VLAN Trunking Protocol (VTP)

by Sophia

WHAT'S COVERED

In this lesson, you will learn about the VLAN trunking protocol and additional features.

Specifically, this lesson will cover the following:

1. Identifying VLANs

Switch ports are Layer-2-only interfaces that are associated with a physical port. A switch port can belong to only one VLAN if it is an access port or all VLANs if it is a trunk port. You can manually configure a port as an access or trunk port, or you can let the dynamic trunking protocol (DTP) operate on a per-port basis to set the switch port mode. DTP does this by negotiating with the port on the other end of the link.

As frames are switched throughout the network, the frames have to be able to keep track of all the different port types plus understand what to do with them depending on the hardware address. Frames are handled differently based on the type of link that they traverse.

There are two different types of links in a switched environment. They are access ports and trunk ports.

1a. Access Ports

An access port belongs to and carries the traffic of only one VLAN. Anything arriving on an access port is simply assumed to belong to the VLAN assigned to the port. Any device attached to an **access link** is unaware of a

VLAN membership.

Switches remove any VLAN information from the frame before it is forwarded out to an access-link device. As discussed previously, access-link devices cannot communicate with devices outside their VLAN unless the packet is routed.

HINT

You can only create a switch port to be either an access port or a trunk port, but not both. So, you have got to choose one or the other, and know that if you make it an access port, that port can be assigned to one VLAN only.

TERM TO KNOW

Access Link

A link connecting a host to a switch at Layer 2.

1b. Trunk Ports

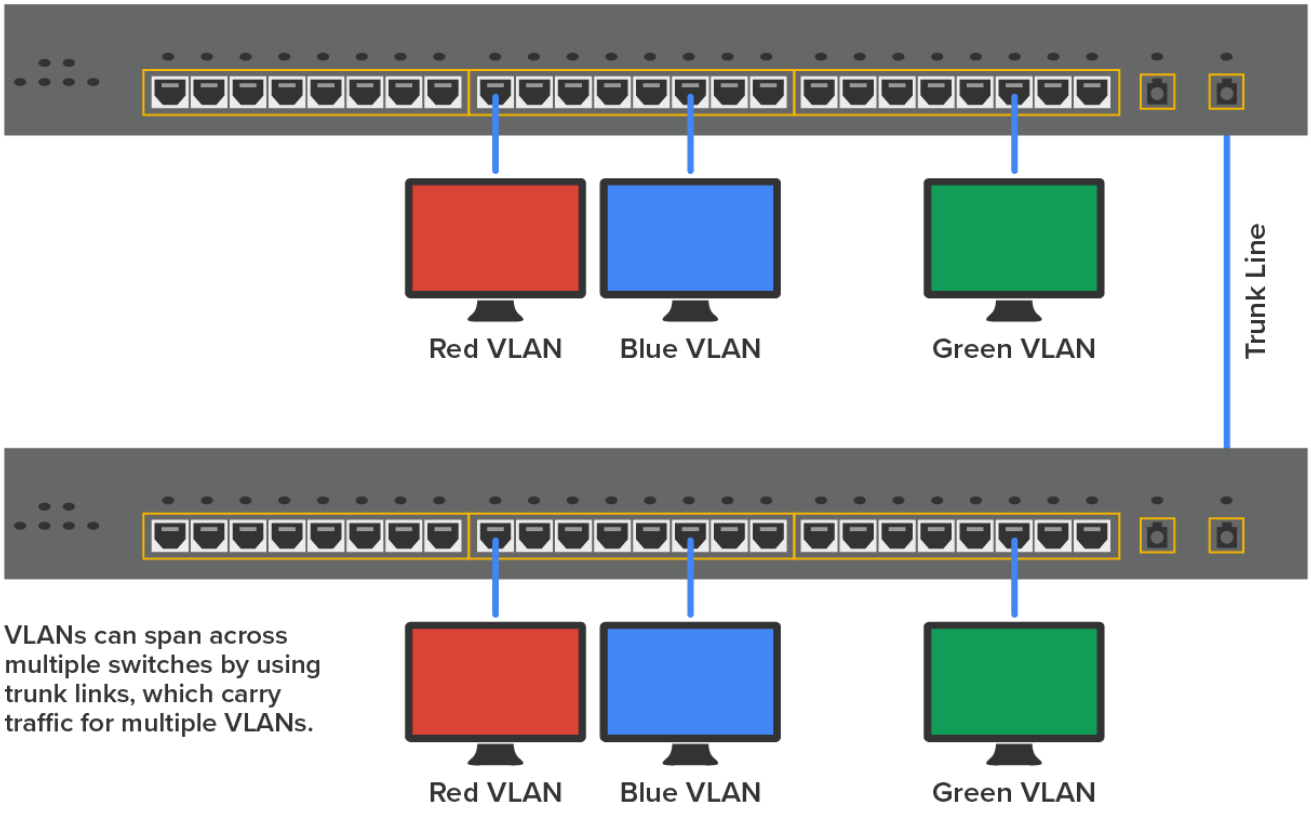
The term **trunk port** was inspired by the telephone system trunks that carry multiple telephone conversations at a time. So, it follows that trunk ports can similarly carry multiple VLANs at a time.

KEY CONCEPT

A **trunk link** is a 100 Mbps or 1000 Mbps point-to-point link between two switches, between a switch and router, or even between a switch and server, and it carries the traffic of multiple VLANs, from 1 to 4,094 VLANs at a time.

Trunking can be a real advantage because, with it, you get to make a single port part of a whole bunch of different VLANs at the same time. This is a great feature because you can actually set ports up to have a server in two separate broadcast domains simultaneously so that your users will not have to cross a Layer 3 device (router) to log in and access it. Another benefit of trunking comes into play when you are connecting switches. Information from multiple VLANs can be carried across trunk links, but by default, if the links between your switches are not trunked, only information from the configured VLAN will be switched across that link.

The diagram below shows how the different links are used in a switched network. All hosts connected to the switches can communicate to all ports in their VLAN because of the trunk link between them. Remember, if we used an access link between the switches, this would allow only one VLAN to communicate between switches. As you can see, these hosts are using access links to connect to the switch, so they are communicating in one VLAN only. This means that without a router, no host can communicate outside its own VLAN, but the hosts can send data over trunked links to hosts on another switch configured in their same VLAN.



Now, let's learn about the protocols that enable a switch to know which VLAN a particular frame belongs to.

TERMS TO KNOW

Trunk Port

A switch port that is set to be a trunk.

Trunk Link

A link that carries traffic from all VLANs between network devices.

2. VLAN Identification Methods

VLAN identification is what switches use to keep track of all those frames as they are traversing a switch fabric, a network topology in which network nodes interconnect via one or more network switches. All of our hosts connect together via a switch fabric in our switched network topology. It is how switches identify which frames belong to which VLANs, and there is more than one trunking method: inter-switch link and 802.1Q.

2a. Inter-Switch Link (ISL)

Inter-switch link (ISL) is a way of explicitly tagging VLAN information onto an Ethernet frame. This tagging information allows VLANs to be multiplexed over a trunk link through an external encapsulation method, which allows the switch to identify the VLAN membership of a frame over the trunked link.

By running ISL, you can interconnect multiple switches and still maintain VLAN information as traffic travels between switches on trunk links. ISL functions at Layer 2 by encapsulating a data frame with a new header and cyclic redundancy check (CRC).

It is important to note that ISL is proprietary to Cisco hardware only. Therefore, if you have a network with mixed-vendor hardware, then ISL is not going to work in that environment. In that case, you will have to use IEEE 802.1Q instead.

TERM TO KNOW

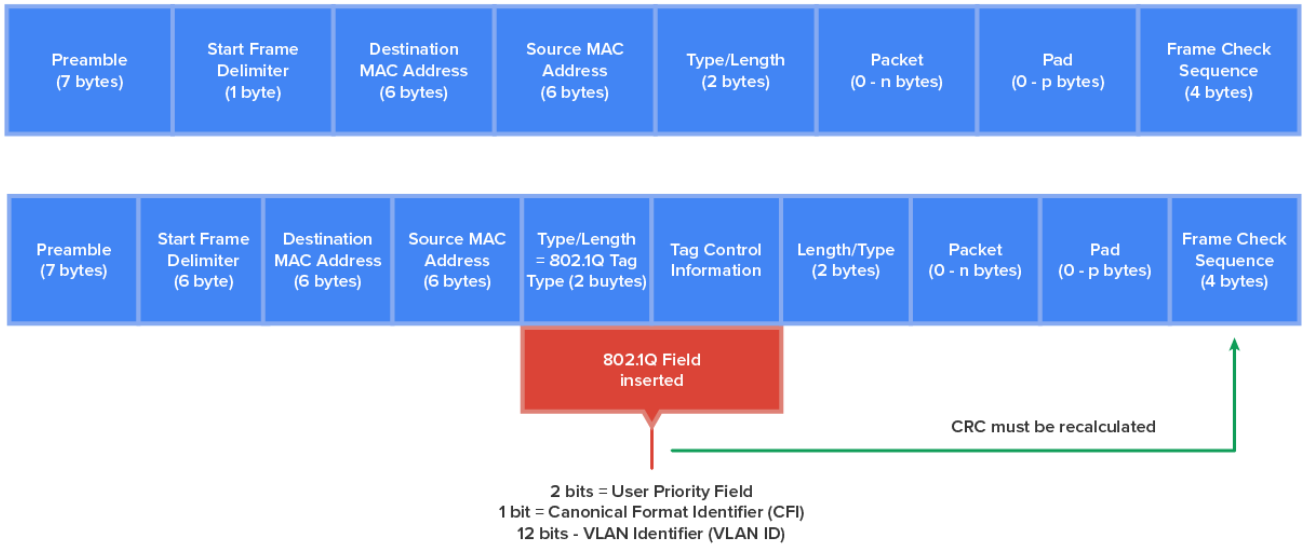
Inter-Switch Link (ISL)

A Cisco proprietary protocol for identifying VLAN membership.

2b. IEEE 802.1Q

Created by the IEEE as a standard method of frame tagging, **IEEE 802.1Q** works by inserting a field into the frame to identify the VLAN. This is one of the aspects of 802.1Q that makes it your only option if you want to trunk between a Cisco switched link and another brand of switch. In a mixed environment, you have just got to use 802.1Q for the trunk to work.

Unlike ISL, which encapsulates the frame with control information, 802.1Q inserts an 802.1Q field along with tag control information, as shown in the illustration below.



The 802.1Q field identifies the VLAN number, which can be from 1 to 4,094.

BIG IDEA

The purpose of the ISL and 802.1Q frame-tagging methods is to provide inter-switch VLAN communication. Remember that any ISL or 802.1Q frame tagging is removed if a frame is forwarded out of an access link, and VLAN tagging is used internally and across trunk links only.

TERM TO KNOW

IEEE 802.1Q

An open proprietary protocol for identifying VLAN membership.

3. VLAN Trunking Protocol

The basic goals of the **VLAN trunking protocol (VTP)** are to manage all configured VLANs across a switched internetwork and to maintain consistency throughout that network. VTP allows you to add, delete, and rename VLANs—and information about those actions is then propagated to all other switches in the VTP domain.

KEY CONCEPT

Here is a list of some of the features VTP has to offer:

- Consistent VLAN configuration across all switches in the network
- Accurate tracking and monitoring of VLANs
- Dynamic reporting of added VLANs to all switches in the VTP domain
- Adding VLANs using plug and play

All switches act as VTP servers by default. All servers that need to share VLAN information must use the same VTP domain name, and a switch can be in only one VTP domain at a time. So basically, this means that a switch can share VTP domain information with other switches only if they are configured into the same VTP domain. You can use a VTP domain if you have more than one switch connected in a network, but if you have got all your switches in only one VLAN, you do not need to use VTP. Do keep in mind that VTP information is sent between switches only via a trunk port.

Switches advertise VTP management domain information as well as a configuration revision number and all known VLANs with any specific parameters. There is also something known as the VTP transparent mode. In this, you can configure switches to forward VTP information through trunk ports but not to accept information updates or update their VTP databases.

Switches detect any added VLANs within a VTP advertisement and then prepare to send information on their trunk ports based on the newly defined VLAN. Updates are sent out as revision numbers that consist of summary advertisements. Any time a switch sees a higher revision number, it knows the information it is getting is more current, so it will overwrite the existing VLAN database with the latest information.

KEY CONCEPT

It is important to know the requirements for VTP to communicate VLAN information between switches. These requirements include:

- The VTP management domain name of both switches must be set as the same.
- One of the switches has to be configured as a VTP server.
- Set a VTP password if one is used.
- No router is necessary, and a router is not a requirement.

Let's delve deeper into the VTP modes.

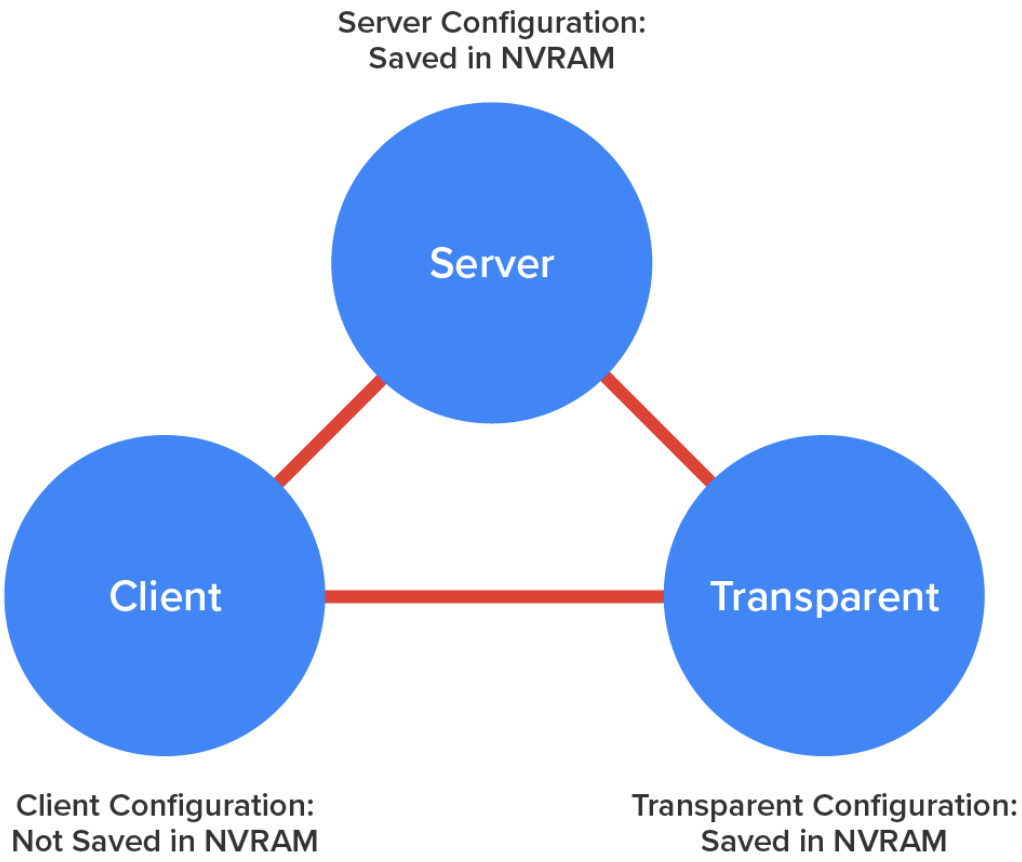
TERM TO KNOW

VLAN Trunking Protocol (VTP)

A protocol that enables switches to propagate VLAN configuration changes to switches in a VTP domain.

3a. VTP Modes of Operation

The diagram below shows you all three different modes of operation within a VTP domain:



Server

VTP server mode is the default mode for all switches. You need at least one server in your VTP domain to propagate VLAN information throughout that domain. Also, it is important for the switch to be in server mode for you to be able to create, add, and delete VLANs in a VTP domain. VLAN information has to be changed in server mode, and any change made to VLANs on a switch in server mode will be advertised to the entire VTP domain. In VTP server mode, VLAN configurations are saved in NVRAM on the switch.

In **VTP client mode**, switches receive information from VTP servers, but they also receive and forward updates; in this way, they behave like VTP servers. The difference is that they cannot create, change, or delete VLANs. Plus, none of the ports on a client switch can be added to a new VLAN before the VTP server notifies the client switch of the new VLAN, and the VLAN exists in the client's VLAN database. It is also good to know that VLAN

information sent from a VTP server is not stored in NVRAM, which is important because it means that if the switch is reset or reloaded, the VLAN information will be deleted.

Switches in **VTP transparent mode** do not participate in the VTP domain or share its VLAN database, but they will still forward VTP advertisements through any configured trunk links. An administrator on a transparent switch can create, modify, and delete VLANs because they keep their own database of VLANs that are local to that particular switch. The whole purpose of transparent mode is to allow remote switches to receive the VLAN database from a VTP-server-configured switch through a switch that is not participating in the same VLAN assignments.

TERMS TO KNOW

VTP Server Mode
Enables a switch to make changes to the VLAN database.

VTP Client Mode
Receives changes to the VLAN database from VTP servers.

VTP Transparent Mode
Forwards VTP updates but does not update its local VLAN database.

SUMMARY

In this lesson, you learned more about **identifying VLANs**. This included the exploration of **access ports** and **trunk ports**. You also learned about **VLAN identification methods** including **inter-switch links** (ISL) and **IEEE 802.1Q**. Finally, you learned about **VLAN trunking protocol** (VTP) and **VTP modes of operation** including server mode, client mode, and transparent mode.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Access Link
A link connecting a host to a switch at Layer 2.

IEEE 802.1Q
An open proprietary protocol for identifying VLAN membership.

Inter-Switch Link (ISL)
A Cisco proprietary protocol for identifying VLAN membership.

Trunk Link

A link that carries traffic from all VLANs between network devices.

Trunk Port

A switch port that is set to be a trunk.

VLAN Trunking Protocol (VTP)

A protocol that enables switches to propagate VLAN configuration changes to switches in a VTP domain.

VTP Client Mode

Receives changes to the VLAN database from VTP servers.

VTP Server Mode

Enables a switch to make changes to the VLAN database.

VTP Transparent Mode

Forwards VTP updates but does not update its local VLAN database.