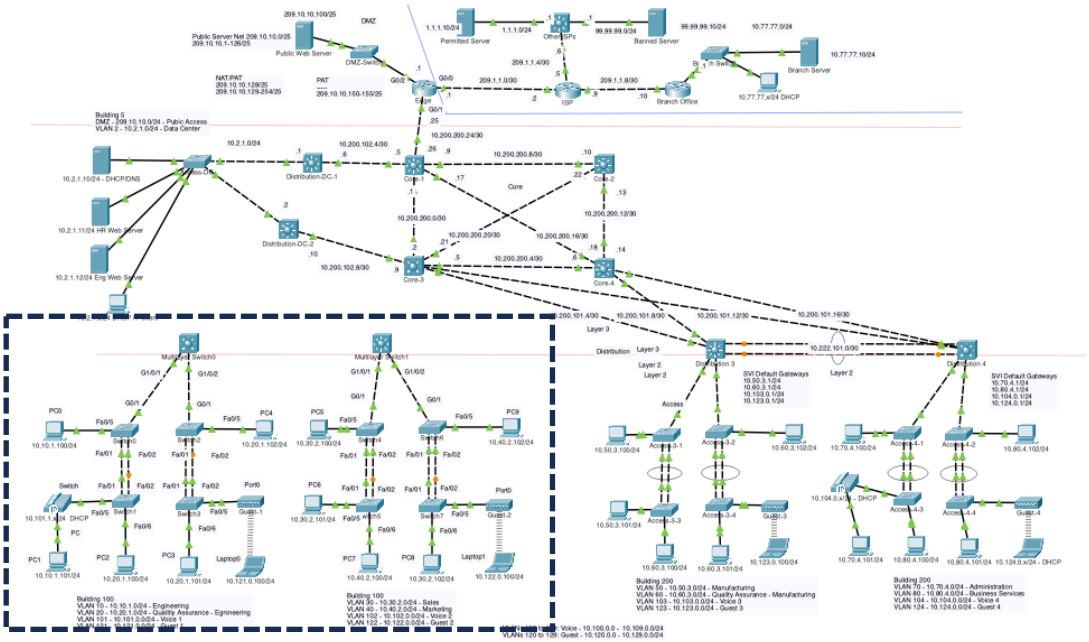
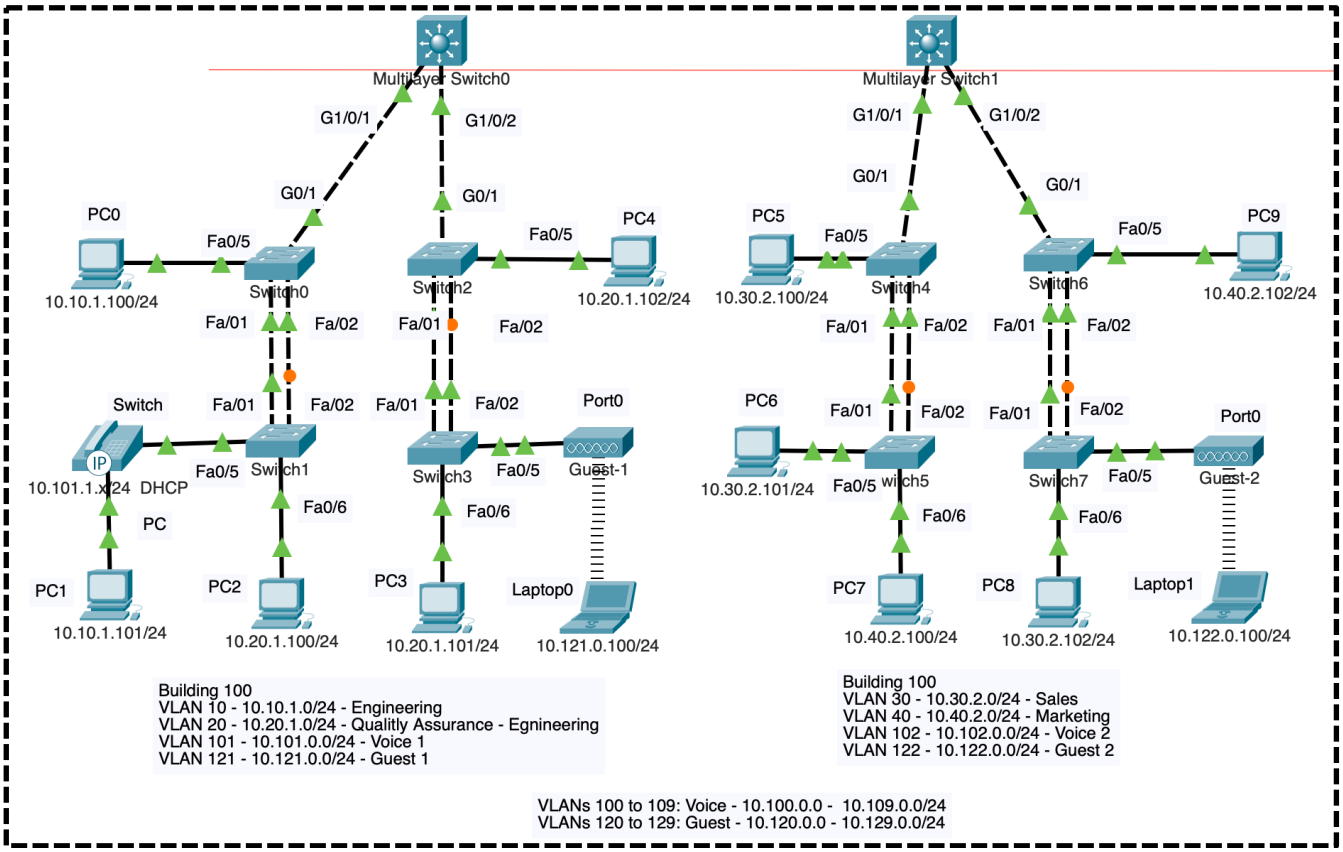
Enterprise Network

Lab 2: VLANs and Trunks





Objectives

List of objectives covered in this lab:

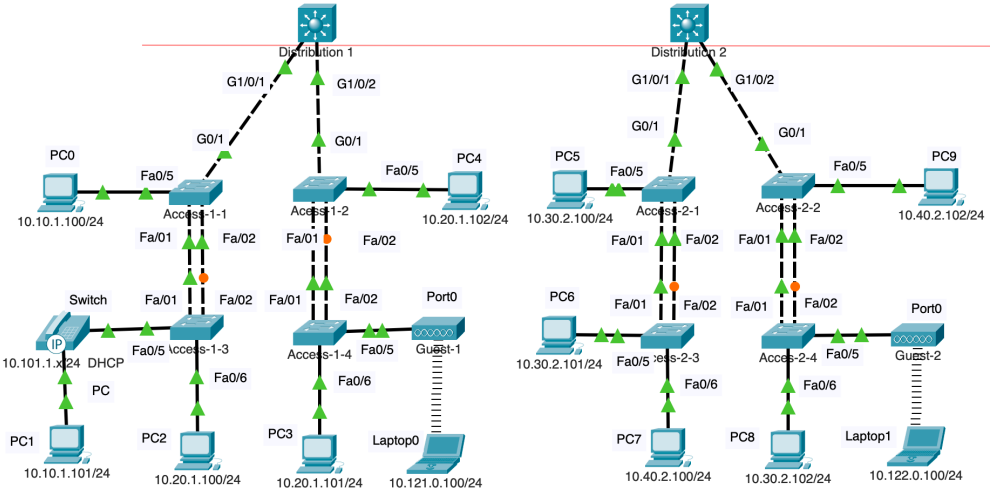
- **Basic IOS CLI Configuration**: Configure switch hostnames, disable DNS lookups, and secure access with encrypted passwords and SSH settings.
- **VLAN Creation and Assignment**: Create VLANs, assign appropriate names, and configure ports to associate with the correct VLANs for logical segmentation.
- **Access Port Configuration**: Configure access ports for end devices, ensuring proper VLAN tagging and traffic isolation.
- **Trunk Port Configuration**: Configure trunk links to carry multiple VLANs across switches, including setting native VLANs, restricting allowed VLANs, and disabling DTP for consistency.
- **Parking-Lot VLAN Configuration**: Assign unused ports to a non-routed VLAN and place them in a shutdown state to enhance security and simplify port management.
- **Verification Commands**: Use commands like show vlan brief, show mac address-table, and show spanning-tree to verify VLAN configurations, MAC address mappings, and ensure loop-free topologies.
- **Network Communication Validation**: Test communication between devices on the same VLAN to confirm proper configuration and traffic isolation.
- **Introduction to Inter-VLAN Routing**: Highlight the need for routing to enable communication between VLANs, to be covered in a future lab.

Display Names and Basic IOS CLI Configuration

Modify Display Names

Modify the display names for each switch:

- Distribution 1, Access-1-1, Access-1-2, Access-1-3, Access-1-4
- Distribution 2, Access-2-1, Access-2-2, Access-2-3, Access-2-4



Basic IOS CLI Configuration

These commands are used to set up the initial configuration of an access layer switch with basic security and access settings. It's important to note that using the passwords 'cisco', 'class', and 'sshadmin' are not secure and it's recommended to use stronger, unique passwords for device security.

Configure all the recently added switches with the following example configuration, including both the 2960 Access and 3650 Multilayer switches. Be sure to change the hostname to match the display name.

```
Switch>enable
Switch#conf t

Switch(config)#hostname access-1-1
access-1-1(config)#no ip domain-lookup

access-1-1(config)#enable secret class

access-1-1(config)#username admin secret sshadmin
access-1-1(config)#ip domain-name SSH-KEY.com

access-1-1(config)#line con 0
access-1-1(config-line)# exec-timeout 0 0
access-1-1(config-line)# logging synchronous
access-1-1(config-line)# password cisco
access-1-1(config-line)# login
access-1-1(config-line)# exit

access-1-1(config)#line vty 0 15
access-1-1(config-line)# login local
access-1-1(config-line)# transport input ssh
access-1-1(config-line)# exit
access-1-1(config)#end

access-1-1#copy running-config startup-config
```

Copy/Paste

```
enable
conf t

hostname HOSTNAME
no ip domain-lookup

enable secret class

username admin secret sshadmin
ip domain-name SSH-KEY.com

line con 0
exec-timeout 0 0
logging synchronous
password cisco
login
exit

line vty 0 15
login local
transport input ssh
exit
end

copy running-config startup-config
```

Hostname and Preventing DNS Lookups

- Switch(config)# **hostname access-1-1**: Changes the switch's hostname to access-1-1 for easier identification.
- access-1-1(config)# **no ip domain-lookup**: Disables DNS lookup to prevent delays when mistyped commands are interpreted as hostnames.

Privileged-Exec and SSH Password/Key

- access-1-1(config)# **enable secret class**: Sets the privileged EXEC mode password to class in an encrypted format for added security.
- access-1-1(config)# **username admin secret sshadmin**: Creates a local user account named admin with the encrypted password sshadmin.
- access-1-1(config)# **ip domain-name SSH-KEY.com**: Sets the domain name for the switch, which is required for generating SSH keys.

Console Port

- access-1-1(config)# **line con 0**: Enters configuration mode for the console line.
- access-1-1(config-line)# **exec-timeout 0 0**: Disables the console idle timeout, allowing the console session to remain open indefinitely. This should only be configured in a lab networks, never in a production network.
- access-1-1(config-line)# **logging synchronous**: Prevents system messages from interrupting command input on the console.
- access-1-1(config-line)# **password cisco**: Sets the password for console access to cisco.
- access-1-1(config-line)# **login**: Enables password authentication for console access.

Remote Access (Virtual Terminal)

- access-1-1(config)# **line vty 0 15**: Enters configuration mode for all virtual terminal (VTY) lines (used for remote access).
- access-1-1(config-line)# **login local**: Configures VTY lines to use the local username and password database for authentication.
- access-1-1(config-line)# **transport input ssh**: Restricts remote access to SSH only, disabling Telnet for enhanced security.

Saving Running-Config to Startup-Config

- access-1-1# **copy running-config startup-config**: Saves the current running configuration to the startup configuration file to ensure changes persist after a reboot.

VLANS

A Virtual Local Area Network (VLAN) is a network construct that allows network administrators to partition and isolate a single physical network into multiple distinct broadcast domains. By doing so, each VLAN operates as if it were a separate physical network, enhancing security and reducing the risk of broadcast storms by limiting the broadcast domain to a single VLAN.

Each VLAN is typically associated with a unique IP network, which means devices within the same VLAN communicate with each other using IP addressing, even if they are spread across different physical locations. This association allows for efficient network management and improved traffic handling, as each VLAN can have its own network policies and resource allocation.

By default, all ports are on the same VLAN, VLAN 1. VLAN 1 is known as the default VLAN.

Same Broadcast Domain

```
access-1-1# show vlan

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
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
access-1-1#
```

VLAN 1 acts as the primary VLAN for management and initial configuration. Since all ports are in the same VLAN by default, they are also part of the same broadcast domain, meaning any broadcast traffic sent from one port is forwarded to all other ports on the switch. This setup allows devices connected to the switch to

communicate without additional configuration but can lead to unnecessary traffic if the network is not segmented into multiple VLANs.

MAC Address Table – By default, one broadcast domain

```
access-1-1# show mac address-table
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.630a.83b0    DYNAMIC     Fa0/5
   1    0001.96e8.0801    DYNAMIC     Fa0/1
   1    0001.96e8.0802    DYNAMIC     Fa0/2
   1    0002.1624.0b33    DYNAMIC     Fa0/1
   1    0002.167b.ac87    DYNAMIC     Gig0/1
   1    0030.f24c.cdb2    DYNAMIC     Gig0/1
   1    0060.4733.61a1    DYNAMIC     Fa0/1
   1    0060.7096.e001    DYNAMIC     Gig0/1
access-1-1#
```

The MAC address table displays learned source MAC addresses and source ports. The MAC address table confirms that all devices on both the 10.10.1.0/24 and 10.20.1.0/24 networks are part of VLAN 1, which operates as a single broadcast domain. This means that broadcast traffic sent by any device in VLAN 1 is propagated to all ports within this VLAN, regardless of the IP subnet. These MAC addresses belong to devices on different IP networks (10.10.1.0/24 and 10.20.1.0/24), but they are all part of VLAN 1, meaning they share the same Layer 2 broadcast domain despite being on separate Layer 3 networks.

An ARP request from 10.20.1.100 to 10.20.1.101 would be broadcast to all devices in VLAN 1, including those on the 10.10.1.0/24 network, even though only devices on the 10.20.1.0/24 network need it. Ideally, devices like 10.10.1.100 shouldn't receive ARP requests from other networks, highlighting the need for VLAN segmentation to limit unnecessary broadcast traffic.

Adding VLAN Numbers and Names

The VLANs on the switches that, which is part of the network you are configuring are:

VLAN ID	**Name**	**10.vlan.0.0/16**
1	Default	N/A
10	Engineering	10.10.0.0/16
20	QA - Engineering	10.20.0.0/16
30	Sales	10.30.0.0/16
40	Marketing	10.40.0/.016
101	Voice-1	10.101.0.0/16
102	Voice-2	10.102.0.0/16
121	Guest-1	10.121.0.0/16
122	Guest-2	10.122.0.0/16
180	Management	10.180.0.0/16
254	Native	10.254.0.0/16
255	Parking-Lot	10.255.0.0/16

Using the chart above add the following VLANs to all switches.

- **vlan <vlan ID>**: This command enters the VLAN configuration mode for a specific VLAN ID. VLANs are used to segment network traffic logically regardless of the physical connections or location of the devices.
- **name <name>**: While in the VLAN configuration mode, this command sets the name of the VLAN to a name. This is a descriptive identifier that helps in managing and identifying the VLAN across the network.

If the **vlan** command is not used, the VLAN will be created when an interface is configured to be a member of that VLAN ID.

Note: Creating these VLANs is required on the Distribution-1 and Distribution-2 switches that are not configured with access VLAN ports.

Add the following VLAN names and numbers to all switches. Note: The **exit** command is not required.

Configure on all switches:

```
access-1-1(config)# vlan 10
access-1-1(config-vlan)# name Engineering
access-1-1(config-vlan)# exit
access-1-1(config)# vlan 20
access-1-1(config-vlan)# name QA-Engineering
access-1-1(config-vlan)# exit
access-1-1(config)# vlan 30
access-1-1(config-vlan)# name Sales
access-1-1(config-vlan)# exit
access-1-1(config)# vlan 40
access-1-1(config-vlan)# name Marketing
access-1-1(config-vlan)# exit
access-1-1(config)# vlan 101
access-1-1(config-vlan)# name Voice-1
access-1-1(config-vlan)# exit
access-1-1(config)# vlan 102
access-1-1(config-vlan)# name Voice-2
access-1-1(config-vlan)# exit
access-1-1(config)# vlan 121
access-1-1(config-vlan)# name Guest-1
access-1-1(config-vlan)# exit
access-1-1(config)# vlan 122
access-1-1(config-vlan)# name Guest-2
access-1-1(config-vlan)# exit
access-1-1(config)# vlan 180
access-1-1(config-vlan)# name Management
access-1-1(config-vlan)# vlan 254
access-1-1(config-vlan)# name Native
access-1-1(config-vlan)# vlan 255
access-1-1(config-vlan)# name Parking-Lot
access-1-1(config-vlan)# exit
```

Re-examine the VLAN table after the new VLANs were created.

```
access-1-1# show vlan

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   Engineering                      active
20   QA-Engineering                   active
30   Sales                            active
40   Marketing                        active
101  Voice-1                          active
102  Voice-2                          active
121  Guest-1                          active
122  Guest-2                          active
180  Management                       active
254  Native                           active
255  Parking-Lot                      active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

<rest of output omitted for brevity>
```

The VLAN table now shows that several VLANs have been created, such as Engineering (VLAN 10), QA-Engineering (VLAN 20), Sales (VLAN 30), and others. However, all switch ports (FastEthernet and GigabitEthernet) remain assigned to VLAN 1 by default, indicating that no ports have yet been moved to the newly created VLANs. This means all devices are still in the same broadcast domain until ports are explicitly assigned to different VLANs.

Configuring Access Ports

Access ports are used to connect end devices, such as PCs or printers, to a switch and are configured to belong to a single VLAN. By configuring an access port, you ensure that all traffic from the connected device is tagged and associated with a specific VLAN for proper segmentation and communication.

```
access-1-1(config)# interface FastEthernet0/5
access-1-1(config-if)# switchport mode access
access-1-1(config-if)# switchport access vlan 10
access-1-1(config-if)# exit
```

The configuration of VLAN 10 on the port associates all traffic from the connected PC, which has an IP address on the 10.10.1.0/24 network, with VLAN 10. This ensures that the PC's traffic is logically segmented and forwarded only to other devices in VLAN 10, maintaining proper communication within the assigned subnet.

- **interface FastEthernet0/5**: Enters configuration mode for the specific interface FastEthernet0/5.
- **switchport mode access**: Configures the port as an access port, ensuring it only carries traffic for a single VLAN.
- **switchport access vlan 10**: Assigns the port to VLAN 10, tagging all traffic on this port as belonging to the Engineering VLAN.

Note: The **switchport mode access** command is not necessary to be explicitly stated if you are **not** using the port as a trunk port. By default, Cisco switch ports are in access mode if not configured otherwise. However, it's a common practice to include it in configurations for clarity, especially if the switch has been used for different configurations in the past. The **switchport mode access** command also prevents the port from becoming a trunk port via Dynamic Trunking Protocol (DTP). By explicitly configuring the port as an access port, it disables DTP negotiations, ensuring the port operates only as an access port and cannot dynamically negotiate to become a trunk.

Here are the commands for the rest of the access VLAN ports on all eight access switches. Notice that each VLAN number is associated with the devices IP network address on that interface.

```
! access-1-1

interface FastEthernet0/5
 switchport mode access
 switchport access vlan 10
 exit

! access-1-2

interface FastEthernet0/5
 switchport mode access
 switchport access vlan 20
 exit

! access-1-3

interface FastEthernet0/5
 switchport mode access
 switchport access vlan 10
 exit

interface FastEthernet0/6
 switchport mode access
 switchport access vlan 20
 exit

! access-1-4

interface FastEthernet0/5
 switchport mode access
 switchport access vlan 121
 exit

interface FastEthernet0/6
 switchport mode access
 switchport access vlan 20
 exit

! access-2-1
```

```
interface FastEthernet0/5
 switchport mode access
 switchport access vlan 30
 exit

! access-2-2

interface FastEthernet0/5
 switchport mode access
 switchport access vlan 40
 exit

! access-2-3

interface FastEthernet0/5
 switchport mode access
 switchport access vlan 30
 exit

interface FastEthernet0/6
 switchport mode access
 switchport access vlan 40
 exit

! access-2-4

interface FastEthernet0/5
 switchport mode access
 switchport access vlan 122
 exit

interface FastEthernet0/6
 switchport mode access
 switchport access vlan 30
 exit
```

Access Points

In our topology, the VLANs configured on the ports connected to access points are associated with the IP address of the end devices that connect to the wireless network through those access points, not the access points themselves. The access point functions as a bridge, transparently forwarding traffic from the wireless devices to the appropriate VLAN on the switch. As a result, the VLAN assignment is determined by the configuration of the switch port and is directly tied to the traffic originating from the connected end devices, ensuring proper segmentation and communication within the network.

Voice VLAN

After configuring the access port on access-1-3 (commands shown below), you will receive and Spanning Tree error message, also shown below.

```
access-1-3(config)# interface FastEthernet0/5
access-1-3(config-if)# switchport mode access
```

```
access-1-3(config-if)# switchport access vlan 10
access-1-3(config-if)# exit

access-1-3#%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id
10 on FastEthernet0/5 VLAN1.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/5 on VLAN0001. Inconsistent
local vlan.
```

The error message indicates a VLAN mismatch on port FastEthernet0/5, where the switch received a BPDU (Bridge Protocol Data Unit) from a connected device (likely the IP phone) with VLAN ID 10, while the local VLAN for Spanning Tree Protocol (STP) on the port is still set to VLAN 1. This inconsistency occurs because the port is configured as an access port for VLAN 10 but has not been properly configured for voice traffic, which likely uses a different VLAN. You will also notice that the link light on the port is amber.

To resolve this, you need to configure the port for the voice VLAN 101, as well as the previously configure data VLAN 10.

```
access-1-3(config)# interface FastEthernet0/5
access-1-3(config-if)# switchport voice vlan 101
access-1-3(config-if)# mls qos trust cos
access-1-3(config-if)# exit
```

We need to separate the voice traffic into its own VLAN, preventing the STP inconsistency and allowing proper communication for both voice and data devices.

- **switchport voice vlan 101**: Configures VLAN 101 as the dedicated VLAN for voice traffic on the port, ensuring proper separation of voice and data traffic.
- **mls qos trust cos**: Enables the switch to trust the Class of Service (CoS) value in incoming traffic, allowing for proper QoS (Quality of Service) prioritization, especially for voice traffic.

You will notice that the link light on port FastEthernet0/5 will now turn green in about 50 seconds.

Verifying the VLAN configuration

```
access-2-3# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                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   Engineering                      active
20   QA-Engineering                   active
30   Sales                            active    Fa0/5
40   Marketing                        active    Fa0/6
101  Voice-1                          active
102  Voice-2                          active
121  Guest-1                          active
```

```
122  Guest-2                          active
180  Management                       active
254  Native                           active
255  Parking-Lot                      active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
access-2-3#
```

The configured ports, such as Fa0/5 and Fa0/6 on access-2-3 switch, are now assigned to specific VLANs (e.g., VLAN 30 and VLAN 40 on access-2-3), meaning traffic on these ports is associated with their respective VLANs and broadcast domains. All other ports that have not been explicitly configured remain part of VLAN 1, the default VLAN, and share a single broadcast domain, as indicated in the **show vlan brief** output.

VLAN Trunks

A trunk is a network link designed to carry multiple VLANs through a single interface by tagging frames with VLAN identification. This allows for efficient VLAN distribution across switches and network segments, enabling devices in different VLANs to communicate through the same physical link while maintaining VLAN separation. This eliminates the need for a separate physical link for each VLAN, significantly reducing the number of required connections and simplifying network design.

```
distribution-1(config)# interface range GigabitEthernet1/0/1-2
distribution-1(config-if-range)# shutdown
distribution-1(config-if-range)# switchport mode trunk
distribution-1(config-if-range)# switchport trunk native vlan 254
distribution-1(config-if-range)# switchport trunk allowed vlan 1,10,20,30,40,101-
102,121-122,180,254
distribution-1(config-if-range)# switchport nonegotiate
distribution-1(config-if-range)# no shutdown
distribution-1(config-if-range)# exit

%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state to administratively
down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed
state to down

%LINK-5-CHANGED: Interface GigabitEthernet1/0/2, changed state to administratively
down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed
state to down

%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed
state to up

%LINK-5-CHANGED: Interface GigabitEthernet1/0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed
state to up

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
GigabitEthernet1/0/2 (254), with access-1-2 GigabitEthernet0/1 (1).
```

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
GigabitEthernet1/0/1 (254), with access-1-1 GigabitEthernet0/1 (1).

distribution-1(config)#
```

The following is brief description of each command:

- **interface range GigabitEthernet1/0/1-2**: Selects and allows configuration of the range of interfaces GigabitEthernet1/0/1 to GigabitEthernet1/0/2.
- **shutdown**: Disables the selected interfaces, effectively taking them offline. This command is not required but recommended before making significant changes to an interface.
- **switchport mode trunk**: Manually configures the interfaces to operate as trunk ports, ensuring they carry traffic for multiple VLANs.
- **switchport trunk native vlan 254**: Sets VLAN 254 as the native VLAN on the trunk, meaning untagged traffic on the trunk link will be associated with VLAN 254.
- **switchport trunk allowed vlan 1,10,20,30,40,101-102,121-122,180,254**: Restricts the trunk to carry only the specified VLANs, preventing unnecessary VLAN traffic on the link.
- **switchport nonegotiate**: Disables DTP (Dynamic Trunking Protocol) on the trunk, requiring manual trunk configuration on both ends of the link.
- **no shutdown**: Re-enables the previously disabled interfaces, bringing them back online.
- **exit**: Exits the interface configuration mode and returns to global configuration mode.

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
GigabitEthernet1/0/2 (254), with access-1-2 GigabitEthernet0/1 (1).
```

This error occurs because the native VLAN on GigabitEthernet1/0/1 (VLAN 254) does not match the native VLAN on the connected interface GigabitEthernet0/1 (VLAN 1). It will be resolved once the other side of the trunk link is configured with the same native VLAN (VLAN 254).

General VLAN Trunking Configuration

All of our trunk links will use the **same, consistent configurations** to ensure proper VLAN tagging and communication across the network. This includes setting the same native VLAN, allowing the same VLANs, and disabling DTP with switchport nonegotiate to maintain uniformity and prevent configuration mismatches.

The **interface range** command allows you to configure multiple interfaces simultaneously, making the process faster, more consistent, and less prone to errors compared to configuring each interface individually. This ensures uniform settings across multiple ports, which is especially useful for applying configurations like trunking or VLAN assignments to multiple links.

Configuring all VLAN Trunks: Same configuration, different interfaces

VLAN trunks will be configured for all inter-switch links. Be careful to include the correct interfaces. Notice that the VLAN trunking commands are identical on all switches.

```
! Distribution-1

! Trunk to both access switches

interface range GigabitEthernet1/0/1-2
 shutdown
 switchport mode trunk
```

```
 switchport trunk native vlan 254
 switchport trunk allowed vlan 1,10,20,30,40,101-102,121-122,180,254
 switchport nonegotiate
 no shutdown
 exit

! Distribution-2

! Trunk to both access switches

interface range GigabitEthernet1/0/1-2
 shutdown
 switchport mode trunk
 switchport trunk native vlan 254
 switchport trunk allowed vlan 1,10,20,30,40,101-102,121-122,180,254
 switchport nonegotiate
 no shutdown
 exit

! access-1-1

! Trunk to Distribution-1

interface GigabitEthernet0/1
 shutdown
 switchport mode trunk
 switchport trunk native vlan 254
 switchport trunk allowed vlan 1,10,20,30,40,101-102,121-122,180,254
 switchport nonegotiate
 no shutdown
 exit

! Trunk to Bottom Access

interface range FastEthernet0/1-2
 shutdown
 switchport mode trunk
 switchport trunk native vlan 254
 switchport trunk allowed vlan 1,10,20,30,40,101-102,121-122,180,254
 switchport nonegotiate
 no shutdown
 exit


! access-1-2

! Trunk to Distribution-1

interface GigabitEthernet0/1
 shutdown
 switchport mode trunk
 switchport trunk native vlan 254
 switchport trunk allowed vlan 1,10,20,30,40,101-102,121-122,180,254
 switchport nonegotiate
 no shutdown
 exit

! Trunk to Bottom Access
```

```
interface range FastEthernet0/1-2
 shutdown
 switchport mode trunk
 switchport trunk native vlan 254
 switchport trunk allowed vlan 1,10,20,30,40,101-102,121-122,180,254
 switchport nonegotiate
 no shutdown
 exit


! access-1-3

! Trunk to Top Access

interface range FastEthernet0/1-2
 shutdown
 switchport mode trunk
 switchport trunk native vlan 254
 switchport trunk allowed vlan 1,10,20,30,40,101-102,121-122,180,254
 switchport nonegotiate
 no shutdown
 exit


! access-1-4

! Trunk to Top Access

interface range FastEthernet0/1-2
 shutdown
 switchport mode trunk
 switchport trunk native vlan 254
 switchport trunk allowed vlan 1,10,20,30,40,101-102,121-122,180,254
 switchport nonegotiate
 no shutdown
 exit


! access-2-1

! Trunk to Distribution-2

interface GigabitEthernet0/1
 shutdown
 switchport mode trunk
 switchport trunk native vlan 254
 switchport trunk allowed vlan 1,10,20,30,40,101-102,121-122,180,254
 switchport nonegotiate
 no shutdown
 exit

! Trunk to Bottom Access

interface range FastEthernet0/1-2
 shutdown
 switchport mode trunk
 switchport trunk native vlan 254
 switchport trunk allowed vlan 1,10,20,30,40,101-102,121-122,180,254
 switchport nonegotiate
```

```
 no shutdown
 exit


! access-2-2

! Trunk to Distribution-2

interface GigabitEthernet0/1
 shutdown
 switchport mode trunk
 switchport trunk native vlan 254
 switchport trunk allowed vlan 1,10,20,30,40,101-102,121-122,180,254
 switchport nonegotiate
 no shutdown
 exit

! Trunk to Bottom Access

interface range FastEthernet0/1-2
 shutdown
 switchport mode trunk
 switchport trunk native vlan 254
 switchport trunk allowed vlan 1,10,20,30,40,101-102,121-122,180,254
 switchport nonegotiate
 no shutdown
 exit


! access-2-3

! Trunk to Top Access

interface range FastEthernet0/1-2
 shutdown
 switchport mode trunk
 switchport trunk native vlan 254
 switchport trunk allowed vlan 1,10,20,30,40,101-102,121-122,180,254
 switchport nonegotiate
 no shutdown
 exit


! access-2-4

! Trunk to Top Access

interface range FastEthernet0/1-2
 shutdown
 switchport mode trunk
 switchport trunk native vlan 254
 switchport trunk allowed vlan 1,10,20,30,40,101-102,121-122,180,254
 switchport nonegotiate
 no shutdown
 exit
```

Reflection: Did we break anything and why did we do all of this?

Did we break anything?

Verify that there are still successful commutations between devices on the same IP network, same VLAN.

From PC-0 10.10.1.100/24 ping PC-1 10.10.1.101.

```
C:\>ping 10.10.1.101

Pinging 10.10.1.101 with 32 bytes of data:

Reply from 10.10.1.101: bytes=32 time<1ms TTL=128
Reply from 10.10.1.101: bytes=32 time<1ms TTL=128
Reply from 10.10.1.101: bytes=32 time<1ms TTL=128
Reply from 10.10.1.101: bytes=32 time=17ms TTL=128

Ping statistics for 10.10.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 4ms

C:\>
```

Notice that this communication is successful.

From PC-2 10.20.1.100/24 ping PC-3 10.20.1.101.

```
C:\>ping 10.20.1.101

Pinging 10.20.1.101 with 32 bytes of data:

Reply from 10.20.1.101: bytes=32 time<1ms TTL=128
Reply from 10.20.1.101: bytes=32 time<1ms TTL=128
Reply from 10.20.1.101: bytes=32 time<1ms TTL=128
Reply from 10.20.1.101: bytes=32 time<1ms TTL=128

Ping statistics for 10.20.1.101:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Notice that this communication is also successful.

This verifies that we still have successful communications between devices in the same IP networks, same VLAN.

Why did we do all of this?

The configuration of VLANs and trunking made significant improvements to the network in several ways:

1. **Broadcast Domains**: By assigning devices to specific VLANs, we reduced the size of each broadcast domain, ensuring that broadcast traffic is contained within the VLAN and does not affect devices outside it. This minimizes unnecessary traffic and improves network efficiency.
2. **Security**: VLANs provide logical segmentation of the network, ensuring that traffic from different departments or functions (e.g., Engineering, Sales, Marketing) is isolated. This prevents unauthorized access between VLANs and enhances security by limiting the scope of potential attacks.
3. **Performance**: With smaller broadcast domains, the network experiences less congestion from broadcast traffic, leading to improved performance for devices within each VLAN. Additionally, the separation of voice traffic into dedicated VLANs ensures better Quality of Service (QoS) for latency-sensitive applications.
4. **Troubleshooting**: VLAN segmentation makes troubleshooting easier by clearly defining which devices should communicate within each VLAN. This allows for quick identification of issues, such as misconfigured VLANs or trunk links, by examining the MAC address table and verifying VLAN memberships.
5. **Scalability**: Trunking allows multiple VLANs to share a single physical link between switches, making it easier to scale the network without requiring additional cables for every VLAN. This setup is especially valuable for larger networks where many VLANs need to span multiple switches.
6. **MAC Address Table**: The MAC address table now reflects the segmentation, with entries for specific VLANs tied to their respective ports. This organization ensures that Layer 2 forwarding is precise and aligns with VLAN configurations, reducing confusion and ensuring traffic flows efficiently.

The MAC address tables will now show MAC address and port numbers associated with a specific VLAN.

```
access-1-1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.96e8.0801    DYNAMIC     Fa0/1
   1    0001.96e8.0802    DYNAMIC     Fa0/2
   1    0060.7096.e001    DYNAMIC     Gig0/1
  10    0001.630a.83b0    DYNAMIC     Fa0/5
  10    0060.4733.61a1    DYNAMIC     Fa0/1
  10    0060.7096.e001    DYNAMIC     Gig0/1
  20    0060.7096.e001    DYNAMIC     Gig0/1
  30    0060.7096.e001    DYNAMIC     Gig0/1
  40    0060.7096.e001    DYNAMIC     Gig0/1
 101    0009.7ced.5a78    DYNAMIC     Fa0/1
 101    0060.7096.e001    DYNAMIC     Gig0/1
 102    0060.7096.e001    DYNAMIC     Gig0/1
 121    0060.7096.e001    DYNAMIC     Gig0/1
 122    0060.7096.e001    DYNAMIC     Gig0/1
 180    0060.7096.e001    DYNAMIC     Gig0/1
 254    0060.7096.e001    DYNAMIC     Gig0/1
access-1-1#
```

Each VLAN in the switch is a separate broadcast domain. In other words, an Ethernet broadcast – an ARP Request, from PC-0 10.10.1.100/24 on Fa0/5 (FastEthernet0/5) will only be sent out other VLAN 10 ports including trunk ports that include VLAN 10. On access-1-1 switch this includes ports Fa0/1 and Gig0/1.

Note: The MAC address table entries for VLANs that do not have any devices correspond to the MAC addresses of interfaces or switches participating in STP (Spanning Tree Protocol). STP is discussed in a later lab.

In summary, the implementation of VLANs and trunking improved network efficiency, security, and scalability while simplifying management and troubleshooting, making the network more robust and better suited for future growth.

Inter-IP/Inter-VLAN Communications

While VLANs and trunking have successfully segmented the network and allowed communication between devices within the same VLAN and IP network, there is still no communication between devices on different VLANs or IP networks. This is because VLANs are isolated at Layer 2, and communication between them requires routing, which operates at Layer 3. To enable inter-VLAN communication, a Layer 3 device, such as a router or a multilayer switch, must be configured to route traffic between the VLANs. Without routing, devices in separate VLANs remain isolated and cannot exchange data.

We will configure inter-IP, inter-VLAN routing in a later lab.

Best Practice: Default Port Configuration and the Parking-Lot VLAN

A default switch configuration like this ensures that all the specified interfaces are set to a known, controlled state, which enhances security and network segmentation. By assigning all ports to a specific “Parking-Lot” VLAN (255 in this case) and disabling them (**shutdown**), it prevents unauthorized access or unintended traffic on those ports until they are explicitly enabled and configured for a specific device or network segment. This kind of configuration is a good practice for maintaining a secure and organized network environment, where network administrators must deliberately activate each port with appropriate settings before it becomes operational.

```
access(config)# interface range fa0/1-24, g0/1-2
access(config-if-range)# switchport mode access
access(config-if-range)# switchport access vlan 255
access(config-if-range)# shutdown
access(config-if-range)# exit
```

If done on all ports, this is done before any specific port configurations.

- **interface range fa0/1-24, g0/1-2**: This command is used to select a range of interfaces for batch configuration.
- **switchport mode access**: This command sets the selected interfaces to access mode. Access ports belong to a single VLAN and are typically used to connect end devices like computers,

printers, and phones. This mode is used to ensure that these interfaces will carry traffic for only one specific VLAN.

- **switchport access vlan 255**: This command assigns the selected interfaces to VLAN 255, which is the Parking-Lot VLAN. The Parking-Lot VLAN 255 is meant for devices not connected to the network and will not be carried over any trunk links.

Note: Other commands we will use in other labs may also be included. For now, you have the option of configuring any unused ports with these commands.

Verification Commands

show vlan brief

```
access-1-3#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/3, Fa0/4, 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   Engineering                         active    Fa0/5
20   QA-Engineering                      active    Fa0/6
30   Sales                               active
40   Marketing                           active
101  Voice-1                             active    Fa0/5
102  Voice-2                             active
121  Guest-1                             active
122  Guest-2                             active
180  Management                          active
254  Native                              active
255  Parking-Lot                         active
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
access-1-3#
```

The **show vlan brief** command is helpful for quickly verifying the VLAN configuration on a switch, ensuring that the correct VLANs are created and that ports are assigned to the appropriate VLANs. This command would be crucial for checking VLAN configurations.

Here's a more in-depth look at what each part of the output means:

- **VLAN ID:** VLANs are identified by a VLAN ID, a number between 1 and 4094. VLAN 1 is the default VLAN on Cisco switches.
- **Name**: By default, VLANs are named "VLANxxxx" where "xxxx" is the VLAN number. Custom names can be assigned to each VLAN to make management easier.
- **Status**: The VLAN's status will typically be "active", but it can also be "suspend". An active status means the VLAN is operational; suspended means it has been manually disabled and is not passing traffic.
- **Ports**: This shows which ports are members of the VLAN. Depending on the switch model and IOS version, it might show individual ports (like Fa0/1) or port ranges (like Fa0/1-4).

show interface <interface> switchport (access)

```
access-1-3# show interface fa 0/6 switchport
Name: Fa0/6
```

```
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: 20 (QA-Engineering)
Trunking Native Mode VLAN: 1 (default)
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 encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

access-1-3# show interface fa 0/5 switchport
Name: Fa0/5
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: 10 (Engineering)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 101
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none


access-1-3#
```

The **show interface <interface> switchport** command on a Cisco switch is a diagnostic tool that provides detailed information about a specific interface's switchport configuration. You replace **<interface>** with the

actual interface identifier, such as **FastEthernet0/5** or **FastEthernet0/6**. Here's what the output generally includes:

- **Name**: The name of the interface.
- **Switchport**: Indicates whether the interface is functioning as a Layer 2 switch port (**Enabled**) or a Layer 3 interface (**Disabled**).
- **Administrative Mode**: The configured VLAN mode of the interface, such as access, trunk, or dynamic.
- **Operational Mode**: The current functioning mode of the interface, which could differ from the Administrative Mode if the interface is in a dynamic state.
- **Administrative Trunking Encapsulation**: The configured trunking encapsulation protocol, such as dot1q or isl (deprecated).
- **Operational Trunking Encapsulation**: The encapsulation protocol currently being used, if the port is in trunk mode.
- **Negotiation of Trunking**: Status of DTP (Dynamic Trunking Protocol) negotiation between switches to determine if the interface should become a trunk or access port.
- **Access Mode VLAN**: The VLAN assigned to this port when it's in access mode.
- **Trunking Native Mode VLAN**: The native VLAN for the trunk; this VLAN's traffic is not tagged by default.
- **Voice VLAN**: If a Voice VLAN is configured, it will be displayed here.
- **Trunking VLANs Enabled**: The range of VLANs allowed on the trunk, if the port is in trunk mode.

This command is particularly useful for troubleshooting issues related to VLAN assignments and trunk configurations on individual ports. It can help verify:

- If an interface is correctly configured to carry traffic for the intended VLAN.
- If the interface is set to the correct mode (access or trunk).
- If DTP is active and may be causing unintended behavior.
- What the native VLAN is on a trunk and which VLANs are allowed over the trunk.
- If a Voice VLAN is set up and operational.

This command can be used to confirm configurations on each switch port, ensuring that their access ports are correctly set up and that any trunk ports are properly negotiated and carrying the right VLAN traffic.

show interfaces trunk

```
access-1-1# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      254
Fa0/2       on           802.1q         trunking      254
Gig0/1      on           802.1q         trunking      254

Port        Vlans allowed on trunk
Fa0/1       1,10,20,30,40,101-102,121-122,180,254
Fa0/2       1,10,20,30,40,101-102,121-122,180,254
Gig0/1      1,10,20,30,40,101-102,121-122,180,254

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,40,101,102,121,122,180,254
Fa0/2       1,10,20,30,40,101,102,121,122,180,254
Gig0/1      1,10,20,30,40,101,102,121,122,180,254

Port        Vlans in spanning tree forwarding state and not pruned
```

```
Fa0/1       1,10,20,30,40,101,102,121,122,180,254
Fa0/2       1,10,20,30,40,101,102,121,122,180,254
Gig0/1      1,10,20,30,40,101,102,121,122,180,254

access-1-1#
```

The **show interfaces trunk** command on a Cisco switch provides an overview of all the switch's interfaces that are configured to operate in trunk mode. This command is extremely useful for verifying the status of trunk links, ensuring that VLANs are allowed across the trunk, and for general troubleshooting of trunk-related issues. The output typically includes:

- **Port**: Lists the interfaces that are configured as trunk ports.
- **Mode**: Displays the trunking mode of the port, which is typically either on (forcing trunking), off (forcing non-trunking), or desirable/auto (negotiating with DTP).
- **Encapsulation**: Shows the encapsulation type being used for trunking on the port, such as 802.1Q, ISL (rarely used today), or negotiate (if using DTP to negotiate the encapsulation type).
- **Status**: Indicates whether the trunk is up and operational.
- **Native VLAN**: Displays the native VLAN configured on the trunk port. Traffic from this VLAN is sent untagged across the trunk link.
- **Vlans Allowed on Trunk**: Provides a list of all VLANs that are allowed to pass through the trunk. This can be a range of VLANs or specific VLANs allowed.
- **Vlans Allowed and Active in Management Domain**: Shows which VLANs are both allowed on the trunk and exist in the switch's VLAN database.
- **Vlans in spanning tree forwarding state and not pruned**: Lists the VLANs that are in a forwarding state according to the Spanning Tree Protocol and have not been pruned.

This command helps network administrators to quickly determine which VLANs are traversing which trunks, identify any mismatches in native VLAN configurations, and troubleshoot issues related to VLANs not passing through trunks as expected. In a lab setting, this is a key command for students to ensure that their trunk configurations are correctly implemented, especially when working on inter-switch connectivity and VLAN routing scenarios.

Understanding the output of this command can be critical when setting up or troubleshooting VLANs that span multiple switches or when ensuring that certain VLANs are isolated to specific trunks for security or traffic flow optimization.

show interface <interface> switchport (trunk)

```
access-1-1# show interfaces g 0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 254 (Native)
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 encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 1,10,20,30,40,101-102,121-122,180,254
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none


access-1-1#
```

The **show interface <interface> switchport** command, when used on a trunk port, will provide information similar to when it's used on an access port, with additional details pertinent to trunk configurations. By substituting **<interface>** with the actual trunk port identifier, such as **GigabitEthernet0/1**, the command displays specific switchport information for that trunk interface.
Here is an overview of the information you would typically see in the output for a trunk port:

- **Name**: The name of the trunk interface, e.g., GigabitEthernet0/1.
- **Switchport**: Shows if the interface is enabled for Layer 2 switching.
- **Administrative Mode**: The switchport mode such as trunk, access, or dynamic desirable.
- **Operational Mode**: The actual operating mode of the interface, which should be trunk if it's properly configured.
- **Administrative Trunking Encapsulation**: The encapsulation type set on the trunk, like dot1q or negotiate if it's using DTP to negotiate encapsulation.
- **Operational Trunking Encapsulation**: The encapsulation type currently in use.
- **Negotiation of Trunking**: The status of trunk negotiation (whether the port is actively negotiating trunking with its link partner).
- **Access Mode VLAN**: The VLAN that the port will default to if it were to switch to access mode.
- **Trunking Native Mode VLAN**: The native VLAN of the trunk, which by default is VLAN 1 unless changed.
- **Administratively Configured Native VLAN**: Shows the administratively configured native VLAN.
- **Voice VLAN**: Indicates if a Voice VLAN is configured and its ID.
- **Trunking VLANs Enabled:** The output indicates that the trunk link on interface GigabitEthernet0/1 is configured to carry traffic for the specified VLANs (1, 10, 20, 30, 40, 101-102, 121-122, 180, 254), allowing communication for these VLANs across the trunk.

Specifically for a trunk port, this output is crucial to verify:

- That the port is indeed functioning as a trunk.
- The native VLAN is correctly set (as mismatches in native VLAN between trunking interfaces can lead to VLAN hopping attacks).
- The encapsulation method is correctly set and operational.
- That DTP is either appropriately enabled or disabled, depending on the network policy.
- Which VLANs would the trunk port revert to if it were to become an access port.

Understanding and using this command is essential for network engineers when they configure trunk ports on a switch and need to troubleshoot issues related to VLAN tagging, trunk encapsulation, and native VLAN configurations.

show spanning-tree

```
access-1-3# show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     0001.4211.6A5A
              Cost        46
              Port        1(FastEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0030.A382.A951
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/5            Desg FWD 19        128.5    P2p

access-1-3#
```

The Fa0/2 interface is in a blocked state to prevent a network loop, as Spanning Tree Protocol (STP) ensures only one active path exists between switches in a network. This blocking is necessary to maintain a loop-free topology and avoid broadcast storms or duplicate frames. The Spanning Tree Protocol will be discussed in more detail in a later lab.

In case you can't wait here is some more information.

The **show spanning-tree** command is used on Cisco switches to display information about the Spanning Tree Protocol (STP) status of the switch. This is crucial for understanding how STP has converged and which ports are in forwarding or blocking state, to prevent loops in your network. We will discuss spanning-tree later, but if you want to know what some of the out is, here's what the output includes:

- **Root ID**: This provides information about the root bridge in the network, which is considered the logical center of the STP topology. It includes the priority of the root bridge and its MAC address.
- **Bridge ID**: Displays the priority and MAC address of the bridge from which you are running the command, which could be the root bridge if you're on it.
- **Root Port**: The port on the switch that is the closest (in terms of STP cost) to the root bridge.
- **Designated Ports**: Ports on the switch that have been determined to be the best path to the network segment they are connected to.
- **Blocking Ports**: Ports that are not forwarding traffic to prevent loops; these ports are in a non-designated role.

- **Path Cost**: The cost of paths to the root bridge, which helps determine the best path for traffic.
- **Port State**: The state of each port; it can be in listening, learning, forwarding, or blocking state.
- **Port Role**: The role that has been assigned to the port, such as root port (best path to the root bridge), designated port (best path to a segment), or alternate port (backup path).
- **STP Protocol**: Indicates which version of STP is running, such as PVST+, RPVST+, or MSTP.

Each active interface participating in STP will be listed, along with its status and STP-related information. This command can be filtered by VLAN to show the STP status for a particular VLAN if multiple VLANs are configured with **show spanning-tree vlan <vlan-id>**.

This command is indispensable for network troubleshooting and maintenance. It allows network engineers to verify the STP topology, identify redundant paths, and ensure that STP is functioning correctly to prevent broadcast storms and network loops.