Enhancing Security with Dell Networking OS 5.x and Above Part I - Private VLAN

A guide to basic security deployment practices for Dell Networking switches using the Private VLAN feature

Version 2.1

Dell Engineering
March 2014

A Dell EMC Deployment and Configuration Guide

Revisions

Date	Description	Authors
March 2014	2.1 Added support for Dell Networking firmware beyond 5.x; Added support for new Dell Networking switches; Fixed error in show command	Victor Teeter
July 2013	2.0 Initial release	Andrew Berry, Victor Teeter

Table of contents

Revisions....2
Executive Summary....4
1 Overview....5
2 Application....6
2.1 Port types....6
2.2 VLAN types....6
2.3 Controlling Access....8
3 Private VLAN Example....9
3.1 Command-line configuration....10
A Definitions....12

Executive Summary

The importance of network security features cannot be overemphasized due to the growing amount of traffic and applications that depend on the network. This includes secure communication paths as well as stable platforms to maintain the paths. Dell Networking switches include security features for monitoring, classifying and manipulating network traffic passing through the switch. The switches also provide security for the users accessing the switch.

When several devices communicate within a Layer 2 broadcast domain DMZ, it is possible for a rogue device to introduce itself into a VLAN and cause serious security issues on the network. This issue can be solved using the Private VLAN Feature.This feature is one of the enhancements to the security portfolio of Dell EMC Networking platforms. Using Private VLANs allows the network administrator to control which VLANs and servers customers are allowed to access at the DMZ, while limiting or prohibiting those same VLANs and servers from communicating with each other except as required. This prevents inadvertent sharing of servers and services to rogue users on the network. Support for this feature is included in most Dell Networking switches loaded with version 5.0 or later.

1 Overview

When several devices communicate with a Layer 2 broadcast domain DMZ, it is possible for a rogue device to introduce itself into a VLAN and cause serious security issues on the network. The previous solution to this problem was to assign a separate VLAN to each user. This resulted in a network that required many VLANs, was difficult to scale, and made IP address management more complicated. Using private VLANs (or PVLANs) addresses the Layer 2 security, without scalability issues, and provides IP address management benefits for service providers.

Advantages of deploying private VLANs in a multi-server network include enhanced security, reduction in IP address space usage, administrative accessibility, less L3 routing, and fewer VLANs. To take advantage of these features, the Dell Networking firmware (starting with version 5.0) allows private VLANs to be configured.

Private VLANs partition a standard VLAN domain into two or more subdomains. Each subdomain is defined by a primary VLAN and a secondary VLAN. The primary VLAN ID is the same for all subdomains that belong to a particular private VLAN instance. The secondary VLAN ID differentiates the subdomains from each other and provides layer 2 isolation between ports on the same private VLAN.

Private VLANs are available on the following Dell Networking OS switches:

N4064	4064F	N4032	N4032F	N3048	N3048P
N3024	N3024P	N2048	N2048P	N2024	N2024P
8164	8164F	8132	8132F	7048	7048P
7048R	7048R-RA	7024	7024P	7024F	8024
8024F	M8024-K	M8024	M6348		

Note: While private VLANS are also available on the Dell Networking 3000 and 5000 series and FTOS platforms, the technology and commands for these systems are not covered in this document.
For configuring PVLANs on those switches, refer to the configuration guides for each available at http://www.dell.com/support/home/us/en/19?c=us&l=en&s=dhs#19/Products/ser_stor_net/networking?&_suid=139360615138706634409444907718

Note: XGS3 silicon based switches (M6220 and 6200) do not support the PVLAN feature.

2 Application

Private VLANs are typically deployed at the edge of a server farm DMZ, where it is desired to limit or prohibit servers from communicating. While isolation of traffic can be achieved by assigning each host connected port a unique L3 VLAN and enabling L3 routing between the VLANs, it is very inefficient in most cases.

Private VLANs:

- reduce the IP address space utilization
- avoid inefficient L3 routing at the edge
- reduces consumed VLANs through common VLAN allocation

Note: Dell Networking also allows Private VLAN configuration on port channels, which is useful for promiscuous ports.

2.1 Port types

There are three port roles associated with private VLANs.

A **promiscuous port** is associated with a primary VLAN, and is able to communicate with all interfaces in the private VLAN, including other promiscuous ports, community ports and isolated ports.

A **host port** is associated with a secondary VLAN. If the secondary VLAN is a *community* VLAN the port can communicate with the promiscuous ports in the VLAN and other ports in the same community. If the secondary VLAN is an *isolated* VLAN, then the port can communicate only with promiscuous ports.

A **community port** is a member of the community VLAN. It can communicate with the promiscuous ports in the primary VLAN and other ports in the same community.

2.2 VLAN types

There are two major VLAN types associated with private VLANs.

A **primary VLAN** (Figure 1) carries unidirectional traffic downstream from promiscuous ports to all other ports (isolated ports, community ports and other promiscuous ports) in the same private VLAN. Only one primary VLAN can be configured per private VLAN. Every port in a private VLAN is a member of the primary VLAN.

Another way to think of it from a switch perspective is that the primary VLAN *is* the private VLAN. There can be several private VLANs on a single switch or switch stack.

A **secondary VLAN** communicates only with other secondary VLANs within the primary VLAN of which it is assigned. There are two types of secondary VLANS.

- An **isolated VLAN** is a secondary VLAN that carries unidirectional traffic upstream from the isolated hosts toward the promiscuous ports and the gateway. Communication among hosts in the isolated VLAN is forbidden. Only one isolated VLAN can be configured per private VLAN.
- A **community VLAN** is a secondary VLAN that carries upstream traffic from the community ports to the promiscuous port gateways and to other host ports in the same community. There can be multiple community VLANs per private VLAN.

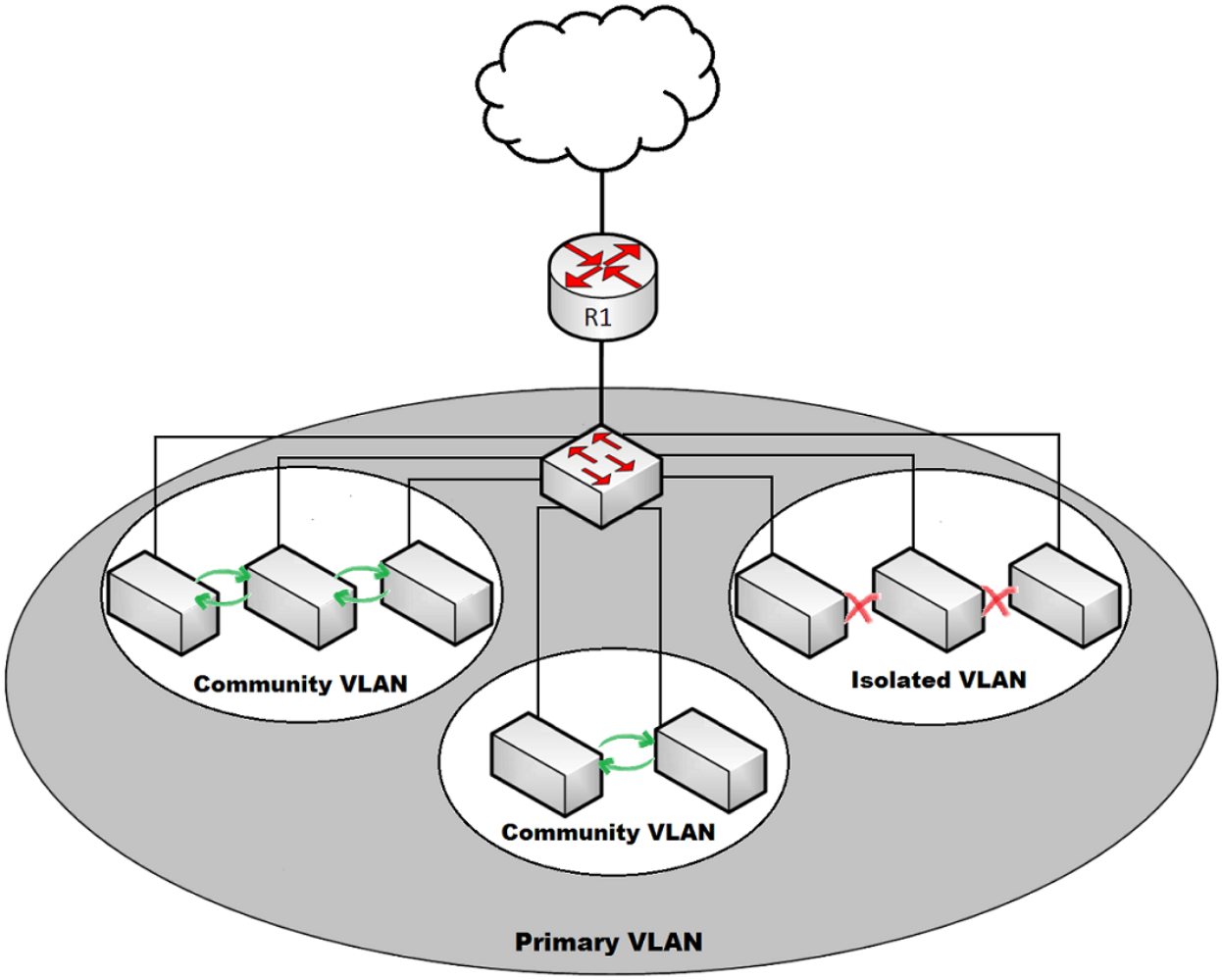

Figure 1 Logical view of primary and secondary VLANs

2.3 Controlling Access

Private VLANs can control access to end stations through the following methods:

- Configuring selected interfaces connected to end stations as isolated ports to prevent any communication at Layer 2. For example, if the end stations are servers, this configuration prevents Layer 2 communication between the servers.

- Configuring interfaces connected to default gateways and selected end stations (ex. backup servers) as promiscuous ports to allow all end stations access to a default gateway.

A promiscuous port can serve only one primary VLAN, one isolated VLAN, and multiple community VLANs. Layer 3 gateways are typically connected to the switch through a promiscuous port. With a promiscuous port, you can connect a wide range of devices as access points to a private VLAN. For example, you can use a promiscuous port to monitor or back up all the private-VLAN servers from an administration workstation.

In a switched environment, you can assign an individual private VLAN and associated IP subnet to each individual or common group of end stations. To communicate outside the private VLAN, the end stations only need to communicate with a default gateway.

3 Private VLAN Example

In this example, TE1/1/1 (SW1 to R1) is configured as a promiscuous port. Hosts A, D, and E can only talk via R1, and hosts B and C can talk to each other directly as well as via R1. The isolated VLAN is shown three times to demonstrate the forbidden communication between the three hosts (A, D, and E), however, all three hosts are in the same isolated VLAN.

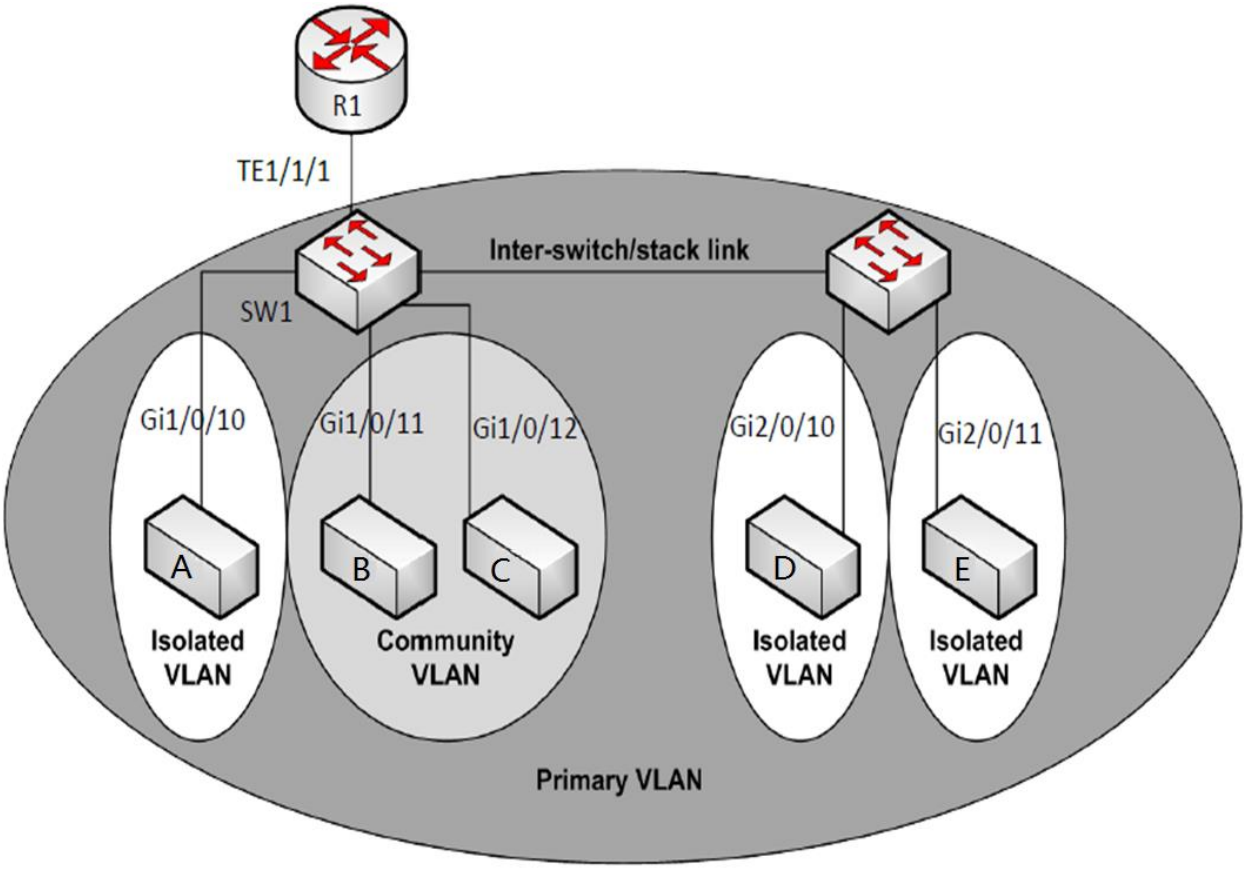

Figure 2 Physical view of primary and secondary VLANs on a switch stack

3.1 Command-line configuration

Use the commands below to configure the example given above.

Note: The commands for different devices sometimes vary slightly. If uncertain, consult the device's User Guide for the exact commands pertaining to your particular device.

Create the VLAN and assign VLAN types

```
console# configure
console(config)# vlan 100
console(config-vlan-100)# private-vlan primary
console(config-vlan-100)# exit
console(config)# vlan 101
console(config-vlan-101)# private-vlan community
console(config-vlan-101)# exit
console(config)# vlan 102
console(config-vlan-102)# private-vlan isolated
console(config-vlan-102)# exit
```

Associate the community and isolated VLANs with the primary VLAN

```
console(config)# vlan 100
console(config-vlan-100)# private-vlan association 101-102
console(config-vlan-100)# exit
```

Assign the router connected port to the primary VLAN

```
console(config)#interface te1/1/1
console(config-if-Te1/1/1)#switchport mode private-vlan promiscuous
console(config-if-Te1/1/1)#switchport private-vlan mapping 100 101-102
console(config-if-Te1/1/1)#exit
```

Assign the community VLAN ports

```
console(config)#interface gi1/0/11
console(config-if-Gi1/0/11)#switchport mode private-vlan host
console(config-if-Gi1/0/11)#switchport private-vlan host-association 100 101
console(config-if-Gi1/0/11)#interface gi1/0/12
console(config-if-Gi1/0/12)#switchport mode private-vlan host
console(config-if-Gi1/0/12)#switchport private-vlan host-association 100 101
```

Assign the isolated VLAN ports

```
console(config)#interface gi1/0/10
console(config-if-Gi1/0/10)#switchport mode private-vlan host
console(config-if-Gi1/0/10)#switchport private-vlan host-association 100 102
console(config-if-Gi1/0/10)#interface gi2/0/10
console(config-if-Gi2/0/10)#switchport mode private-vlan host
console(config-if-Gi2/0/10)#switchport private-vlan host-association 100 102
console(config-if-Gi2/0/10)#interface gi2/0/11
console(config-if-Gi2/0/11)#switchport mode private-vlan host
console(config-if-Gi2/0/11)#switchport private-vlan host-association 100 102
```

Confirm the Private VLAN settings with "show" commands

```
console(config)#show vlan private-vlan type
VLAN  Type
-------  -----------------------
100      primary
101      community
102      isolated


console(config)#show vlan private-vlan

Primary VLAN   Secondary VLAN   Type          Ports
-------------  --------------   ------------  -------------------------
100            102               Isolated        Gi1/0/10,Gi2/0/10-11,Te1/1/1
100            101               Community       Gi1/0/11-12,Te1/1/1

console(config)#show vlan
      VLAN        Name          Ports            Type
      ----     ---------    ------------        -----------
      1           default      Po1-128,         Default
                               Gi1/0/1-9,
                               Gi1/0/13-24,
                               Gi2/0/1-9,
                               Gi2/0/12-24
                               Fo1/1/2,
                               Te1/1/2-4

      100         VLAN0100     Gi1/0/10-12,     Static
                               Gi2/0/10-11
                               Te1/1/1
      101         VLAN0101     Gi1/0/11-12,     Static
                               Te1/1/1
      102         VLAN0102     Gi1/0/10,        Static
                               Gi2/0/10-11,
                               Te1/1/1
```

A Definitions

Community port: A member of the community VLAN. It can communicate with the promiscuous ports in the primary VLAN and other ports in the same community.

Community VLAN : A secondary VLAN. It carries upstream traffic from the community ports to the promiscuous port gateways and to other host ports in the same community. There can be multiple community VLANs per private VLAN.

DMZ : The area of an organization's network that is exposed to an untrusted network (such as the internet) in order to provide services to customers. Typically, legitimate patrons as well as rogue users have access to equipment in the DMZ.

Host port: A port associated with a secondary VLAN (isolated or community) in a private VLAN.

Isolated VLAN : A secondary VLAN. It carries unidirectional traffic upstream from the isolated hosts toward the promiscuous ports and the gateway. Communication among hosts in the isolated VLAN is forbidden. Only one isolated VLAN can be configured per private VLAN.

Isolated port : A member of the isolated VLAN. It carries unidirectional traffic upstream from the isolated hosts toward the promiscuous ports and the gateway.

Private VLAN : Contains a single primary VLAN and one or more secondary VLANs. In a multi-server network DMZ, it is a preferred method used to enhance security.

Promiscuous port : A port associated with a primary VLAN, able to communicate with all other interfaces.

Primary VLAN : Carries unidirectional traffic from promiscuous ports to all other ports (isolated, community, promiscuous) in the same private VLAN.

Rogue device : Any unauthorized host on a network, but particularly that with a malicious intent.

Secondary VLAN : Can be either a community VLAN or an isolated VLAN.

VLAN : Virtual local area network, or virtual LAN. Is the concept of partitioning a physical network in order to create separate broadcast domains.

For more information on Dell Networking products and features, visit www.dell.com/networking.