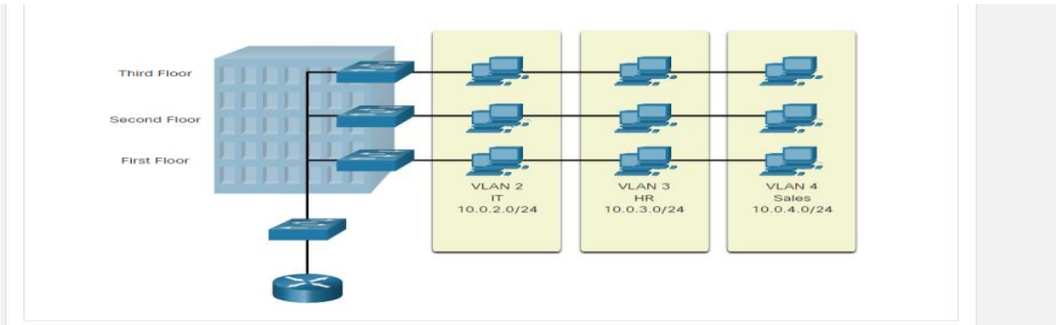
MODULE 3: VLANs
WEEK 3

Learning Outcomes:

After completing this course you are expected to demonstrate the following:

Explain how network protocols enable devices to access local and remote network resources.

A. Engage



Organizing your network into smaller networks is not as simple as separating screws and putting them into jars. But it will make your network easier to manage. Virtual LANs (VLANs) provide segmentation and organizational flexibility in a switched network. A group of devices within a VLAN communicate as if each device was attached to the same cable. VLANs are based on logical connections, instead of physical connections.

As shown in the figure, VLANs in a switched network enable users in various departments (i.e., IT, HR, and Sales) to connect to the same network regardless of the physical switch being used or location in a campus LAN.

B. Explore

Video Animation:
Network without VLANs and with VLANs

Netacad Academy account
https://contenthub.netacad.com/srwe/3.2.2

C. Explain

When a switch receives a broadcast frame on one of its ports, it forwards the frame out all other ports except the port where the broadcast was received. The entire network is configured in the same subnet (172.17.40.0/24) and no VLANs are configured. As a result, when the faculty computer (PC1) sends out a broadcast frame, switch S2 sends that broadcast frame out all of its ports. Eventually the entire network receives the broadcast because the network is one broadcast domain.

The ports that comprise the connection between switches S2 and S1 (ports F0/1), and between S1 and S3 (ports F0/3) are trunks and have been configured to support all the VLANs in the network.

When S1 receives the broadcast frame on port F0/1, S1 forwards that broadcast frame out of the only other port configured to support VLAN 10, which is port F0/3. When S3 receives the broadcast frame on port F0/3, it forwards that broadcast frame out the only other port configured to support VLAN 10, which is port F0/11. The broadcast frame arrives at the only other computer in the network configured in VLAN 10, which is faculty computer PC4.

When VLANs are implemented on a switch, the transmission of unicast, multicast, and broadcast traffic from a host in a particular VLAN are restricted to the devices that are in that VLAN.

D. Elaborate

3.1 Overview of VLANs

3.1.1 VLAN Definitions

VLANs are logical connections with other similar devices.

Placing devices into various VLANs have the following characteristics:

- Provides segmentation of the various groups of devices on the same switches
- Provide organization that is more manageable
    - Broadcasts, multicasts and unicasts are isolated in the individual VLAN
    - Each VLAN will have its own unique range of IP addressing
    - Smaller broadcast domains

3.1.2

Benefits	Description
Smaller Broadcast Domains	Dividing the LAN reduces the number of broadcast domains
Improved Security	Only users in the same VLAN can communicate together
Improved IT Efficiency	VLANs can group devices with similar requirements, e.g. faculty vs. students
Reduced Cost	One switch can support multiple groups or VLANs
Better Performance	Small broadcast domains reduce traffic, improving bandwidth
Simpler Management	Similar groups will need similar applications and other network resources

3.1.3. Types of VLANs

Default VLAN

VLAN 1 is the following:

- The default VLAN
- The default Native VLAN
- The default Management VLAN
- Cannot be deleted or renamed

```
Switch# 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
                                                Gi0/1, Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Note: While we cannot delete VLAN1 Cisco will recommend that we assign these default features to other VLANs

Data VLAN

- Dedicated to user-generated traffic (email and web traffic).
- VLAN 1 is the default data VLAN because all interfaces are assigned to this VLAN.

Native VLAN

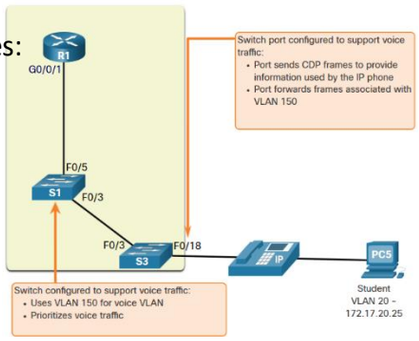
- This is used for trunk links only.
- All frames are tagged on an 802.1Q trunk link except for those on the native VLAN.

Management VLAN

- This is used for SSH/Telnet VTY traffic and should not be carried with end user traffic.
- Typically, the VLAN that is the SVI for the Layer 2 switch.

Voice VLAN

- A separate VLAN is required because Voice traffic requires:
  - Assured bandwidth
  - High QoS priority
  - Ability to avoid congestion
  - Delay less that 150 ms from source to destination
- The entire network must be designed to support voice.



3.2. VLANs in a Multi-Switched Environment

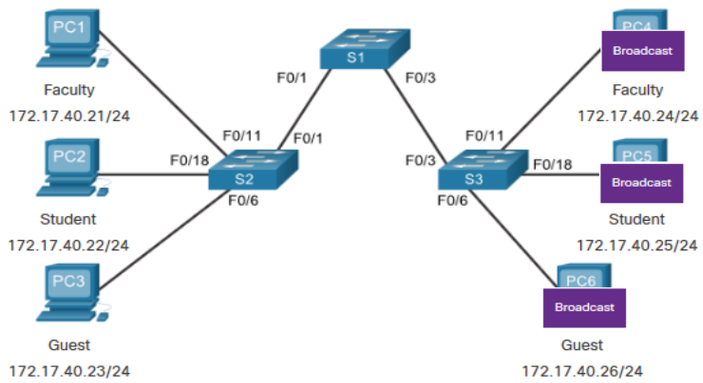
3.2.1. Defining VLAN Trunks

A trunk is a point-to-point link between two network devices.
Cisco trunk functions:

- Allow more than one VLAN
- Extend the VLAN across the entire network
- By default, supports all VLANs
- Supports 802.1Q trunking

3.2.2. Networks without VLANs

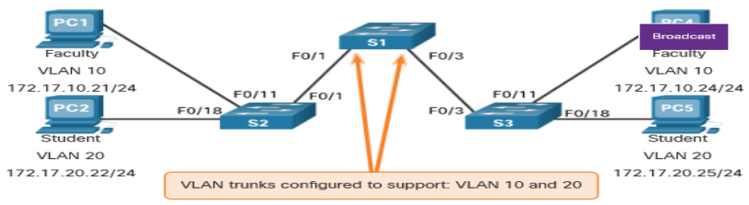
Without VLANs, all devices connected to the switches will receive all unicast, multicast, and broadcast traffic.



PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame out all available ports.

3.2.3 Networks with VLANs

With VLANs, unicast, multicast, and broadcast traffic is confined to a VLAN. Without a Layer 3 device to connect the VLANs, devices in different VLANs cannot communicate.



PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame only out ports configured for VLAN10.

3.2.4. VLAN Identification with a Tag

- The IEEE 802.1Q header is 4 Bytes
- When the tag is created the FCS must be recalculated.
- When sent to end devices, this tag must be removed and the FCS recalculated back to its original number.

802.1Q VLAN Tag Field	Function
Type	• 2-Byte field with hexadecimal 0x8100 • This is referred to as Tag Protocol ID (TPID)
User Priority	• 3-bit value that supports
Canonical Format Identifier (CFI)	• 1-bit value that can support token ring frames on Ethernet
VLAN ID (VID)	• 12-bit VLAN identifier that can support up to 4096 VLANs

3.2.5. Native VLANs and 802.1Q Tagging

802.1Q trunk basics:

- Tagging is typically done on all VLANs.
- The use of a native VLAN was designed for legacy use, like the hub in the example.
- Unless changed, VLAN1 is the native VLAN.
- Both ends of a trunk link must be configured with the same native VLAN.
- Each trunk is configured separately, so it is possible to have a different native VLANs on separate trunks.

3.2.6. Voice VLAN Tagging

The VoIP phone is a three port switch:

- The switch will use CDP to inform the phone of the Voice VLAN.
- The phone will tag its own traffic (Voice) and can set Cost of Service (CoS). CoS is QoS for layer 2.
- The phone may or may not tag frames from the PC.

Traffic	Tagging Function
Voice VLAN	tagged with an appropriate Layer 2 class of service (CoS) priority value
Access VLAN	can also be tagged with a Layer 2 CoS priority value
Access VLAN	is not tagged (no Layer 2 CoS priority value)

3.2.7. Voice VLAN Verification Example

The show interfaces fa0/18 switchport command can show us both data and voice VLANs assigned to the interface.

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (voice)
```

3.3. VLAN Configuration

3.3.1. VLAN Ranges on Catalyst Switches

Catalyst switches 2960 and 3650 support over 4000 VLANs.

Normal Range VLAN 1 – 1005	Extended Range VLAN 1006 - 4095
Used in Small to Medium sized businesses	Used by Service Providers
1002 – 1005 are reserved for legacy VLANs	Are in Running-Config
1, 1002 – 1005 are auto created and cannot be deleted	Supports fewer VLAN features
Stored in the vlan.dat file in flash	Requires VTP configurations
VTP can synchronize between switches	

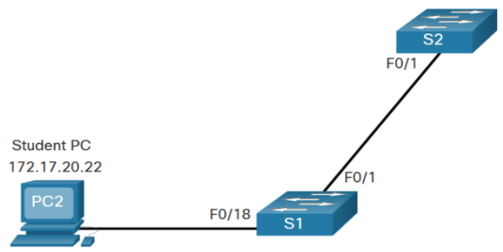
3.3.2. VLAN Creation Commands

VLAN details are stored in the vlan.dat file. You create VLANs in the global configuration mode.

Task	IOS Command
Enter global configuration mode.	Switch# **configure terminal**
Create a VLAN with a valid ID number.	Switch(config)# **vlan** *vlan-id*
Specify a unique name to identify the VLAN.	Switch(config-vlan)# **name** *vlan-name*
Return to the privileged EXEC mode.	Switch(config-vlan)# **end**
Enter global configuration mode.	Switch# **configure terminal**

3.3.3. VLAN Creation Example

- If the Student PC is going to be in VLAN 20, we will create the VLAN first and then name it.
- If you do not name it, the Cisco IOS will give it a default name of vlan and the four digit number of the VLAN. E.g. vlan0020 for VLAN 20.



Prompt	Command
S1#	Configure terminal
S1(config)#	vlan 20
S1(config-vlan)#	name student
S1(config-vlan)#	end

3.3.4. VLAN Port Assignment Commands

Once the VLAN is created, we can then assign it to the correct interfaces.

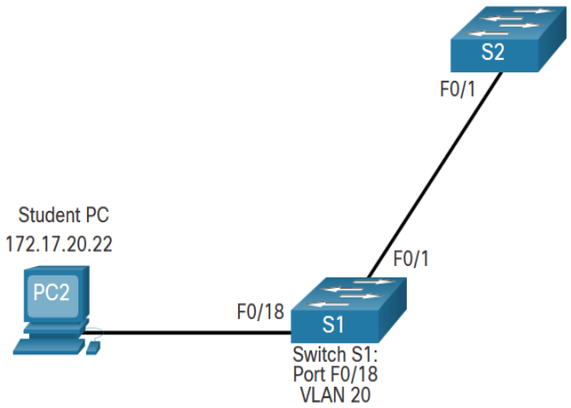
Task	Command
Enter global configuration mode.	Switch# configure terminal
Enter interface configuration mode.	Switch(config)# interface *interface-id*
Set the port to access mode.	Switch(config-if)# switchport mode access
Assign the port to a VLAN.	Switch(config-if)# switchport access vlan *vlan-id*
Return to the privileged EXEC mode.	Switch(config-if)# end

3.3.5. VLAN Port Assignment Example

We can assign the VLAN to the port interface.

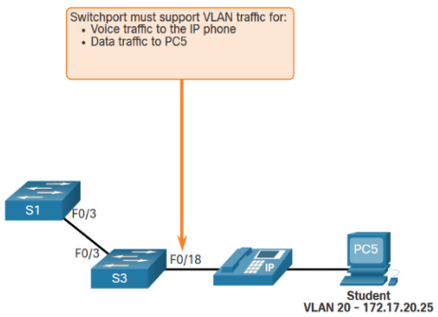
- Once the device is assigned the VLAN, then the end device will need the IP address information for that VLAN
- Here, Student PC receives 172.17.20.22

Prompt	Command
S1#	Configure terminal
S1(config)#	Interface fa0/18
S1(config-if)#	Switchport mode access
S1(config-if)#	Switchport access vlan 20
S1(config-if)#	end



3.3.6. Data and Voice VLANs

An access port may only be assigned to one data VLAN. However it may also be assigned to one Voice VLAN for when a phone and an end device are off of the same switchport.



3.3.7. Data and Voice VLAN Example

- We will want to create and name both Voice and Data VLANs.
- In addition to assigning the data VLAN, we will also assign the Voice VLAN and turn on QoS for the voice traffic to the interface.
- The newer catalyst switch will automatically create the VLAN, if it does not already exist, when it is assigned to an interface.

Note: QoS is beyond the scope of this course. Here we do show the use of the mls qos trust [cos | device cisco-phone | dscp | ip-precedence] command.

```
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# vlan 150
S1(config-vlan)# name VOICE
S1(config-vlan)# exit
S1(config)# interface fa0/18
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# mls qos trust cos
S1(config-if)# switchport voice vlan 150
S1(config-if)# end

% Access VLAN does not exist. Creating vlan 30
```

3.3.8 Verify VLAN Information

Use the show vlan command. The complete syntax is:

show vlan [brief | id *vlan-id* | name *vlan-name* | summary]

Task	Command Option
Display VLAN name, status, and its ports one VLAN per line.	brief
Display information about the identified VLAN ID number.	id *vlan-id*

Display information about the identified VLAN name. The *vlan-name* is an ASCII string from 1 to 32 characters.	name *vlan-name*
Display VLAN summary information.	summary

3.3.9 Change VLAN Port Membership

There are a number of ways to change VLAN membership:

- re-enter switchport access vlan *vlan-id* command
- use the no switchport access vlan to place association. interface back in VLAN 1

Use the show vlan brief or the show interface fa0/18 switchport commands to verify the correct VLAN

```
S1(config)# interface fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1#
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
                                                Gi0/1, Gi0/2
20   student                          active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

3.3.10. Delete VLANs

Delete VLANs with the no vlan *vlan-id* command.

Caution: Before deleting a VLAN, reassign all member ports to a different VLAN.

- Delete all VLANs with the delete flash:vlan.dat or delete vlan.dat commands.
- Reload the switch when deleting all VLANs.

Note: To restore to factory default – unplug all data cables, erase the startup-configuration and delete the vlan.dat file, then reload the device.

3.4. VLAN Trunks

3.4.1. Trunk Configuration Commands

Configure and verify VLAN trunks. Trunks are layer 2 and carry traffic for all VLANs.

Task	IOS Command
Enter global configuration mode.	Switch# **configure terminal**
Enter interface configuration mode.	Switch(config)# **interface** *interface-id*
Set the port to permanent trunking mode.	Switch(config-if)# **switchport mode trunk**
Sets the native VLAN to something other than VLAN 1.	Switch(config-if)# **switchport trunk native vlan** *vlan-id*
Specify the list of VLANs to be allowed on the trunk link.	Switch(config-if)# **switchport trunk allowed vlan** *vlan-list*
Return to the privileged EXEC mode.	Switch(config-if)# **end**

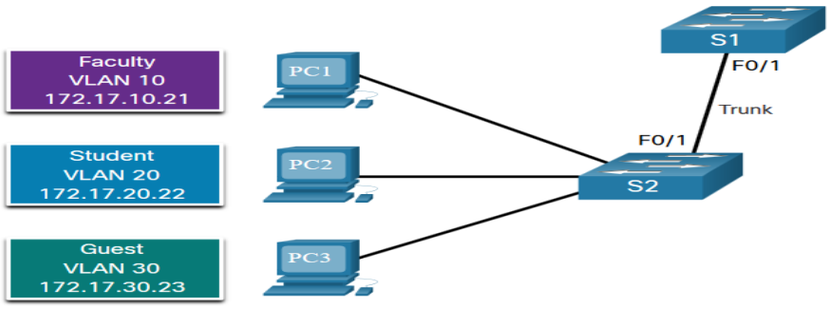
3.4.2. Trunk Configuration Example

The subnets associated with each VLAN are:

- VLAN 10 - Faculty/Staff - 172.17.10.0/24
- VLAN 20 - Students - 172.17.20.0/24
- VLAN 30 - Guests - 172.17.30.0/24
- VLAN 99 - Native - 172.17.99.0/24

F0/1 port on S1 is configured as a trunk port.

Note: This assumes a 2960 switch using 802.1q tagging. Layer 3 switches require the encapsulation to be configured before the trunk mode.



Prompt	Command
S1(config)#	**Interface fa0/1**
S1(config-if)#	Switchport mode trunk
S1(config-if)#	Switchport trunk native vlan 99
S1(config-if)#	Switchport trunk allowed vlan 10,20,30,99
S1(config-if)#	end

3.4.3. Verify Trunk Configuration

Set the trunk mode and native vlan.

Notice sh int fa0/1 switchport command:

- Is set to trunk administratively
- Is set as trunk operationally (functioning)
- Encapsulation is dot1q
- Native VLAN set to VLAN 99
- All VLANs created on the switch will pass traffic on this trunk

3.4.4. Reset the Trunk to the Default State

- Reset the default trunk settings with the no command.
  - All VLANs allowed to pass traffic
  - Native VLAN = VLAN 1
- Verify the default settings with a **sh int fa0/1 switchport** command.

Reset the trunk to an access mode with the **switchport mode access** command:

- Is set to an access interface administratively
- Is set as an access interface operationally (functioning)

3.5. Dynamic Trunking Protocol

3.5.1. Introduction to DTP

Dynamic Trunking Protocol (DTP) is a proprietary Cisco protocol.

DTP characteristics are as follows:

- On by default on Catalyst 2960 and 2950 switches
- Dynamic-auto is default on the 2960 and 2950 switches
- May be turned off with the nonegotiate command
- May be turned back on by setting the interface to dynamic-auto

- Setting a switch to a static trunk or static access will avoid negotiation issues with the switchport mode trunk or the switchport mode access commands.

```
S1(config-if)# switchport mode trunk
S1(config-if)# switchport nonegotiate
```

```
S1(config-if)# switchport mode dynamic auto
```

3.5.2. Negotiated Interface Modes

The switchport mode command has additional options.

Use the switchport nonegotiate interface configuration command to stop DTP negotiation.

Option	Description
access	Permanent access mode and negotiates to convert the neighboring link into an access link
dynamic auto	Will becomes a trunk interface if the neighboring interface is set to trunk or desirable mode
dynamic desirable	Actively seeks to become a trunk by negotiating with other auto or desirable interfaces
trunk	Permanent trunking mode and negotiates to convert the neighboring link into a trunk link

3.5.3. Results of a DTP Configuration

DTP configuration options are as follows:

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited connectivity
Access	Access	Access	Limited connectivity	Access

3.5.4. Verify DTP Mode

The default DTP configuration is dependent on the Cisco IOS version and platform.

- Use the show dtp interface command to determine the current DTP mode.
- Best practice recommends that the interfaces be set to access or trunk and to turnoff DTP

E. Evaluate

Packet Tracer Activity:

1. Packet Tracer 3.1.4: Who Hears the Broadcast?

In this Packet Tracer activity, you will do the following:

- Observe Broadcast Traffic in a VLAN Implementation
- Complete Review Questions

2. Packet Tracer 3.2.8: Investigate a VLAN Implementation

In this Packet Tracer activity, you will:

- Part 1: Observe Broadcast Traffic in a VLAN Implementation
- Part 2: Observe Broadcast Traffic without VLANs

3. **Packet Tracer 3.3.12: VLAN Configuration**

In this Packet Tracer activity, you will perform the following:

- Verify the Default VLAN Configuration
- Configure VLANs
- Assign VLANs to Ports

4. **Packet Tracer 3.4.5: Configure Trunks**

In this Packet Tracer activity, you will perform the following:

- Verify VLANs
- Configure Trunks

5. **Lab Activity 3.4.6: Configure VLANs and Trunks**

In this lab, you will perform the following:

- Build the Network and Configure Basic Device Settings
- Create VLANs and Assign Switch Ports
- Maintain VLAN Port Assignments and the VLAN Database
- Configure an 802.1Q Trunk between the Switches
- Delete the VLAN Database

6. **Packet Tracer 3.5.5: Configure DTP**

In this Packet Tracer activity, you will perform the following:

- Configure static trunking
- Configure and verify DTP

7. **Packet Tracer 3.6.1: Implement VLANs and Trunking**

In this Packet Tracer activity, you will perform the following:

- Configure VLANs
- Assign Ports to VLANs
- Configure Static Trunking
- Configure Dynamic Trunking

8. **Lab Activity 3.6.2: Implement VLANs and Trunking**

In this lab, you will perform the following:

- Build the Network and Configure Basic Device Settings
- Create VLANs and Assign Switch Ports
- Configure an 802.1Q Trunk between the Switches

Instruction: Module Quiz 3.6.4: Check your understanding of VLANs by choosing the BEST answer to the following questions.

1. Which distinct type of VLAN is used by an administrator to access and configure a switch?
   a. default VLAN
   b. native VLAN
   c. data VLAN
   d. management VLAN
2. What are three primary benefits of using VLANs? (Choose three.)
   a. security
   b. a reduction in the number of trunk links
   c. cost reduction
   d. end user satisfaction
   e. improved IT staff efficiency
   f. no required configuration
3. What happens to a port that is associated with VLAN 10 when the administrator deletes VLAN 10 from the switch?
   a. The port becomes inactive.
   b. The port goes back to the default VLAN.

c. The port automatically associates itself with the native VLAN.
d. The port creates the VLAN again.

4. In which memory location are the VLAN configurations of normal range VLANs stored on a Catalyst switch?
   a. flash
   b. NVRAM
   c. RAM
   d. ROM
5. An administrator is investigating a failure on a trunk link between a Cisco switch and a switch from another vendor. After a few show commands, the administrator notices that the the switches are not negotiating a trunk. What is a probable cause for this issue?
   a. Both switches are in trunk mode.
   b. Both switches are in nonegotiate mode.
   c. Switches from other vendors do not support DTP.
   d. DTP frames are flooding the entire network.
6. What is the purpose of the vlan.dat file on a switch?
   a. It holds the running configuration.
   b. It holds the saved configuration.
   c. It holds the VLAN database.
   d. It holds the operating system.
7. Where is the vlan.dat file stored on a switch?
   a. in RAM
   b. in NVRAM
   c. in flash memory
   d. on the externally attached storage media or internal hard drive
8. On a Cisco switch, where is extended range VLAN information stored?
   a. running configuration file
   b. startup configuration file
   c. NVRAM
   d. flash
9. If an organization is changing to include Cisco IP phones in its network, what design feature must be considered to ensure voice quality?
   a. Voice traffic needs to be tagged with the native VLAN.
   b. A separate VLAN is needed for voice traffic.
   c. Additional switch ports that are dedicated to Cisco IP phones are required.
   d. Voice traffic and data traffic require separate trunk links between switches.
10. In which location are the normal range VLANs stored on a Cisco switch by default?
    a. flash memory
    b. startup-config
    c. running-config
    d. RAM
11. A Cisco switch currently allows traffic tagged with VLANs 10 and 20 across trunk port Fa0/5. What is the effect of issuing a switchport trunk allowed vlan 30 command on Fa0/5?
    a. It allows VLANs 1 to 30 on Fa0/5.
    b. It allows VLANs 10, 20, and 30 on Fa0/5.
    c. It allows only VLAN 30 on Fa0/5.
    d. It allows a native VLAN of 30 to be implemented on Fa0/5.
12. What is the purpose of setting the native VLAN separate from data VLANs?
    a. The native VLAN is for carrying VLAN management traffic only.
    b. The security of management frames that are carried in the native VLAN can be enhanced.
    c. A separate VLAN should be used to carry uncommon untagged frames to avoid bandwidth contention on data VLANs.

d. The native VLAN is for routers and switches to exchange their management information, so it should be different from data VLANs.

13. When a Cisco switch receives untagged frames on a 802.1Q trunk port, which VLAN ID is the traffic switched to by default?
    a. unused VLAN ID
    b. native VLAN ID
    c. data VLAN ID
    d. management VLAN ID
14. A network administrator is determining the best placement of VLAN trunk links. Which two types of point-to-point connections utilize VLAN trunking? (Choose two.)
    a. between two switches that utilize multiple VLANs
    b. between a switch and a client PC
    c. between a switch and a server that has an 802.1Q NIC
    d. between a switch and a network printer
    e. between two switches that share a common VLAN
15. Which type of VLAN is assigned to 802.1Q trunk ports to carry untagged traffic?
    a. Default
    b. Native
    c. Data
    d. Management

References

1. *CCNAv7 Switching, Routing and Wireless Essential*
   https://www.netacad.com

Contact Information of the Facilitator

Name	:	*Herminigilda E.Pabillo*
MS Teams Account (email)	:	*herminigilda.pabillo@aics.edu.ph*
Smart Phone Number	:	*09235936747*