VLAN-Based Network Segmentation

This Application Note relates to the following Dell PowerConnect™ products:

- PowerConnect 33xx
- PowerConnect 52xx

Abstract

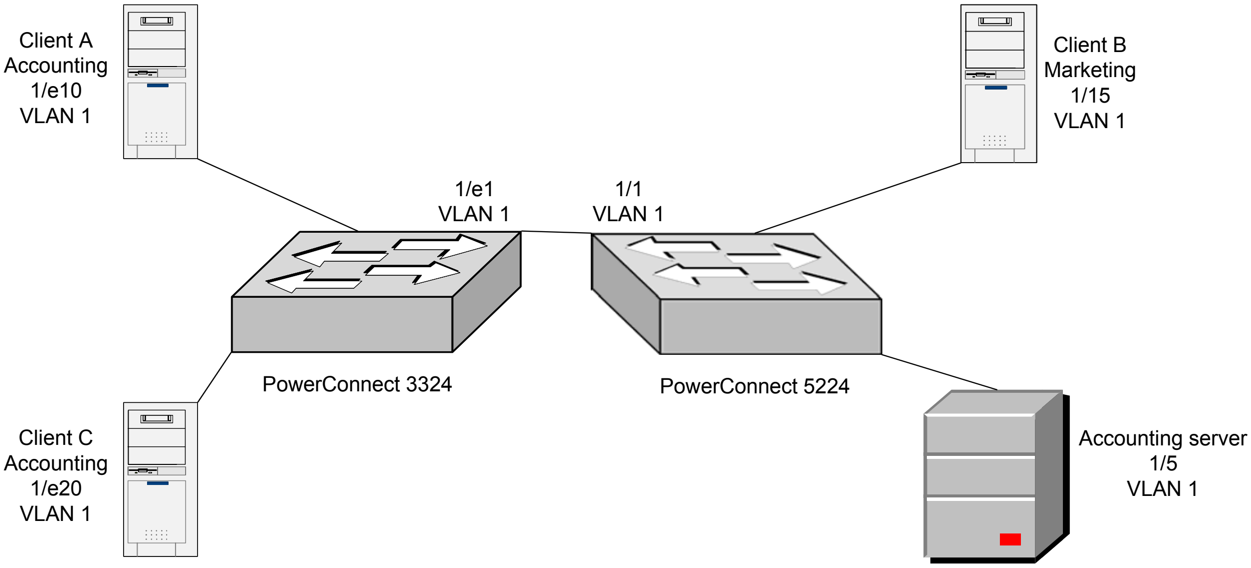
This Application Note explains the benefits of using virtual local area networks (VLANs) to segment a switched network. This document describes VLAN fundamentals and provides configuration instructions for setting up multiple VLANs on Dell PowerConnect switches.

Applicable Network Scenarios

VLANs are useful in situations where the need exists to separate the *logical* topology of network segments from the *physical* topology. For example, VLANs can be used to restrict a broadcast domain to a given workgroup, enhancing both security and performance.

The following diagram shows a switched network using Dell PowerConnect 33xx and 52xx switches in a default VLAN configuration. Client A from the accounting workgroup requires access to a central server, while Clients B and C from the marketing workgroup should not have access to the accounting server.

Note that all switch interfaces are members of VLAN 1.This is the default configuration for all Dell PowerConnect switches. Since all switch interfaces are members of VLAN 1 by default, all nodes attached to both switches are members of the same broadcast domain. This configuration provides no data privacy and it can degrade application performance. Security may be compromised because Clients B and C can see network traffic from the accounting workgroup. Performance suffers because all nodes attached to



both switches must process all broadcast frames. Broadcast traffic also can contribute to excessive network utilization.

Technology Background

A VLAN is a single logical broadcast domain comprised of interfaces on one or more switches. Not all interfaces on a switch must be members of a given VLAN; in fact, a major benefit of VLANs is the ability to subdivide one physical switch into multiple logical networks. The “virtual” aspect of VLANs is that they enable the construction of multiple virtual networks from one physical switch, or vice versa; a single VLAN may span multiple physical switches through the use of trunk links between the switches. VLANs can be used to logically segment groups of connected nodes into individual broadcast domains.

The VLAN implementation in Dell PowerConnect switches is based on the IEEE 802.1Q standard. As such, VLANs is an Ethernet mechanism, meaning it works at layer 2 of the seven-layer ISO model.

Any inter-VLAN traffic must first traverse a layer-3 device such as a router in order to communicate with another VLAN. Thus, logical segmentation not only optimizes bandwidth utilization, but also provides security by isolating segments behind layer-3 devices, which typically can filter traffic using access control lists (ACLs). Even if two nodes share a common IP subnet, they will not be able to directly communicate if they are in separate VLANs.

The IEEE 802.1Q standard describes a tagging mechanism that allows switches to differentiate frames based on a 12-bit VLAN ID (VID) field. Tagging is useful on trunk interfaces that connect the Dell PowerConnect switch to a neighboring 802.1Q-compliant router or switch. With tagging, the two devices can logically separate traffic from different VLANs.

Depending on configuration, a Dell PowerConnect switch will either keep or strip off the tag of an inbound tagged frame. If the ingress interface (the interface on which a frame arrives) is configured as a member of an untagged VLAN, the switch will strip off the frame’s tag before transmitting it. On the other hand, if the interface is configured as a member of a tagged VLAN (for example, if the interface is part of a trunk link between switches), the switch will not remove the frame’s tag before transmitting it.

Dell PowerConnect 33xx series switches offer three main modes for handling VLAN traffic on a given interface. *Access mode* specifies a single, untagged VLAN to which the interface belongs; this is useful for when the attached node is an end-station. *General mode* allows the administrator to configure multiple VLANs that can be either tagged or untagged; this is useful for nodes that must communicate on more than one VLAN. *Trunk mode* inserts an 802.1Q-compliant VLAN tag into all frames; this is useful for trunk links that connect the Dell PowerConnect switch with another 802.1Q-compliant switch or router.

Dell PowerConnect 52xx switches do not support general mode. However, the 52xx series switches allow multiple VLANs to be added in access mode.

When a frame enters an interface in access mode or general mode, the switch assigns the frame the default port VLAN identifier (PVID) specified for that interface and performs a lookup in its VLAN-aware media access control (MAC) table. If the ingress interface is in access mode, the switch verifies the destination is in the same VLAN. If the ingress interface is in general mode, the switch verifies the VLAN exists.

The switch then forwards the frame if the destination is valid or discards it if not. If the destination (egress) interface is in access mode, the switch strips off the 802.1Q tag before transmitting the frame. If the destination interface is in general mode and the target VLAN is configured as tagged, the switch forwards the frame with its VLAN tag intact.

All traffic entering and leaving a trunk interface must be tagged. Interfaces configured for trunk mode or general mode can be configured with a port VLAN ID (PVID) that specifies a default VLAN to use for tagging if the frame is untagged upon entry.

Dell PowerConnect switches use ingress filtering to discard frames belonging to VLANs that are not associated with the ingress interface. Ingress filtering is enabled by default and can only be disabled on interfaces configured in general mode.

Proposed Solution

To optimize bandwidth utilization and help secure sensitive data, we will segment the network into two separate VLANs, one for each department. The central fileserver will have access to both VLANs.

Overview
To implement VLANs on Dell PowerConnect switches, use the following steps:

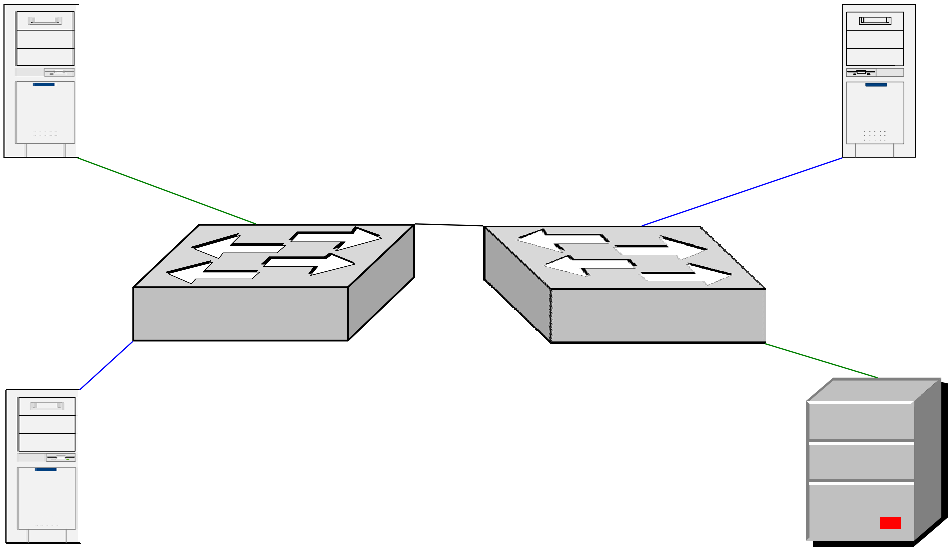
On Dell PowerConnect switches:

1. Create VLANs in the VLAN database.
2. Configure interfaces associated with end-stations for access mode and their respective VLANs.
3. Configure interface associated with the server for general mode and respective VLANs.
4. Place uplink interfaces into trunking mode.

Note: This example assumes a network consisting of two switching connected with a trunk link. For a single-switch network, omit step 4 above.

Typical Network Designs

We will set up one VLAN for each department. We assign accounting to VLAN 10 and marketing to VLAN 20. The accounting server's associated switch interface will be placed in general mode and have access to the accounting VLAN, enhancing security and performance.



Step-By-Step Instructions

The following configuration guidelines work with any Dell PowerConnect 33xx or 52xx switch.

1. Create VLANs 10 and 20.

PowerConnect 33xx:

```
console> en
console# config
console(config)# vlan database
console(config-vlan)# vlan 10
console(config-vlan)# vlan 20
```

PowerConnect 52xx:

```
console# config
console(config)# vlan database
console(config-vlan)# vlan 10 name vlan_10 media ethernet
console(config-vlan)# vlan 20 name vlan_20 media ethernet
console(config-vlan)# exit
```

2. Configure interfaces associated with end-stations for access mode and their respective VLANs:

PowerConnect 33xx:

```
console(config)# interface ethernet 1/e10
console(config-if)# switchport access vlan 10
console(config-if)# exit
console(config)# interface ethernet 1/e20
console(config-if)# switchport access vlan 20
console(config-if)# exit
```

PowerConnect 52xx:

```
console(config)# interface ethernet 1/15
console(config-if)# switchport allowed vlan add 20
console(config-if)# switchport native vlan 20
console(config-if)# exit
```

3. Configure the interface associated with server for general mode and VLAN 10.

PowerConnect 33xx:
(**Note:** The example assumes the server is attached to a Dell PowerConnect 52xx switch. The following configuration commands are not used in the example, and are given only for the sake of completeness.)

```
console(config)# interface ethernet 1/e5
console(config-if)# switchport mode general
console(config-if)# switchport general allowed vlan add 10 untagged
```

PowerConnect 52xx:
(Note: PowerConnect 52xx switches do not support general mode. Instead, we simply add VIDs to the list of allowed untagged VLANs)

```
console(config)# interface ethernet 1/e5
console(config-if)# switchport allowed vlan add 10 untagged
```

4. Place uplink interfaces into trunking mode. (**Note:** Omit this step for a single-switch network.)

PowerConnect 33xx:

```
console(config)# interface ethernet 1/e1
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 10,20
console(config-if)# exit
```

PowerConnect 52xx

```
console(config)# interface ethernet 1/1
console(config-if)# switchport mode trunk
console(config-if)# switchport allowed vlan add 10,20 tagged
console(config-if)# exit
```

Conclusion

We have set up VLANs and separated traffic between the accounting and marketing workgroups. As a result, Clients B and C can no longer see Client A and vice versa. Further, Clients B and C can no longer reach the accounting server. The two VLANs have isolated the accounting workgroup's sensitive data from the rest of the network. The two VLANs also segregate broadcast traffic, helping to reduce bandwidth consumption and processing overhead on both segments.

Information in this document is subject to change without notice.

This Application Note is for informational purposes only, and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.