PVTD - Technical Data Sheet

www.marathon-networks.com

Marathon Networks' PVTD appliance - brings order to your private VLAN networks.

Overview

Private VLANs are deployed in various networks to provide high security and micro segmentation.

However, Private VLANs come with a price. There are many challenges when deploying and operating Private VLANs. Marathon Networks' PVTD appliance helps with a successful implementation of Private VLAN networks and ease their operation.

Private VLAN challenges

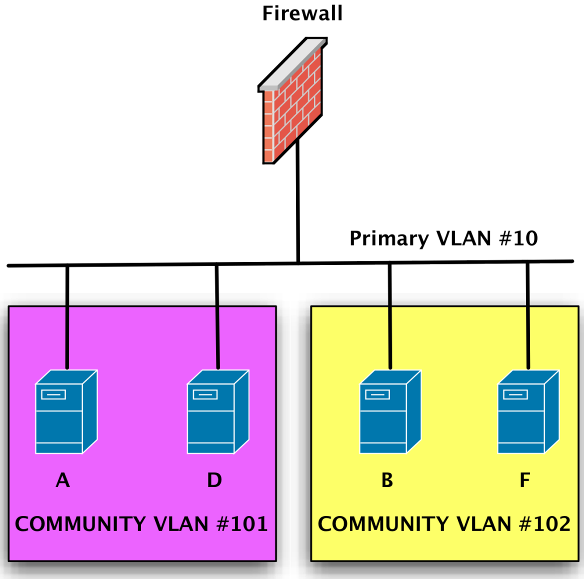
Private VLANs provide many security benefits, unfortunately they are not easy to implement and support.

Manually configured routes on hosts

Look at the diagram. When server A want to communicate with server B, server A will naturally try to send an ARP searching for server B. Since server B is on a different Community VLAN, it will never receive the request, nor will it be able to send a reply.

In order for the two to talk with each other through the FW, server A needs a manual configuration of a route to server B via the firewall, and the same for server B. Server B also needs to be manually configured with a route to A via the firewall.

For some servers, like a DNS server or a central SQL server, there might be tens or even hundreds of manually configured routes causing operational and maintenance burden.



What happens when a new server is added or reinstalled, what manual routes are needed to be configured? What other hosts are expected to connect the new server, and what manual routes are needed to configured over there?

Manually configured routes are very hard to configure and operate. Private VLAN networks starting small are later grow to be one large manually configured monstrosity.

Real time mapping

The typical process for finding out to which Secondary VLAN a host belongs is very cumbersome.

The server team supply the IP address, then Security team SSH to the firewall to find the ARP mapping for the host, and finally, the networking team use the MAC address to locate the port and look at its configuration.

A simple question like to which Secondary VLAN a hosts belongs, turns into a laborious interdepartmental process.

No History

“What happened to my DNS connection? Yesterday it worked! Could somebody have moved my server to a new Community VLAN?”

Since there is no mapping, there is no history. With no history, its very hard for the server admins to remember to which Community VLAN the server should be returned to.

Complicated troubleshooting

When Private VLAN blocks traffic, there is no log entry, or any other indication of its silent operation.

For example, a connection to the SQL server is not working. The server team call the security team, but the security team see no log entries for the request. After long troubleshooting process, the networking team is called in to check that perhaps Private VLANs are to blame.

The most typical Private VLAN problems are caused by missing manually configured routes on hosts and hosts misplaced into the wrong Secondary VLAN. However, without proper tools it is hard to detect those problems.

Key benefits

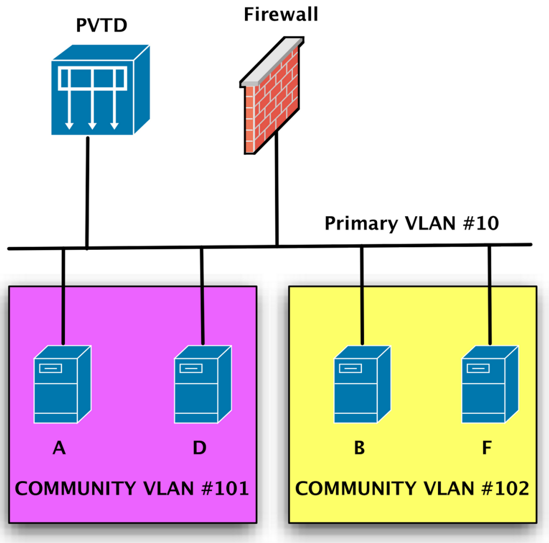
Marathon Networks’ PVTD appliance has three key features to help with Private VLAN challenges.

ARP Fixup

Host A send an ARP request for host B. Since host B is on another Community VLAN it will never be able to receive the ARP request. Host A and host B must communicate through the firewall.

When PVTD sees such an ARP request, it will send an ARP Fixup to host A, telling it that to reach host B, it must use the MAC address of the firewall as its destination.

ARP Fixup brings the end to manually configured routes on hosts. All inter Secondary VLAN or intra Isolated VLAN traffic will automatically go through the firewall, without any manual configuration on the hosts.



Real time mapping

PVTD maps all IP addresses, to their MAC and Secondary VLAN assignments.

There is no need to manually track the host to find to which Secondary VLAN it belongs.

The mapped data can be accessed by the servers team, the security team and the networking team. No need for unnecessary phone calls to other IT departments for the simple task of finding to which Secondary VLAN a server belongs.

Private VLAN history

PVTD can create a log entry when hosts are added, removed or change their Secondary VLAN mappings.

Viewing the Private VLAN history of a host is very simple, no more guessing...

How It works

Connect

Connect one PVTD's port to the Private VLAN network, and connect the other port to a management network.

Since traffic is not passing through the PVTD appliance, the bandwidth requirements are very low.

Configure

There are 3 configuration steps:

1. Configure system settings, such as management IP address, users and SSH access
2. Configure the Private VLAN structure to reflect your network
3. Configure additional services, such as SYSLOG, NTP and RADIUS

Relax

Let PVTD do all the hard work for you.

Models

PVTD-5K01R

- Up to 5000 hosts per device
- 19” rack mountable.
- No moving parts.
- Low power consumption: 40 Watt Max
- Operation temperature: 0-60 C
- Optical port optional.

PVTD-5H01R

- Up to 500 hosts per device
- Small form factor.
- No moving parts.
- Low power consumption: 15 Watt Max
- Operation temperature: 0-60 C

PVTD-VR

vmware®

- VMWare Virtual Appliance
- vDS and Nexus1000V compatible