Computer Network Topologies

CST 05202: BASICS OF DATA COMMUNICATION NETWORKS

With Ms. Jamila L. Mshana

Contents

Computer Network

A **computer network** is a collection of computers other nodes (devices)connected together via communications transmission media for the purpose of sharing information and resources.

***A network node can be defined as the connection point among network devices.

Example of network nodes are routers, printers, hub, switches, bridge, repeater and etc that can receive and send data from one endpoint to the other.

Network Topology

A **network topology** refers to the layout of the computers and devices in a communication network.

Simply; Network topology is the logical or physical arrangement of the elements of a communication network.

Three commonly used network topologies are bus, ring, and star. Networks usually use combinations of these topologies.

Topology can be physical or logical

Physical Topology:

Is the physical layout of nodes, workstations and cables in the network.

Logical topology :

Is the way information flows between different components.

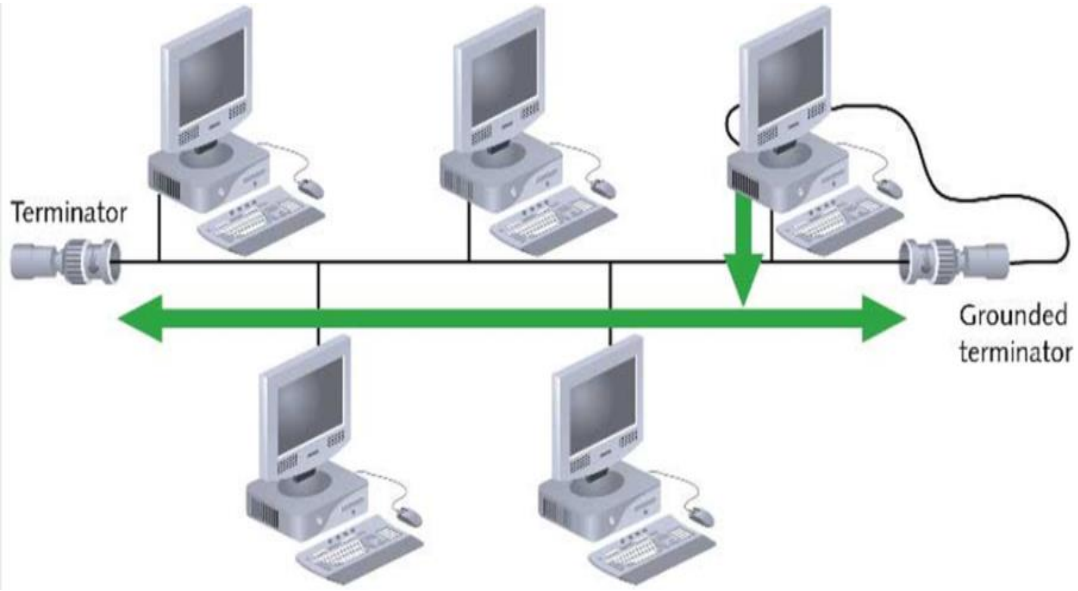
Types of Physical Network Topologies

i. Bus Topology
ii. Star Topology
iii. Ring Topology
iv. Mesh Topology
v. Hybrid Topology i.e. Tree topology

Bus Topology

A **Bus topology** consists of a single cable— called a **backbone**— connecting all nodes on a network without intervening connectivity devices

- Devices share responsibility for getting data from one point to another
- Terminators stop signals after reaching end of wire Prevent signal bounce
- Its Inexpensive, not very scalable
- Difficult to troubleshoot, not fault-tolerant



Bus Topology

Advantages:

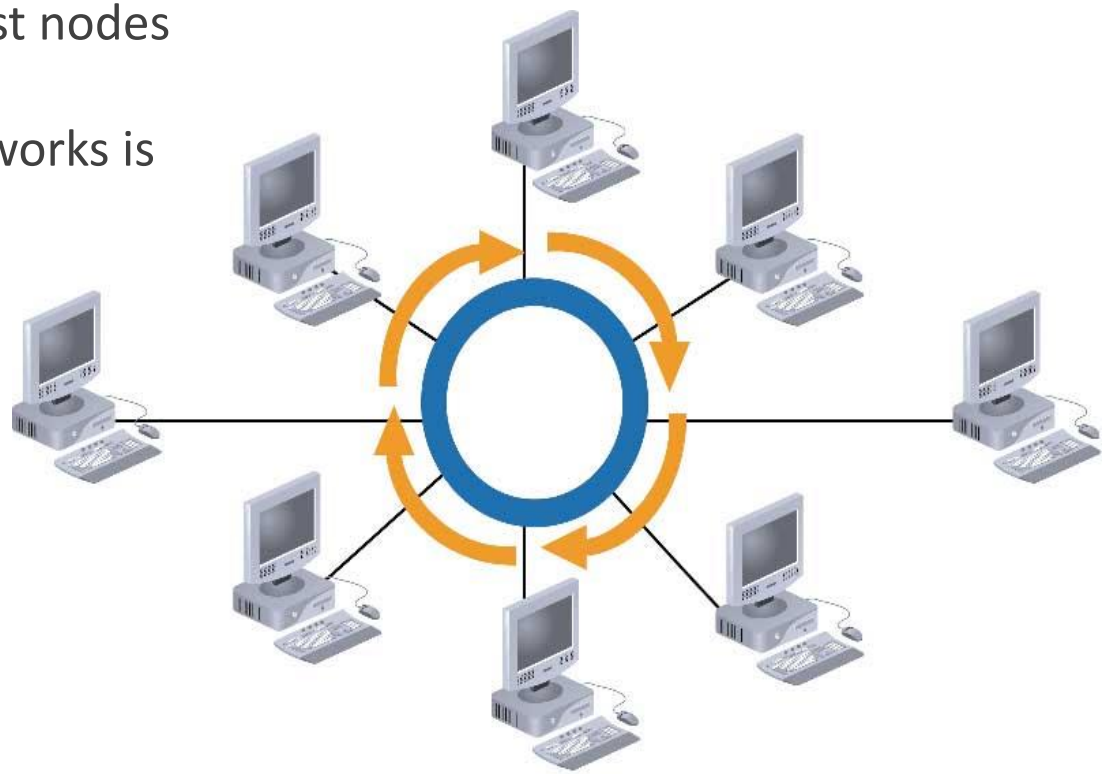
- Works well for small networks
- Easy to install
- Relatively inexpensive to implement

Disadvantages:

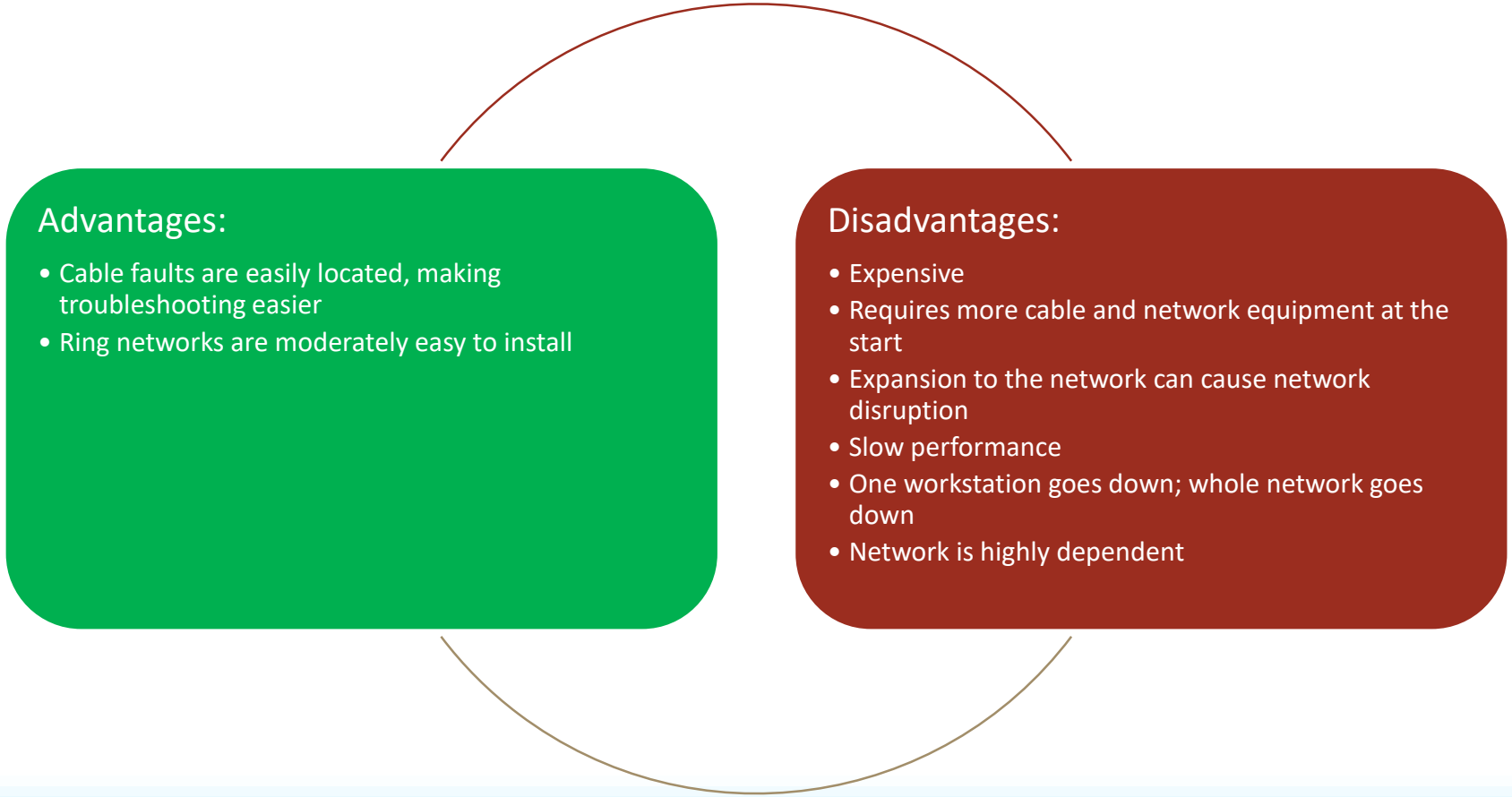
- Management costs can be high
- Network disruption when computers are added or removed
- A break in the cable will prevent all systems from accessing the network.
- Difficult to troubleshoot and not fault-tolerant

Ring Topology

- Ring topology
  - Each node is connected to the two nearest nodes so the entire network forms a circle
  - One method for passing data on ring networks is **token passing**
  - Data travels around the network
  - Traffic flows in one direction.



Ring Topology



Star Topology

Every node on the network is connected through a central device called **hub or switch**.

Any single cable connects only two devices

- Cabling problems affect two nodes at most

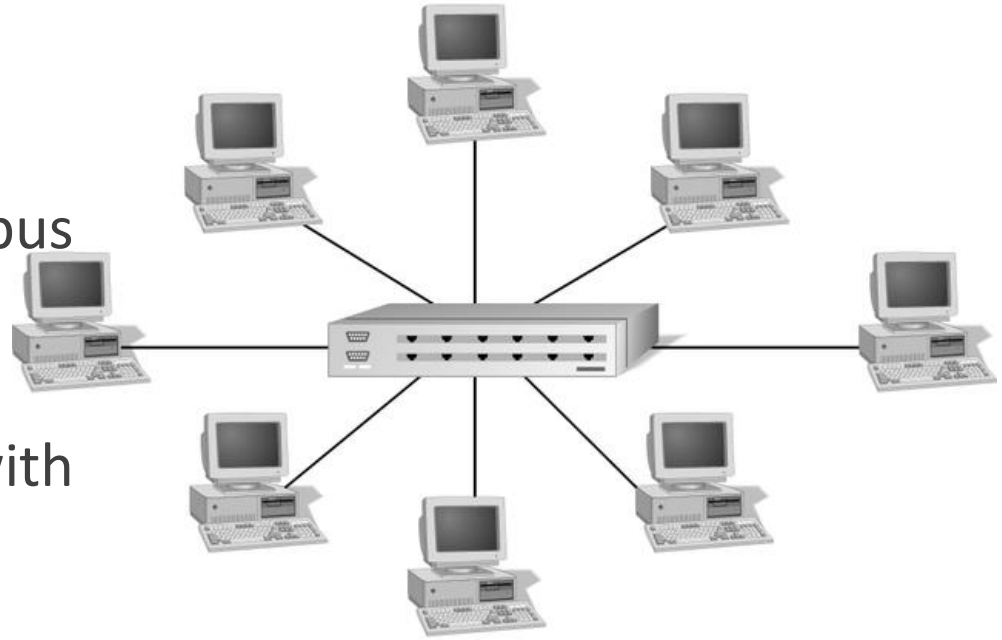
Requires more cabling than ring or bus networks

- More fault-tolerant

Easily moved, isolated, or interconnected with other networks

- Scalable

Supports max of 1024 addressable nodes on logical network



Star Topology

Advantages:

- Good option for modern networks
- Low startup costs
- Easy to manage
- Offers opportunities for expansion
- Most popular topology in use; wide variety of equipment available

Disadvantages:

- Hub or switch is a single point of failure
- Requires more cable than the bus

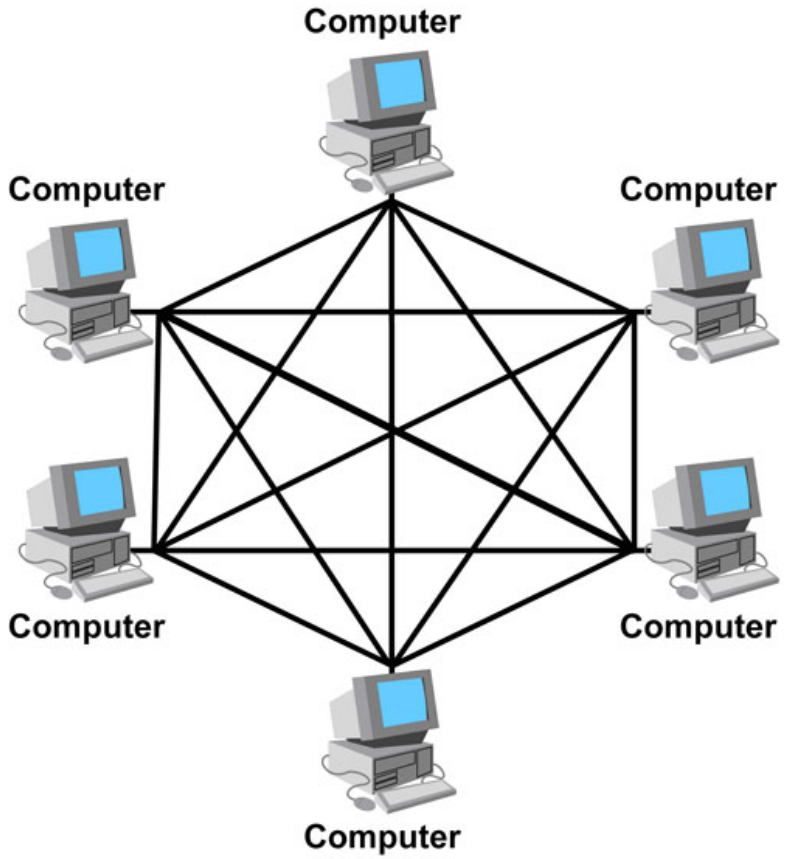
Mesh Topology

Each computer connects to every other.

High level of redundancy.

Rarely used.

- Wiring is very complicated
- Cabling cost is high
- Troubleshooting a failed cable is tricky
- A variation hybrid mesh – create point to point connection between specific network devices, often seen in WAN implementation.



Mesh Topology

Advantages:

- Robust and reliable
- There is the advantage of privacy or security
- The network can be expanded without disruption to current uses
- Point to point links make fault identification and fault isolation easy

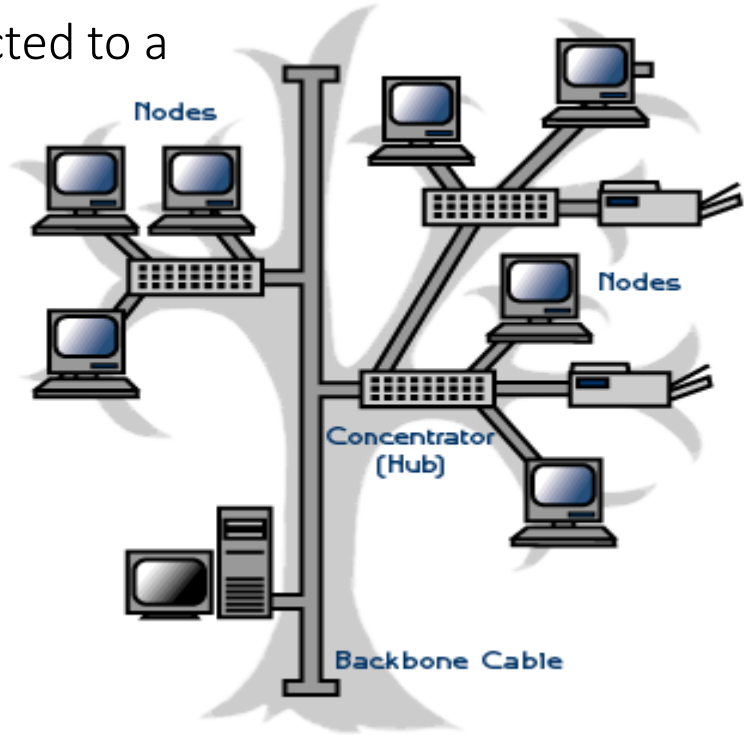
Disadvantages:

- Requires more cable than the other LAN topologies
- Complicated implementation
  - Installation and reconnection are difficult.
  - Sheer bulk of wiring can be greater than the available space can accommodate
  - Expensive

Mesh Topology

One example of Hybrid Topology is **Tree topology**

- **Tree topology** is a combination of Bus and Star topology.
- It consists of groups of star-configured workstations connected to a linear bus backbone cable.
- If the backbone line breaks, the entire segment goes down
- An example of this network could be cable TV



Why we need a topology

Choosing one topology over another can impact :

- type of equipment the network needs
- capabilities of the equipment
- network's growth
- way a network is managed

Choosing a Topology

- **BUS**
  - network is small
  - network will not be frequently reconfigured
  - least expensive solution is required
  - network is not expected to grow much
- **STAR**
  - it must be easy to add/remove PCs
  - it must be easy to troubleshoot
  - network is large
  - network is expected to grow in the future
- **RING**
  - network must operate reasonably under heavy load
  - higher speed network is required
  - network will not be frequently reconfigured

Network Topology Software

Topology software uses various methodologies and integrations to locate connected devices. It helps IT administrators identify network inefficiencies and bottlenecks and conduct root cause analyses of network problems. The following are some of the types of software for creating topology:

1. **SolarWinds** Network Topology Mapper
2. **Intermapper**
3. **Lucidchart**
4. **Net-Probe**
5. **Spiceworks** Network Mapping Tool

Hierarchical Network Design

Structured Engineering Principles

Regardless of network size or requirements, a critical factor for the successful implementation of any network design is to follow good structured engineering principles.

These principles include:

- Hierarchy: A hierarchical network model is a useful high-level tool for designing a reliable network infrastructure. It breaks the complex problem of network design into smaller and more manageable areas.

- Modularity: By separating the various functions that exist on a network into modules, the network is easier to design. Cisco has identified several modules, including the enterprise campus, services block, data center, and Internet edge.

- Resiliency: The network must remain available for use under both normal and abnormal conditions. Normal conditions include normal or expected traffic flows and traffic patterns, as well as scheduled events such as maintenance windows. Abnormal conditions include hardware or software failures, extreme traffic loads, unusual traffic patterns, denial-of-service (DoS) events, whether intentional or unintentional, and other unplanned events.

- Flexibility: The ability to modify portions of the network, add new services, or increase capacity without going through a major forklift upgrade (i.e., replacing major hardware devices).

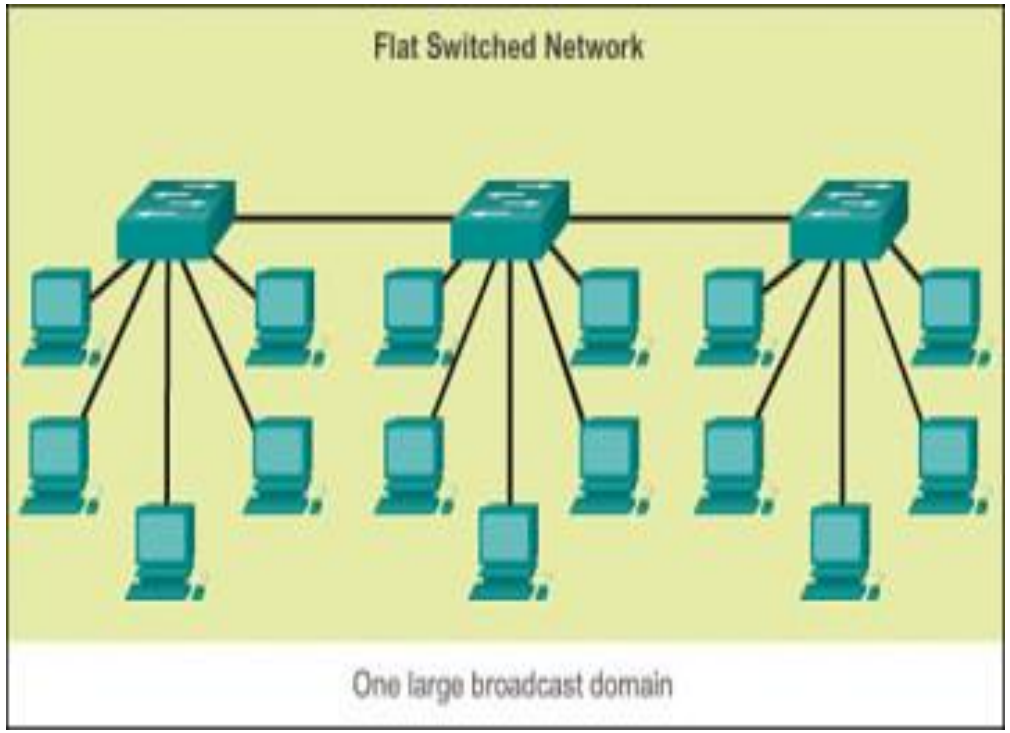
Introduction

Initially, networks had a **flat design** and could only be expanded in one direction through hubs and switches, making it challenging to filter out undesirable traffic and control broadcasts.

As a network grew in size, response times would degrade.

A new network design was necessary, resulting in the hierarchical approach.

Flat network design is still in use today, but is primarily reserved for very small networks, or designs looking to minimize cost by using a limited number of routers or switches.

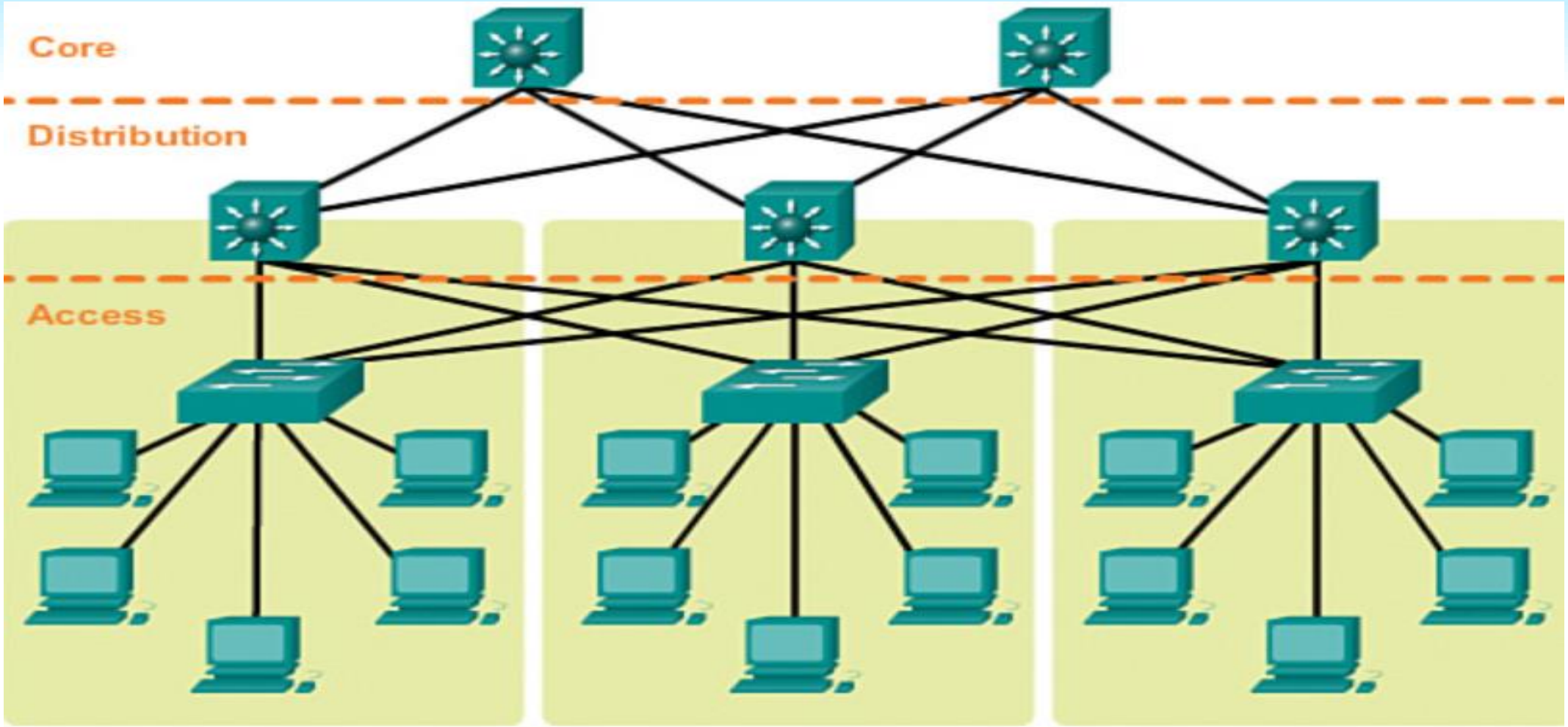


Hierarchical network design

The Cisco hierarchical (three-layer) internetworking model (hierarchical network design) has become an industry-wide best practice for developing reliable, scalable, and cost-effective network.

- A hierarchical network design involves dividing the network into discrete layers.
- Each layer, or tier, in the hierarchy provides specific functions that define its role within the overall network.
- This helps the network designer and architect to optimize and select the right network hardware, software, and features to perform specific roles for that network layer.
- Hierarchical models apply to both LAN and WAN design.
- The benefit of dividing a flat network into smaller, more manageable blocks is that local traffic remains local. Only traffic that is destined for other networks is moved to a higher layer.

Hierarchical network design



Three separate broadcast domains

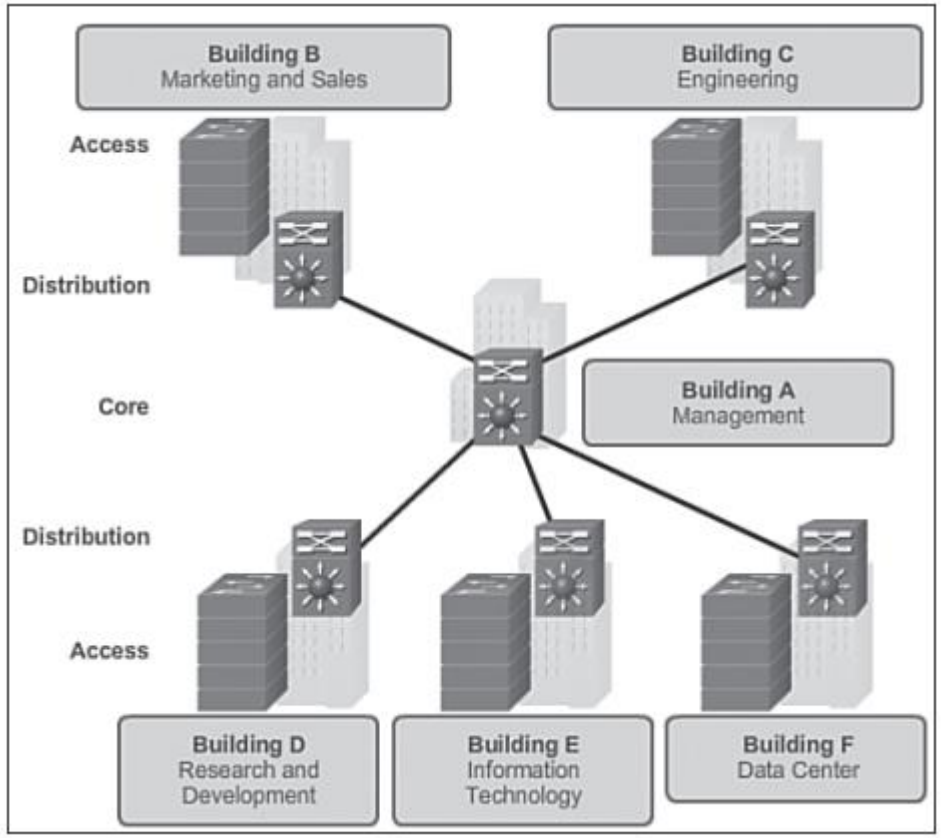
Hierarchical network design layers

A typical enterprise hierarchical LAN campus network design includes the following three layers:

Access layer: Provides workgroup/user access to the network

Distribution layer: Provides policy-based connectivity and controls the boundary between the access and core layers.

Core layer: Provides fast transport between distribution switches within the enterprise campus



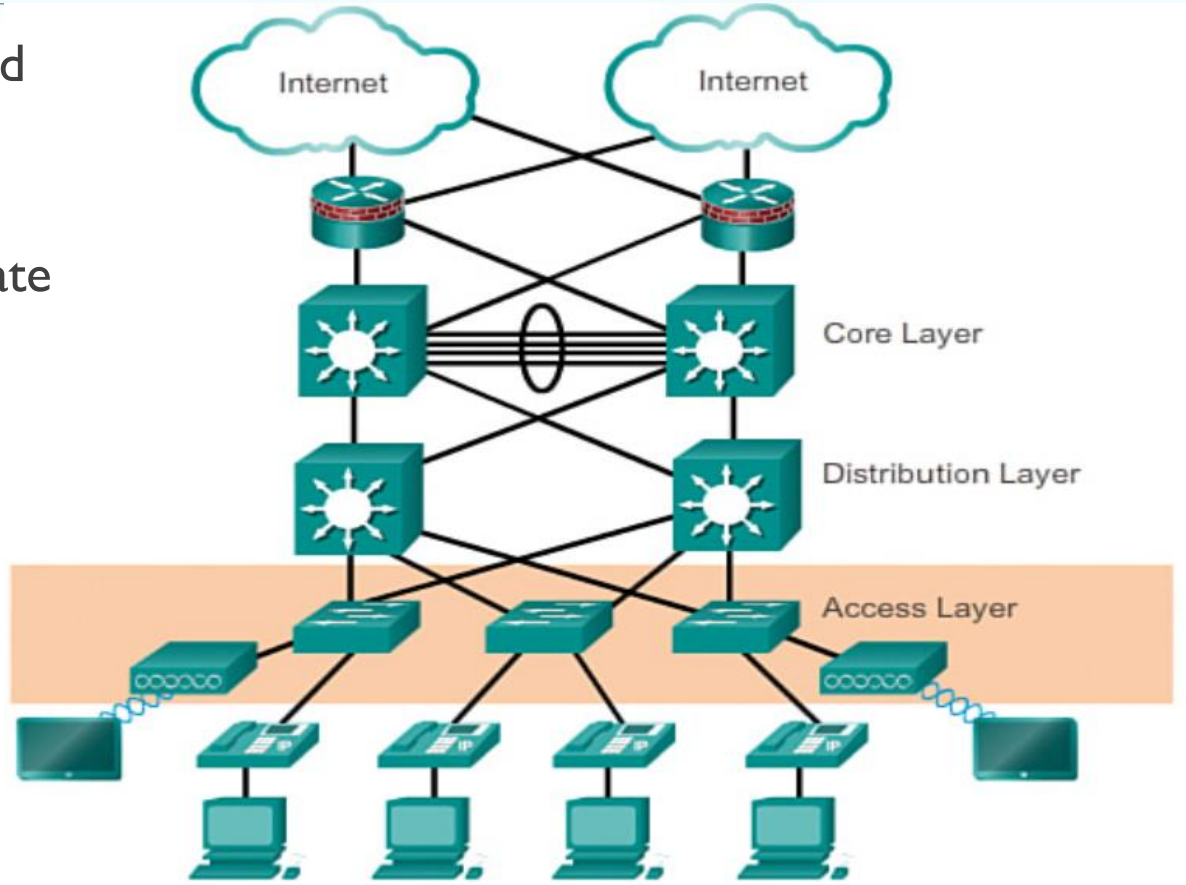
Multi Building Enterprise Network Design

The Access Layer

In a LAN environment, the ***access layer*** highlighted grants end devices access to the network.

In the WAN environment, it may provide teleworkers or remote sites access to the corporate network across WAN connections.

As shown in Figure, the access layer for a small business network generally incorporates Layer 2 switches and access points providing connectivity between workstations and servers.



Services provided by access layer

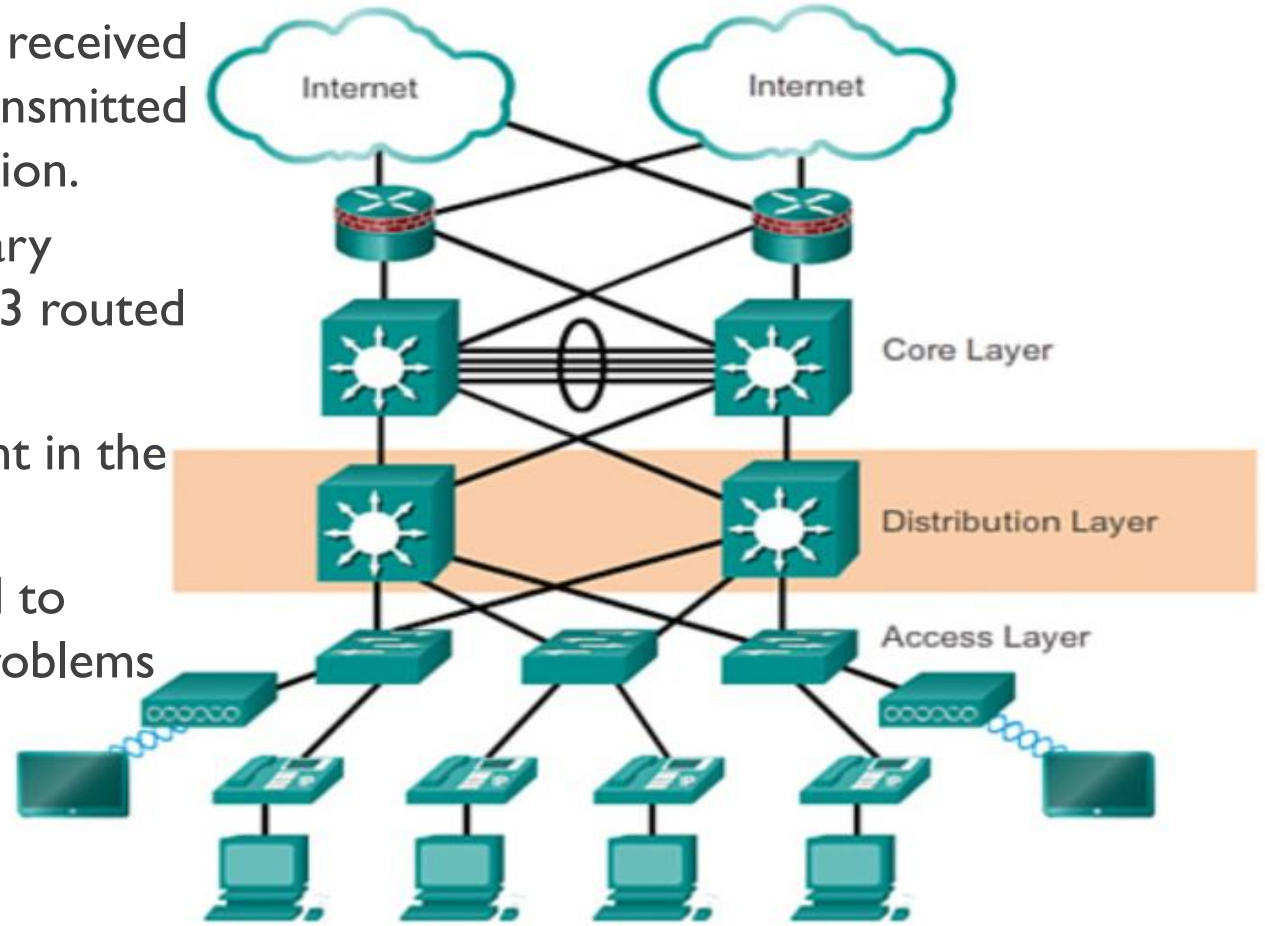
- Layer 2 switching
- High availability
- Port security
- QoS classification and marking and trust boundaries
- Address Resolution Protocol (ARP) inspection
- Virtual access control lists (VACLs)
- Power over Ethernet (PoE) and auxiliary VLANs for VoIP

***The access layer feeds into the distribution layer via **OSI Layer 2** trunk ports, or Layer 3 routed ports. End-user devices connect to switches in the access layer at Layer 2

The Distribution Layer

The ***distribution layer*** aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination.

- In Figure, the distribution layer is the boundary between the Layer 2 domains and the Layer 3 routed network.
- The distribution layer device is the focal point in the wiring closets.
- Either a router or a multilayer switch is used to segment workgroups and isolate network problems in a campus environment.



Services provided by distribution layer

- Aggregation of LAN or WAN links.
- Policy-based security in the form of access control lists (ACLs) and filtering.
- Routing services between LANs and VLANs and between routing domains (e.g., EIGRP to OSPF).
- Redundancy and load balancing.
- A boundary for route aggregation and summarization configured on interfaces toward the core layer.
- Broadcast domain control, because routers or multilayer switches do not forward broadcasts.
- The device acts as the separation point between broadcast domain

The core layer

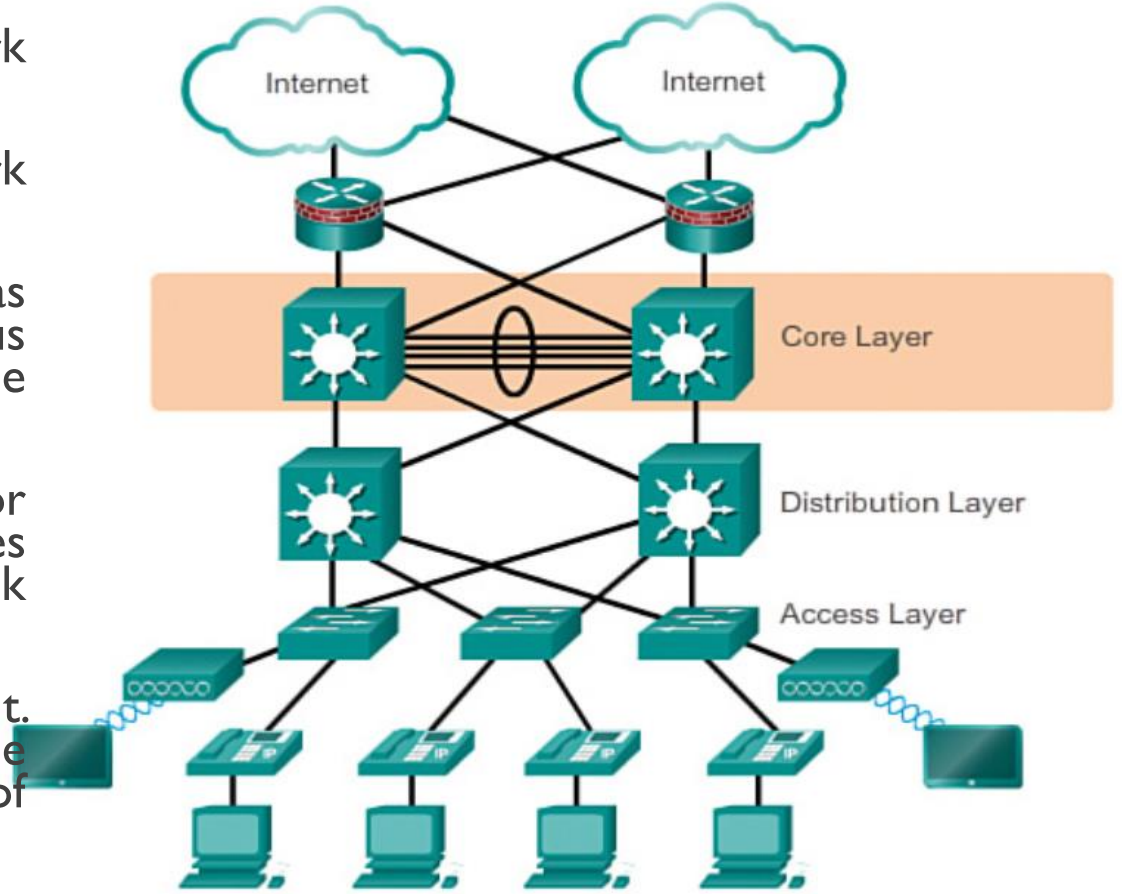
The ***core layer*** is also referred to as the network backbone.

The core layer consists of high-speed network devices such as the Cisco Catalyst 6500 or 6800.

These are designed to switch packets as fast as possible and interconnect multiple campus components, such as distribution modules, service modules, the data center, and the WAN edge.

As shown in Figure, the core layer is critical for interconnectivity between distribution layer devices (for example, interconnecting the distribution block to the WAN and Internet edge).

The core should be highly available and redundant. The core aggregates the traffic from all the distribution layer devices, so it must be capable of forwarding large amounts of data quickly.



Services provided by core layer

Considerations at the core layer include

- Providing high-speed switching (i.e., fast transport)
- Providing reliability and fault tolerance
- Scaling by using faster, and not more, equipment
- Avoiding CPU-intensive packet manipulation caused by security, inspection, quality of service (QoS) classification, or other processes

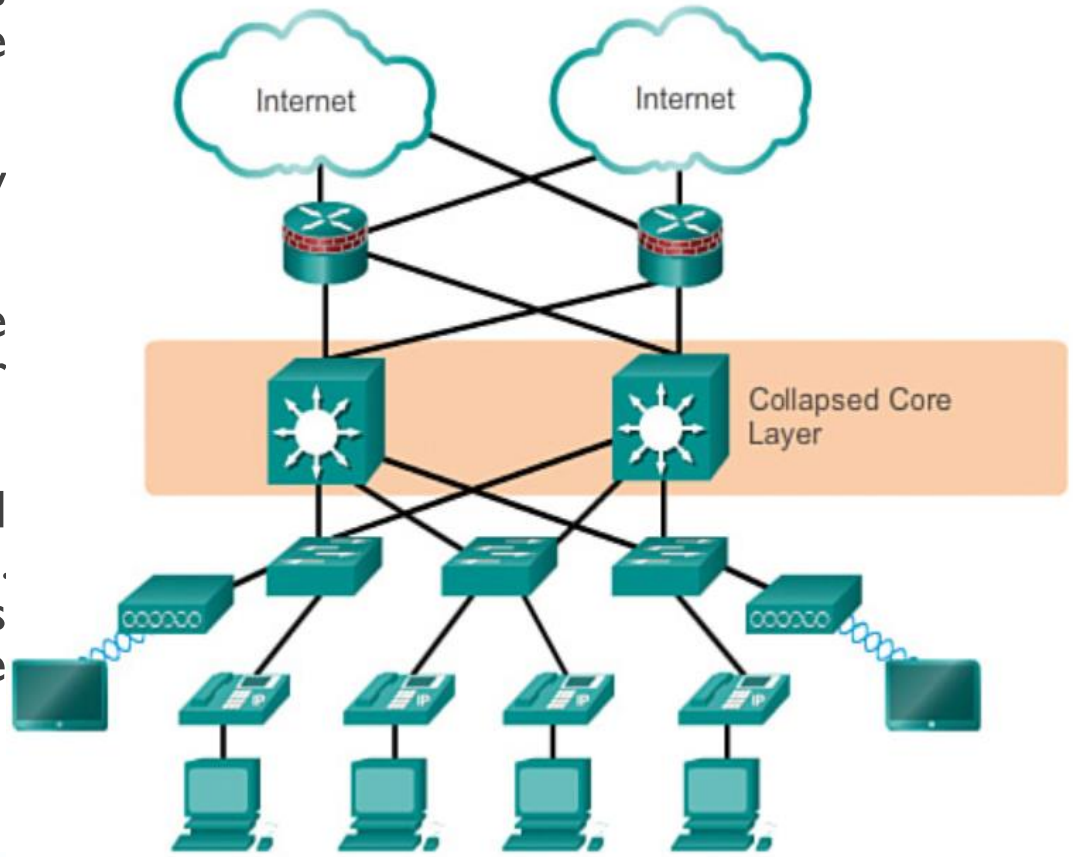
Two-Tier Collapsed Core Design

The ***three-tier hierarchical design*** maximizes performance, network availability, and the ability to scale the network design.

However, many small enterprise networks do not grow significantly larger over time.

Therefore, a ***two-tier hierarchical design*** where the core and distribution layers are collapsed into one layer is often more practical.

A "***collapsed core***" is when the distribution layer and core layer functions are implemented by a single device. The primary motivation for the collapsed core design is reducing network cost, while maintaining most of the benefits of the three-tier hierarchical model.



Benefits of hierarchical network design

Enhanced performance: A hierarchical network design means data is routed through aggregated switch port links at close to wire rate, instead of being sent through lower performance intermediary switches.

Improved reliability: The modular nature of a hierarchical network translates into a more reliable network as a whole, as segments that fail or become degraded can be isolated and routed around. The rest of the network won't be affected.

Increased scalability: Hierarchical networks are more flexible than their counterparts. Segments and elements can easily be added without significantly disrupting the existing network.

Better security: In terms of security, a hierarchical network permits a greater level of control. Access control lists can be more complex and granular, and traffic can be shaped and blocked more effectively.

Easer to manage: Since each network layer is designed for specific and consistent functionality, these networks are easier to manage.

PPDIOO: The network design methodology

PPDIOO Lifecycle Approach to Network Design and Implementation

PPDIOO stands for **Prepare, Plan, Design, Implement, Operate, and Optimize.** PPDIOO is a Cisco methodology that defines the continuous life-cycle of services required for a network.

The PPDIOO phases are as follows:

Prepare: Involves establishing the organizational requirements, developing a network strategy, and proposing a high-level conceptual architecture identifying technologies that can best support the architecture.

Plan: Involves identifying initial network requirements based on goals, facilities, user needs, and so on.

Design: The network design specification is a comprehensive detailed design that meets current business and technical requirements, and incorporates specifications to support availability, reliability, security, scalability, and performance.

PPDIOO: The network design methodology

Implement: The network is built or additional components are incorporated according to the design specifications, with the goal of integrating devices without disrupting the existing network or creating points of vulnerability.

Operate: Operation is the final test of the appropriateness of the design. It involves maintaining network health through day-to-day operations, including maintaining high availability and reducing expenses.

The fault detection, correction, and performance monitoring that occur in daily operations provide the initial data for the optimization phase.

Optimize: Involves proactive management of the network. The goal of proactive management is to identify and resolve issues before they affect the organization. Reactive fault detection and correction (troubleshooting) is needed when proactive management cannot predict and mitigate failures.

Thank you!

For listen