*                                                         *
***********************************************************

Username: myadmin
Password: <myadminpass>
PVTD-Demo#show whoami
Username: myadmin Group: ADMIN
```

Final Configuration

```
PVTD-Demo#show conf_all
!
! General configuration
!
set mac_address 404c.6f37.7ad0
set arp_timeout 600
set interface vr1
set fixup_enable
set tracking_enable
set lldp_enable
!
! System configuration
!
set sys_time_zone Asia_Jerusalem
set sys_host_name PVTD-Demo
set sys_host_domain mydomain.com
set sys_ipv4 10.0.123.207 255.255.255.0
set sys_ipv4_gw 10.0.123.1
set sys_interface_speed auto
set sys_interface_duplex full
set interface_speed auto
set interface_duplex full
!
! Users Config
!
add user pvt_admin
set user_group pvt_admin ADMIN
set user_hash pvt_admin 28d432130cb4be9346fac87b7735d0064e15001e031904eb6ee6640920bd3214 b9df595d
add user pvt_operator
set user_group pvt_operator OPER
set user_hash pvt_operator 6ae403894817f2489f4c1bcd8e090f99265909b7839f96a30c02b8896e15f719 bdfe95b4
add user pvt_viewer
```

```
set user_group pvt_viewer VIEWER
set user_hash pvt_viewer 5f19842151c8147ea189f66faa52bdd038e708f00ff1bbf2b15b3c563a1f8550 c238196c
add user sysadmin
set user_group sysadmin ADMIN
set user_hash sysadmin 3a2867f3f2249afdd579737707de7a12f517efba66c46f3b7550b38d87db19aa be37d25e
!
! Radius Config
!
add radius_host 10.0.123.210
set radius_obscure 10.0.123.210 63716a60786576
set radius_enable
!
! SSH Config
!
add ssh_allowedv4 10.0.123.0 255.255.255.0
!
! SNMP Config
!
add snmp_allowedv4 10.0.123.0 255.255.255.0
set snmp_contact
set snmp_description
set snmp_location
set snmp_community mycommunity
set snmp_enable
!
! Syslog Config
!
add syslog_host 10.0.123.211
!
! NTP Config
!
add ntp_host 10.0.123.212
set ntp_enable
!
! 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 1000-1004
set svlan_pvlan 10 vlan 1000-1004
set svlan_type C vlan 1001-1004
set svlan_type I vlan 1000
!
! PVLAN 11
!
add pvlan 11
set pvlan_ipv4 11 10.11.255.220
set pvlan_maskv4 11 255.255.0.0
set pvlan_gwv4 11 10.11.255.254
add svlan vlan 1100-1104
set svlan_pvlan 11 vlan 1100-1104
set svlan_type C vlan 1101-1104
set svlan_type I vlan 1100
!
! PVLAN 12
!
add pvlan 12
set pvlan_ipv4 12 10.12.255.220
set pvlan_maskv4 12 255.255.0.0
set pvlan_gwv4 12 10.12.255.254
add svlan vlan 1200-1204
set svlan_pvlan 12 vlan 1200-1204
set svlan_type C vlan 1201-1204
set svlan_type I vlan 1200
```

```
!
! Unassociated SVLAN
!
```

Factory default

The are two types of factory default:

- Deleting Private VLAN configuration and services configurations using the *del conf_all* command
- Reset to Factory default, which resets the device as if it is a new device, deleting all system configuration, all logs and all internal data.

Deleting Private VLAN configuration and service configurations

Use the *del conf_all* command to clear all Private VLAN related configuration

```
PVTD-Demo#del conf_all
Confirm deletion of all configuration [NO|yes]yes
PVTD-Demo#show conf_all
!
! General configuration
!
set mac_address 404c.6ff3.6fdc
set arp_timeout 600
set interface vr1
set fixup_disable
set tracking_disable
set lldp_disable
!
! System configuration
!
set sys_time_zone Asia_Jerusalem
set sys_host_name PVTD-Demo
set sys_host_domain mydomain.com
set sys_ipv4 10.0.123.207 255.255.255.0
set sys_ipv4_gw 10.0.123.1
set sys_interface_speed auto
set sys_interface_duplex full
set interface_speed auto
set interface_duplex full
!
! Users Config
!
add user sysadmin
set user_group sysadmin ADMIN
set user_hash sysadmin 128284c866702b5002f6828f0bafeb545085e6ed6b88091c4fed83e706d57b36 631bf078
!
! Radius Config
!
set radius_disable
!
! SSH Config
!
!
! SNMP Config
!
set snmp_contact
set snmp_description
set snmp_location
set snmp_community
set snmp_disable
!
! Syslog Config
```

```
!
!
! NTP Config
!
set ntp_disable
!
! Unassociated SVLAN
!
```

Notice: This command will also generate a random MAC address for ARP Fixup.

Reset to factory default

Resetting to factory default can only happen when using the serial port, or from the VM's Console and only during the first 10 minutes after booting the device.

To reset to factory default, login using *recovery* username and *recovery* password

```
login: marathon
Password: <networks>
Last login: Fri Jun 29 00:47:20 on tty00
OpenBSD 5.1 (GENERIC) #160: Sun Feb 12 09:46:33 MST 2012

***********************************************************
*       Marathon Networks Command Line Interface (CLI)    *
*       for PVTD                                          *
*                                                         *
*       Copyright (c) 2012 by Marathon Networks, Inc.     *
*                                                         *
*             Restricted Rights Legend                    *
*                                                         *
* Use,  duplication,  or disclosure by the Government is  *
* subject  to  restrictions as set forth in subparagraph  *
* (c)  of  the Commercial Computer Software - Restricted  *
* Rights  clause at FAR  sec. 52.227-19 and subparagraph  *
* (c)(1)(ii) of the Rights in Technical Data and Computer *
* Software clause at DFARS sec. 252.227-7013.             *
*                                                         *
*        Marathon Netowrks, Inc.                          *
*        www.marathonnetworks.com                         *
*        e-mail: support@marathon-networks.com            *
*                                                         *
***********************************************************

Username: recovery
Password: <recovery>
PVTD will erase configurations. Continue [NO|yes]yes
######################Recovery completed. Rebooting
```