1.1 Implementing a Network Design

Scaling Networks

Cisco | Networking Academy®
Mind Wide Open™

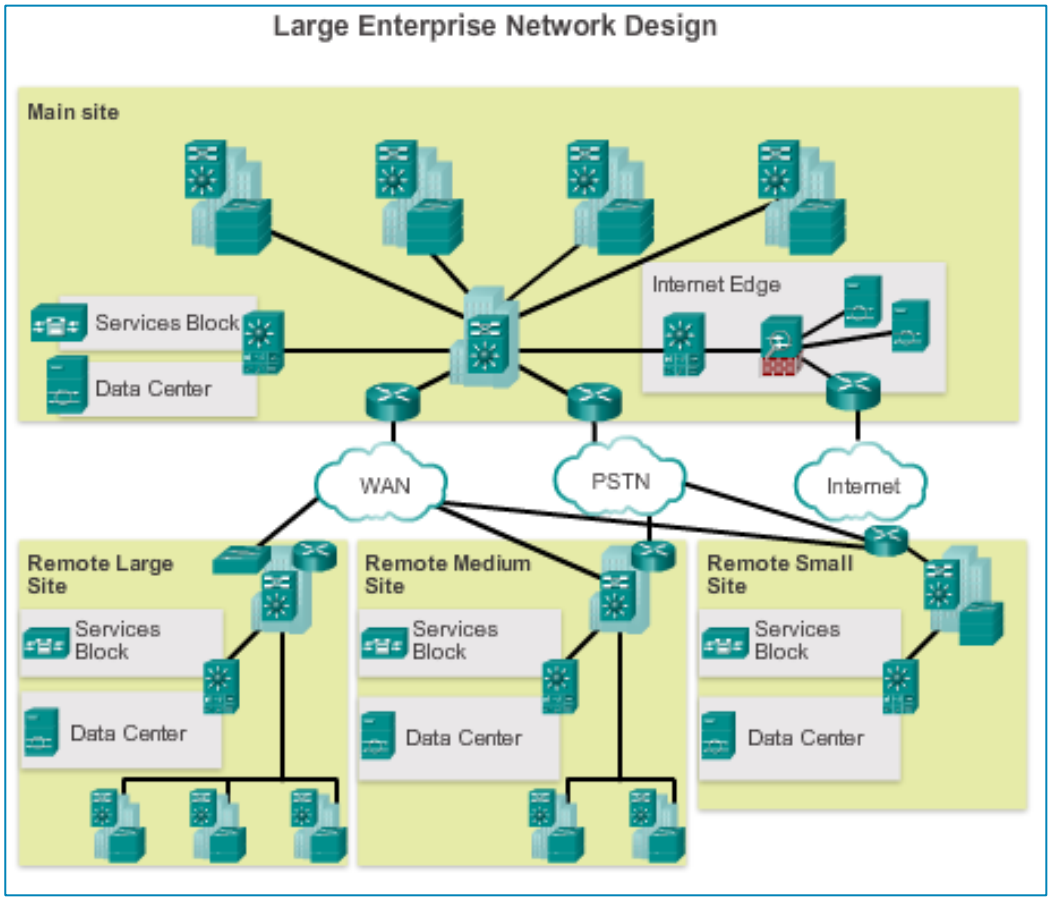
Network Scaling Needs

As they grow and expand, all enterprise networks must:

- Support critical applications
- Support converged network traffic
- Support diverse business needs
- Provide centralized administrative control

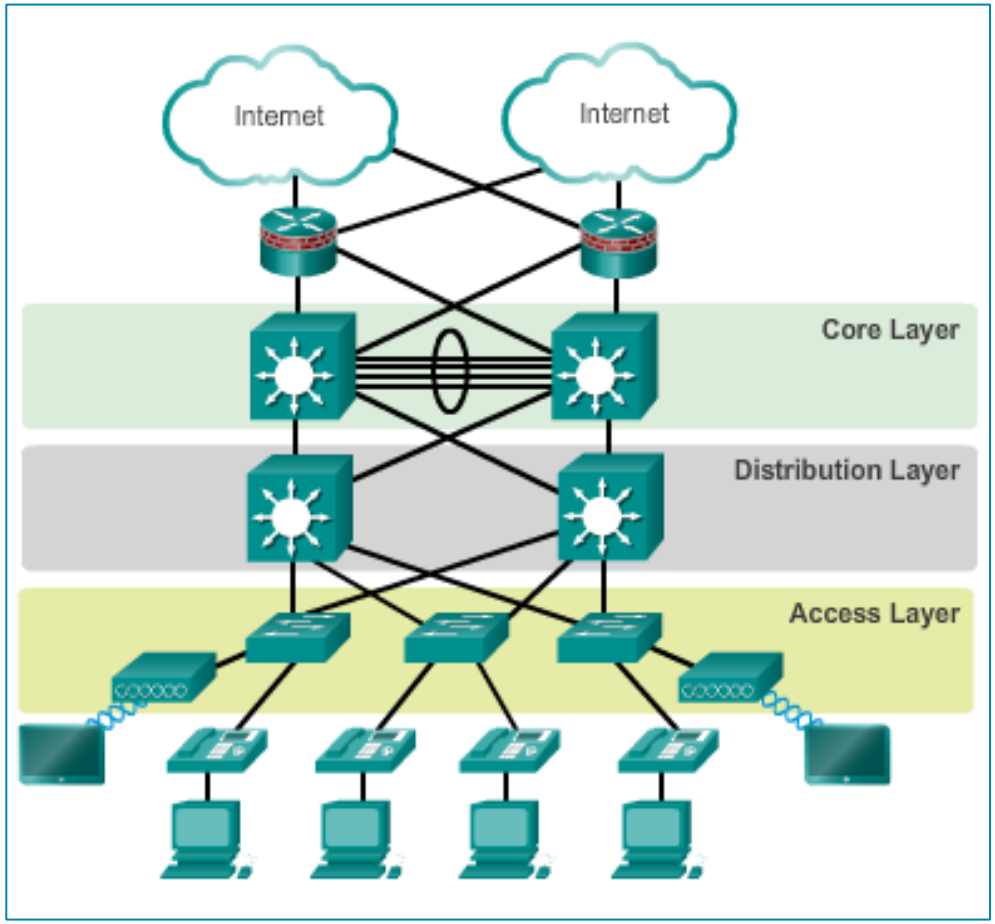
Enterprise Business Devices

To provide a high-reliability network, enterprise class equipment is installed in the enterprise network.



Hierarchical Network Design

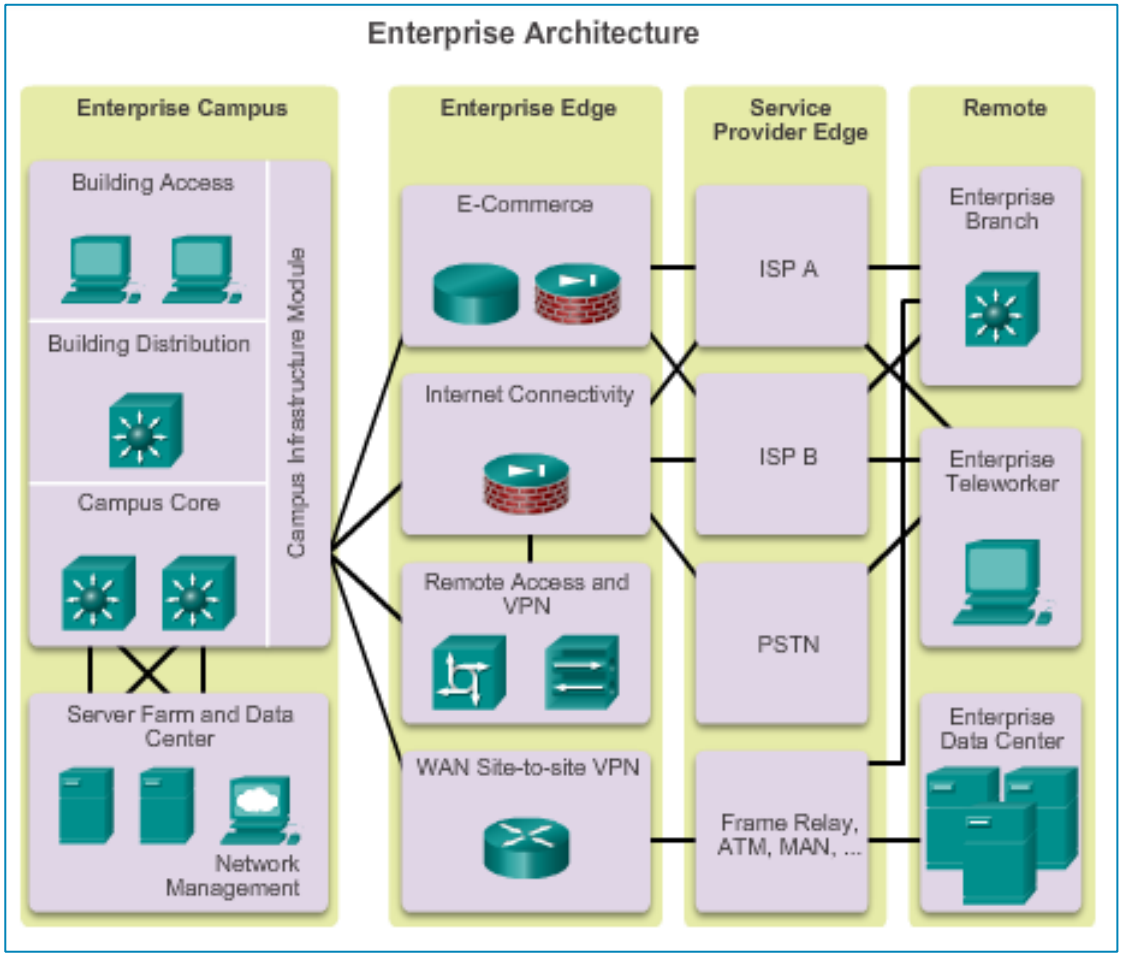
This model divides the network functionality into three distinct layers.



Cisco Enterprise Architecture

The primary Cisco Enterprise Architecture modules include:

- Enterprise Campus
- Enterprise Edge
- Service Provider Edge
- Remote



Failure Domains

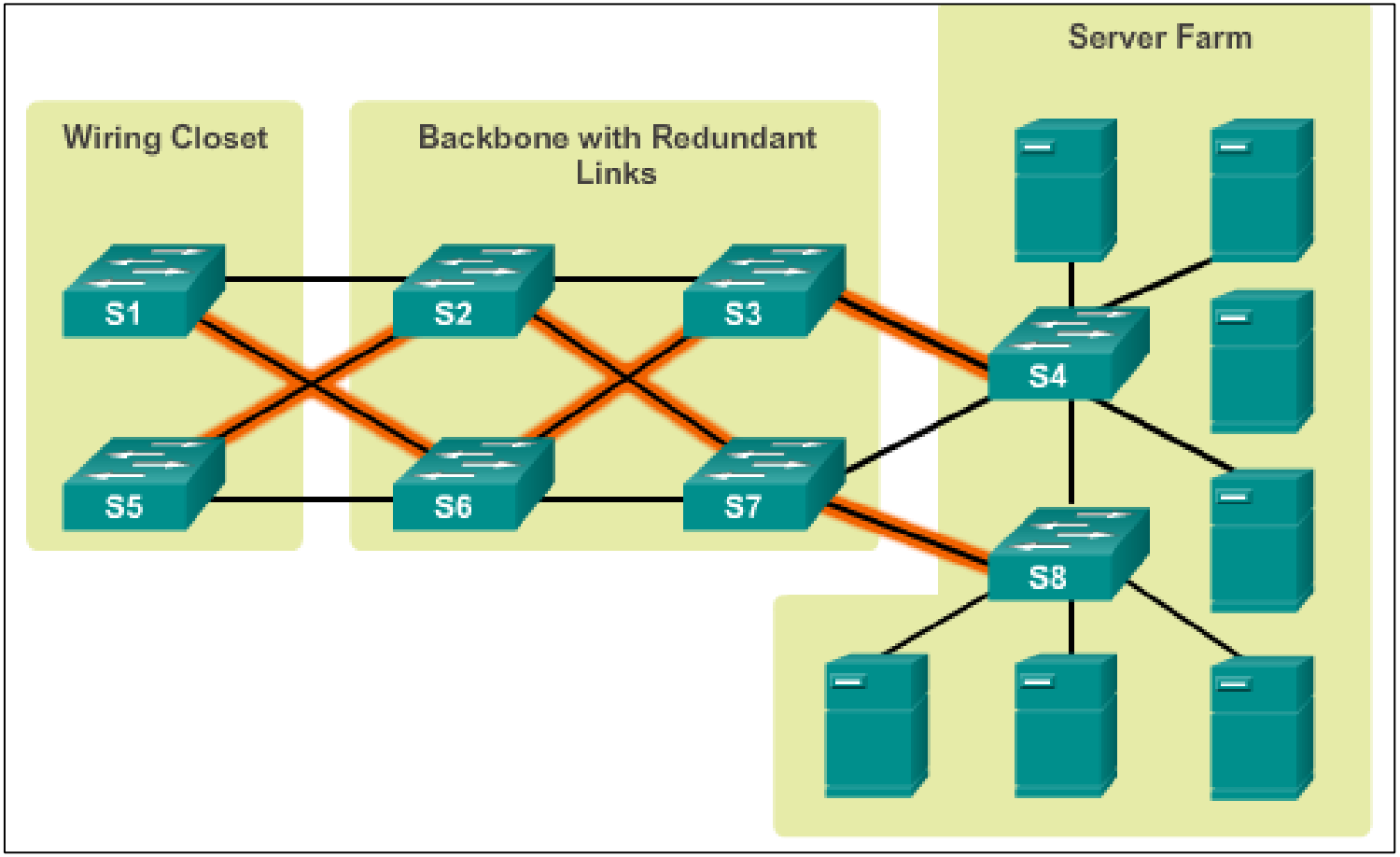
- Failure Domains are areas of a network that are impacted when a critical device or network service experiences problems.
- Redundant links and enterprise class equipment minimize disruption of network.
- Smaller failure domains reduce the impact of a failure on company productivity.
- Smaller failure domains also simplify troubleshooting.
- Switch block deployment – each switch block acts independently of the others. Failure of a single device does not impact the whole network.

Designing for Scalability

- Use expandable, modular equipment or clustered devices.
- Include design modules that can be added, upgraded, and modified, without affecting the design of the other functional areas of the network.
- Create a hierarchical addressing scheme.
- Use routers or multilayer switches to limit broadcasts and filter traffic.

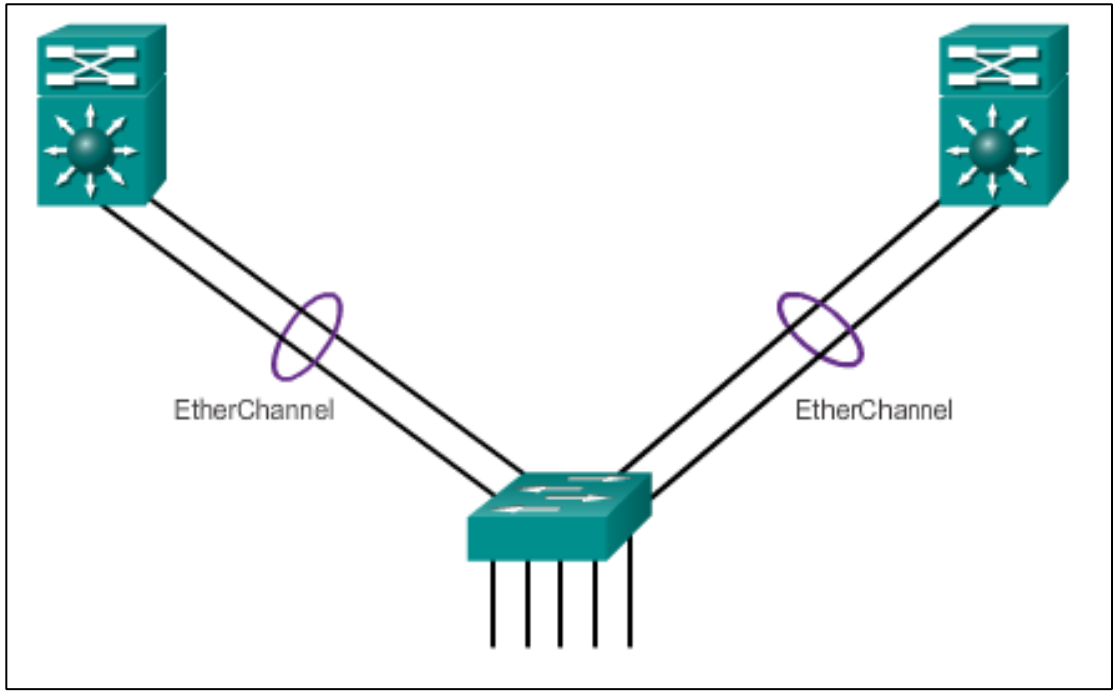
Planning for Redundancy

- Installing duplicate equipment
- Providing redundant paths



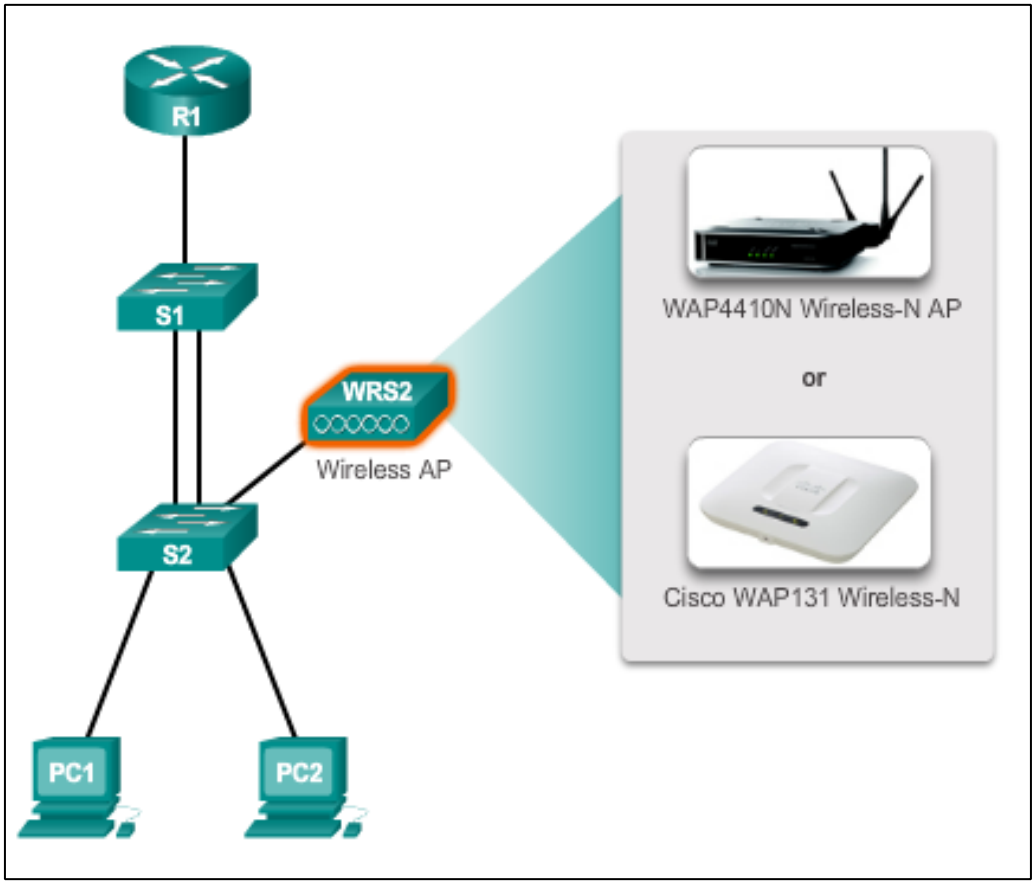
Increasing Bandwidth

- Link aggregation increases 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.



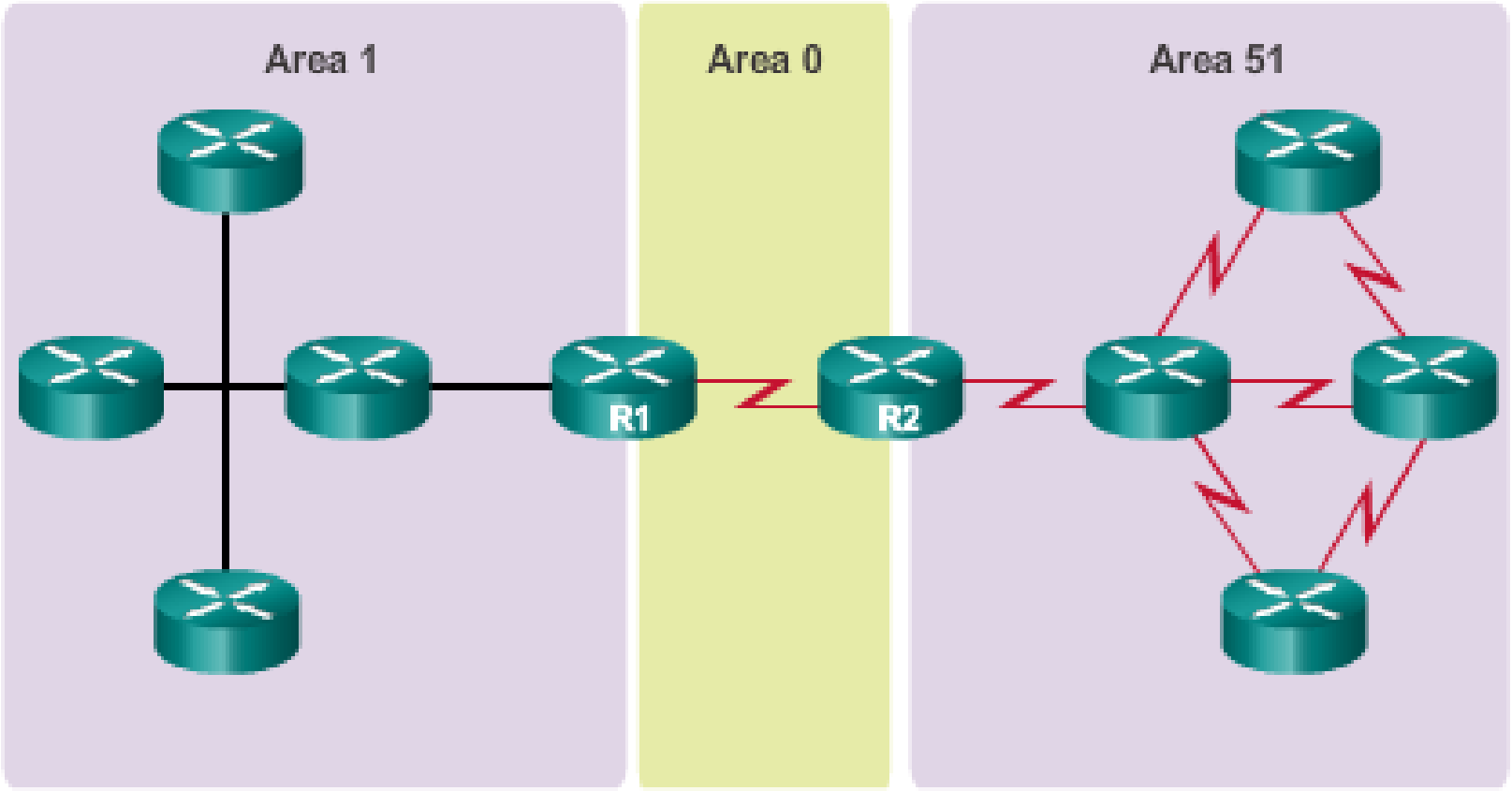
Expanding the Access Layer

Access layer connectivity can be extended through wireless connectivity.



Fine-Tuning Routing Protocols

OSPF works well for large, hierarchical networks.



1.2 Selecting Network Devices

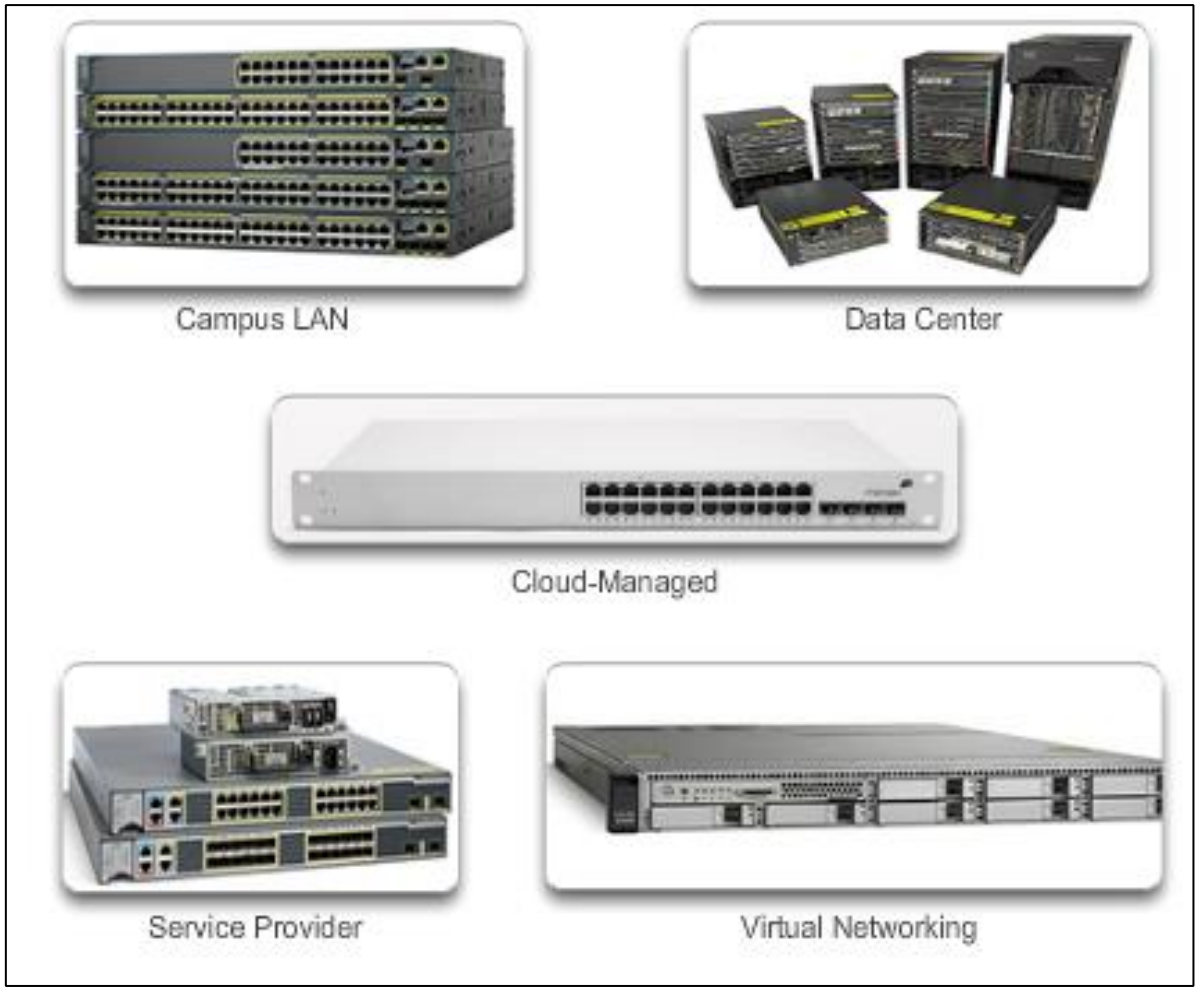
Scaling Networks

Cisco | Networking Academy®
Mind Wide Open™

Switch Platforms

Select form factor:

- Fixed
- Modular
- Stackable
- Non-stackable



Switch Hardware

Port Density

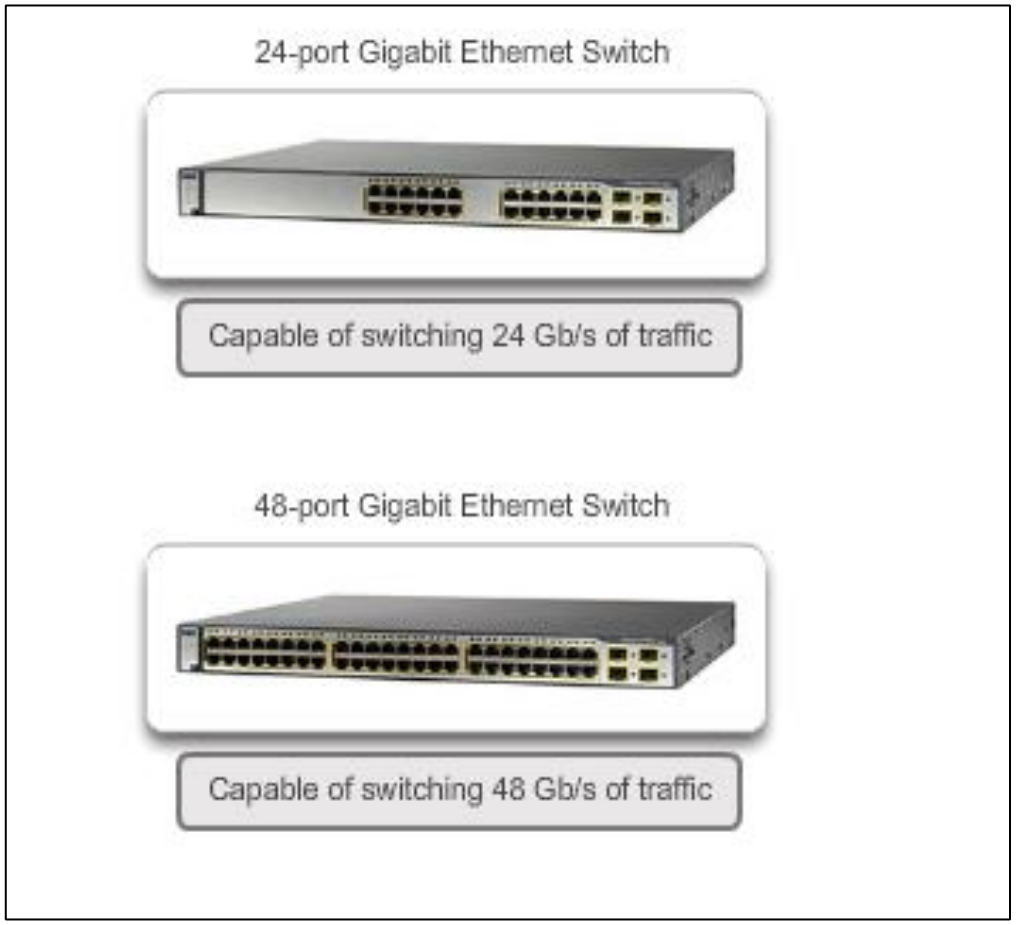
24-port switch

48-port switch

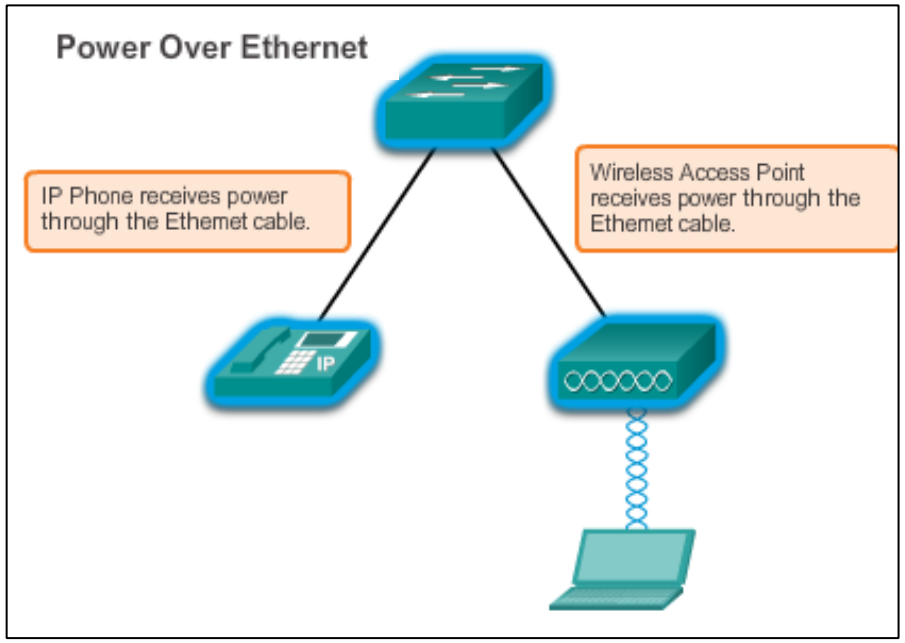
Modular switch with up to 1000+ ports

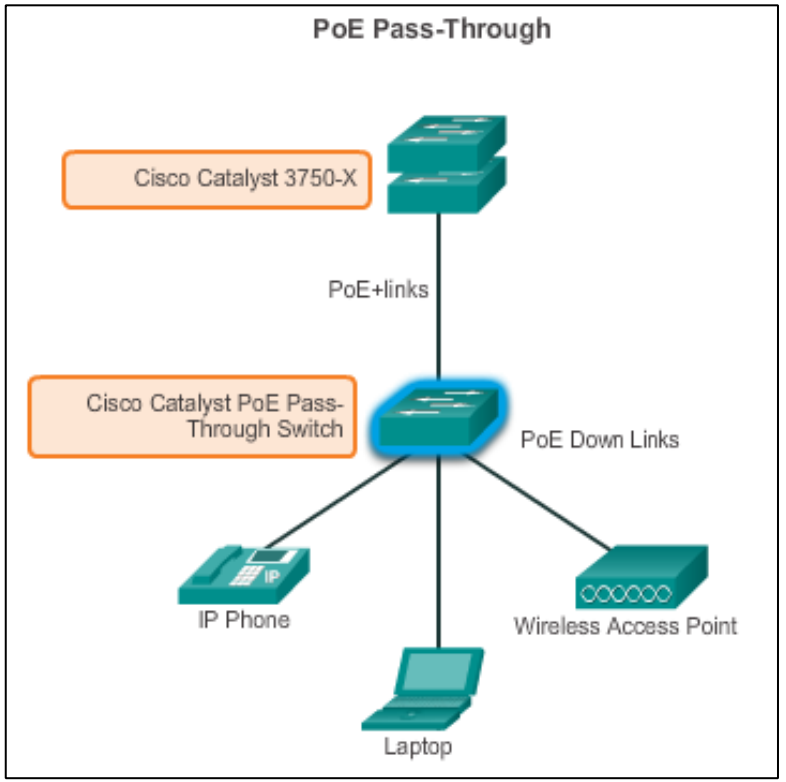
Forwarding Rates

The processing capabilities of a switch are rated by how much data the switch can process per second.



Power over Ethernet





Multilayer Switching

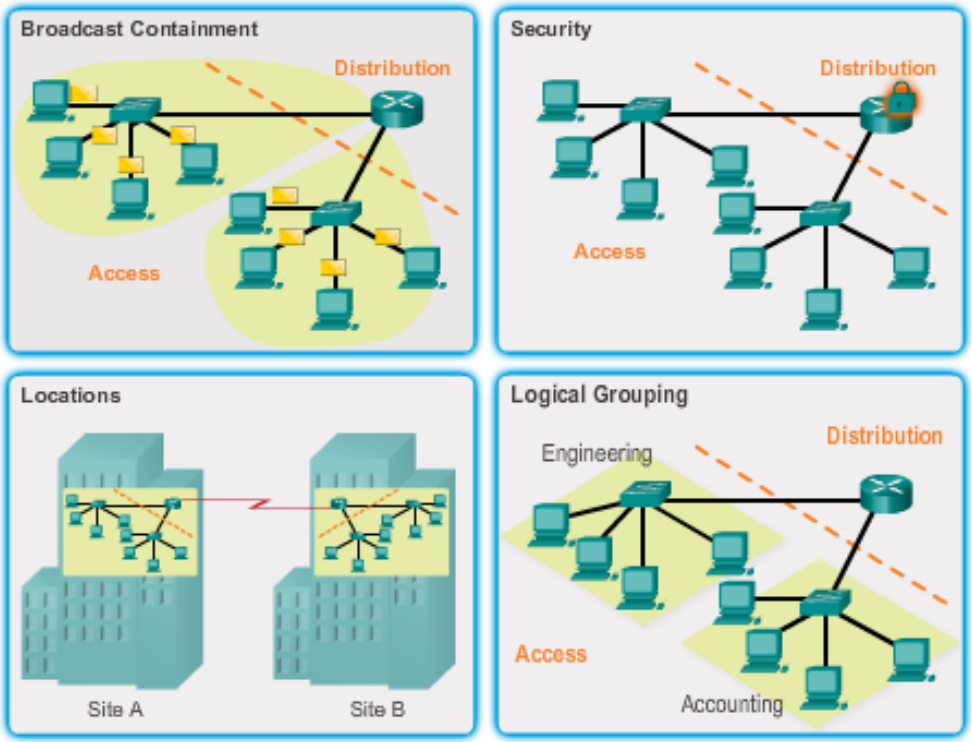
- Deployed in the core and distribution layers of an organization's switched network.
- Can build a routing table, support a few routing protocols, and forward IP packets.

Cisco Catalyst 2960 Series Switches

Router Requirements

Role of routers:

- Interconnect multiple sites
- Provide redundant paths
- Connect ISPs
- Translate between media types and protocols



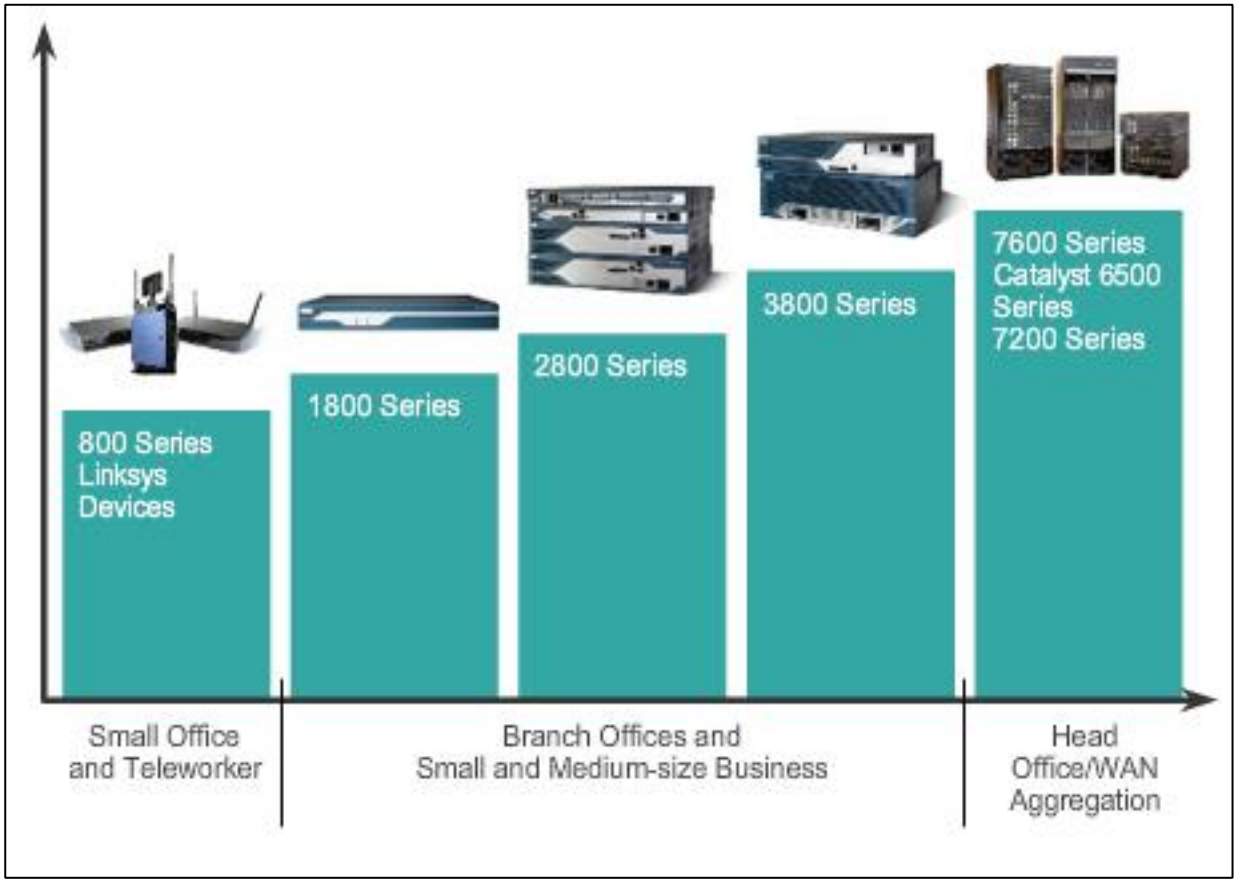
Cisco Routers

Three categories of routers:

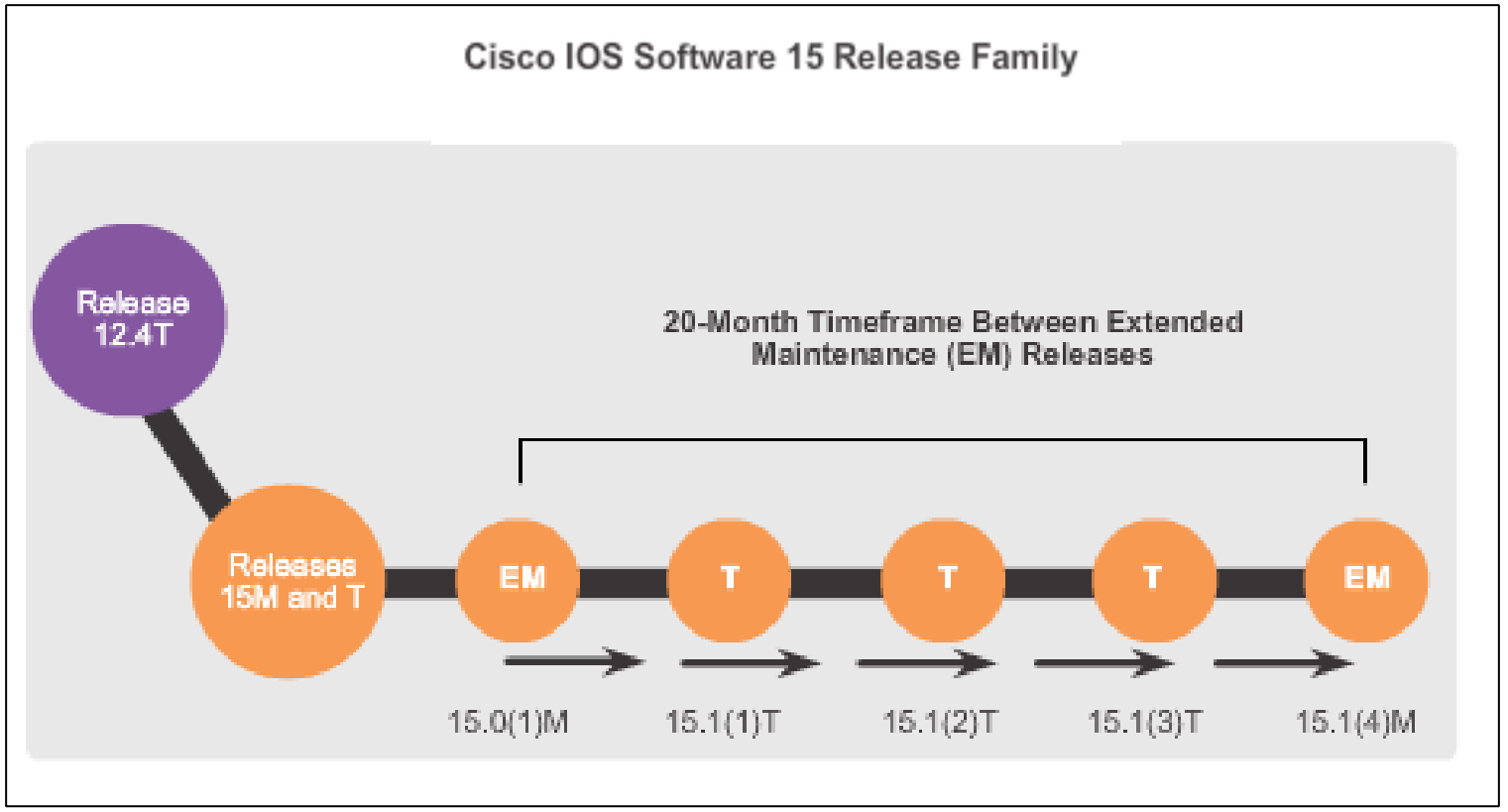
- Branch – Highly available 24/7.
- Network Edge – High performance, high security, and reliable services. Connect campus, data center, and branch networks.
- Service provider routers

Router Hardware

- Fixed configuration – Built-in interfaces.
- Modular – Slots allow different interfaces to be added.

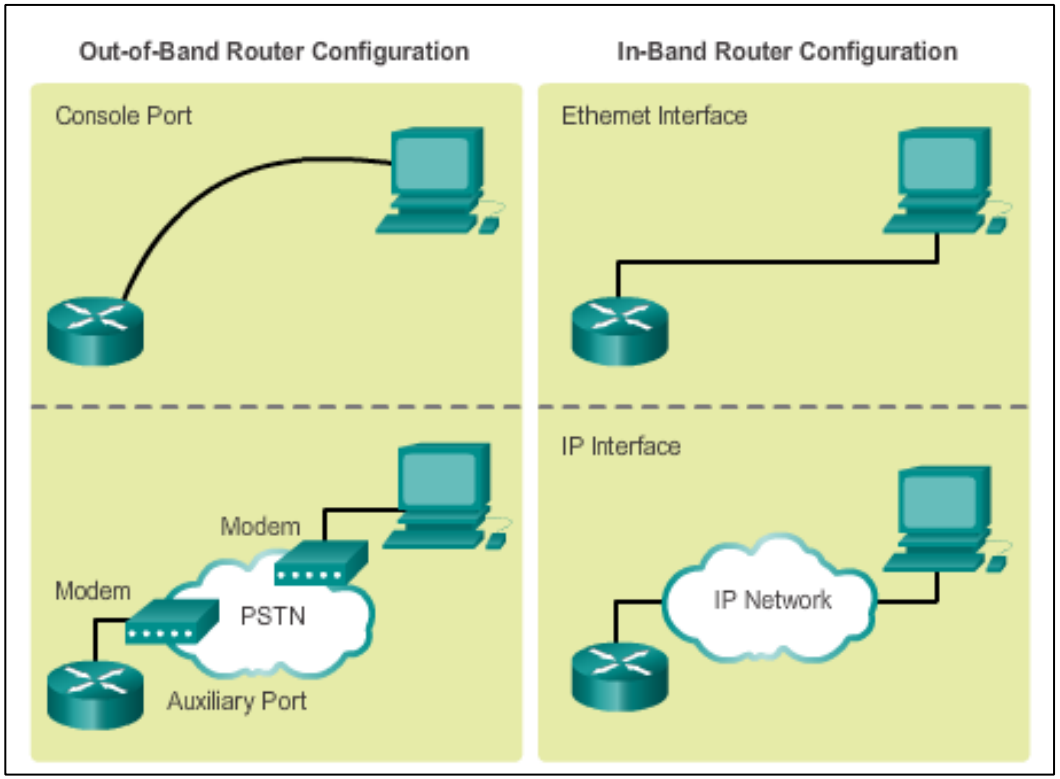


Managing IOS Files and Licensing



In-Band vs. Out-of-Band Management

- **In-Band** requires, at least, one interface to be connected and operational and use of Telnet, SSH, or HTTP to access device.
- **Out-of-Band** requires direct connection to console or AUX port and Terminal Emulation client to access device.



Basic Router CLI commands

Basic router configuration includes:

- Hostname
- Passwords (console, Telnet/SSH, and privileged mode)
- Interface IP addresses
- Enabling a routing protocol

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exec-timeout 0 0
R1(config-line)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)# banner motd $ Authorized Access Only! $
R1(config)# interface GigabitEthernet0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 172.16.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface Serial0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ip address 172.16.3.1 255.255.255.252
R1(config-if)# clock rate 128000
R1(config-if)# no shut
R1(config-if)# interface Serial0/0/1
R1(config-if)# description Link to R3
```

Basic Router show Commands

- **`show ip protocols`** – Displays information about routing protocol configured.
- **`show ip route`** – Displays routing table information.
- **`show ip ospf neighbor`** – Displays information about OSPF neighbors.
- **`show ip interfaces`** – Displays detailed information about interfaces.
- **`show ip interface brief`** – Displays all interfaces with IP addressing , interface, and line protocol status.
- **`show cdp neighbors`** – Displays information about all directly connected Cisco devices.

Basic Switch CLI Commands

- Hostname
- Passwords
- In-Band access requires the Switch to have an IP address (assigned to VLAN 1).
- Save configuration – **copy running-config startup-config** command.
- To clear switch – **erase startup-config**, and then **reload**.
- To erase VLAN information – **delete flash:vlan.dat**.

```
Switch# enable
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname S1
S1(config)# banner motd %Unauthorized access prohibited%
S1(config)# enable password cisco
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)# interface vlan 1
S1(config-if)# ip address 192.168.1.5 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)# 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)# interface fa0/3
S1(config-if)# speed 10
S1(config-if)# duplex half
S1(config)# end
```

Basic Switch Show Commands

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

1.3 Summary

Scaling Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 1: Summary

This chapter:

- Introduces the hierarchical network design model that divides network functionality into the access layer, the distribution layer, and the core layer.
- Describes how the Cisco Enterprise Architecture further divides the network into functional components called *modules*.
- Defines how routers and multilayer switches are used to limit failure domains.
- Explains that a good network design includes a scalable IP scheme, fast converging and scalable routing protocols, appropriate Layer 2 protocols and devices that are modular or easily upgraded.

Chapter 1: Summary (cont.)

- Identifies that a mission-critical server should have a connection to two different access layer switches. It should also have redundant modules and backup power.
- Recognizes that routers and switches should be selected from the appropriate categories to meet the network's requirements.