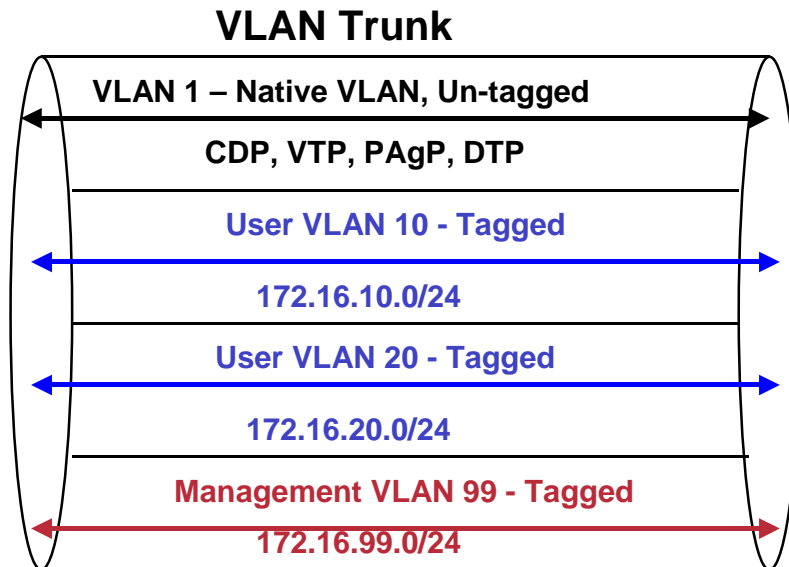


The Native VLAN

By Rick Graziani and Wayne Lewis

Figure 1 – Native VLANs



Role of the different VLANs

Overview

There are various types of VLANs including:

- VLAN 1
- The default VLAN
- The user VLANs
- The native VLAN
- The management VLAN

By default, all Ethernet interfaces on Cisco switches are on VLAN 1. On Catalyst switches all of these VLANs listed above default to VLAN 1, which can add to the difficulty of understanding their differences. This section will help explain the various types of VLANs and attempt to clear up some of this confusion.

VLAN 1

The reason VLAN 1 became a special VLAN is that Layer 2 devices needed to have a default VLAN to assign to their ports, including their management port(s). In addition to that, many Layer 2 protocols such as CDP, PAgP, and VTP needed to be sent on a specific VLAN on trunk links. For all these purposes VLAN 1 was chosen. [1]

CDP, VTP, PAgP, and DTP are always transmitted over VLAN 1. This is always the case and cannot be changed. Cisco recommends that VLAN 1 be used only for these protocols. The management VLAN and user VLANs should all be configured to use VLANs other than VLAN 1.

Default VLAN

By default, VLAN 1 is also the VLAN assigned to all switch interfaces, unless configured otherwise. VLAN 1 is also known as the default VLAN. Because it is the default, the other types of VLANs, the native VLAN, the management VLAN and the user VLANs, are all automatically members of VLAN 1. [1]

All Ethernet interfaces on Catalyst switches default to VLAN 1. Any device connected to an interface on a switch, will be a member of VLAN 1 unless that interface is configured to use a different VLAN with the `switchport access vlan` interface command.

User VLANs

User VLANs is what is normally thought of when we think of VLANs. A user VLAN is a VLAN that is created to segment a group of users, either geographically or logically, from the rest of the network. The `switchport access vlan` interface command is used to assign interfaces to these various user VLANs. [1]

Native VLAN

A topic that causes considerable confusion is the native VLAN.

“802.1Q is the IEEE standard for tagging frames on a trunk and supports up to 4096 VLANs. In 802.1Q, the trunking device inserts a 4-byte tag into the original frame and recomputes the frame check sequence (FCS) before the device sends the frame over the trunk link. At the receiving end, the tag is removed and the frame is forwarded to the assigned VLAN. **802.1Q does not tag frames on the native VLAN.** It tags all other frames that are transmitted and received on the trunk. When you configure an 802.1Q trunk, you must make sure that you configure the same native VLAN on both sides of the trunk.” *Inter-Switch Link and IEEE 802.1Q Frame Format, Cisco Systems, Document ID: 17056*

The native VLAN is a term used with interfaces that are configured as 802.1Q VLAN trunks. When a switch port is configured as an 802.1Q trunk, it tags frames with the appropriate VLAN number. Frames from all VLANs are carried across the trunk link containing the 802.1Q tag, except for frames belonging to VLAN 1.

By default, frames from VLAN 1 belong to the native VLAN, and are carried across the trunk untagged. Frames from the native VLAN, VLAN 1, are carried across this trunk link untagged. [1]

The IEEE committee that defined 802.1Q decided that because of backward compatibility it was desirable to support the so-called native VLAN, that is to say, a VLAN that is not associated explicitly to any tag on an 802.1Q link. This VLAN is implicitly used for all the untagged traffic received on an 802.1Q capable port.

This capability is desirable because it allows 802.1Q capable ports to talk to old 802.3 ports directly by sending and receiving untagged traffic. However, in all other cases, it may be very detrimental because packets associated with the native VLAN lose their tags, for example, their identity enforcement, as well as their Class of Service (802.1p bits) when transmitted over an 802.1Q link.

For these reasons, loss of means of identification and loss of classification, the use of the native VLAN should be avoided. There are very few reasons why the native VLAN would ever need to be used.

The native VLAN can be modified to a VLAN other than VLAN 1 with the following interface command:

```
Switch(config-if)#switchport trunk native vlan vlan-id
```

It is recommended that the native VLAN should never be used as a user VLAN or the management VLAN.

Earlier it was stated that the control traffic, CDP, VTP, PAgP, and DTP, is transmitted over VLAN 1, the native VLAN. If the native VLAN is changed to something other than VLAN 1, then the control traffic would then be transmitted on VLAN 1 as tagged. This will have no ill effects on the control traffic.

In most cases, it is fine to leave the control traffic on VLAN 1 with the default native VLAN, also VLAN 1. Usually, this should be the only information that should be carried across the VLAN 1.

It is also important to ensure that both ends of a switch-to-switch link have consistent native VLANs. If the native VLANs at both ends of a link are not the same, there will effectively be a bridge between the two VLANs and they will no longer be independent broadcast domains. Fortunately, recent versions of the IOS alert the user when mismatches in the native VLAN occur.

Management VLAN

Most of today's switches and routers can be accessed remotely by telnetting to the IP address of the device. It is recommended practice to put these and other networking devices in their own VLAN known as the management VLAN. This should be a separate VLAN, independent of any user VLANs, and the native VLAN. In case there are network problems, such as broadcast storms or spanning tree convergence issues, an independent management VLAN allows the network administrator to still be able to access these devices and troubleshoot the problem. [1]

Another reason to keep the management VLAN independent of user VLANs, is that it keeps "trusted devices" separated from "untrusted devices" lessening the possibility either by misconfiguration, by accident, or by intent, that users gain access to the routers or switches.

Configuring the Router

When a router's interface is configured as a trunk link, frames received on that interface from the native VLAN on the switch enter the interface untagged. Frames from the other non-native VLANs enter the interface tagged as ISL or 802.1Q.

Configuring the router's interface as a trunk link requires the use of subinterfaces. Each VLAN is configured on a separate subinterface. Each subinterface is configured to match the proper trunking protocol on the switch (ISL or 802.1Q). This is done with the router interface command:

```
encapsulation [ dot1q | isl ] vlan.
```

However, the router's subinterface that receives the native VLAN traffic must be configured to expect those frames to be untagged. This is done using the native option on that subinterface:

```
encapsulation [ dot1q | isl ] vlan.native
```

Prior to IOS 12.1(3)T the router had to be configured with the native VLAN on the physical interface and non-native VLANs were configured on the subinterfaces with the ISL or 802.1Q tag.

Summary

To summarize the different VLANs and how they should be used:

- By default, VLAN 1 is the native VLAN on Cisco switches and should only be used to carry control traffic, CDP, VTP, PAGP, and DTP. With 802.1Q trunks, this information is transmitted across trunk links untagged.
- User VLANs should not include the native VLAN, VLAN 1. We want user data to be sent as tagged frames across VLAN trunks.
- The Management VLAN should be a VLAN separate from the user VLANs and should not be the native VLAN. This will insure access to networking devices in case of problems with the network.
- The subinterface on a router that is used to send and receive native VLAN traffic must be configured with the **native** option on the **encapsulation** interface command. This will let the router know that any frames coming in untagged belong to that subinterface and are members of the native VLAN (whether the native VLAN is the default of VLAN 1 or otherwise).