



Module 3: VLANs

Instructor Materials

Switching, Routing, and
Wireless Essentials v7.0
(SRWE)



What to Expect in this Module

- To facilitate learning, the following features within the GUI may be included in this module:

| Feature | Description |
|-------------------------------|--|
| Animations | Expose learners to new skills and concepts. |
| Videos | Expose learners to new skills and concepts. |
| Check Your Understanding(CYU) | Per topic online quiz to help learners gauge content understanding. |
| Interactive Activities | A variety of formats to help learners gauge content understanding. |
| Syntax Checker | Small simulations that expose learners to Cisco command line to practice configuration skills. |
| PT Activity | Simulation and modeling activities designed to explore, acquire, reinforce, and expand skills. |

What to Expect in this Module (Cont.)

- To facilitate learning, the following features may be included in this module:

| Feature | Description |
|------------------|--|
| Hands-On Labs | Labs designed for working with physical equipment. |
| Class Activities | These are found on the Instructor Resources page. Class Activities are designed to facilitate learning, class discussion, and collaboration. |
| Module Quizzes | Self-assessments that integrate concepts and skills learned throughout the series of topics presented in the module. |
| Module Summary | Briefly recaps module content. |



Module 3: VLANs

Switching, Routing, and
Wireless Essentials v7.0
(SRWE)



Module Objectives

Module Title: Protocols and Models

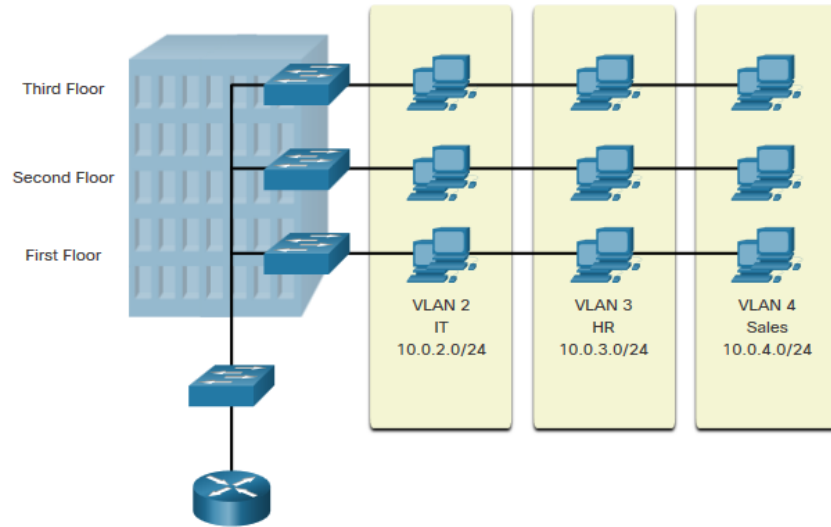
Module Objective: Explain how network protocols enable devices to access local and remote network resources.

| Topic Title | Topic Objective |
|---------------------------------------|---|
| Overview of VLANs | Explain the purpose of VLANs in a switched network. |
| VLANs in a Multi-Switched Environment | Explain how a switch forwards frames based on VLAN configuration in a multi-switch environment. |
| VLAN Configuration | Configure a switch port to be assigned to a VLAN based on requirements. |
| VLAN Trunks | Configure a trunk port on a LAN switch. |
| Dynamic Trunking Protocol | Configure Dynamic Trunking Protocol (DTP). |

3.1 Overview of VLANs

Overview of VLANs

VLAN Definitions



VLANs are logical connections with other similar devices.

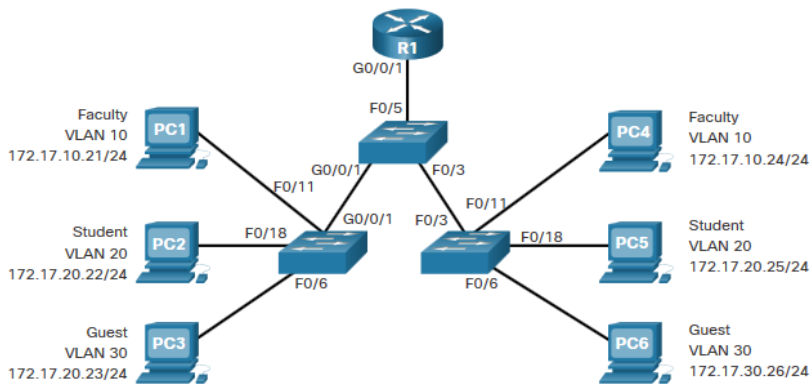
Placing devices into various VLANs have the following characteristics:

- 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

Overview of VLANs

Benefits of a VLAN Design

Benefits of using VLANs are as follows:



| 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 |

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

Types of VLANs (Cont.)

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.

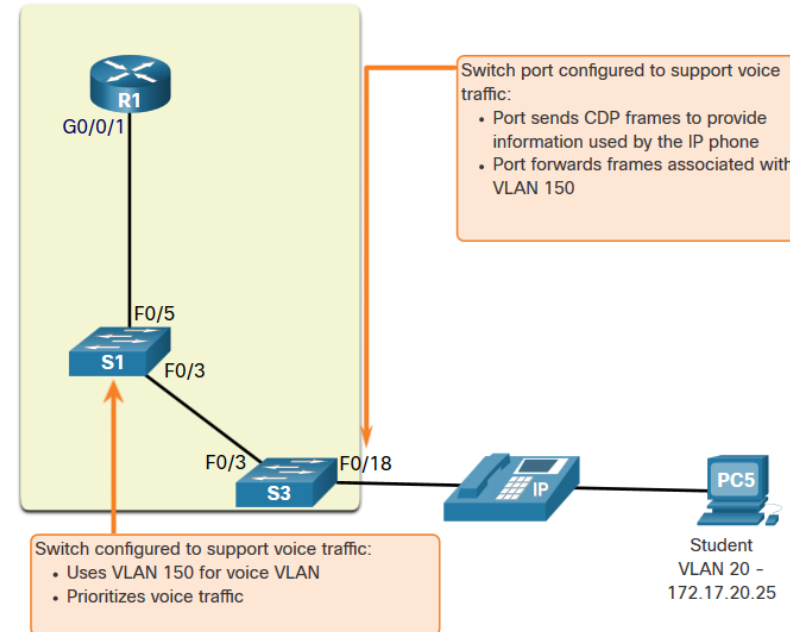
Management VLAN

- 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.

Types of VLANs (Cont.)

Voice VLAN

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



Packet Tracer – Who Hears the Broadcast?

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

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

3.2 VLANs in a Multi-Switched Environment

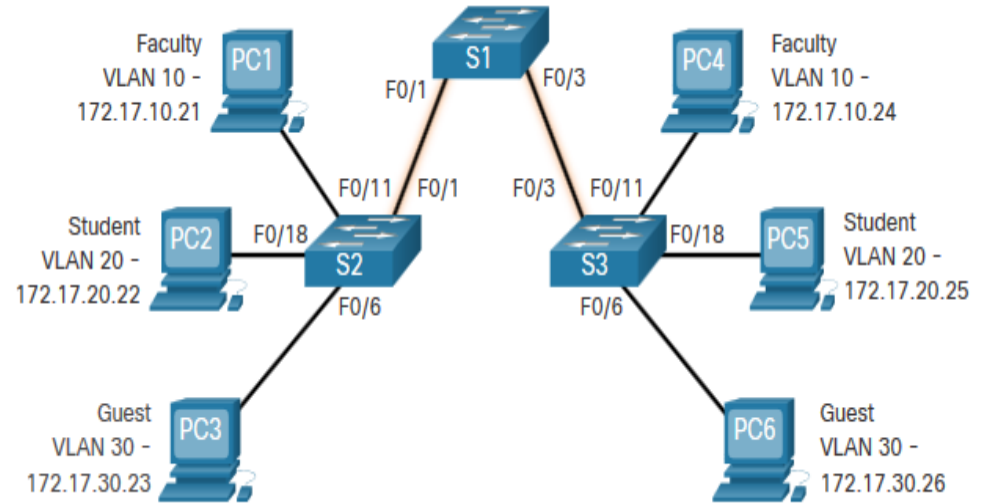
VLANs in a Multi-Switched Environment

Defining VLAN Trunks

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

Cisco trunk functions:

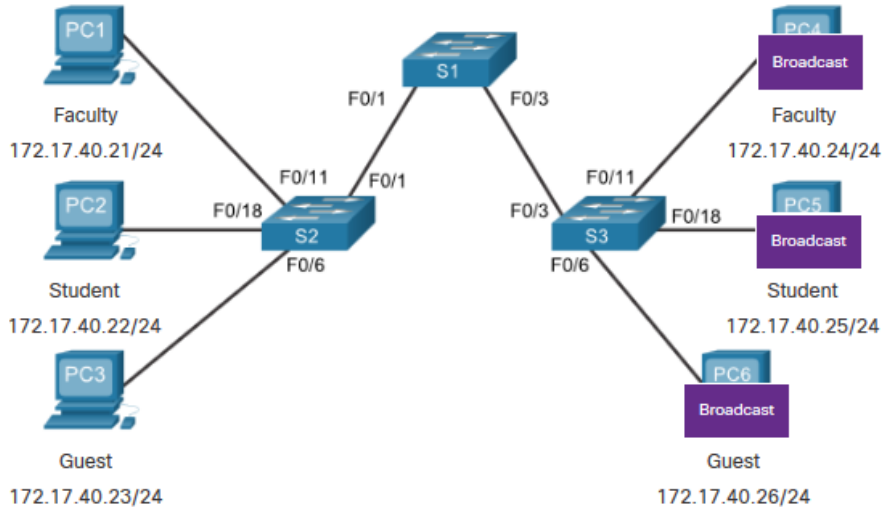
- Allow more than one VLAN
- Extend the VLAN across the entire network
- By default, supports all VLANs
- Supports 802.1Q trunking



VLANs in a Multi-Switched Environment

Networks without VLANs

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

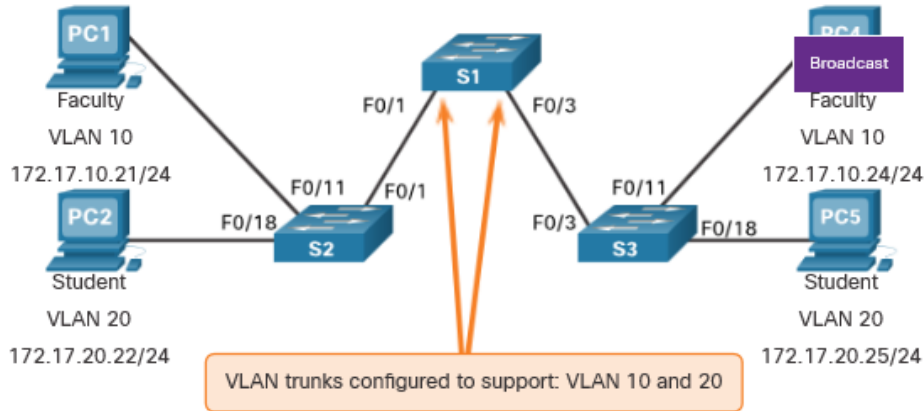


PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame out all available ports.

VLANs in a Multi-Switched Environment

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.

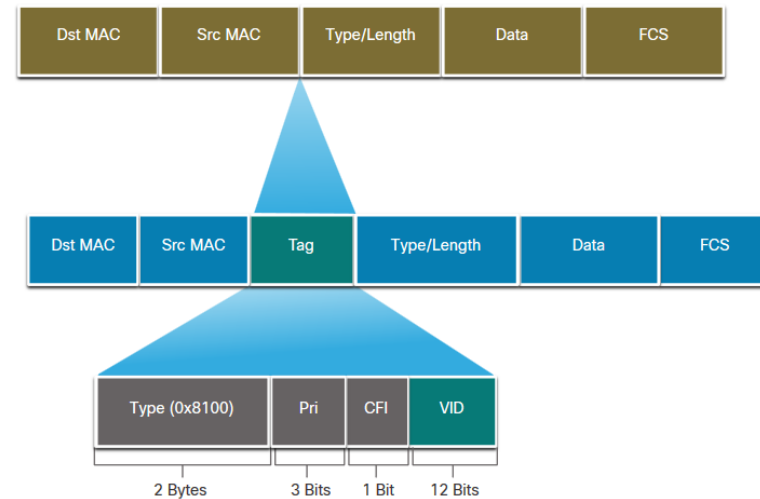


PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame only out ports configured for VLAN10.

VLANs in a Multi-Switched Environment

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.



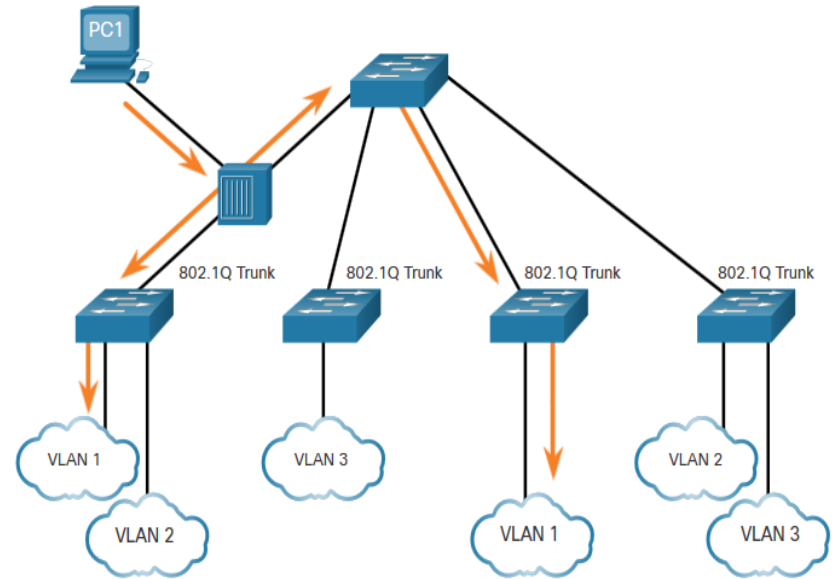
| 802.1Q VLAN Tag Field | Function |
|-----------------------------------|--|
| Type | <ul style="list-style-type: none">• 2-Byte field with hexadecimal 0x8100• This is referred to as Tag Protocol ID (TPID) |
| User Priority | <ul style="list-style-type: none">• 3-bit value that supports |
| Canonical Format Identifier (CFI) | <ul style="list-style-type: none">• 1-bit value that can support token ring frames on Ethernet |
| VLAN ID (VID) | <ul style="list-style-type: none">• 12-bit VLAN identifier that can support up to 4096 VLANs |

VLANs in a Multi-Switched Environment

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.

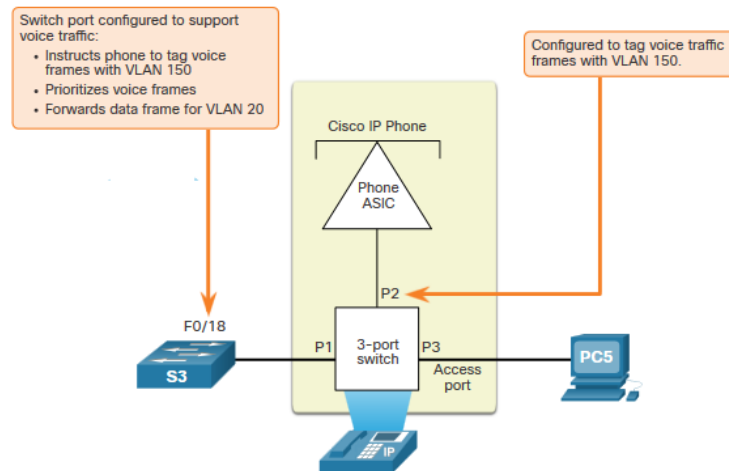


VLANs in a Multi-Switched Environment

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) |

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)
```

Packet Tracer – 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

3.3 VLAN Configuration

VLAN Ranges on Catalyst Switches

Catalyst switches 2960 and 3650 support over 4000 VLANs.

```
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 |

Normal Range VLAN 1 – 1005

Used in Small to Medium sized businesses

1002 – 1005 are reserved for legacy VLANs

1, 1002 – 1005 are auto created and cannot be deleted

Stored in the vlan.dat file in flash

VTP can synchronize between switches

Extended Range VLAN 1006 - 4095

Used by Service Providers

Are in Running-Config

Supports fewer VLAN features

Requires VTP configurations

VLAN Creation Commands

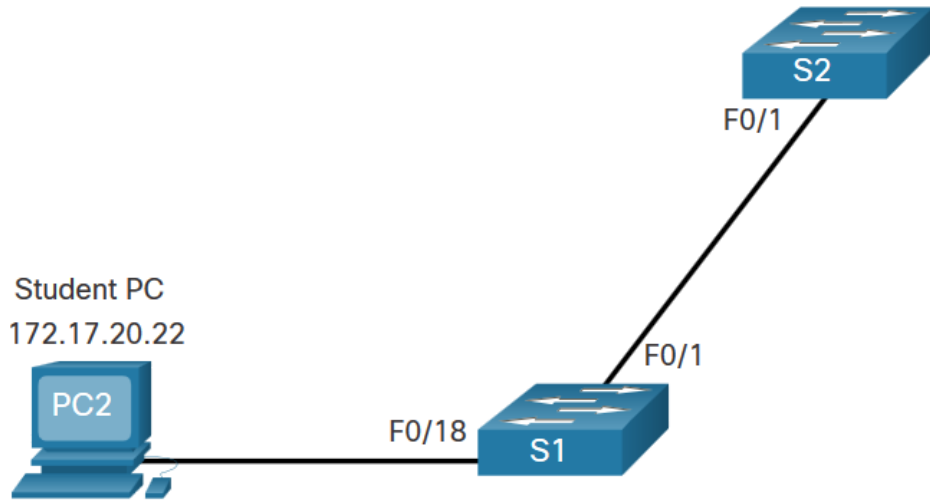
VLAN details are stored in the `vlan.dat` file. You create VLANs in the global configuration mode.

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

VLAN Configuration

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 |

VLAN Port Assignment Commands

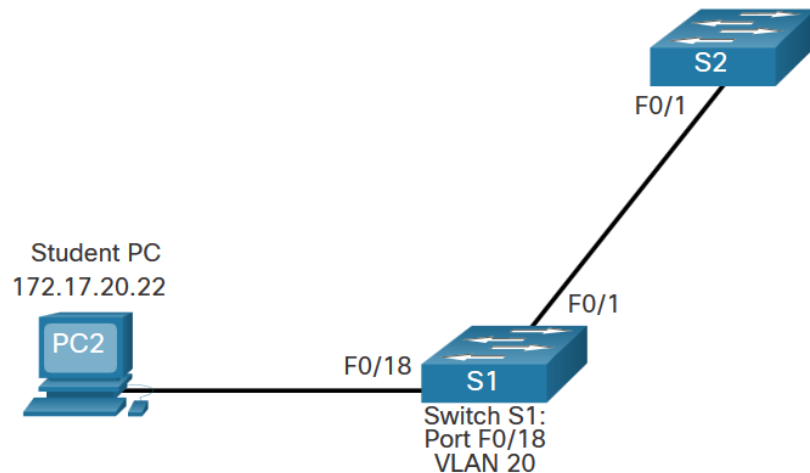
Once the VLAN is created, we can then assign it to the correct interfaces.

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

VLAN Port Assignment Example

We can assign the VLAN to the port interface.

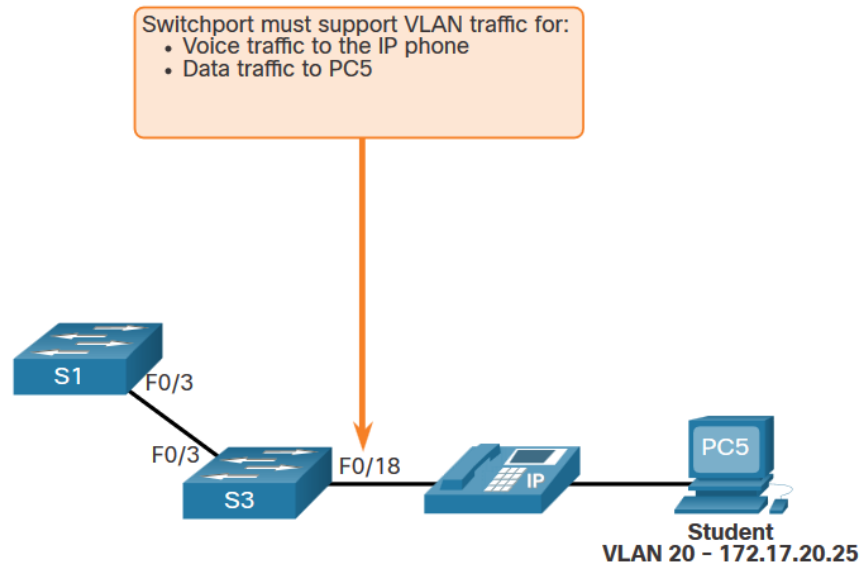
- Once the device is assigned the VLAN, then the end device will need the IP address information for that VLAN
- Here, Student PC receives 172.17.20.22



| 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 |

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.



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
```

VLAN Configuration

Verify VLAN Information

Use the **show vlan** command. The complete syntax is:

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

```
S1# show vlan summary
Number of existing VLANs           : 7
Number of existing VTP VLANs      : 7
Number of existing extended VLANs : 0
```

```
S1# show interface vlan 20
Vlan20 is up, line protocol is up
  Hardware is EtherSVI, address is 001f.6ddb.3ec1 (bia 001f.6ddb.3ec1)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set

(Output omitted)
```

| Task | Command Option |
|--|------------------------------|
| Display VLAN name, status, and its ports one VLAN per line. | brief |
| Display information about the identified VLAN ID number. | id <i>vlan-id</i> |
| Display information about the identified VLAN name. The <i>vlan-name</i> is an ASCII string from 1 to 32 characters. | name <i>vlan-name</i> |
| Display VLAN summary information. | summary |

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 interface back in VLAN 1

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

```
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)
```

VLAN Configuration

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.

Packet Tracer – VLAN Configuration

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

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

3.4 VLAN Trunks

Trunk Configuration Commands

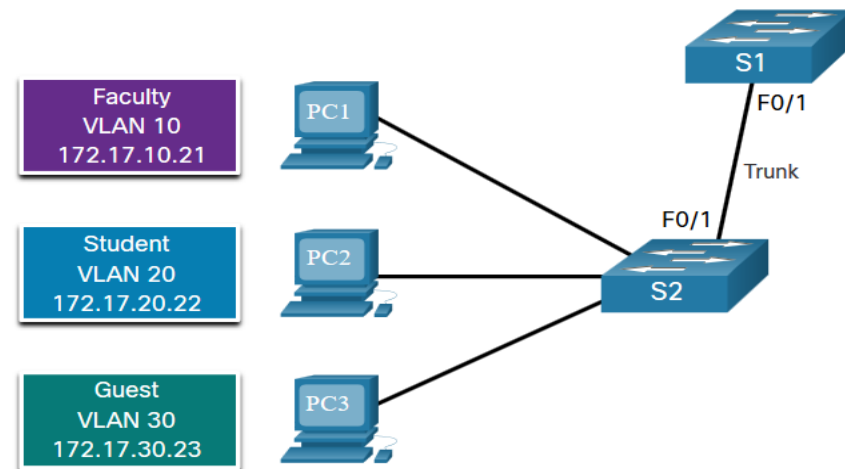
Configure and verify VLAN trunks. Trunks are layer 2 and carry traffic for all VLANs.

| Task | IOS Command |
|--|--|
| Enter global configuration mode. | Switch# configure terminal |
| Enter interface configuration mode. | Switch(config)# interface <i>interface-id</i> |
| 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 <i>vlan-id</i> |
| Specify the list of VLANs to be allowed on the trunk link. | Switch(config-if)# switchport trunk allowed vlan <i>vlan-list</i> |
| Return to the privileged EXEC mode. | Switch(config-if)# end |

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 |

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

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
S1(config-if)# no switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

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.

```
S1(config)# interface fa0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
```

```
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

Reset the Trunk to the Default State (Cont.)

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)

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
(output omitted)
```

Packet Tracer – Configure Trunks

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

- Verify VLANs
- Configure Trunks

Lab – 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

3.5 Dynamic Trunking Protocol

Dynamic Trunking Protocol

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
```

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 |

Dynamic Trunking Protocol

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 |

Dynamic Trunking Protocol

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

```
S1# show dtp interface fa0/1
DTP information for FastEthernet0/1:
TOS/TAS/TNS: ACCESS/AUTO/ACCESS
TOT/TAT/TNT: NATIVE/NEGOTIATE/NATIVE
Neighbor address 1: C80084AEF101
Neighbor address 2: 000000000000
Hello timer expiration (sec/state): 11/RUNNING
Access timer expiration (sec/state): never/STOPPED
Negotiation timer expiration (sec/state): never/STOPPED
Multidrop timer expiration (sec/state): never/STOPPED
FSM state: S2:ACCESS
# times multi & trunk 0
Enabled: yes
In STP: no
```

Packet Tracer – Configure DTP

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

- Configure static trunking
- Configure and verify DTP

3.6 Module Practice and Quiz

Packet Tracer – 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

Lab – 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

What did I learn in this module?

- VLANs are based on logical instead of physical connections.
- VLANs can segment networks based on function, team, or application.
- Each VLAN is considered a separate logical network.
- A trunk is a point-to-point link that carries more than one VLAN.
- VLAN tag fields include the type, user priority, CFI and VID.
- A separate voice VLAN is required to support VoIP.
- Normal range VLAN configurations are stored in the vlan.dat file in flash.
- An access port can belong to one data VLAN at a time, but may also have a Voice VLAN.

What did I learn in this module? (Cont.)

- A trunk is a Layer 2 link between two switches that carries traffic for all VLANs.
- Trunks will need tagging for the various VLANs, typically 802.1q .
- IEEE 802.1q tagging makes provision for one native VLAN that will remain untagged.
- An interface can be set to trunking or nontrunking.
- Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP).
- DTP is a Cisco proprietary protocol that manages trunk negotiations.

