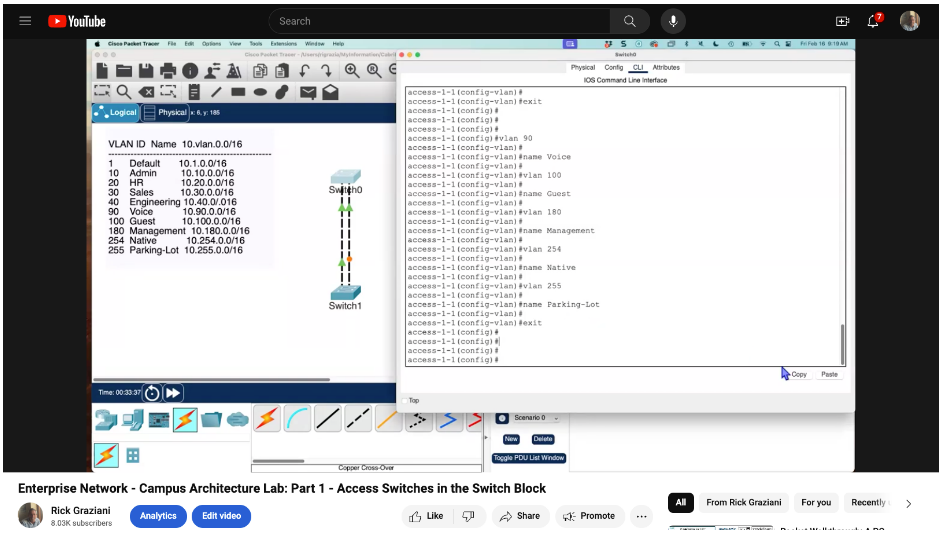
Building an Enterprise Network

Part 1: VLANs

Refer to the following YouTube Video: https://www.youtube.com/watch?v=zqGVurgZ1wo



```
VLAN ID  Name  10.vlan.0.0/16
----------------------------------------------
1     Default      10.1.0.0/16
10    Admin        10.10.0.0/16
20    HR           10.20.0.0/16
30    Sales        10.30.0.0/16
40    Engineering  10.40.0/.016
90    Voice        10.90.0.0/16
100   Guest        10.100.0.0/16
180   Management   10.180.0.0/16
254   Native       10.254.0.0/16
255   Parking-Lot  10.255.0.0/16
```

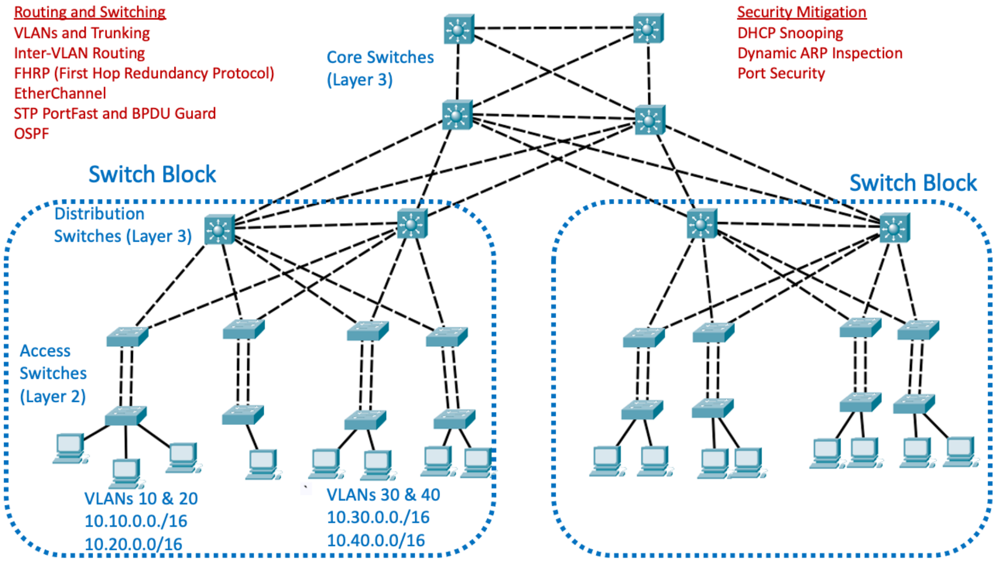
```
access-1-1(config-vlan)#
access-1-1(config-vlan)#exit
access-1-1(config)#
access-1-1(config)#
access-1-1(config)#
access-1-1(config)#vlan 90
access-1-1(config-vlan)#
access-1-1(config-vlan)#name Voice
access-1-1(config-vlan)#
access-1-1(config-vlan)#vlan 100
access-1-1(config-vlan)#
access-1-1(config-vlan)#name Guest
access-1-1(config-vlan)#
access-1-1(config-vlan)#vlan 180
access-1-1(config-vlan)#
access-1-1(config-vlan)#name Management
access-1-1(config-vlan)#
access-1-1(config-vlan)#vlan 254
access-1-1(config-vlan)#
access-1-1(config-vlan)#name Native
access-1-1(config-vlan)#
access-1-1(config-vlan)#vlan 255
access-1-1(config-vlan)#
access-1-1(config-vlan)#name Parking-Lot
access-1-1(config-vlan)#
access-1-1(config-vlan)#exit
access-1-1(config)#
access-1-1(config)#
access-1-1(config)#
access-1-1(config)#
```

Enterprise Network - Campus Architecture Lab: Part 1 - Access Switches in the Switch Block

Rick Graziani
8.03K subscribers

Design

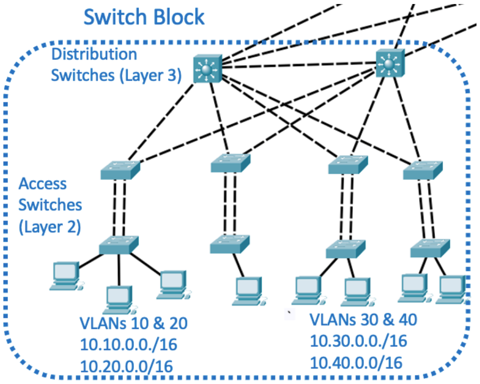
We begin building our enterprise network using the campus architecture design by creating and configuring a switch block.



An enterprise network using the campus architecture design.

Campus Architecture specifically pertains to the design and structure of a network within a campus setting, such as a university, corporate campus, or any large organization's premises. It focuses on the physical and logical layout of networking devices and infrastructure to support communication and services within that localized area. The campus architecture is often discussed in terms of layers (access, distribution, and core) to ensure efficient management, scalability, and performance of the network.

A **switch block** in Cisco networking refers to a design concept used in hierarchical network models, particularly within the Campus Architecture. It typically consists of a set of switches that are grouped together to efficiently manage data traffic within a specific area of a network, such as a department or floor in a building, enhancing performance, security, and manageability.



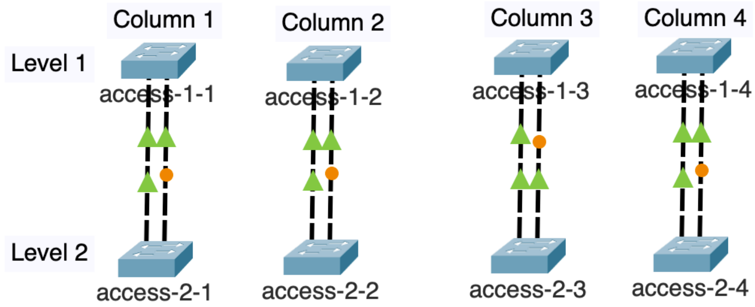
In a switch block you will typically find the following devices:

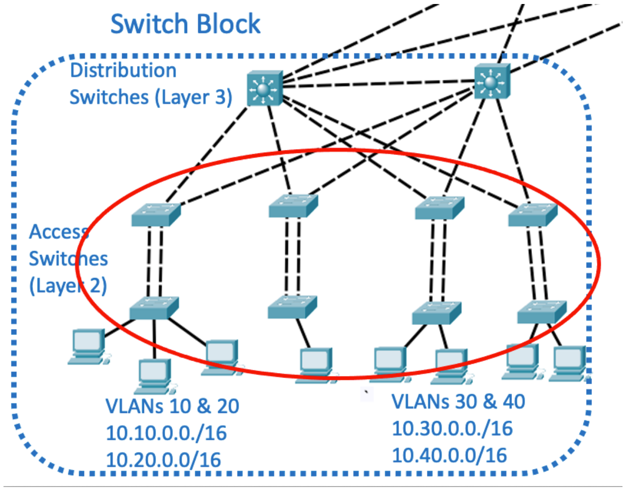
Access Switches: These are the switches that connect directly to end devices within the network, such as computers, printers, and phones. Their main role is to provide network access to these devices.

Distribution Switches: These switches serve as the intermediaries between access switches and the core layer of the network. They aggregate the data traffic from multiple access switches and enforce network policies such as security, traffic management, and routing decisions to ensure efficient data distribution to the core layer.

The Lab

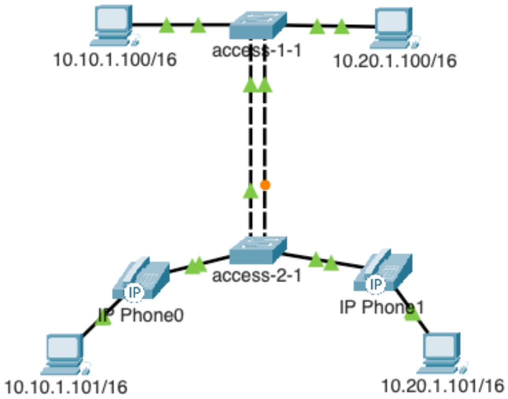
We will begin building or switch block which consists of 4 pairs of access switches. Each pair will consist of a top and bottom switch interconnected to by two links. For now, the pairs of switches have no connection between them. This will happen later. Refer enterprise network topology in the diagram above.

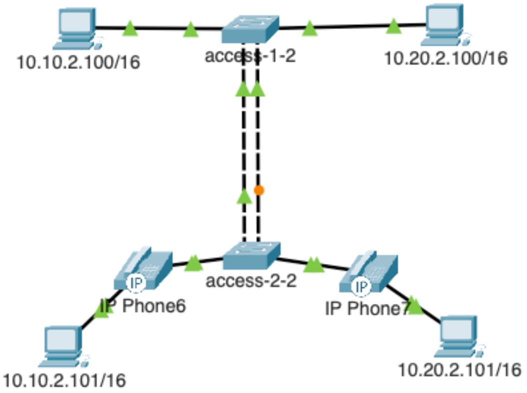




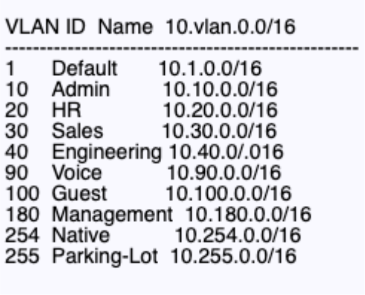
IMPORTANT:

- You will begin by configuring the two column 1 switches, followed by the two column 2 switches.
- In the Packet Tracer startup file, the column 3 and 4 switches have already been created and configured for you. However, you are welcome to re-do those configurations yourself.

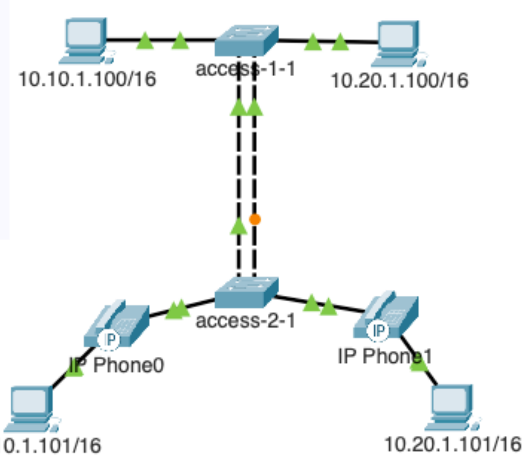




Configuring Column 1 - Level 1 and Level 2 Switches



```
VLAN ID  Name  10.vlan.0.0/16
---------------------------------------------------
1     Default      10.1.0.0/16
10    Admin        10.10.0.0/16
20    HR           10.20.0.0/16
30    Sales        10.30.0.0/16
40    Engineering 10.40.0/.016
90    Voice        10.90.0.0/16
100   Guest        10.100.0.0/16
180   Management  10.180.0.0/16
254   Native       10.254.0.0/16
255   Parking-Lot  10.255.0.0/16
```



Basic Access Layer Switch 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 'cisco' as a password is not secure and it's recommended to use stronger, unique passwords for device security. Also, transitioning from telnet to SSH is a critical security improvement because SSH encrypts the session, preventing eavesdropping.

Add the following commands to each switch.

- **hostname access-<level-column>** This command sets the hostname of the switch to help identify it in a network. The **<level-column>** part is a placeholder for the actual level or column in the naming convention you are using.
- **no ip domain-lookup** This command disables the automatic translation of unrecognized command entries into domain names, thus preventing the switch from attempting to translate these into IP addresses, which can delay the command-line interface if the switch is not configured with a proper DNS server.
- **banner motd (optional)** This optional command configures a message that will be displayed on all terminals when users log in, commonly used for legal warnings or welcome messages.
- **enable secret class** This sets the encryption password for entering the privileged EXEC mode (enable mode), which provides access to all other router commands. "class" is the password in this example.
- **line console 0 -** This refers to the configuration of the console port used to initial device configuration or when needing to access the device directly through the console port.
    1. **password cisco -** This command sets the password for accessing the switch console port.
    2. **logging synchronous** This prevents console messages from interrupting command-line input by making sure syslog messages do not interfere with the typed CLI command lines.
    3. **exec-timeout 0 0** This command sets the timeout for the console session to zero, which means the console will never time out due to inactivity.
- **line vty 0 4** - This refers to the configuration for the virtual terminal lines (telnet or SSH access) for remote management of the switch.

1. **transport input telnet (later SSH)** Initially, this allows telnet connections to the switch. The note "(later SSH)" suggests that at a later point, this will be changed to "transport input ssh" to use the more secure SSH protocol instead of telnet.
2. **password cisco** Sets the password for remote access to the switch using the VTY lines. Here again, "cisco" is used as the password.

Commands for both LEVEL 1 and LEVEL 2 Switches

```
Switch> enable
Switch# conf t

! Example of hostname for an access switch at level 1 in column 1
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)# line con 0
access-1-1(config-line)# logging synchronous
access-1-1(config-line)# exec-timeout 0 0
access-1-1(config-line)# exit

access-1-1(config)# line vty 0 4
access-1-1(config-line)# password cisco
access-1-1(config-line)# login
access-1-1(config-line)# transport input telnet
access-1-1(config-line)# exit
access-1-1(config)#
```

Configuring VLANS

VLAN ID	Name	10.vlan.0.0/16
1	Default	10.1.0.0/16
10	Admin	10.10.0.0/16
20	HR	10.20.0.0/16
30	Sales	10.30.0.0/16
40	Engineering	10.40.0/.016
90	Voice	10.90.0.0/16
100	Guest	10.100.0.0/16
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 each switch.

- **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.

The commands are not required. 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.

Commands for both LEVEL 1 and LEVEL 2 Switches

```
access-1-1(config)# vlan 10
access-1-1(config-vlan)# name admin
access-1-1(config-vlan)# exit
access-1-1(config)# vlan 20
access-1-1(config-vlan)# name HR
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 Engineering
access-1-1(config-vlan)# exit
access-1-1(config)# vlan 90
access-1-1(config-vlan)# name Voice
access-1-1(config-vlan)# vlan 100
access-1-1(config-vlan)# name Guest
access-1-1(config-vlan)# 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
access-1-1(config)#
```

Default Port Configuration

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.

- **interface range fa0/1-24, g0/1-2**: This command is used to select a range of interfaces for batch configuration. **fa0/1-24** refers to FastEthernet ports 1 through 24, and **g0/1-2** refers to GigabitEthernet ports 1 and 2. By using the **interface range** command, you can apply the same configuration to multiple interfaces at once, which makes the configuration process faster and more consistent.
- **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.

Commands for both LEVEL 1 and LEVEL 2 Switches

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

Configuring Active Access Ports

We will be connecting PCs and or IP Phones to ports on the switch. The VLAN ID configured on the port or interface of the switch is associated with the IP network address of the end device connected to that port.

The following commands are for LEVEL 1 switches, which in our scenario do not have any IP Phones connected.

- **interface fa0/10**: This command selects interface FastEthernet 0/10 for configuration. This is the interface that will be configured with the subsequent commands.
- **switchport mode access**: This sets the selected interface (fa0/10) to access mode. An access port can only belong to one VLAN and is typically used to connect end devices, like computers and printers, that don't need to be aware of VLAN information.
- **switchport access vlan 10 or 20**: This assigns VLAN 10 or 20 to the selected interface. Any device connected to fa0/10 will now be part of VLAN 10 or 20, and the traffic from this device will be associated with that VLAN. VLAN 10 in our scenario is associated with the 10.10.0.0/16 network. VLAN 20 is associated with the 10.20.0.0/16 network.
- **no shutdown**: This command enables the interface, changing its state from administratively down (disabled) to up (enabled). This is necessary for the interface to actively transmit and receive data.

These commands are configuring interfaces to be an active port within a specific VLAN, allowing devices connected to this port to communicate with other devices within the same VLAN. Each VLAN is associated with a specific IP network and its own broadcast domain.

Commands for LEVEL 1 Switches

```
access-1-1(config)# interface fa0/10
access-1-1(config-if)# switchport mode access
access-1-1(config-if)# switchport access vlan 10
access-1-1(config-if)# no shutdown
access-1-1(config-if)# exit

access-1-1(config)# interface fa0/20
access-1-1(config-if)# switchport mode access
access-1-1(config-if)# switchport access vlan 20
access-1-1(config-if)# no shutdown
access-1-1(config-if)# exit
access-1-1(config)#
```

The following commands are for LEVEL 2 switches, which in our scenario have both a PC and an IP Phones connected.

- **interface fa0/10**: This selects the interface FastEthernet 0/10 for configuration.
- **switchport mode access** ensures that the port is set to access mode, which is required for carrying voice VLAN traffic. 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.
- **switchport access vlan 10 or 20**: This assigns VLAN 10 or 20 to the interface as the access VLAN, which is the VLAN that a connected PC will use.
- **switchport voice vlan 90**: This command configures the interface to support a voice VLAN (VLAN 90), which is used by an IP Phone. This allows the port to carry both voice and data traffic, with the voice traffic being tagged to VLAN 90.
- **mls qos trust cos**: This command enables Quality of Service (QoS) on the interface and sets it to trust the Class of Service (CoS) values received. This is important for voice traffic to ensure it is given priority over the network, maintaining the quality of the phone calls.
- **no shutdown**: This command activates the interface, changing its state from administratively down to up.

These commands configure the switch ports to handle both data traffic for a connected PC and voice traffic for an IP Phone. VLAN 10 and VLAN 20 are used for data traffic from PCs connected to ports fa0/10 and fa0/20, respectively, while VLAN 90 is designated for voice traffic from IP Phones connected to both ports. QoS settings are applied to prioritize voice traffic, ensuring clear and uninterrupted voice communication. The **no shutdown** command ensures that the ports are enabled and ready for use.

Commands for LEVEL 2 Switches

```
access-1-1(config)# interface fa0/10
access-1-1(config-if)# switchport mode access
access-1-1(config-if)# switchport access vlan 10
access-1-1(config-if)# switchport voice vlan 90
access-1-1(config-if)# mls qos trust cos
access-1-1(config-if)# no shutdown
access-1-1(config-if)# exit

access-1-1(config)# interface fa0/20
access-1-1(config-if)# switchport mode access
access-1-1(config-if)# switchport access vlan 20
access-1-1(config-if)# switchport voice vlan 90
access-1-1(config-if)# mls qos trust cos
access-1-1(config-if)# no shutdown
access-1-1(config-if)# exit
access-1-1(config)#
```

Trunking

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 configuration is commonly used between switches to allow VLANs to span across the network.

- **interface range fa0/1-2**: This selects a range of interfaces (FastEthernet 0/1 and 0/2) to apply the following configurations to both interfaces simultaneously.
- **no switchport access vlan 255**: This command removes VLAN 255 from being assigned as the access VLAN for these ports. This is typically done when the ports are being transitioned from access mode to trunk mode.
- **switchport mode trunk**: Sets the selected interfaces to trunk mode. In trunk mode, the ports can carry traffic from multiple VLANs, as specified in subsequent commands.
- **switchport nonegotiate**: This command prevents the interfaces from using Dynamic Trunking Protocol (DTP) to negotiate with the connected device whether to use trunk mode. It forces the port into trunk mode without negotiation.
- **switchport trunk allowed vlan 1,10,20,30,40,90,100,180,254**: This command specifies which VLANs are allowed to be transported across the trunk. Only traffic from VLANs 1, 10, 20, 30, 40, 90, 100, 180, and 254 will be allowed across these trunk ports.
- **switchport trunk native vlan 254**: Sets VLAN 254 as the native VLAN for these trunk ports. Traffic from this VLAN will not be tagged when traversing the trunk, while traffic from all other allowed VLANs will be tagged with their respective VLAN IDs.
- **no shutdown**: This command enables the interfaces, allowing them to start forwarding traffic.

Since these commands configure two interfaces as trunk links between the same two switches, Spanning Tree Protocol (STP) will come into play to prevent loops. STP will block one of these links to prevent a broadcast storm caused by multiple active paths between the two switches. The link that remains in forwarding state will carry traffic for the allowed VLANs, while the blocked link will remain inactive unless the active link fails, at which point STP will automatically unblock the redundant link to maintain network connectivity.

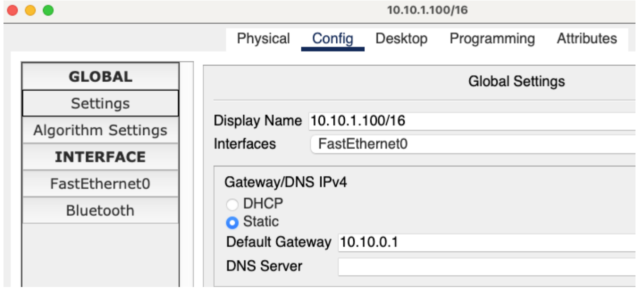
Commands for both LEVEL 1 and LEVEL 2 Switches

```
access-1-1(config)# interface range fa0/1-2
access-1-1(config-if-range)# no switchport access vlan 255
access-1-1(config-if-range)# switchport mode trunk
access-1-1(config-if-range)# switchport nonegotiate
access-1-1(config-if-range)# switchport trunk allowed vlan
1,10,20,30,40,90,100,180,254
access-1-1(config-if-range)# switchport trunk native vlan 254
access-1-1(config-if-range)# no shutdown
access-1-1(config-if-range)# exit
access-1-1(config)#
```

End Devices

End devices:

- Add PCs (and IP Phones if needed) for the VLAN 10, 20, 30 and 40 ports configured previously.
- Configure statically the IPv4 addresses for each device
- Use the first IPv4 address of the subnet for the default gateway (not added yet)



Global Settings

Display Name 10.10.1.100/16

Interfaces FastEthernet0

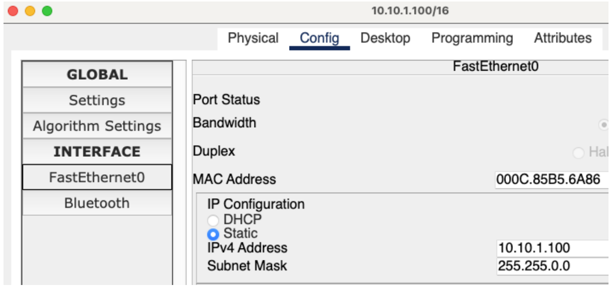
Gateway/DNS IPv4

○ DHCP

● Static

Default Gateway 10.10.0.1

DNS Server



FastEthernet0

Port Status

Bandwidth

Duplex ○ Hal

MAC Address 000C.85B5.6A86

IP Configuration

○ DHCP

● Static

IPv4 Address 10.10.1.100

Subnet Mask 255.255.0.0

PC-left

- **Interface Fa 0:** 10.10.0.100 255.255.255.0
- **Global Settings > Default Gateway:** 10.10.0.1
- **Global Settings > Display Name:** 10.10.0.100

PC-left

- **Interface Fa 0:** 10.10.0.101 255.255.255.0
- **Global Settings > Default Gateway:** 10.10.0.1
- **Global Settings > Display Name:** 10.10.0.101

PC-right

- **Interface Fa 0:** 10.20.0.100 255.255.255.0
- **Global Settings > Default Gateway:** 10.20.0.1
- **Global Settings > Display Name:** 10.20.0.100

PC-right

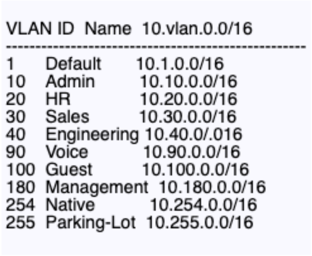
- **Interface Fa 0:** 10.20.0.101 255.255.255.0
- **Global Settings > Default Gateway:** 10.20.0.1
- **Global Settings > Display Name:** 10.20.0.101

Packet Tracer Display Names for Switches

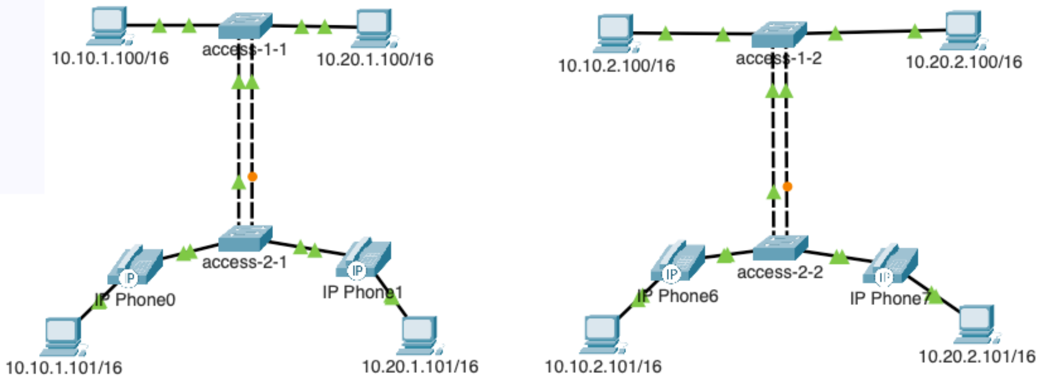
LEVEL 1 AND LEVEL 2 Switches

- **Global Settings > Display Name:** “Hostname”

Second Pair of Switches - Column 2: Level 1 and Level 2



```
VLAN ID  Name  10.vlan.0.0/16
-----------------------------------------------
1    Default      10.1.0.0/16
10   Admin        10.10.0.0/16
20   HR           10.20.0.0/16
30   Sales        10.30.0.0/16
40   Engineering 10.40.0/.016
90   Voice        10.90.0.0/16
100  Guest        10.100.0.0/16
180  Management  10.180.0.0/16
254  Native        10.254.0.0/16
255  Parking-Lot  10.255.0.0/16
```

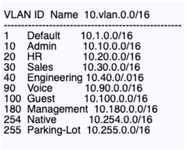


Do the same for the next pair of Level 1 and Level 2 switches in column 2:

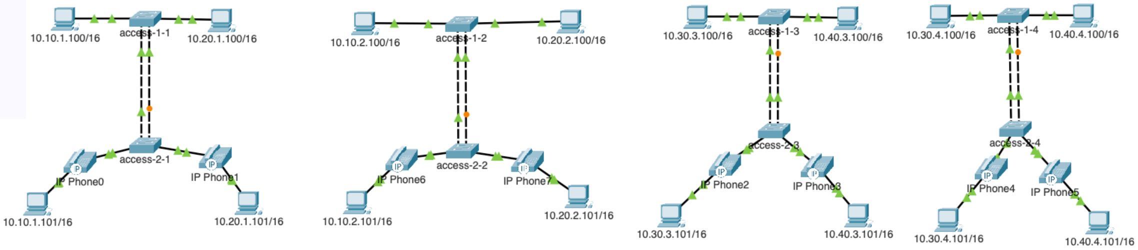
- access-1-2
- access-2-2

Make the necessary changes to hostnames and IPv4 addresses.

Third and Fourth Pairs of Switches – Columns 3 and 4: Level 1 and Level 2



```
VLAN ID  Name  10.vlan.0.0/16
-----------------------------------------------
1    Default      10.1.0.0/16
10   Admin        10.10.0.0/16
20   HR           10.20.0.0/16
30   Sales        10.30.0.0/16
40   Engineering 10.40.0/.016
90   Voice        10.90.0.0/16
100  Guest        10.100.0.0/16
180  Management  10.180.0.0/16
254  Native        10.254.0.0/16
255  Parking-Lot  10.255.0.0/16
```



These switches have already been created and configured for you in the Packet Tracer startup file. You may wish to use these switches or redo it yourself.

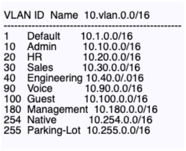
Under Construction

No communications between "columns": We still need to make some connections. Currently there is no connection between the column 1 and 2 or column 3 and 4, so device in the same VLAN, the same IPv4 network cannot communicate with each other.

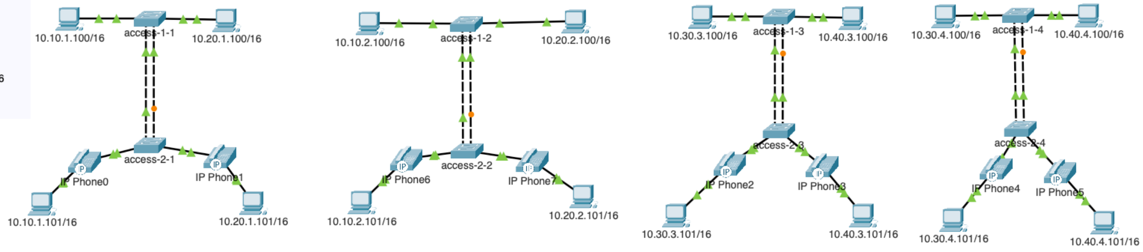
No communications between IP networks or VLANs: Also, devices in different IPv4 networks, even in the same column, cannot communicate because we do not have a router or layer 3 switch in our network.

We will solve both of these issues in our next lab with a our layer 3 distribution switches.

COLUMN 3 AND COLUMN 4 - LEVEL 1



VLAN ID	Name	10.vlan.0.0/16
1	Default	10.1.0.0/16
10	Admin	10.10.0.0/16
20	HR	10.20.0.0/16
30	Sales	10.30.0.0/16
40	Engineering	10.40.0/.016
90	Voice	10.90.0.0/16
100	Guest	10.100.0.0/16
180	Management	10.180.0.0/16
254	Native	10.254.0.0/16
255	Parking-Lot	10.255.0.0/16



```
! BASIC CONFIG

enable
conf t

no ip domain-lookup

hostname access-1-3
hostname access-1-4

enable secret class

line con 0
logging synchronous
exec-timeout 0 0
exit

line vty 0 4
password cisco
login
transport input telnet
exit

! CREATE VLANS

vlan 10
name admin
exit
vlan 20
name HR
exit
vlan 30
name Sales
exit
vlan 40
name Engineering
exit
vlan 90
name Voice
vlan 100
name Guest
vlan 180
name Management
vlan 254
name Native
vlan 255
```

```
name Parking-Lot
exit

! DEFAULT

interface range fa0/1-24, g0/1-2
switchport mode access
switchport access vlan 255


shutdown
exit

! LEVEL 1 PC PORTS

interface fa0/10
switchport mode access
switchport access vlan 30
no shutdown
exit

interface fa0/20
switchport mode access
switchport access vlan 40
no shutdown
exit

! TRUNK

interface range fa0/1-2
no switchport access vlan 255
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 1,10,20,30,40,90,100,180,254
switchport trunk native vlan 254
no shutdown
exit

end

copy run start
```

COLUMN 3 AND COLUMN 4 - LEVEL 2

```
! BASIC CONFIG

enable
conf t

no ip domain-lookup

hostname access-2-3
hostname access-2-4
```

```
enable secret class

line con 0
logging synchronous
exec-timeout 0 0
exit

line vty 0 4
password cisco
login
transport input telnet
exit

! CREATE VLANS

vlan 10
name admin
exit
vlan 20
name HR
exit
vlan 30
name Sales
exit
vlan 40
name Engineering
exit
vlan 90
name Voice
vlan 100
name Guest
vlan 180
name Management
vlan 254
name Native
vlan 255
name Parking-Lot
exit

! DEFAULT

interface range fa0/1-24, g0/1-2
switchport mode access
switchport access vlan 255
shutdown
exit

! LEVEL 2 PC PORTS

interface fa0/10
switchport mode access
switchport access vlan 30
switchport voice vlan 90
mls qos trust cos
no shutdown
exit

interface fa0/20
```

```
switchport mode access
switchport access vlan 40
switchport voice vlan 90
mls qos trust cos
no shutdown
exit

! TRUNK

interface range fa0/1-2
no switchport access vlan 255
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 1,10,20,30,40,90,100,180,254
switchport trunk native vlan 254
no shutdown
exit

end

copy run start
```