Switching Basics & Intermediate Routing (LAN Switching and Wireless)

Lecture 2: LAN Design & Scaling VLANs

CCNA Routing and Switching 3
- Scaling Networks

Objective for this lecture:

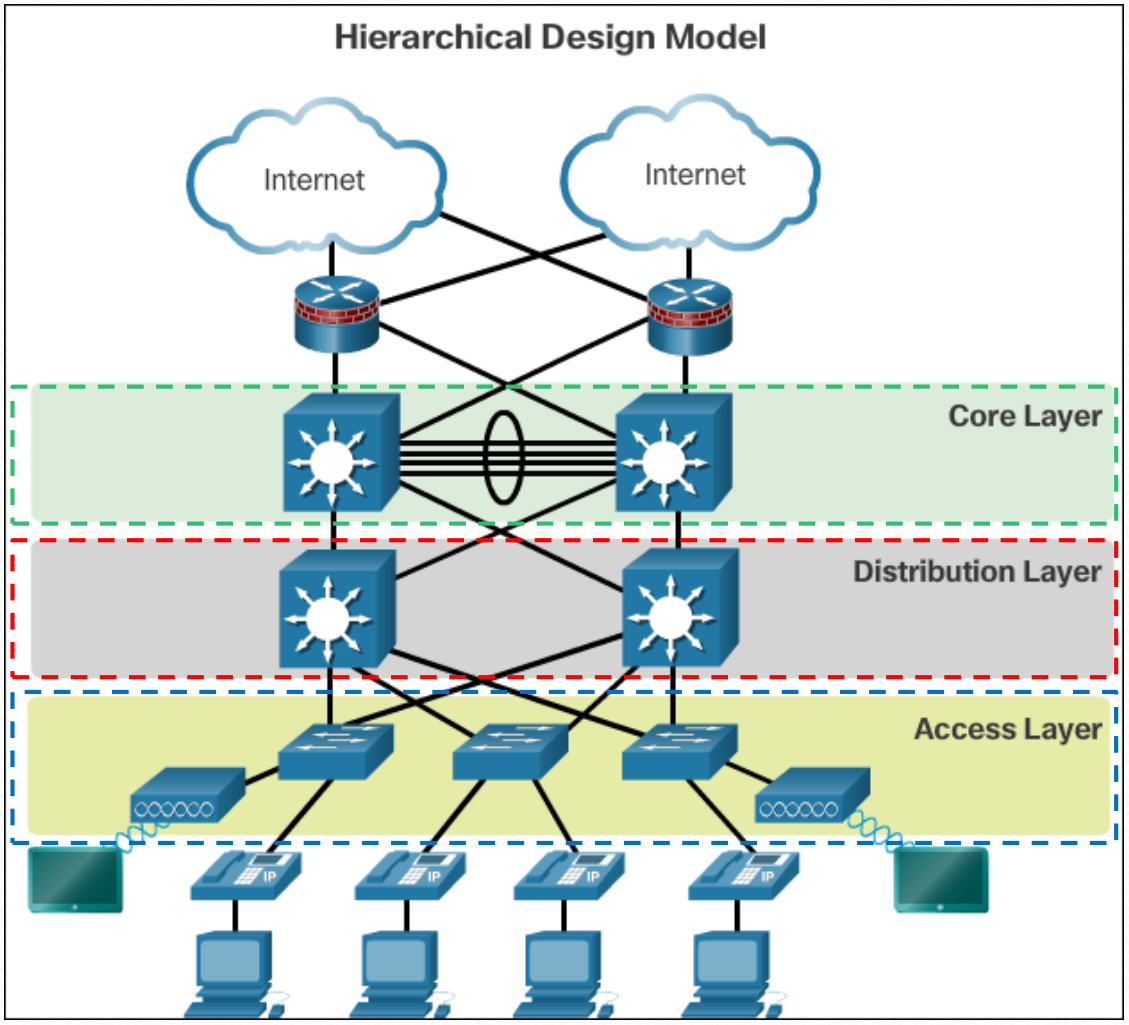
- Campus Wired LAN Designs
  - Explain why it is important to design a scalable hierarchical network
- Selecting Network Devices
  - Select network devices based on feature compatibility and network requirements
- VTP, Extended VLANs, and DTP
  - Configure enhanced inter-switch connectivity technologies
- Troubleshoot Multi-VLAN Issues
  - Troubleshoot issues in an inter-VLAN routing environment.
- Layer 3 Switching
  - Implement inter-VLAN routing using Layer 3 switching to forward data in a small to medium-sized business LAN

Campus Wired LAN Designs

Cisco Validated Designs

- The Need to Scale the Network
- All enterprise networks must:
  - support critical applications
  - support converged network traffic
  - support diverse business needs
  - provide centralized administrative control
- Campus network designs include small networks that use a single LAN switch, up to very large networks with thousands of connections

Hierarchical Design Model



A hierarchical LAN design includes the access, distribution, and core layers:

- The access layer provides endpoints and users direct access to the network
- The distribution layer aggregates access layers and provides connectivity to services
- The core layer provides connectivity between distribution layers for large LAN environments

Advantages of Hierarchical Design

- Some of the advantages of this approach include:
  - Network is more scalable and can easily be expanded without having to redesign entire topology
  - Upgrades can be performed without effecting other functional areas of the network
  - Local traffic stays local and so bandwidth is optimised
  - Redundancy is blended into the network and single points of failure are minimised which results in increased up time

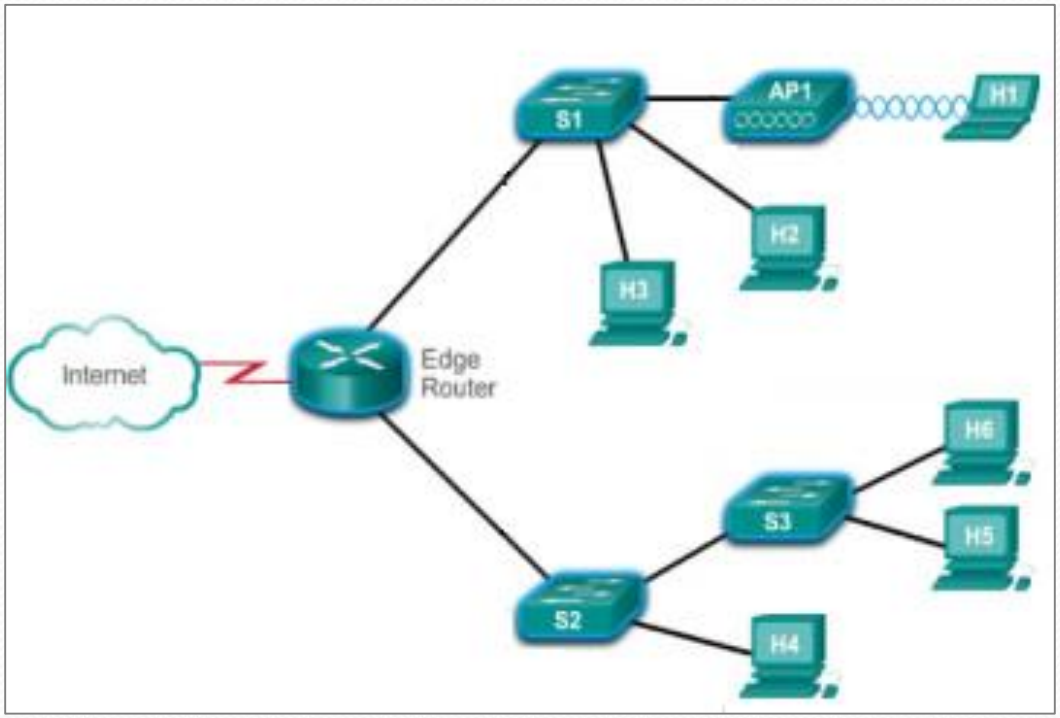
Failure Domains

- Another motivation for a well-designed network is to limit the size of failure domains
- A failure domain is the area of a network that is impacted when a critical device or network service experiences problems
- Smaller failure domains reduce the impact of a failure on company productivity

Exercise

What would be the failure domain if there was a failure to each of the below devices (i.e. what devices would be impacted):

1. S3
2. AP1
3. S2
4. S1
5. Edge Router



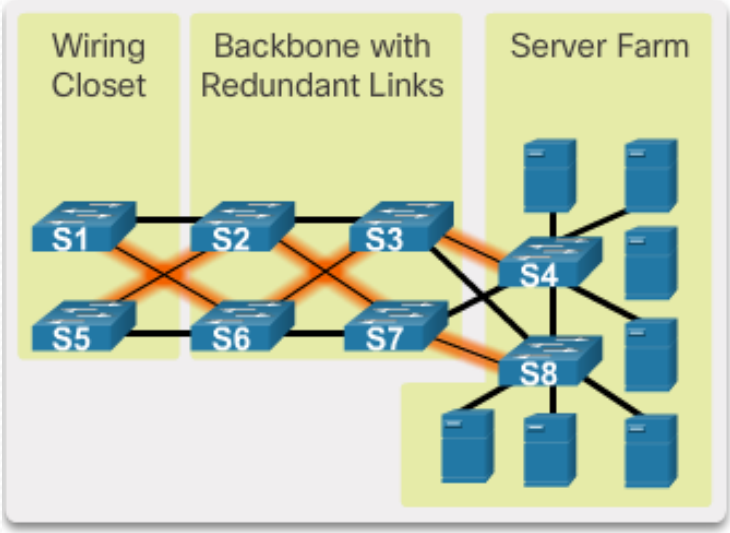
Design for Scale

- To support an enterprise network, the network designer must develop a strategy to enable the network to be available and to scale effectively and easily

1. Use expandable, modular equipment or clustered devices that can be easily upgraded to increase capabilities
2. Design a hierarchical network to include modules that can be added, upgraded, and modified, as necessary, without affecting the design of the other functional areas of the network
3. Create an IPv4 or IPv6 address strategy that is hierarchical
4. Choose routers or multilayer switches to limit broadcasts and filter other undesirable traffic from the network

Design for Redundancy

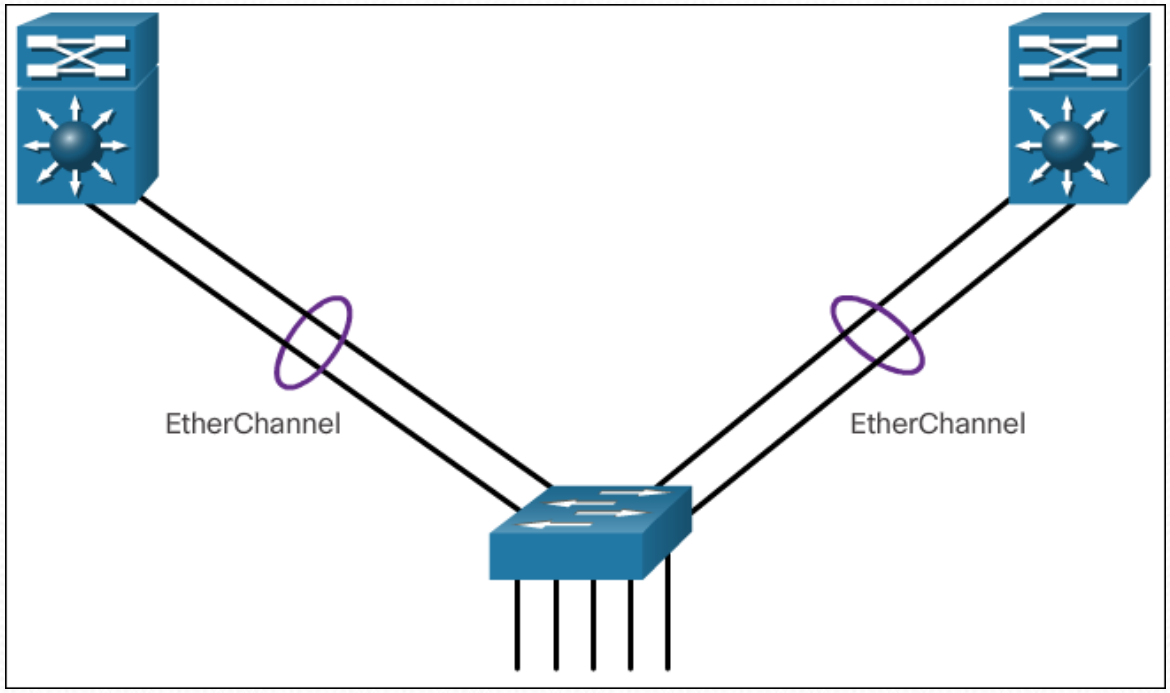
- Redundancy is an important part of network design for preventing disruption of network services
- One method of implementing redundancy is by installing duplicate equipment and providing failover services for critical devices
- Another method of implementing redundancy is redundant paths



Note: We will look at Spanning Tree in more detail in the next lecture

Avoiding Bottlenecks

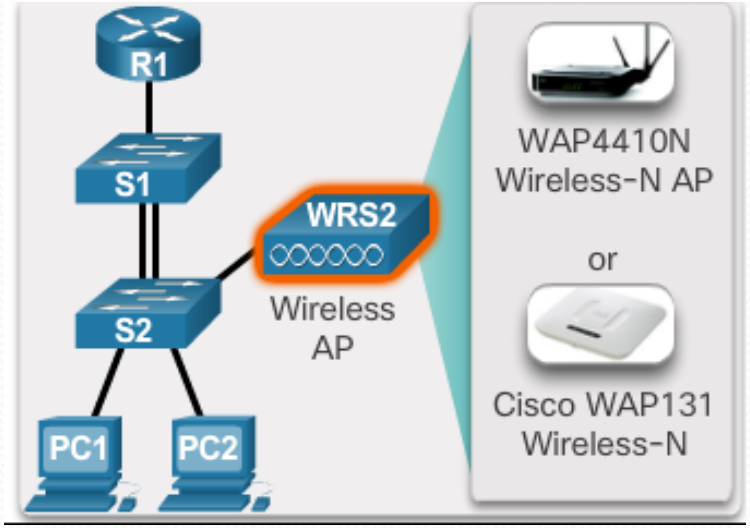
- Link aggregation allows an administrator to increase the amount of bandwidth between devices by creating one logical link made up of several physical links
- EtherChannel is a form of link aggregation used in switched networks



Note: We will look at EtherChannel in more detail in lecture 3 or 4

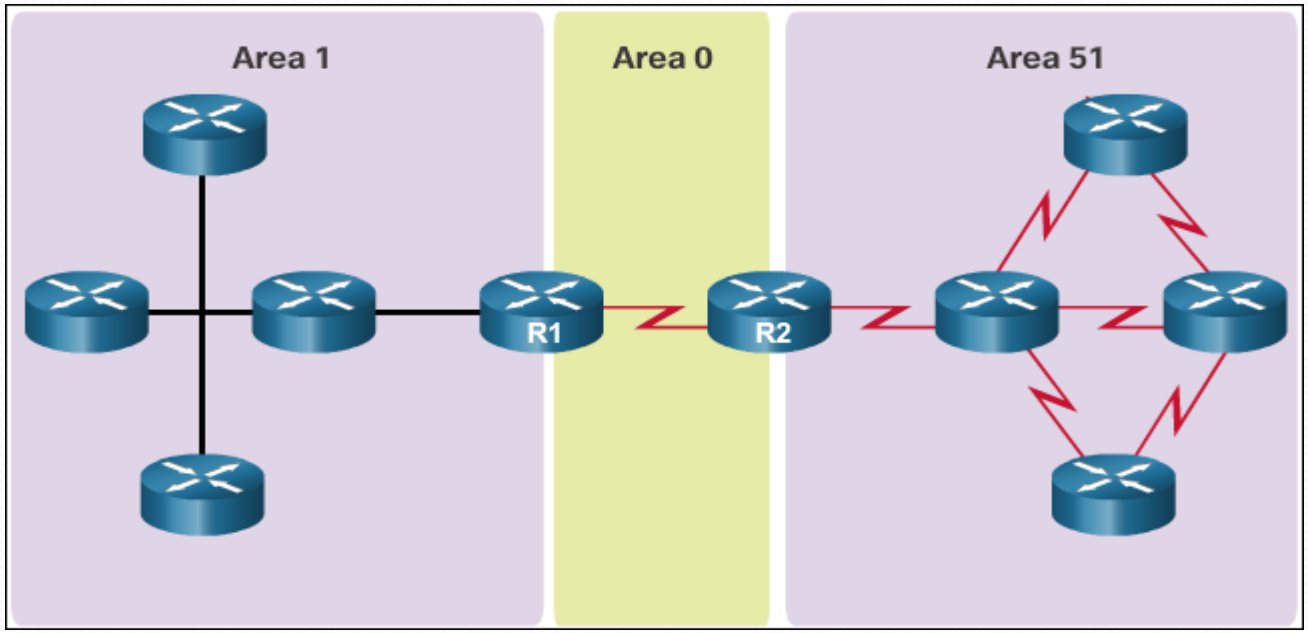
Design for Mobility

- Providing wireless connectivity offers many advantages, such as increased flexibility, reduced costs, and the ability to grow and adapt to changing network and business requirements
- To communicate wirelessly, a wireless router or a wireless access point (AP) is required for users to connect



Fine-tuning Routing Protocols

- Link-state routing protocols, such as Open Shortest Path First (OSPF), works well for larger hierarchical networks where fast convergence is important
- OSPF routers establish and maintain neighbor adjacency or adjacencies, with other connected OSPF routers
- Additionally, OSPF supports a 2-layer hierarchical design (called multiarea OSPF) where Area 0 is the backbone and other non-backbone area can be created



Exercise

- Match each network scalability design term to its description

Descriptions
Protocol with distance-vector behaviors.
Alternate data pathway.
Multiple Ethernet interface links combined into a single bandwidth channel.
Protocol which uses a backbone area.

Selecting Network Devices

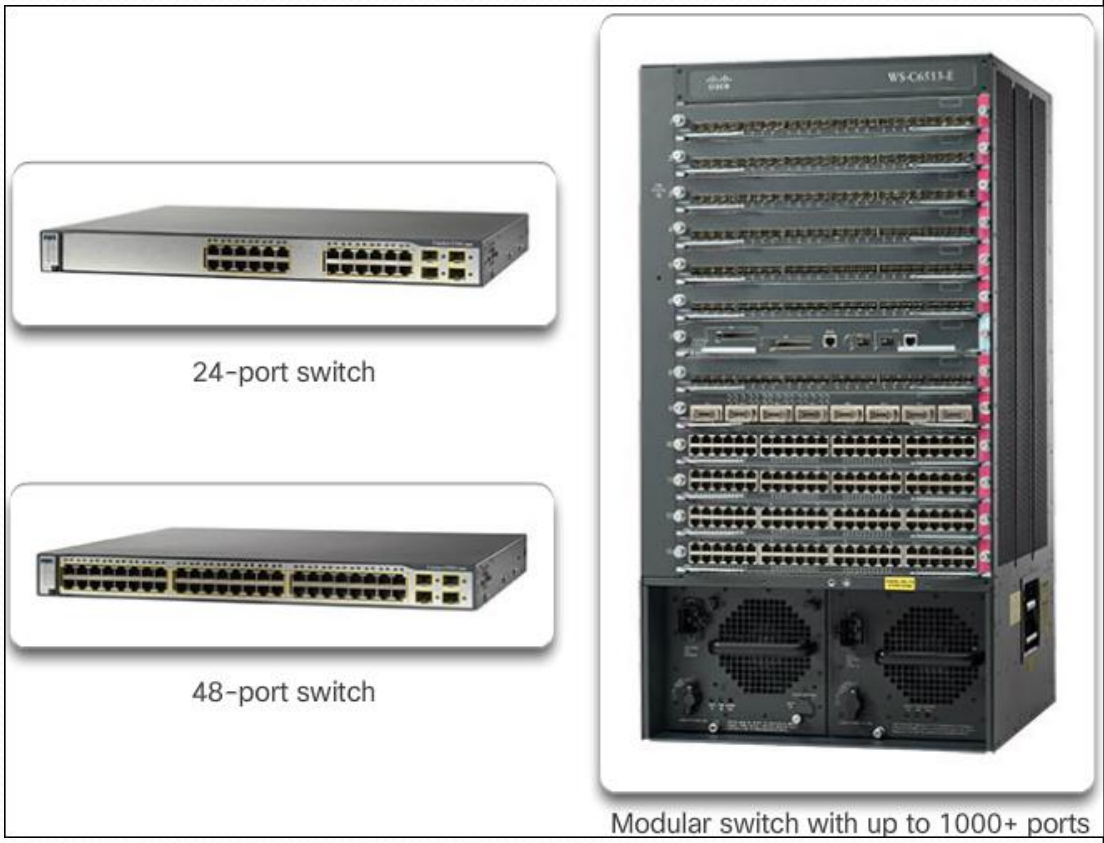
Switch Categories

- There are five categories of switches for enterprise networks:

1. Campus LAN Switches: must support all 3 hierarchical layers (i.e. access, distribution & access). E.g.: 2960 to 6800 series.
2. Data Center Switches: should support infrastructure scalabiity, operational continuity & transport flexibility. E.g. Nexus, 6500 series
3. Cloud-Managed Switches: configuration & management of switches takes place over the web. E.g. Cisco Meraki switches
4. Service Provider Switches: service provider switches fall under two categories: aggregation switches and Ethernet access switches.
5. Virtual Networking: supports secure multitenant services by adding virtualization intelligence technology to the data center network. E.g. Nexus 1000v

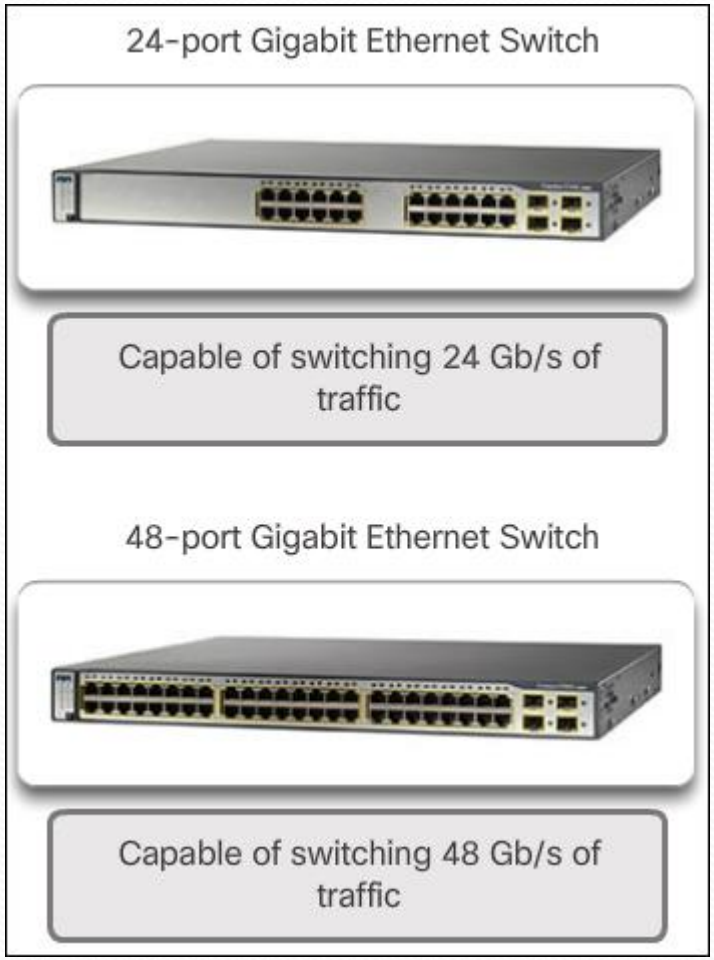
Switch Selection Considerations – Port Density

- The port density of a switch refers to the number of ports available on a single switch
- Fixed configuration switches typically support up to 48 ports on a single device
- Modular switches can support very high-port densities through the addition of multiple switch port line cards.



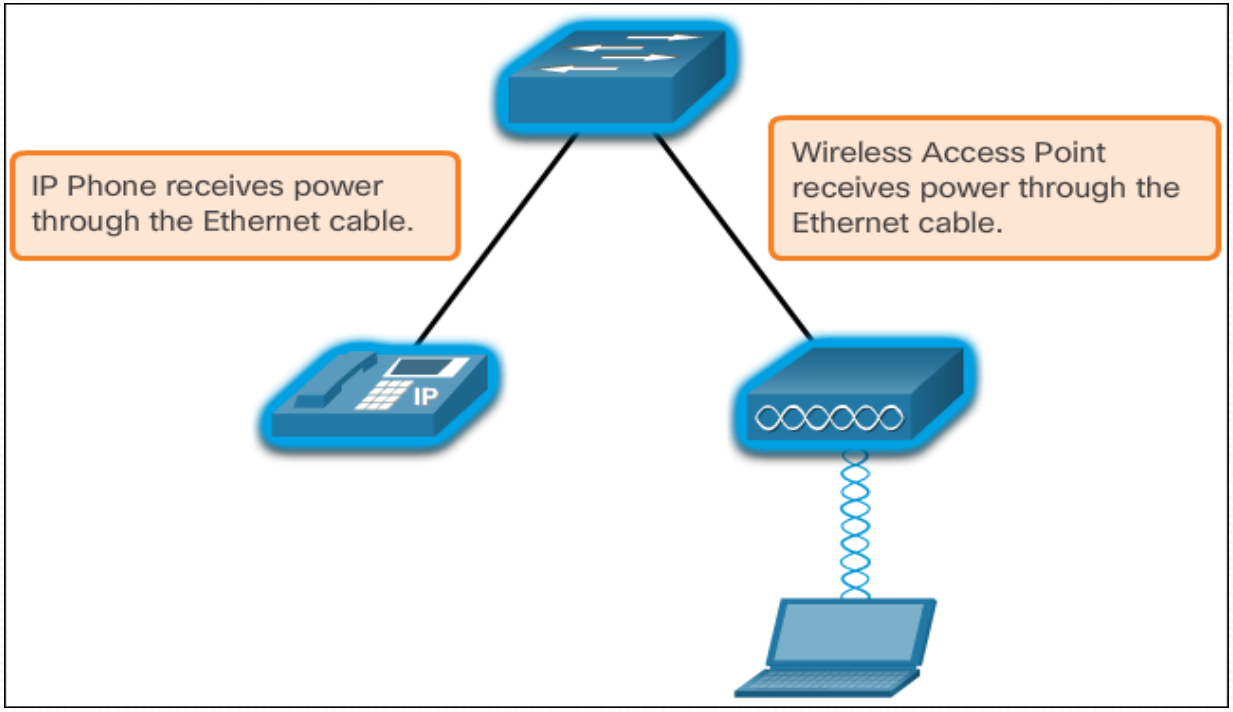
Switch Selection – Forwarding Rate & Wire Speed

- Forwarding rates define the processing capabilities of a switch by rating how much data the switch can process per second
- Wire speed is the data rate that each Ethernet port on the switch is capable of attaining. Data rates can be 100 Mb/s, 1 Gb/s, 10 Gb/s, or 100 Gb/s
- Less expensive, lower performing switches can be used at the access layer, and more expensive, higher performing switches can be used at the distribution and core layers, where the forwarding rate has a greater impact on network performance



Switch Selection Considerations – PoE

- Power over Ethernet (PoE) allows the switch to deliver power to a device over the existing Ethernet cabling
- PoE allows more flexibility when installing wireless access points and IP phones, allowing them to be installed anywhere that there is an Ethernet cable



Switch Selection – Multilayer Switching

- Multilayer switches are typically deployed in the core and distribution layers of an organization's switched network
- Multilayer switches are characterized by their ability to build a routing table, support a few routing protocols, and forward IP packets at a rate close to that of Layer 2 forwarding
- It is likely that soon all switches will incorporate a route processor because the cost of doing so is decreasing relative to other constraints

Exercise

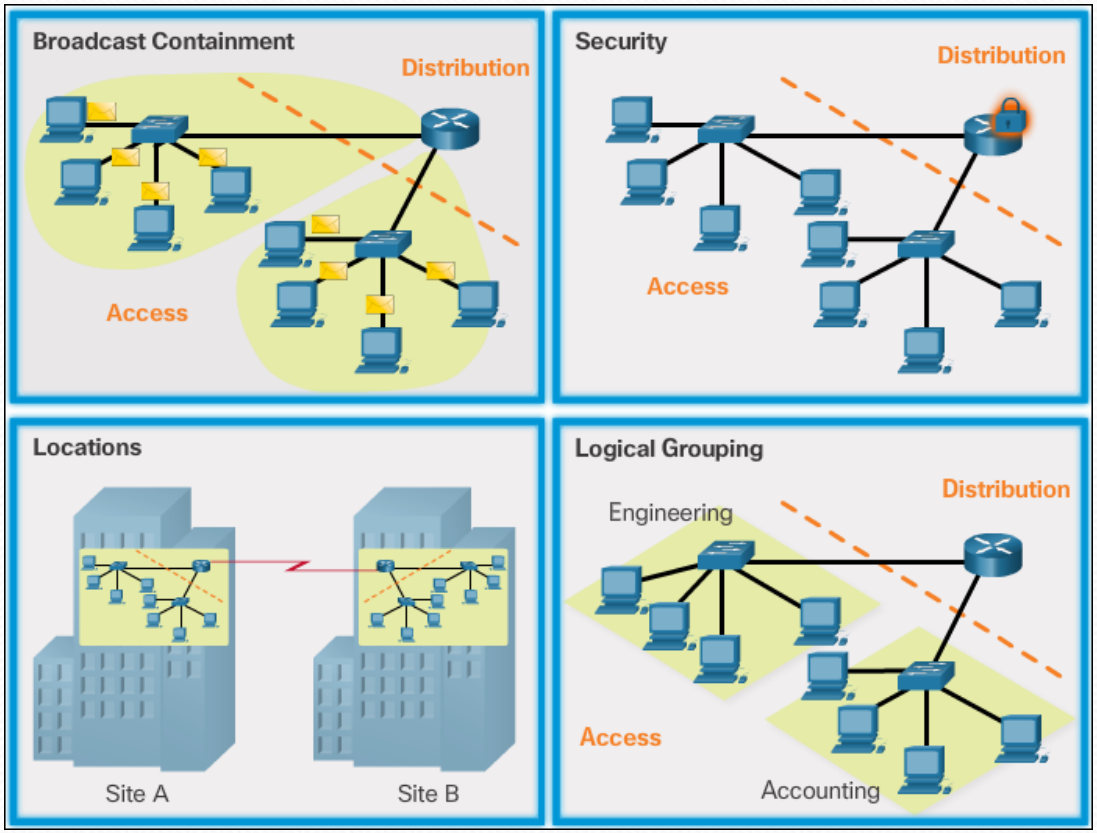
Match each feature to its switch selection criteria.

Feature	Switch Selection Criteria
Modular Configuration	End device electrical power provided through the Ethernet data cabling.
Port Density	How fast interfaces will process Ethernet frames.
Fixed Configuration	Expansion of capacity and speed using upgradable line/port cards.
Forwarding Rates	Built-in, permanent interfaces, and ports.
Stackable	Ability to interconnect multiple switches to effectively manage them as one large switch.
PoE	Number of ports on a switch.

Router Selection

- Routers play a critical role in networking by connecting homes and businesses to the Internet, interconnecting multiple sites within an enterprise network, providing redundant paths, and connecting ISPs on the Internet. They also act as a translator between different media types and protocols

Limit broadcasts to the local network



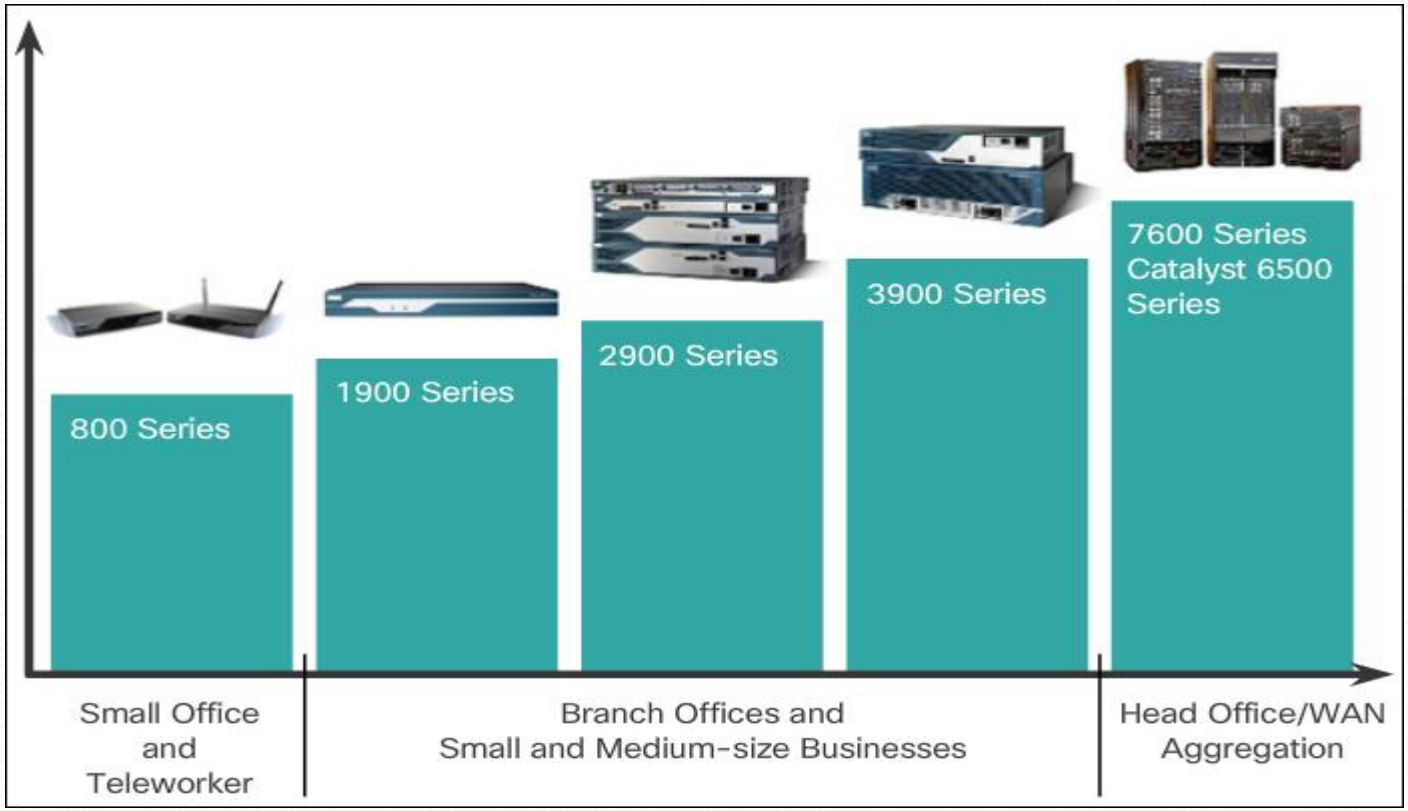
Can use ACL's to filter unwanted traffic

Interconnect separated locations

Logically group users requiring access to same resources

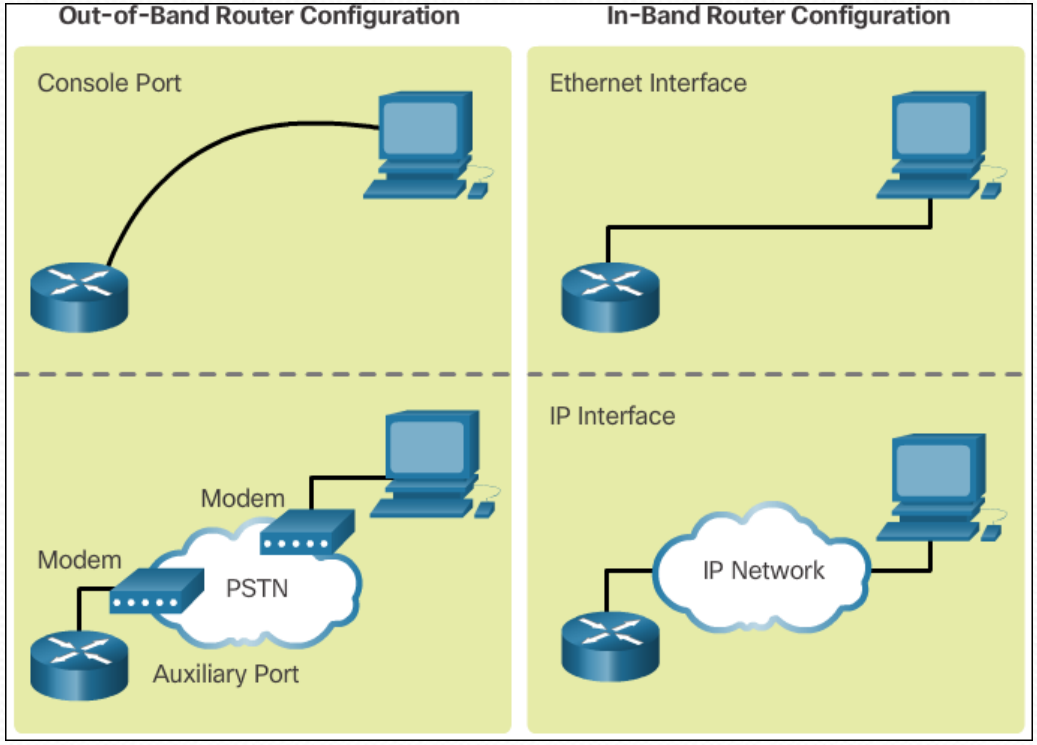
Router Categories

- There are three categories of routers: Branch, Network Edge, and Service Provider
- Routers also come in many form factors. Network administrators in an enterprise environment should be able to support a variety of routers, from a small desktop router to a rack-mounted or blade model



Router Management

- IOS refers to the package of routing, switching, security, and other internetworking technologies integrated into a single multitasking operating system
- Out-of-band management is used for initial configuration or when a network connection is unavailable
- In-band management is used to monitor and make configuration changes to a network device over a network connection



Router Management – Basic CLI Commands

- A basic router configuration includes:
  - the hostname for identification
  - passwords for security
  - assignment of IP addresses to interfaces for connectivity
  - Enabling a routing protocol

- Verify and save configuration changes using the `copy running-config startup-config` command

- To clear the router configuration, use the `erase startup-config` command and then the reload command

Router Management – Basic Show Commands

Some of the most commonly used IOS commands to display and verify the operational status of the router and related IPv4 network functionality are:

- `show ip protocols` - Displays information about the routing protocols configured
- `show ip route` - Displays routing table information, including: routing codes, known networks, administrative distance and metrics, how routes were learned, next hop, static routes, and default routes
- `show interfaces` - Displays interfaces with line (protocol) status, bandwidth, delay, reliability, encapsulation, duplex, and I/O statistics
- `show ip interfaces` - Displays interface information, including: protocol status, the IPv4 address, if a helper address is configured, and whether an ACL is enabled on the interface

Router Management – Basic Show Commands (cont.)

- `show ip interface brief` - Displays all interfaces with IPv4 addressing information and interface and line protocols status

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status
Embedded-Service-Engine0/0 unassigned      YES unset  administrativ
GigabitEthernet0/0         172.16.1.1      YES manual up
GigabitEthernet0/1         unassigned      YES unset  administrativ
Serial0/0/0                172.16.3.1      YES manual up
Serial0/0/1                192.168.10.5    YES manual up
```

- `show protocols` - Displays information about the routed protocol that is enabled, and the protocol status of interfaces
- `show cdp neighbors` - Displays information about all directly connected Cisco devices
- `show ip ospf neighbor` - Displays information about OSPF neighbours that have been learned, including the Router ID of the neighbour, the priority, the state (Full = adjacency has been formed), the IP address, and the local interface that learned of the neighbour

Switch Management – Basic CLI Commands

A basic switch configuration includes:

- Setting hostname & passwords
- In-Band access requires the Switch to have an IP address (assigned to VLAN 1)
- Save switch configuration using the `copy running-config startup-config` command
- To clear the switch configuration, use the `erase startup-config` command and then the `reload` command
- Erase any VLAN information using the command `delete flash:vlan.dat`
- When switch configurations are in place, view the configurations using the `show running-config` command

```
Switch# enable
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# enable secret class
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# service password-encryption
S1(config)# banner motd $ Authorized Access Only! $
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.5 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# ip default-gateway 192.168.1.1
S1(config)# interface fa0/2
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1# copy running-config startup-config
```

Switch Management – Basic Show Commands

Switches make use of common IOS commands for configuration, to check for connectivity and to display current switch status:

- `show port-security` – Displays any ports with security enabled
- `show port-security address` – Displays all secure MAC addresses

```
S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type              Ports    Remaining Age
                                                       (mins)
----    -----------       ----              -----    -------------
1       0025.83e6.4b01    SecureDynamic     Fa0/18       -
1       0025.83e6.4b02    SecureSticky      Fa0/19       -
```

- `show interfaces` – Displays detailed information about interfaces
- `show mac-address-table` – Displays all MAC addresses the switch has learned
- `show cdp neighbors` – Displays all directly connected Cisco devices

VTP, Extended VLANs and DTP

VLAN trunking protocol (VTP)

- VLAN trunking protocol (VTP) allows a network administrator to manage VLANs centrally on a switch configured as a VTP server
- The VTP server distributes and synchronizes VLAN information over trunk links to VTP-enabled switches throughout the switched network
- VTP stores VLAN configurations in a database called vlan.dat

VTP Modes

A switch can be configured in one of three VTP modes:

- **Server (default mode)**: You can make changes and propagate those changes out to all other switches in the VTP domain. VTP servers store VLAN information for the entire domain in NVRAM

- **Client**: Your switch will only receive configurations from other devices and will not allow changes to VLANs to be made on that specific switch

- **Transparent**: You can set and store VLANs locally on that switch, but those changes are not sent to other switches on the network. You can forward VTP through the switch, but the switch will not participate with VTP

VTP Advertisement Types

VTP includes three types of advertisements:

- **Summary advertisements** - These inform adjacent switches of VTP domain name and configuration revision number
- **Advertisement request** - These are in response to a summary advertisement message when the summary advertisement contains a higher configuration revision number than the current value
- **Subset advertisements** - These contain VLAN information including any changes

VTP Concepts and Operation

VTP Components	Definition
VTP Domain	• Consists of one or more interconnected switches. • All switches in a domain share VLAN configuration details using VTP advertisements. • Switches that are in different VTP domains do not exchange VTP messages. • A router or Layer 3 switch defines the boundary of each domain.
VTP Advertisements	• Each switch in the VTP domain sends periodic global configuration advertisements from each trunk port to a reserved multicast address. • Neighboring switches receive these advertisements and update their VTP and VLAN configurations as necessary.
VTP Modes	A switch can be configured in one of three VTP modes: server, client, or transparent.
VTP Password	Switches in the VTP domain can be also be configured with a password.

VTP Configuration Status

- There are 3 versions of VTP (i.e. v1, v2 & v3) and switches in the same VTP domain must use the same VTP version
- The `show vtp status` privileged EXEC command displays the VTP status. This should always be used when a switch is added to a network to ensure it has a default VTP configuration – very important!

```
S1# show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : f078.167c.9900
Configuration last modified by 0.0.0.0 at 3-1-93 00:02:11

Feature VLAN:
--------------
VTP Operating Mode                : Transparent
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 12
Configuration Revision            : 0
MD5 digest                        : 0x57 0xCD 0x40 0x65 0x63 0x59
0x47 0xBD
                                    0x56 0x9D 0x4A 0x3E 0xA5 0x69
0x35 0xBC
S1#
```

Switch MAC address

The configuration revision number is used when determining whether a switch should keep its existing VLAN database, or overwrite it with the VTP update sent by another switch

VTP Configuration

- There are 5 steps to VTP configuration:

1. Configure the VTP Server
   - First check all switches are configured with default setting and then configure S1 as VTP server using **`vtp mode server`** global config command. Re-check configuration.
2. Configure the VTP Domain Name and Password
   - Use the **`vtp domain`** *`domain-name`* and **`vtp password`** *`password`* commands to configure on S1. If other switches in the network have the default NULL domain name they will accept the new VTP domain name from S1.
3. Configure the VTP Clients
   - Use the **`vtp mode client`** command.

VTP Configuration (continued)

4. Configure VLANs on the VTP Server

```
S1(config)# vlan 10
S1(config-vlan)# name SALES
S1(config-vlan)# vlan 20
S1(config-vlan)# name MARKETING
S1(config-vlan)# vlan 30
S1(config-vlan)# name ACCOUNTING
S1(config-vlan)# end
S1#
```

5. Verify the VTP Clients have received the new VLAN information

```
S2# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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
10   SALES                            active
20   MARKETING                        active
30   ACCOUNTING                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
S2#
```

Normal & Extended Range VLANs

- Normal range VLANs are identified by a VLAN ID between 1 and 1005
- IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs
- IDs 1 and 1002 to 1005 are automatically created and cannot be removed
- Extended range VLANs are identified by a VLAN ID between 1006 and 4094 (switch support dependent)
- VTP does not learn extended range VLANs
- In order to configure an extended VLAN on a 2960 switch it must be set to VTP transparent mode

Exercise

- Choose the correct VTP mode (client, server or transparent) for each definition:

1. Cannot create, change, or delete VLANs
2. VLANs that are created, renamed, or deleted on these are local to that switch only
3. Where VLANs can be created, deleted, or renamed for the domain
4. Only stores the VLAN information for the entire domain while the switch is on
5. Advertises the VTP domain VLAN information to other VTP-enabled switches in the same VTP domain
6. Must be configured in this mode to create extended VLANs
7. Does not participate in VTP
8. Stores the VLAN information for the entire domain in NVRAM
9. A switch reset deletes the VLAN information
10. Forwards VTP advertisements without making changes to the local VLAN database

Creating a VLAN

Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Create a VLAN with a valid id number.	`S1(config)# vlan vlan-id`
Specify a unique name to identify the VLAN.	`S1(config-vlan)# name vlan-name`
Return to the privileged EXEC mode.	`S1(config-vlan)# end`

- In addition to entering a single VLAN ID, a series of VLAN IDs can be entered that are separated by commas, or as range of VLAN IDs separated by hyphens
  - Example:

```
S1(config)# vlan 100,102,105-107
```

Assigning Ports to VLANs

- After creating a VLAN, the next step is to assign ports to the VLAN

Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Set the port to access mode.	`S1(config-if)# switchport mode access`
Assign the port to a VLAN.	`S1(config-if)# switchport access vlan vlan_id`
Return to the privileged EXEC mode.	`S1(config-if)# end`

- An `access` port can belong to only one VLAN at a time (except when the port is connected to an IP phone/)
- The `switchport mode access` command changes the interface to permanent access mode (i.e. nontrunking). This command is optional but recommended for security

Dynamic Trunking Protocol (DTP)

- Dynamic Trunking Protocol (DTP) manages trunk negotiation only if the port on the neighbor switch is configured in a trunk mode that supports DTP – i.e. point-to-point operation
- Turn off DTP on interfaces on a Cisco switch that is connected to devices that do not support DTP
- To enable trunking from a Cisco switch to a device that does not support DTP, use the `switchport mode trunk` and `switchport nonegotiate` interface configuration mode commands

DTP Trunking Modes

There are 5 commands to support different trunking modes:

1. switchport mode access: puts interface to permanent access mode (i.e. nontrunking) regardless of neighbour
2. switchport mode dynamic auto (default): allows the interface to be converted to a trunk link if neighboring interface is set to trunk or desirable mode
3. switchport mode dynamic desirable: makes interface actively attempt to convert link to a trunk link. Will become trunk if neighboring interface is set to trunk, desirable, or dynamic auto mode

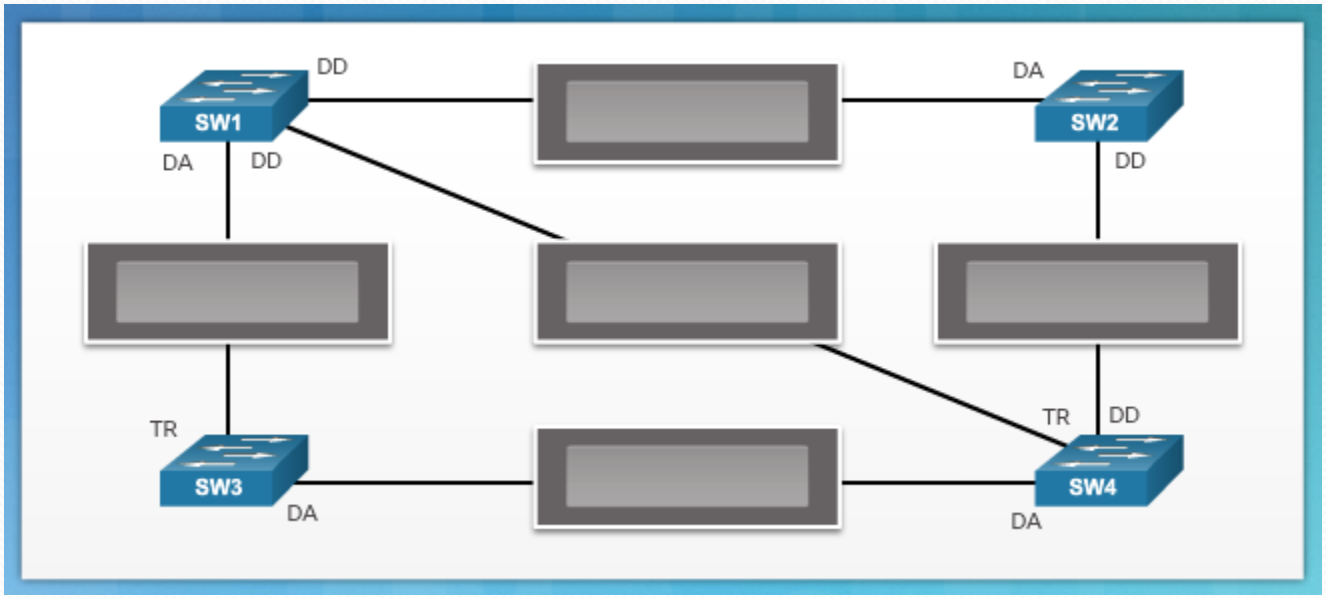
DTP Trunking Modes

4. switchport mode trunk: Puts interface into permanent trunking mode and negotiates to convert the neighbouring link into a trunk link. Becomes trunk interface even if neighbouring interface is not a trunk interface
5. switchport nonegotiate: Prevents interface from generating DTP frames. This command is only valid when the interface switchport mode is **access** or **trunk**

	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

Exercise

- Which DTP mode combinations between two switches will become trunk links and which will become access links?



KEY TO ABBREVIATIONS
TR = Trunk
AC = Access
DA = Dynamic Auto
DD = Dynamic Desirable

Troubleshoot Multi-VLAN Issues

Deleting a VLAN

- To delete a VLAN, use the `no vlan vlan-id` global configuration mode command

```
S1(config)# no vlan 99
S1(config)# exit
S1# show vlan id 99
VLAN id 99 not found in current VLAN database
```

- If switch is in VTP server mode, VLAN is removed from the VLAN database for all switches in the VTP domain
- When you delete a VLAN, any ports assigned to that VLAN become inactive until you assign them to a new VLAN

Switch Configuration Problems

- If a switch port is not configured for the correct VLAN, devices configured on that VLAN cannot connect to the router interface
- When a problem is suspected with a switch configuration, use the various verification commands to examine the configuration and identify the problem

```
S1# show interfaces FastEthernet 0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: up
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
<output omitted>
S1#
```

Router Configuration Problems

- When enabling inter-VLAN routing on a router, one of the most common configuration errors is to connect the physical router interface to the wrong switch port
- With router-on-a-stick configurations, a common problem is assigning the wrong VLAN ID to the subinterface
- Using the show interfaces and the show running-config commands can be useful in troubleshooting this type of issue

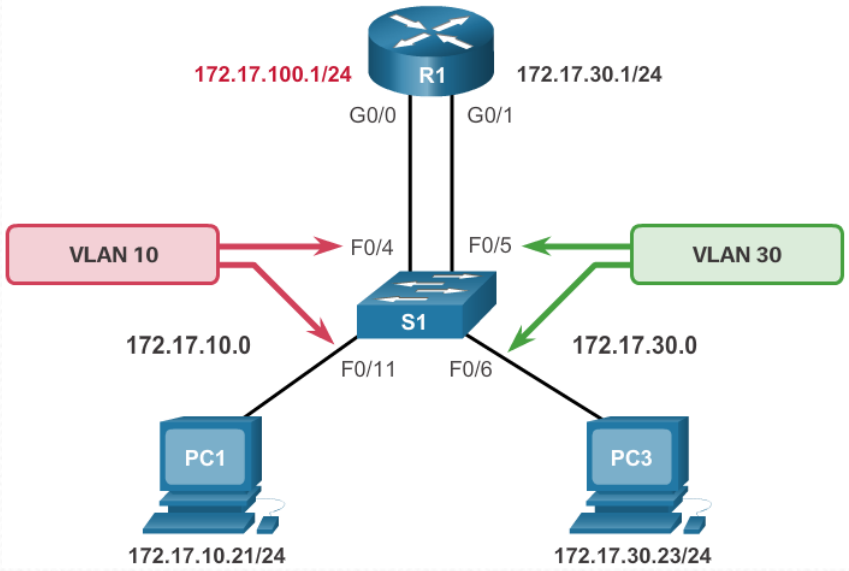
```
R1# show interfaces

<output omitted>

GigabitEthernet0/0.10 is up,line protocol is down (disabled)
 Encapsulation 802.1Q Virtual Lan,Vlan ID 100
 ARP type :ARPA,ARP Timeout 04:00:00,
 Last clearing of "show interface" counters never
```

Errors with IP Addresses and Subnet Masks

- For inter-VLAN routing to operate, a router must be connected to all VLANs, either by separate physical interfaces or by subinterfaces



- Each interface, or subinterface, must be assigned an IP address that corresponds to the subnet to which it is connected.
- Use the show running-config and show ip interface commands to verify IP address and subnet masks.

Troubleshooting VTP Issues

There are 5 common problems with VTP:

- Incompatible VTP Versions - Ensure that all switches are capable of supporting the required VTP version
- VTP Password Issues - If VTP authentication is enabled, switches must all have the same password configured to participate in VTP
- Incorrect VTP Domain Name - improperly configured VTP domain affects VLAN synchronization between switches and if a switch receives the wrong VTP advertisement, the switch discards the message. Should only be set by server
- All Switches Set to Client Mode – Cannot manage VLANs
- Incorrect Configuration Revision Number – Caused by a switch being added to the domain with the same VTP domain name but a higher configuration number

Troubleshooting DTP Issues

- There are three common problems associated with trunks.

VTP Components	Definition
Trunk mode mismatches	• For example, one trunk port is configured to trunk and the other side is configured as an access port. Another example is that both sides are configure in DTP auto mode. Other mismatches are also possible. • This configuration error causes the trunk link to stop working. • Correct the situation by shutting down the interface, correcting the DTP mode settings, and re-enabling the interface.
Allowed VLANs on trunks	• The list of allowed VLANs on a trunk has not been updated with the current VLAN trunking requirements. • In this situation, unexpected traffic or no traffic is being sent over the trunk. • Configure the correct VLANs that are allowed on the trunk.
Native VLAN mismatches	• When native VLANs do not match, the switches will generate informational messages letting you know of the problem. • Ensure that both sides of a trunk link are using the same native VLAN.

Layer 3 Switching

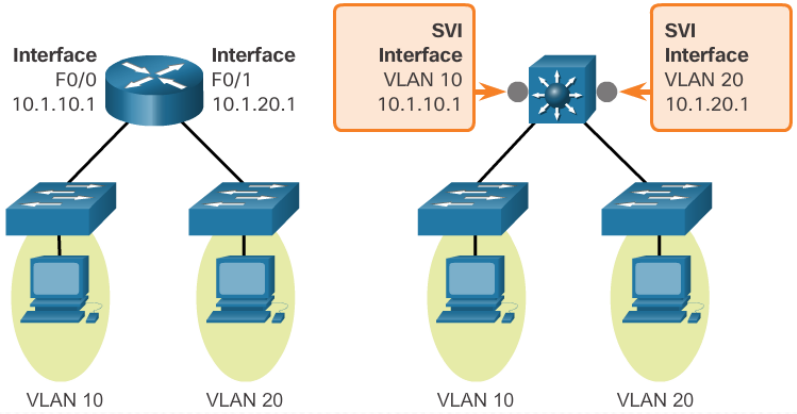
Layer 3 Switching Introduction

- Modern enterprise networks use multilayer switches to achieve high-packet processing rates using hardware-based switching

- Catalyst multilayer switches support the following types of Layer 3 interfaces:
  - Routed port: A pure Layer 3 interface similar to a physical interface on a Cisco IOS router
  - Switch virtual interface (SVI): A virtual VLAN interface for inter-VLAN routing. In other words, SVIs are the virtual-routed VLAN interfaces

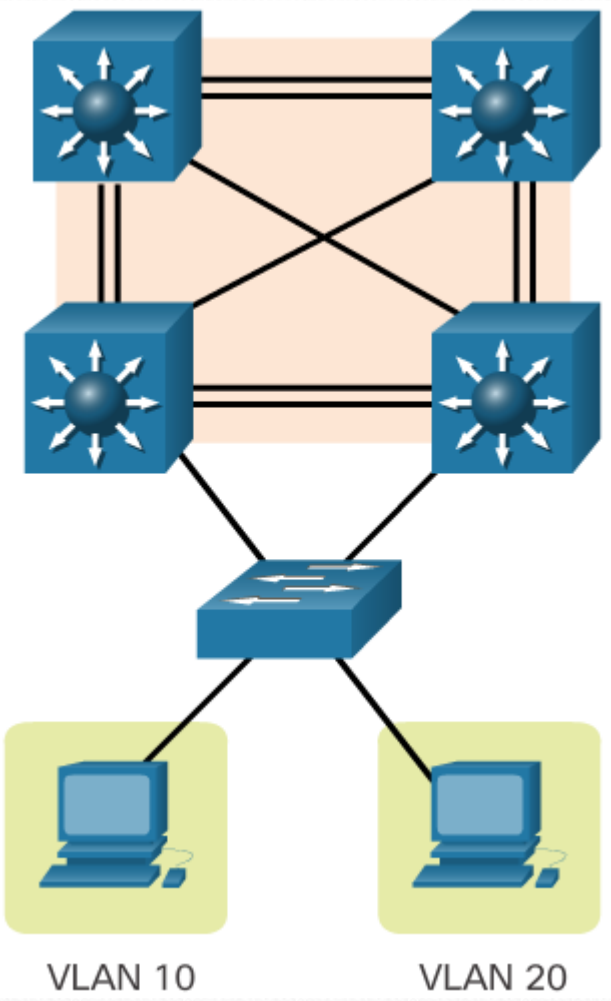
Inter-VLAN Routing and SVIs

- Routing can be transferred to the core and the distribution layers (and sometimes even the access layer) without impacting network performance
- An SVI can be created for any VLAN that exists on the switch
- SVIs are created the first time the VLAN interface configuration mode is entered for a particular VLAN SVI



Inter-VLAN Routing with Routed Ports

- A routed port is a physical port that acts similarly to an interface on a router
- A routed port is not associated with a particular VLAN
- Routed ports on a Cisco IOS switch do not support subinterfaces
- Routed ports are used for point-to-point links
- To configure routed ports, use the `no switchport interface` configuratio mode command on the appropriate ports



Troubleshooting Layer 3 Switching Configuration Issues

Check the following configurations for accuracy:

- VLANs - VLANs must be defined across all the switches. VLANs must be enabled on the trunk ports. Ports must be in the right VLANs
- SVIs - SVIs must have the correct IP address or subnet mask. SVIs must be up. Each SVI must match with the VLAN number
- Routing - Routing must be enabled. Each interface or network should be added to the routing protocol, or static routes entered, where appropriate.
- Hosts - Hosts must have the correct IP address or subnet mask. Hosts must have a default gateway associated with an SVI or routed port.

Summary

- The hierarchical network design model divides network functionality into the access layer, the distribution layer, and the core layer
- A well-designed network limits the size of failure domains, is scalable, has build in redundancy and avoids bottlenecks
- It is important to deploy the appropriate type of routers & switches for a given set of requirements, features/specifications & expected traffic flow
- VLAN Trunking Protocol (VTP) reduces administration of VLANs in a switched network
- A switch configured as the VTP server distributes and synchronizes VLAN information over trunk links to VTP-enabled switches throughout domain
- The three VTP modes are Server, Client and Transparent
- The configuration revision number is used when determining whether a VTP switch should keep or update its existing VLAN database
- Troubleshooting VTP can also involve solving errors with incompatible VTP versions & incorrectly configured domain names/passwords

Summary (Cont.)

- Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which operates on a point-to-point basis between network devices.
- A general best practice when a trunk link is required is to set the interface to trunk and nonegotiate. On links where trunking is not intended, DTP should be turned off
- When troubleshooting DTP, problems can be related to trunk mode mismatches, allowed VLANS on a trunk, and native VLAN mismatches
- SVIs is a method of inter-VLAN routing on Layer 3 switching. An SVI with appropriate IP addressing is configured for each VLAN
- Another method of Layer 3 inter-VLAN routing is using routed ports. A routed port is a physical port that acts similarly to an interface on a router
- Troubleshooting inter-VLAN routing with a router or a Layer 3 switch are similar. Common errors involve VLAN, trunk, Layer 3 interface, and IP address configurations