

University of Information Technology



Deployment of VLANs in Multiswitch Environment

Advanced Networking (CST - 31404)

Ei Khine Moe

3CS - 1456

23 February 2023

Table of contents

Overview	1
Objectives	2
Theory Background	3
Design Approach	9
Configuration and Testing	11
Conclusion	18
References	18

Overview

Nowadays, internet is widely used all over the world for many purposes in different fields. Therefore, the network technology becomes more essential and important to get the internet from anywhere at anytime. Today's network technology plays an essential role becoming more popular and advanced. Almost all organization industries from different fields use the network technology to run and manage their industries well. Not only the private organizations but also the public organization use network technology. They include business companies, schools, government institutes and so on. A computer network technology allows institutions and businesses to communicate by sharing information based on the organization's requirements with the help of information systems. Therefore, the organizations deploy network technology with the purpose of communication and data sharing. The classification of network technology can be done based on transmission and scale. Those based on transmission can be done using the two concepts like point-to-point and multipoint network, and those based on scale can be done using the concepts like VPN, PAN, WAN, MAN and LAN. One of the network structures used by the organization is VLAN. A virtual local area network (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). This project mainly discusses on the deployment of VLANs in multiswitch environment as a case study. In this project, the deployment of VLANs is studied on simulation. The simulator used in this case study is Cisco Packet Tracer: a cross-platform visual simulation tool designed by Cisco Systems.

Objectives

- To study the advancement of network technologies
- To study the deployment of VLANs in multiswitch environments
- To perform how the simulation works in the network technology

Theory Background

Network Technology

Networking technology has had a massive impact on the world today and is among the reasons why it's so important. It is also one of the primary reasons the economies of nearly all countries didn't crash during the COVID 19 pandemic. And, besides financial benefits, networks helped us remain connected with friends, families, and colleagues. In doing so, it reduced the mental and physical impact a wide and rapid spread of the virus inevitably causes. Network technology is a technology that enables data exchange between large and small information systems within an infrastructure via the use of communication/network protocols. The infrastructure consists of nodes, which can be a redistribution point or a network/communication endpoint. The primary network technology representative is a computer network.

There are two ways to deploy network topologies: Wireless and Ethernet.

A wireless network is a computer network that uses wireless data connections between network nodes. Wireless networking is a method by which homes, telecommunications networks and business installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.

Ethernet is a family of wired computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN). It enables devices to communicate with each other via a protocol, which is a set of rules or common network language. Ethernet describes how network devices format and transmit data so other devices on the same LAN or campus network can recognize, receive and process the information.

Wired Ethernet LANs

In today's world, wired Ethernet LANs is still a popular form of network connection and it is used for local networks used by specific organizations such as company offices, school campuses, hospitals, business organizations and so on due to its high speed, security, and reliability. Ethernet is the most popular local area networks (LAN) technology in use today. Other LAN types include Token Rings, Fiber Distributed Data Interface (FDDI) and Localtalk. Ethernet became popular due to its relatively low cost when compared to the competing technology of the time. Technically Ethernet is a standard communication protocol and the technology most commonly used in wired Ethernet LANs.

Local Area Network (LAN)

LAN is a group of computers located in the same room, on the same floor, or in the same building that are connected to form a single network. Local area networks (LANs) allow users to share storage devices, printers, applications, data, and other network resources. They are limited to specific geographical area, usually less than 2 kilometers in diameter. They use a dedicated backbone to connect multiple subnetworks. In order to get connection with an Ethernet LAN network, IP addresses are need for every device we used.

Internet Protocol Address

IP address stands for “Internet Protocol address”. The Internet Protocol is a set of rules for communication over the internet, such as sending mail, streaming video, or connecting to a website. An IP address identifies a network or device on the internet. Every single device that is connected to the internet must have an IP address. There are two types of IP addresses: IPv4 and IPv6. It’s easy to recognize the difference if you count the numbers. IPv4 addresses contain a series of four numbers, ranging from 0 (except the first one) to 255, each separated from the next by a period — such as 5.62.42.77. IPv6 addresses are represented as eight groups of four hexadecimal digits, with the groups separated by colons. A typical IPv6 address might look like this: 2620:0aba2:0d01:2042:0100:8c4d:d370:72b4.

The Problem of Large Broadcast Domain

There are some problems concerning with the wired Ethernet LAN. For example, in an organization which has multiple users, the broadcast domain would be extremely large because every host must listen to every broadcast message on the network. A broadcast domain is a logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer. A broadcast domain can be within the same LAN segment or it can be bridged to other LAN segments. In a broadcast domain, anytime there is a broadcast, every host meant to listen to it gives the message a priority treatment. They abandon all other activities to listen and possibly respond to the broadcast. all packets colliding here and there and having their routes changed endlessly by the numerous collisions they encounter. This will cause packets to remain en route to their destination longer than they should. This results in many packets remaining on the network undelivered, causing a clog up of the network bandwidth. If all hosts have to pause their current event and give attention to the broadcasts whenever there is one, this will cause our PCs to crawl.

Network Segmentation

This can be solved by segmenting the network. Network segmentation is the process of dividing a network into multiple smaller networks (subnets and segments). IP subnetting provides a way to uniquely define the subnet and the specified device address inside a computer network. Segmenting a network by can reduce overall network congestion by limiting traffic to each individual segment, directing data to destination systems within the segment rather than allowing unnecessary data movement across the entire network in search for destinations before arriving at a system within the segmented area.

Implementation of VLANs

One way of breaking a larger network into smaller sections is by implementing VLANs. VLANs allow segmentation or breaking a large network into smaller ones. A virtual local area network (VLAN) is a subdivision of a local area network at the datalink layer of the protocol stack. You can create VLANs for local area networks that use switch technology. You can assign interfaces on the same system to different VLANs. A VLAN is a switched network that is logically segmented, by functions, project teams, or applications rather than on a physical or geographical basis. A network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. You use VLANs to reconfigure the network through software rather than physically unplugging and moving devices or wires. Devices within a VLAN act as if they are in their own independent network, even if they share a common infrastructure with other VLANs. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations within the VLAN where the packets are sourced. Each VLAN is considered a separate logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a device that supports routing. A VLAN creates a logical broadcast domain that can span multiple physical LAN segments. VLANs improve network performance by separating large broadcast domains into smaller ones. If a device in one VLAN sends a broadcast Ethernet frame, all devices in the VLAN receive the frame, but devices in other VLANs do not. VLANs enable the implementation of access and security policies according to specific groupings of users. Each switch port can be assigned to only one VLAN (with the exception of a port connected to an IP phone or to another switch).

Benefits of VLANs

User productivity and network adaptability are important for business growth and success. VLANs make it easier to design a network to support the goals of an organization.

There are few reasons why we should use VLANs:

- Create a logical division of workgroups. If all systems on a floor of a building are connected on one switch-based local network, you could create a separate VLAN for each workgroup on the floor.
- Create more flexible designs that group users by department, or by groups that work together instead of by physical location.
- Enforce differing security policies for the workgroups. The security requirements of a finance department and an information technology department are quite different. You can create a separate VLAN for each department and enforce the appropriate security policy on a per-VLAN basis. We can ensure better security by keeping hosts that work with sensitive data on a separate VLAN.
- Reduce the size of broadcast domain and improve network efficiency. You can split workgroups into manageable broadcast domains.
- Can break apart the network as desired and needed without having to go and move cables around.

Each VLAN in a switched network corresponds to an IP network; therefore, VLAN design must take into consideration the implementation of a hierarchical network addressing scheme. A hierarchical network addressing scheme means that IP network numbers are applied to network segments or VLANs in an orderly fashion that takes the network as a whole into consideration. Blocks of contiguous network addresses are reserved for and configured on devices in a specific area of the network.

The Types of VLANs

There are a number of distinct types of VLANs used in modern networks. Some VLAN types are defined by traffic classes. Other types of VLANs are defined by the specific function that they perform.

✓ Data VLAN

A data VLAN is a VLAN that is configured to carry user-generated traffic. A VLAN carrying voice or management traffic would not be part of a data VLAN. It is common practice to separate voice and management traffic from data traffic. A data VLAN, is sometimes referred to as a user VLAN. Data VLANs are used to separate the network into groups of users or devices.

✓ **Default VLAN**

All switch ports become a part of the default VLAN after the initial boot up of a switch loading the default configuration. Switch ports that participate in the default VLAN are part of the same broadcast domain. This allows any device connected to any switch port to communicate with other devices on other switch ports. The default VLAN for Cisco switches is VLAN 1. The “show vlan brief” command was issued on a switch running the default configuration. All ports are assigned to VLAN 1 by default. VLAN 1 has all the features of any VLAN, except it cannot be renamed or deleted. By default, all Layer 2 control traffic is associated with VLAN 1.

✓ **Native VLAN**

A native VLAN is assigned to an 802.1Q trunk port. Trunk ports are the links between switches that support the transmission of traffic associated with more than one VLAN. An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic), as well as traffic that does not come from a VLAN (untagged traffic). The 802.1Q trunk port places untagged traffic on the native VLAN, which by default is VLAN 1. Native VLANs are defined in the IEEE 802.1Q specification to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. A native VLAN serves as a common identifier on opposite ends of a trunk link. It is a best practice to configure the native VLAN as an unused VLAN, distinct from VLAN 1 and other VLANs. In fact, it is not unusual to dedicate a fixed VLAN to serve the role of the native VLAN for all trunk ports in the switched domain.

✓ **Management VLAN**

A management VLAN is any VLAN configured to access the management capabilities of a switch. VLAN 1 is the management VLAN by default. To create the management VLAN, the switch virtual interface (SVI) of that VLAN is assigned an IP address and subnet mask, allowing the switch to be managed via HTTP, Telnet, SSH, or SNMP.

VLAN Trunking

You can't describe VLANs without mentioning trunks. It's a known fact that you can control and segment network broadcasts with VLANs. VLAN trunking enables the movement of traffic to different parts of the network configured as a VLAN. For multiswitch environments, trunks are required to connect a switch to a switch or to another network device such as a router. A VLAN trunk, or trunk, is a point-to-point link between two network devices that carries more than one VLAN. A VLAN trunk extends VLANs across two or more network devices. VLANs would not be very useful without VLAN trunks. VLAN trunks allow all VLAN traffic to propagate between switches, so that devices which are in the same VLAN, but connected to different switches, can communicate without the intervention of a router. A VLAN trunk does not belong to a specific

VLAN; rather, it is a conduit for multiple VLANs between switches and routers. A trunk could also be used between a network device and server or other device that is equipped with an appropriate 802.1Q-capable NIC.

Enable VLAN configured with trunk link to traffic frames between switches on the network, it is made possible by a link protocol called VLAN Trunking Protocol VTP. VLAN Trunking Protocol (VTP) is a Cisco-proprietary link protocol, it provides a means by which Cisco switches can exchange VLAN configuration information.

Design Approach

In this case study, we are going to deploy a LAN segment of an organization. In this topology, there are three Cisco switches (S1, S2 and S3) and four different VLANs. These VLANs are named Accounting (vlan 10), IT (vlan 20), Sales (vlan 30) and Native (vlan 99). Each of these VLANs is used to segment the network into smaller broadcast domains which helps improve security as well as performance. This type of setup allows for greater flexibility in terms of how devices can be grouped together on a single switch or across multiple switches depending on their needs.

Network Deployment

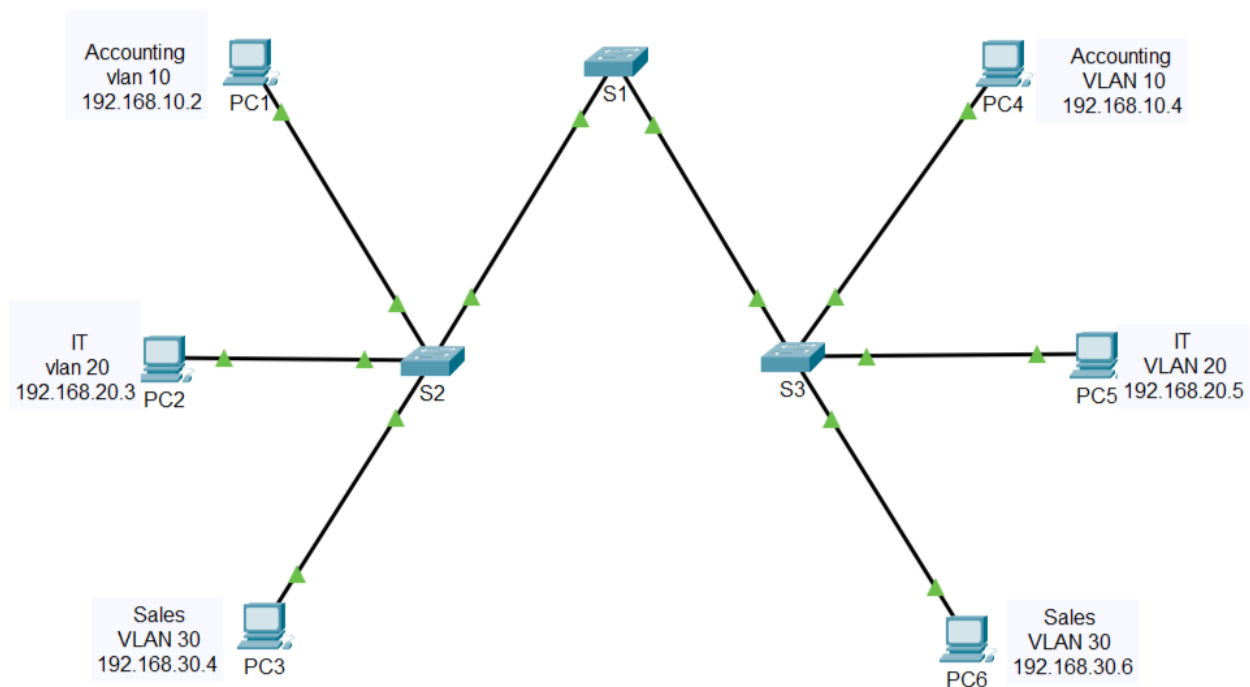


Figure1. Deployment Of VLANs in Multiswitch Environment

In this topology, PC1, PC2 and PC3 are connected to S2. PC4, PC5 and PC6 are connected to S3. PC1 and PC4 are in the Accounting (vlan 10), PC2 and PC5 are in the IT (vlan 20), and PC3 and PC6 are in the Sales (vlan 30). In this topology above, the links between switches S1 and S2, S1, and S3 are configured as trunk links to enable traffic between VLAN 10, 20, and 30. This network

simply could not function without VLAN trunks. The IP addresses and subnet masks of the respective PCs are as follows.

Addressing Table

Device	IP Address	Subnet Mask	Switch Port	VLAN
PC1	192.168.10.2	255.255.255.0	S2 F0/5	10
PC2	192.168.20.3	255.255.255.0	S2 F0/7	20
PC3	192.168.30.4	255.255.255.0	S2 F0/11	30
PC4	192.168.10.4	255.255.255.0	S3 F0/5	10
PC5	192.168.20.5	255.255.255.0	S3 F0/7	20
PC6	192.168.30.6	255.255.255.0	S3 F0/11	30

Configuration and Testing

Instructions

✓ Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the PC hosts and switches.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the Figure1, and cable as necessary.

Step 2: Configure basic settings for each switch.

- a. Console into the switch and enter global configuration mode.

Switch> enable

Switch# configure terminal

- b. Configure the hostnames as shown in the Figure1 by issuing the command **hostname name**.

✓ Part 2: Configure the VLANs.

Step 1: Configure VLANs on all three switches refer to the VLAN table.

VLAN Table

VLAN Number	VLAN Name
10	Accounting
20	IT
30	Sales
99	Native

Write these commands on all three switches.

```
S1(config)#vlan 10
S1(config-vlan)#name Accounting
S1(config-vlan)#vlan 20
S1(config-vlan)#name IT
S1(config-vlan)#vlan 30
S1(config-vlan)#name Sales
S1(config-vlan)#vlan 99
S1(config-vlan)#name Native
```

Step 2: Verify VLANs.

Write the command show vlan brief to verify the VLANs we created.

```
S1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
10	Accounting	active	
20	IT	active	
30	Sales	active	
99	Native	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

There should be 9 VLANs in total on all three switches. All 26 ports are assigned to the VLAN 1 by default.

✓ Part 3: Assign ports to VLANs.

Step 1: Assign access ports to VLANs.

On S2 and S3, assign ports to VLANs according to the Addressing Table.

On S2, do the following. It is the same for S3.

```
S2>en
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int f0/5
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#int f0/7
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S2(config-if)#int f0/11
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
```

Step 2: Verify that all VLANs are assigned to the correct switch ports according to the Addressing Table.

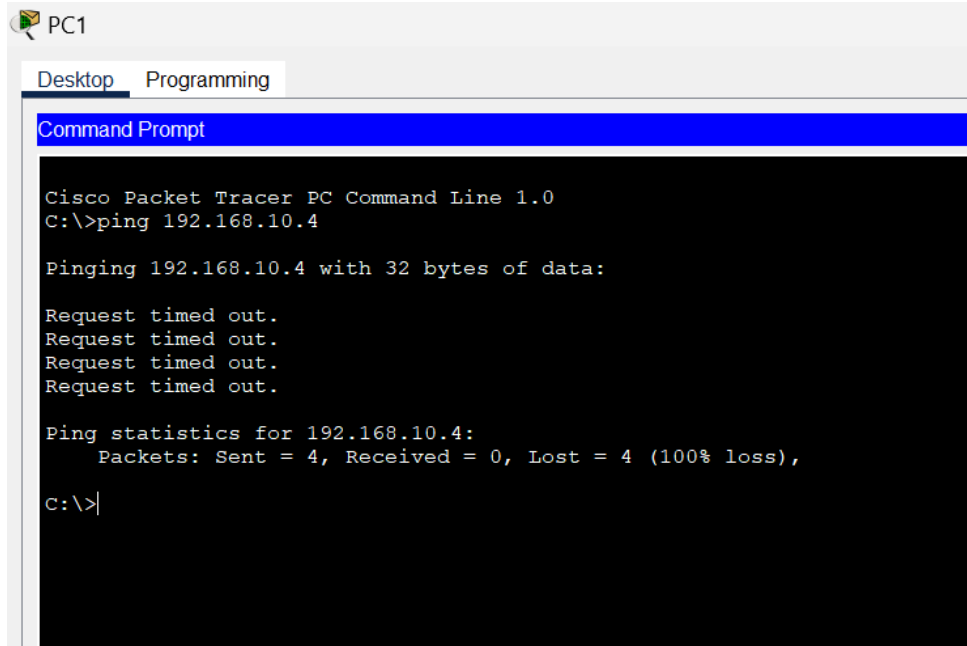
Issue the command show vlan brief on both S2 and S3 to verify the VLANs and their assigned ports.

```
S2>en
S2#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/6, Fa0/8, Fa0/9, Fa0/10 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig0/1, Gig0/2
10	Accounting	active	Fa0/5
20	IT	active	Fa0/7
30	Sales	active	Fa0/11
99	Native	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Now F0/5, F0/7 and F0/11 are assigned to their corresponding VLANs.

Step 3: Verify the loss of connectivity between PCs on the same network.



Ping between hosts on the same VLAN on different switches. Although PC1 and PC4 are in the same network, they cannot ping one another. This is because the ports connecting the switches are assigned to the VLAN 1 by default. To get connectivity between the PCs on the same network and VLAN, trunks must be configured.

✓ Part 4: Configure Trunk.

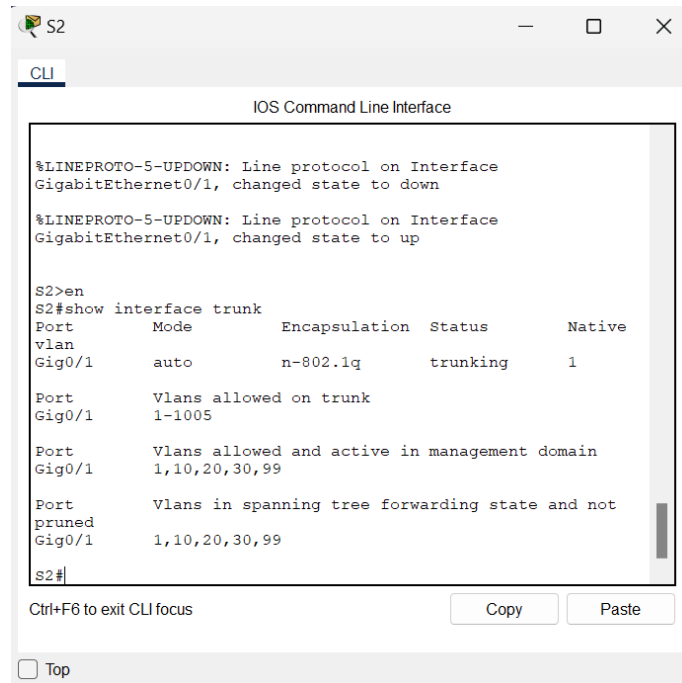
Step 1: Configure trunking on S1.

```
S1(config)#int range g0/1-2
S1(config-if-range)#switchport mode trunk

S1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up
```


Step 2: Verify trunking is enabled on S2 and S3.

On S2 and S3, issue the command `show interface trunk` to confirm that DTP (Dynamic Trunking Protocol) has successfully negotiated trunking with S1. The output also displays the trunk interfaces on S2 and S3.



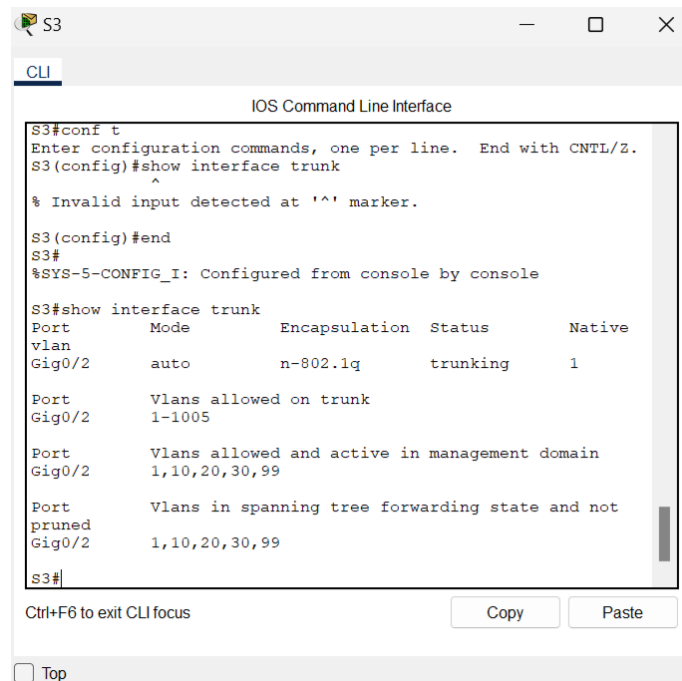
The screenshot shows the CLI of switch S2. It displays messages about the line protocol on GigabitEthernet0/1 changing from down to up. Then, the command `show interface trunk` is executed, showing that Gig0/1 is in trunking mode with encapsulation n-802.1q and native VLAN 1. It also lists the allowed VLANs (1-1005) and the active VLANs (1,10,20,30,99).

```
S2>en
S2#show interface trunk
Port      Mode      Encapsulation  Status      Native
vlan
Gig0/1    auto      n-802.1q       trunking    1

Port      Vlans allowed on trunk
Gig0/1    1-1005

Port      Vlans allowed and active in management domain
Gig0/1    1,10,20,30,99

Port      Vlans in spanning tree forwarding state and not
pruned
Gig0/1    1,10,20,30,99
S2#
```



The screenshot shows the CLI of switch S3. It displays an error message for an invalid input character. Then, the command `show interface trunk` is executed, showing that Gig0/2 is in trunking mode with encapsulation n-802.1q and native VLAN 1. It also lists the allowed VLANs (1-1005) and the active VLANs (1,10,20,30,99).

```
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#show interface trunk
^
% Invalid input detected at '^' marker.

S3(config)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#show interface trunk
Port      Mode      Encapsulation  Status      Native
vlan
Gig0/2    auto      n-802.1q       trunking    1

Port      Vlans allowed on trunk
Gig0/2    1-1005

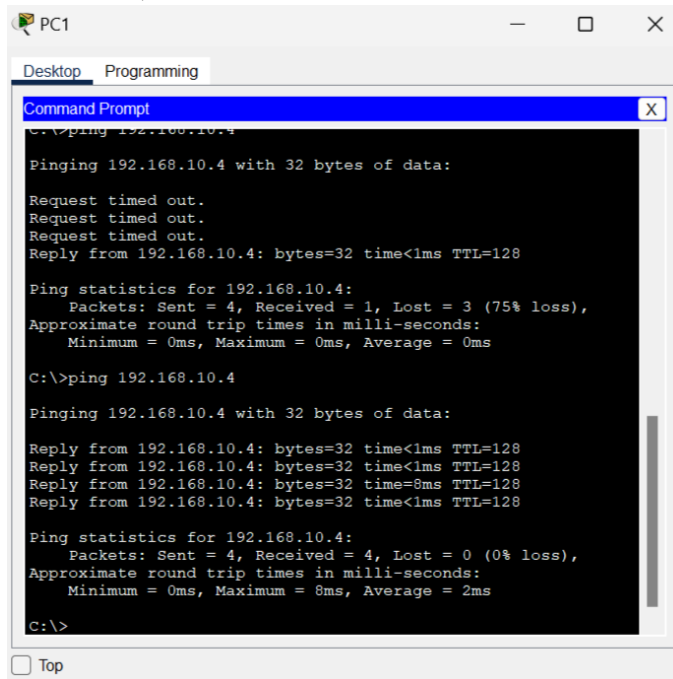
Port      Vlans allowed and active in management domain
Gig0/2    1,10,20,30,99

Port      Vlans in spanning tree forwarding state and not
pruned
Gig0/2    1,10,20,30,99
S3#
```

Testing

Test connectivity between PCs on the same network.

From PC1 to PC4,



The screenshot shows a Windows desktop window titled 'PC1' with a 'Command Prompt' window open. The command prompt shows the execution of a ping command to 192.168.10.4. The first attempt shows three 'Request timed out.' messages followed by a successful reply. The second attempt shows four successful replies. The statistics for both attempts indicate a 75% loss for the first and 0% loss for the second.

```
C:\>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.4

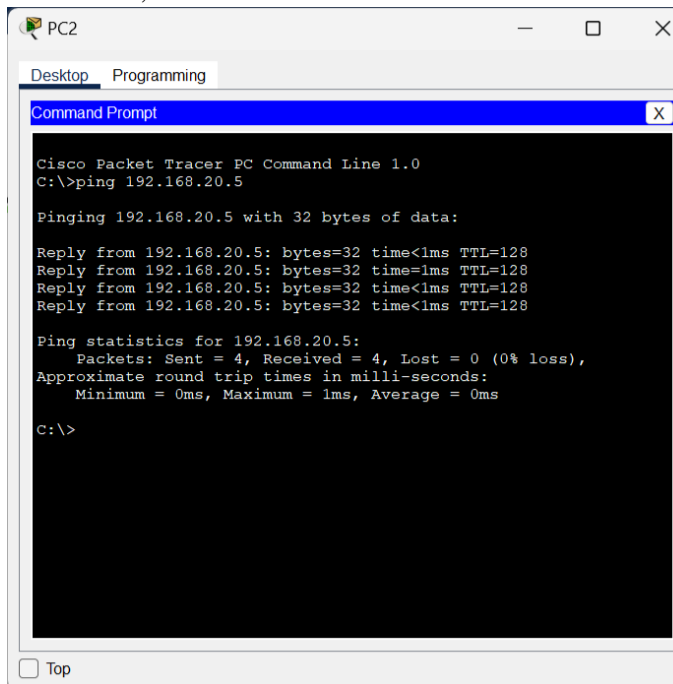
Pinging 192.168.10.4 with 32 bytes of data:

Reply from 192.168.10.4: bytes=32 time<1ms TTL=128
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128
Reply from 192.168.10.4: bytes=32 time=8ms TTL=128
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\>
```

From PC2 to PC5,



The screenshot shows a Windows desktop window titled 'PC2' with a 'Command Prompt' window open. The command prompt shows the execution of a ping command to 192.168.20.5. All four attempts are successful, showing replies from 192.168.20.5 with various round trip times. The statistics indicate 0% loss.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.5

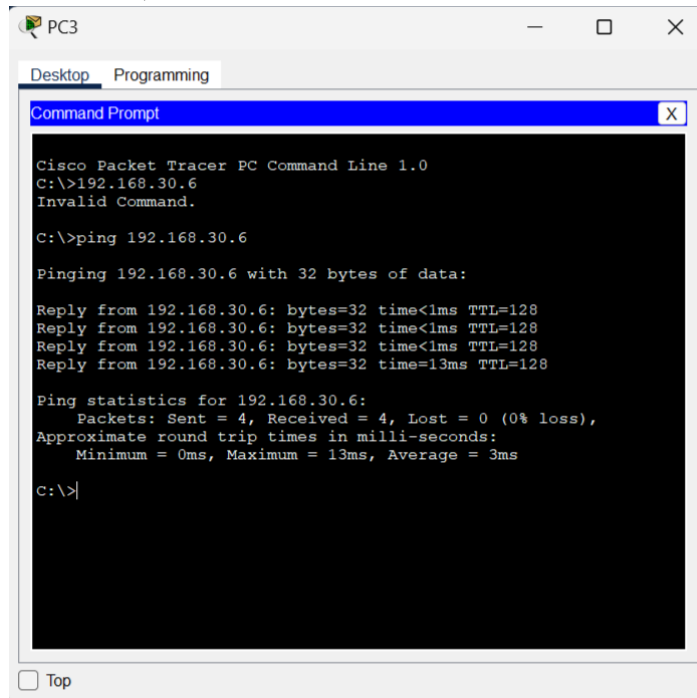
Pinging 192.168.20.5 with 32 bytes of data:

Reply from 192.168.20.5: bytes=32 time<1ms TTL=128
Reply from 192.168.20.5: bytes=32 time<1ms TTL=128
Reply from 192.168.20.5: bytes=32 time<1ms TTL=128
Reply from 192.168.20.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

From PC3 to PC6,



```
Cisco Packet Tracer PC Command Line 1.0
C:\>192.168.30.6
Invalid Command.

C:\>ping 192.168.30.6

Pinging 192.168.30.6 with 32 bytes of data:

Reply from 192.168.30.6: bytes=32 time<1ms TTL=128
Reply from 192.168.30.6: bytes=32 time<1ms TTL=128
Reply from 192.168.30.6: bytes=32 time<1ms TTL=128
Reply from 192.168.30.6: bytes=32 time=13ms TTL=128

Ping statistics for 192.168.30.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 3ms

C:\>|
```

Conclusion

By implementing this type of topology with multiple interconnected Cisco Switches and distinct Virtual LAN segments we gain both increased security due to better isolation between our various networks but also improved performance through more efficient routing decisions when forwarding frames along our paths throughout the entire infrastructure environment overall. Additionally, by using trunking protocols like 802.1q the same physical connection between two switches can carry multiple virtual connections with data from any number of different networks being segregated out based on their assigned tag values within the frame header information itself before reaching its destination port(s).

References

- ✓ <https://www.ciscopress.com/articles/article.asp?p=2208697&seqNum=5>
- ✓ <https://www.networkacademy.io/ccna/ethernet/vlan-trunking>
- ✓ <https://www.orbit-computer-solutions.com/how-to-configure-vlan-trunk/>