Chapter III

Designing Basic Campus and Data Center Networks

09 Hours

Campus Design Considerations:-

The multilayer approach to campus network design combines data link layer and multilayer switching to achieve robust, highly available campus networks. This section discusses factors to consider in a Campus LAN design.

The following three characteristics should be considered when designing the campus network:

1. *Network application characteristics*: The organizational requirements, services, and applications place stringent requirements on a campus network solution—for example, in terms of bandwidth and delay.

2. *Environmental characteristics*: The network's environment includes its geography and the transmission media used.

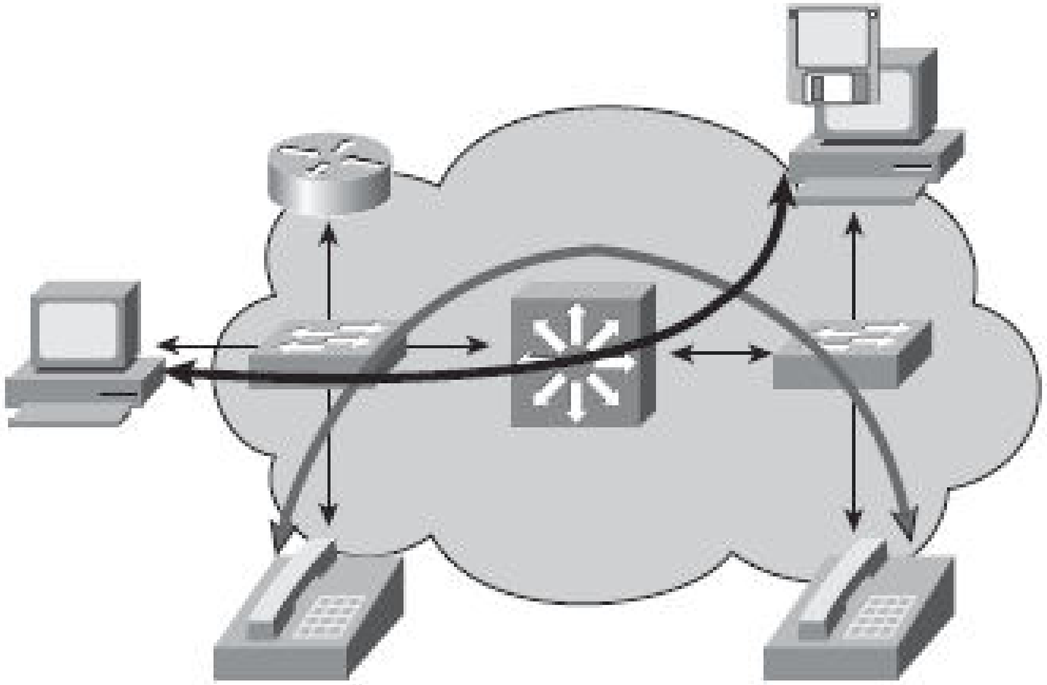
3. *Infrastructure device characteristics:* The characteristics of the network devices selected influence the design (for example, they determine the network's flexibility) and contribute to the overall delay.

Network Application Characteristics and Considerations

- The network application's characteristics and requirements influence the design in many ways.
- The applications that are critical to the organization, and the network demands of these applications, determine enterprise traffic patterns inside the Enterprise Campus network, which influences bandwidth usage, response times, and the selection of the transmission medium.
- Different types of application communication result in varying network demands. The following sections review four types of application communication:
- Peer-peer
- Client–local server
- Client–Server Farm
- Client–Enterprise Edge server

- Peer-Peer Applications

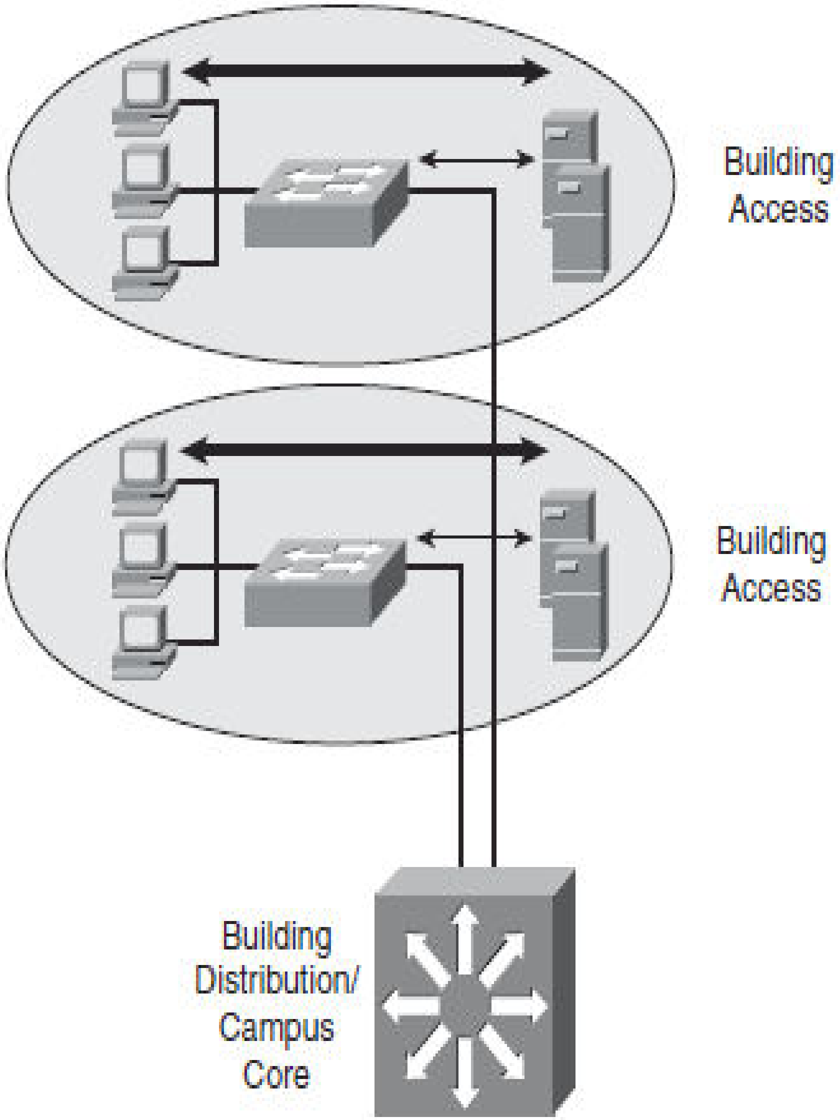
From the network designer’s perspective, peer-peer applications include applications in which the majority of network traffic passes from one network edge device to another through the organization’s network

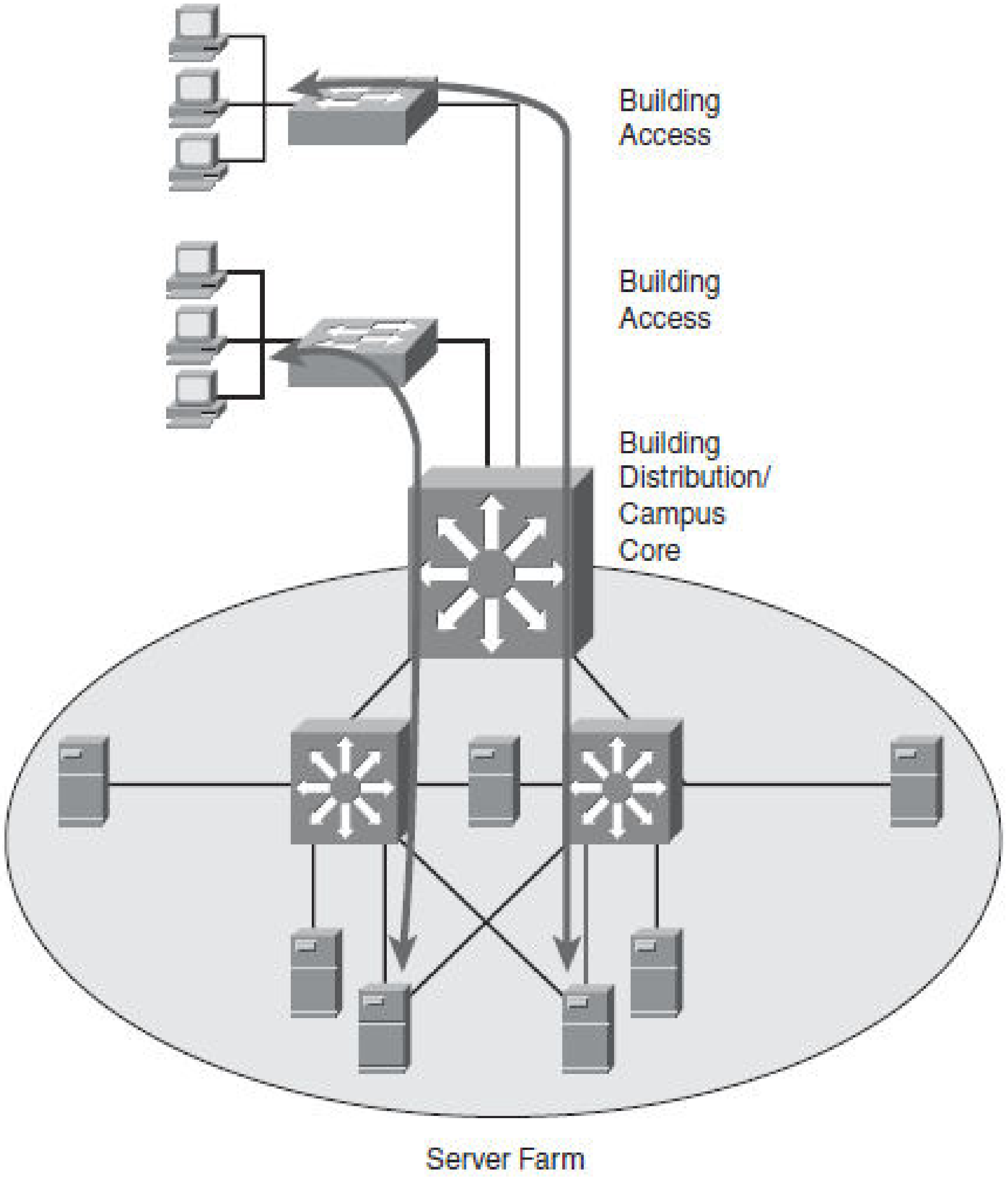


- Client–Local Server Applications

✓Historically, clients and servers were attached to a network device on the same LAN segment and followed the 80/20 workgroup rule for client/server applications. This rule indicates that 80 percent of the traffic is local to the LAN segment and 20 percent leaves the segment.

✓With increased traffic on the corporate network and a relatively fixed location for users, an organization might split the network into several isolated segments, as shown in Figure Each of these segments has its own servers, known as local servers, for its application.


Building Access
Building Access
Building Distribution/ Campus Core


Building Access
Building Access
Building Distribution/ Campus Core
Server Farm

- Client–Server Farm Applications

✓Large organizations require their users to have fast, reliable, and controlled access to critical applications.

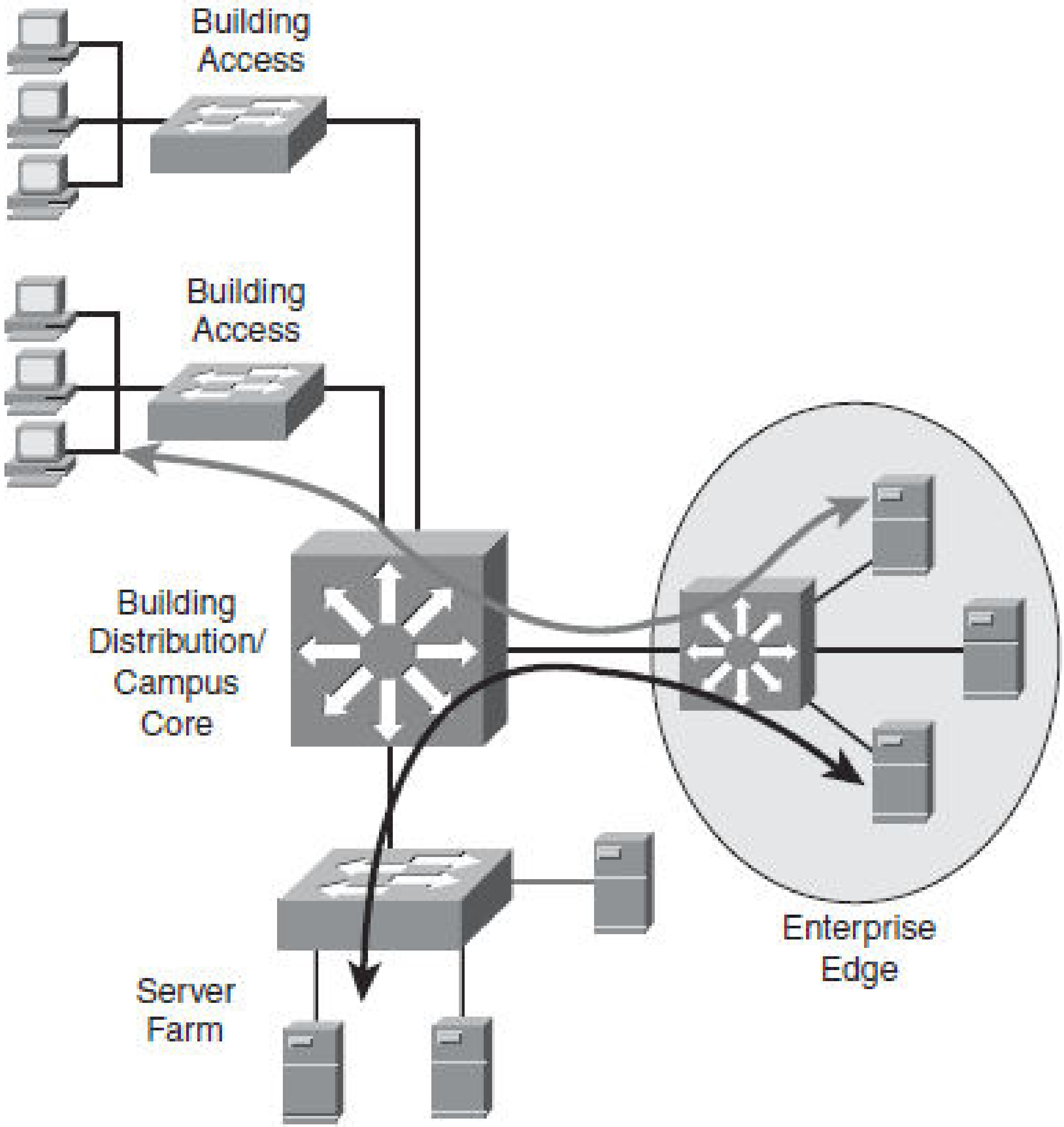
✓Because high-performance multilayer switches have an insignificant switch delay, and because of the reduced cost of network bandwidth, locating the servers centrally rather than in the workgroup is technically feasible and reduces support costs.

✓To fulfill these demands and keep administrative costs down, the servers are located in a common Server Farm, as shown in Figure.

- Client–Enterprise Edge Applications

✓As shown in Figure, client–Enterprise Edge applications use servers on the Enterprise Edge to exchange data between the organization and its public servers. The most important issues between the Enterprise Campus network and the Enterprise Edge are security and high availability; data exchange with external entities must be in constant operation.

✓Applications installed on the Enterprise Edge can be crucial to organizational process flow; therefore, any outages can increase costs.


Building
Access
Building
Access
Building
Distribution/
Campus
Core
Enterprise
Edge
Server
Farm

Environmental Characteristics and Considerations

- The campus environment, including the location of the network nodes, the distance between the nodes, and the transmission media used, influences the network topology.
- Network Geography Considerations :- The location of Enterprise Campus nodes and the distances between them determine the network’s geography.
- Nodes, including end-user workstations and servers, can be located in one or multiple buildings.
- Based on the location of nodes and the distance between them, the network designer decideswhich technology should interconnect them based on the required maximum speed, distance, and so forth.

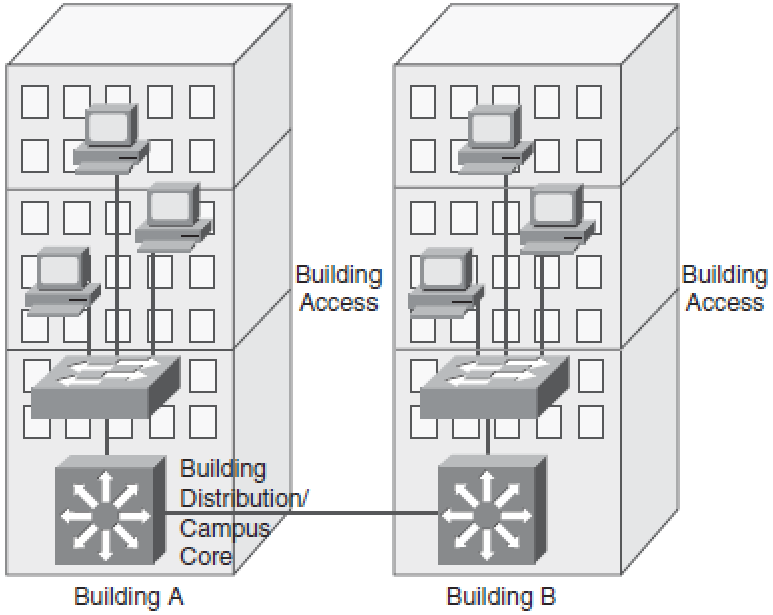
- Consider the following structures with respect to the network geography:
- Intrabuilding
- Interbuilding
- Distant remote building

Intrabuilding Structure

An intrabuilding campus network structure provides connectivity for all end nodes located in the same building and gives them access to the network resources. The Building Access and Building Distribution layers are typically located in the same building.

Interbuilding Structure

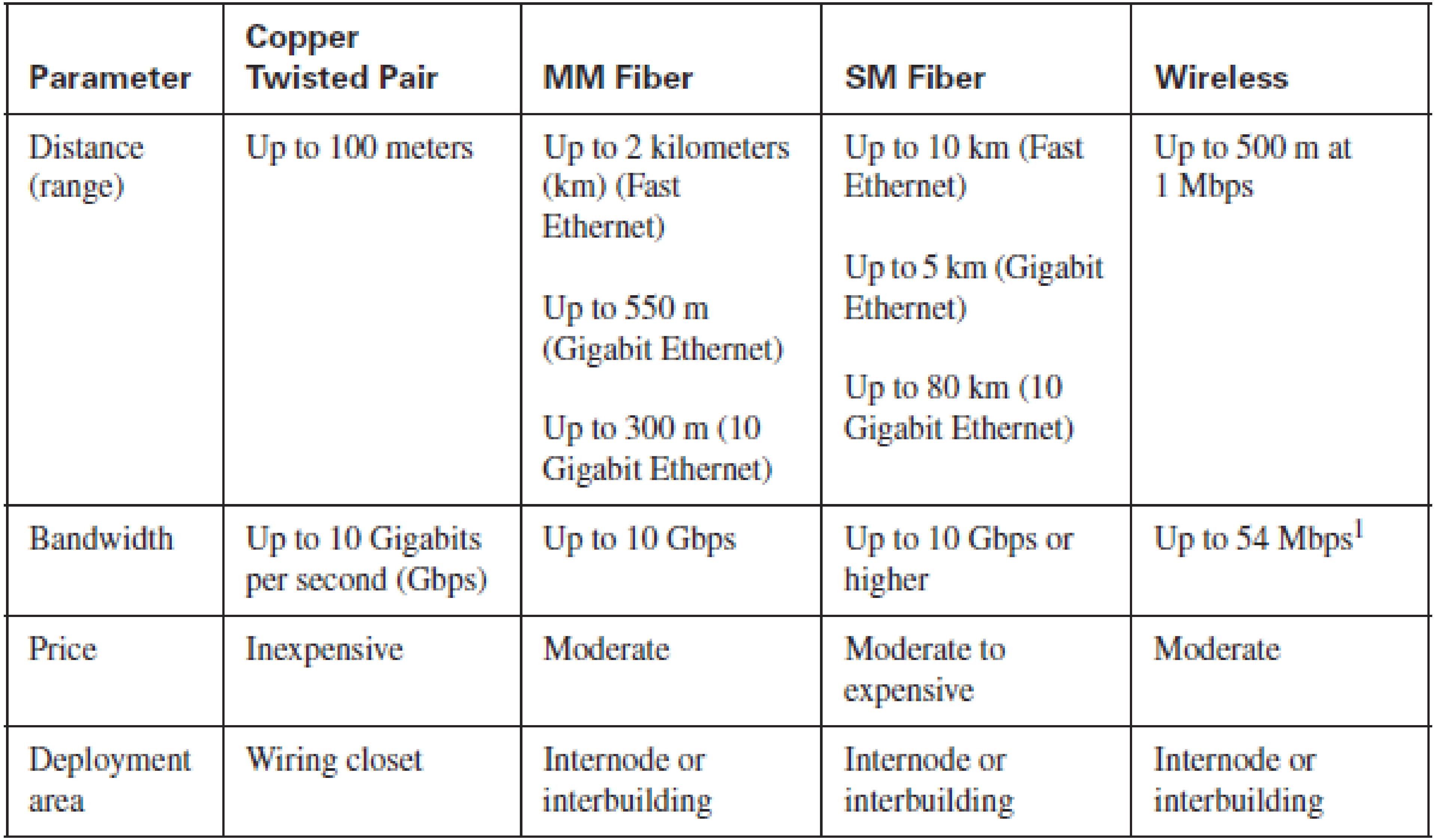
- As shown in Figure , an interbuilding network structure provides connectivity between the individual campus buildings’ central switches (in the Building Distribution and/or Campus Core layers).
- These buildings are usually in close proximity, typically only a few hundred meters to a few kilometers apart.



Distant Remote Building Structure

- When connecting buildings at distances that exceed a few kilometers (but still within a metropolitan area), the most important factor to consider is the physical media.
- The speed and cost of the network infrastructure depend heavily on the media selection.
- If the bandwidth requirements are higher than the physical connectivity options can support, the network designer must identify the organization’s critical applications and then select the equipment that supports intelligent network services—such as QoS and filtering capabilities—that allow optimal use of the bandwidth.

Transmission Media Characteristics



Parameter	Copper Twisted Pair	MM Fiber	SM Fiber	Wireless
Distance (range)	Up to 100 meters	Up to 2 kilometers (km) (Fast Ethernet) Up to 550 m (Gigabit Ethernet) Up to 300 m (10 Gigabit Ethernet)	Up to 10 km (Fast Ethernet) Up to 5 km (Gigabit Ethernet) Up to 80 km (10 Gigabit Ethernet)	Up to 500 m at 1 Mbps
Bandwidth	Up to 10 Gigabits per second (Gbps)	Up to 10 Gbps	Up to 10 Gbps or higher	Up to 54 Mbps[1]
Price	Inexpensive	Moderate	Moderate to expensive	Moderate
Deployment area	Wiring closet	Internode or interbuilding	Internode or interbuilding	Internode or interbuilding

- *Distance*: The maximum distance between network devices (such as workstations, servers, printers, and IP phones) and network nodes, and between network nodes. The distances supported with fiber vary, depending on whether it supports Fast Ethernet or Gigabit Ethernet, the type of fiber used, and the fiber interface used.
- *Bandwidth*: The required bandwidth in a particular segment of the network, or the connection speed between the nodes inside or outside the building.
- *Price*: Along with the price of the medium, the installation cost must be considered. For example, fiber installation costs are significantly higher than copper installation costs because of strict requirements for optical cable coupling.
- *Deployment area*: Indicates whether wiring is for wiring closet only (where users access the network), for internode, or for interbuilding connections.

Infrastructure Device Characteristics and Considerations:-

- ✓Network end-user devices are commonly connected using switched technology rather than using a shared media segment.
- ✓Switched technology provides dedicated network bandwidth for each device on the network. Switched networks can support network infrastructure services, such as QoS, security, and management; a shared media segment cannot support these features.

(The mechanism for exchange of information between different computer networks and network segments is called switching in Networking.)

- ✓A network switch is a hardware device that channels incoming data from multiple input ports to a specific output port that will take it toward its intended destination. It is a small device that transfers data packets between multiple network devices such as computers, routers, servers or other switches.

- The difference between data link layer and multilayer switching is the type of information used inside the frame to determine the correct output interface.
- Data link layer switching forwards frames based on data link layer information (the MAC address), whereas multilayer switching forwards frames based on network layer information (such as IP address).

When deciding on the type of switch to use and the features to be deployed in a network, consider the following factors:

- *Infrastructure service capabilities*: The network services that the organization requires (IP multicast, QoS, and so on).
- *Size of the network segments*: How the network is segmented and how many end devices will be connected, based on traffic characteristics.
- *Convergence time*: The maximum amount of time the network will be unavailable in the event of network outages.
- *Cost*: The budget for the network infrastructure.

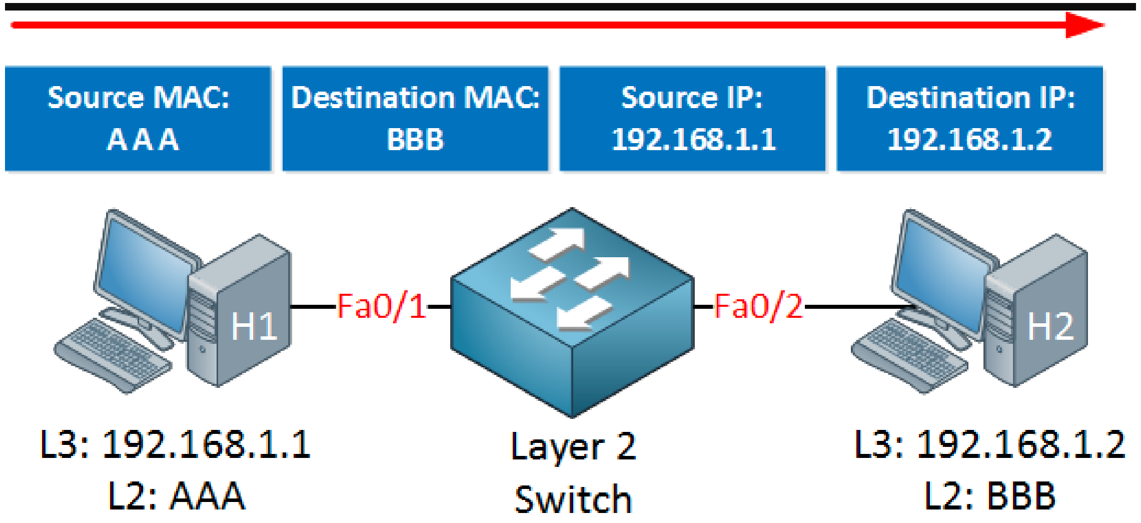
Multilayer Switching and Cisco Express Forwarding:-

- ✓Forwarding on layer 2 is based on the destination MAC address. Our switch learns the source MAC addresses on incoming frames and it builds the MAC address table. Whenever an Ethernet frame enters one of our interfaces, we’ll check the MAC address table to find the destination MAC address and we’ll send it out the correct interface.
- ✓Forwarding on layer 3 is based on the destination IP address.

- Forwarding happens when the switch receives an IP packet where the source IP address is in a different subnet than the destination IP address.
- When our multilayer switch receives an IP packet with its own MAC address as the destination in the Ethernet header there are two possibilities:

✓If the destination IP address is an address that is configured on the multilayer switch then the IP packet was destined for this switch.

✓If the destination IP address is an address that is not configured on the multilayer switch then we have to act as a gateway and “route” the packet. This means we’ll have to do a lookup in the routing table to check for the longest match.



Source MAC: AAA

Destination MAC: BBB

Source IP: 192.168.1.1

Destination IP: 192.168.1.2

L3: 192.168.1.1
L2: AAA

Layer 2
Switch

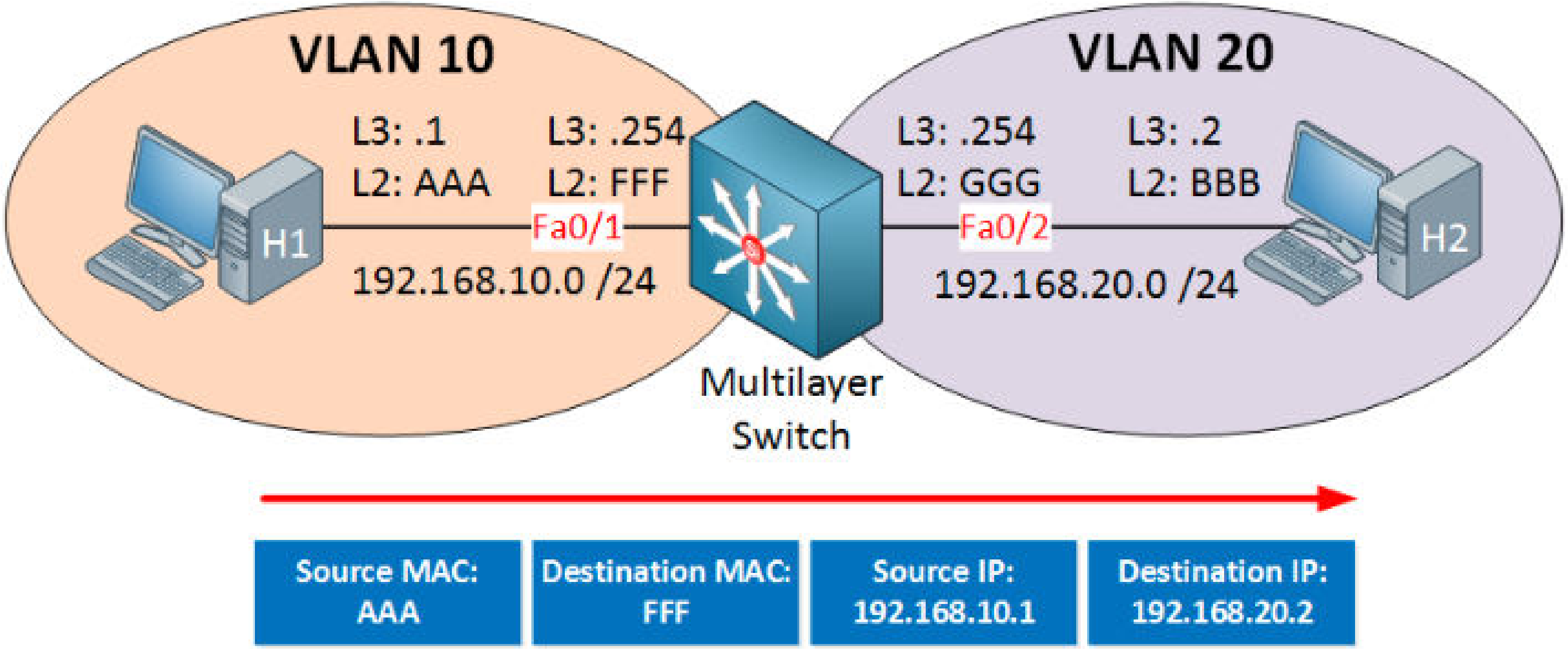
L3: 192.168.1.2
L2: BBB

MAC Address Table:

Fa0/1	AAA
Fa0/2	BBB

The life of a layer 2 switch is simple:

1. The switch will verify the checksum of the Ethernet frame to make it sure it’s not corrupted or altered.
2. The switch receives an Ethernet frame and adds the source MAC address to the MAC address table.
3. The switch forwards the Ethernet frame to the correct interface if it knows the destination MAC address. If not, it will be flooded.



Source MAC:	Destination MAC:	Source IP:	Destination IP:
AAA	FFF	192.168.10.1	192.168.20.2

In the example above H1 is sending an IP packet towards H2. Note that they are in different subnets so we will have to route it. When our multilayer switch receives the IP packet this is what will happen:

The switch will verify the checksum of the Ethernet frame to make it sure it’s not corrupted or altered.
The switch will verify the checksum of the IP packet to make it sure it’s not corrupted or altered.

- The multilayer switch will check the routing table, notices that 192.168.20 /24 is directly connected and the following will happen:

1. Check the ARP table to see if there's a layer 2 to 3 mapping for H2. If there is no mapping the multilayer switch will send an ARP request.

2. The destination MAC address changes from FFF (Multilayer switch Fa0/1) to BBB (H2).

3. The source MAC address changes from AAA (H1) to GGG (Multilayer switch Fa0/2).

4. The TTL (time to live) field in the IP packet is decreased by 1 and because of this the IP header checksum will be recalculated.

5. The Ethernet frame checksum must be recalculated.

6. The Ethernet frame carrying the IP packet will be sent out of the interface towards H2.

✓Cisco Express Forwarding (CEF) is a packet-switching technique used within Cisco routers. The main purpose of CEF is to optimize the forwarding of packets and increase the packet switching speed.

✓Prior to CEF there were 2 methods for packet-switching - Process- Switching and Fast-Switching.

✓PROCESS-SWITCHING

The first method, process-switching is the oldest and slowest. In short the CPU is involved in every forwarding decision.

✓FAST-SWITCHING

With fast-switching, the CPU is still used to determine the destination, but only for the initial packet. This information is stored with a fast-switching cache. Subsequent packets are then switched using the cache rather then CPU.

- CEF is built around 2 main components - the Forwarding Information Base (FIB) and the Adjacency Table.

FIB

- The FIB is an optimized version of the routing table (RIB).
- The FIB contains destination reachability information as well as next hop information. This information is then used by the router to make forwarding decisions.

ADJACENCY TABLE

- The adjacency table maintains layer 2 or switching information linked to a particular FIB entry, avoiding the need for an ARP request for each table lookup

Enterprise Campus Design

Campus Infrastructure—This module includes three layers:

— The Building Access layer

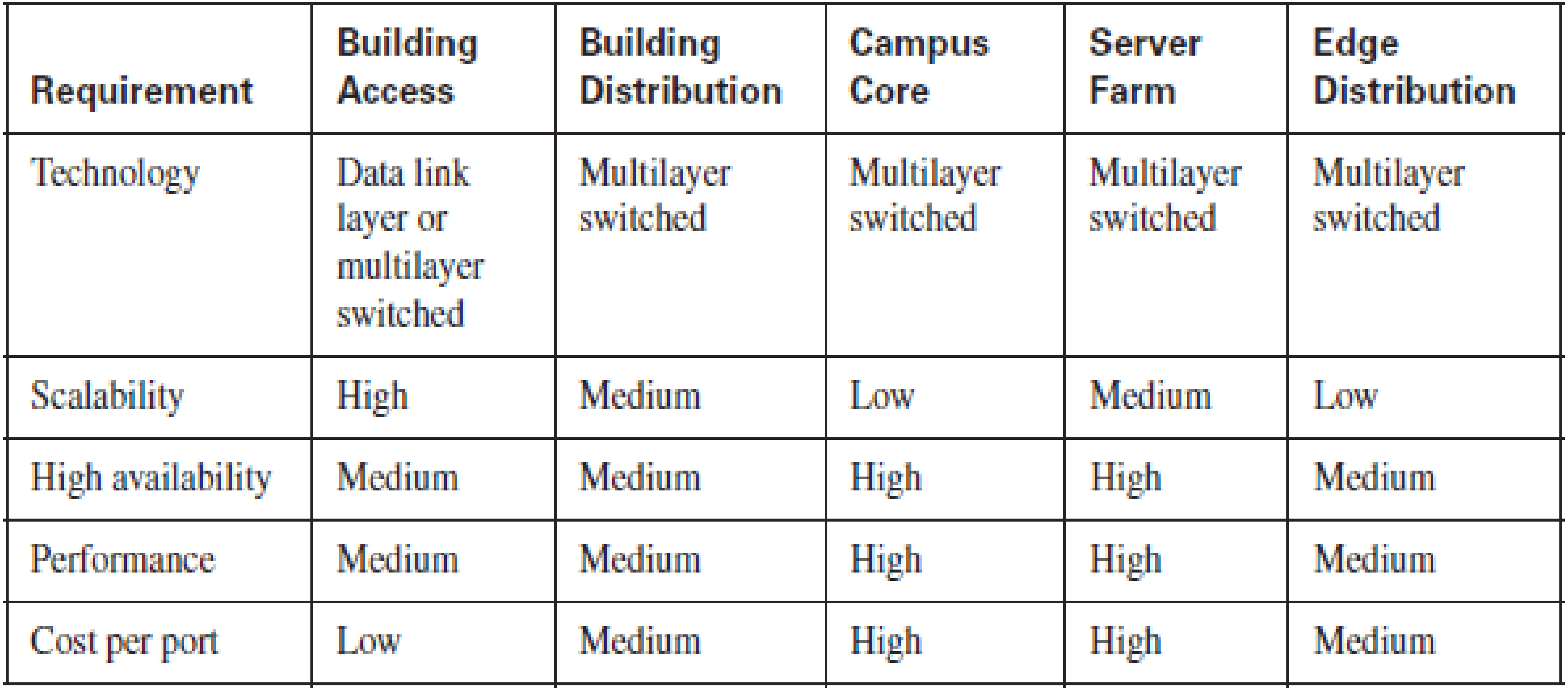
— The Building Distribution layer

— The Campus Core layer

■ Server Farm

■ Edge Distribution (optional)

Enterprise Campus Design Requirements



Requirement	Building Access	Building Distribution	Campus Core	Server Farm	Edge Distribution
Technology	Data link layer or multilayer switched	Multilayer switched	Multilayer switched	Multilayer switched	Multilayer switched
Scalability	High	Medium	Low	Medium	Low
High availability	Medium	Medium	High	High	Medium
Performance	Medium	Medium	High	High	Medium
Cost per port	Low	Medium	High	High	Medium

Building Access Layer Design Considerations

When implementing the campus infrastructure’s Building Access layer, consider the following questions:

- How many users or host ports are currently required in the wiring closet, and how many will
- it require in the future? Should the switches be fixed or modular configuration?
- How many ports are available for end-user connectivity at the walls of the buildings?
- How many access switches are not located in wiring closets?
- What cabling is currently available in the wiring closet, and what cabling options exist for
- uplink connectivity?

Building Access Layer Design Considerations

- What data link layer performance does the node need?
- What level of redundancy is needed?
- What is the required link capacity to the Building Distribution layer switches?

Building Distribution Layer Design Considerations

The Building Distribution layer aggregates the Building Access layer, segments workgroups, and isolates segments from failures and broadcast storms. This layer implements many policies based on access lists and QoS settings. The Building Distribution layer can protect the Campus Core network from any impact of Building Access layer problems by implementing all the organization’s policies.

When implementing the Building Distribution layer, consider the following questions:

- How many devices will each Building Distribution switch handle?
- What type and level of redundancy are required?
- How many uplinks are needed?
- What speed do the uplinks need to be to the building core switches?
- What cabling is currently available in the wiring closet, and what cabling options exist for uplink connectivity?

The network designer must pay special attention to the following network characteristics:

Performance: Building Distribution switches should provide wire-speed performance on all ports. This feature is important because of Building Access layer aggregation on one side and high-speed connectivity of the Campus Core module on the other side.

Redundancy: Redundant Building Distribution layer switches and redundant connections to the Campus Core should be implemented. Using equal-cost redundant connections to the core supports fast convergence and avoids routing black holes.

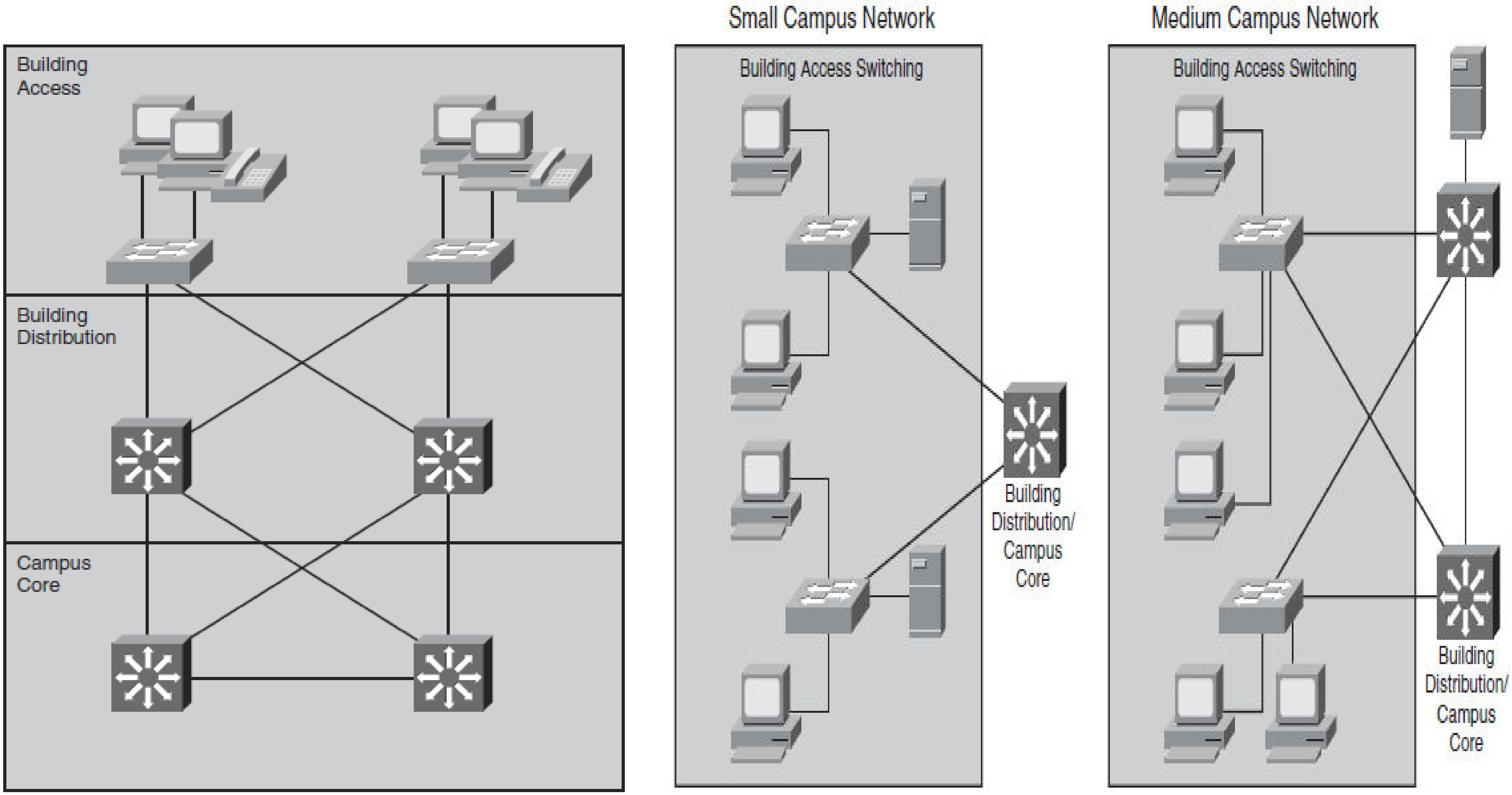
Infrastructure services: Building Distribution switches should not only support fast multilayer switching, but should also incorporate network services such as high availability, QoS, security, and policy enforcement.

Campus Core Design Considerations

Low price per port and high port density can govern switch choice for wiring closet environments, but high-performance wire-rate multilayer switching drives the Campus Core design. Using Campus Core switches reduces the number of connections between the Building Distribution layer switches and simplifies the integration of the Server Farm module and Enterprise Edge modules.

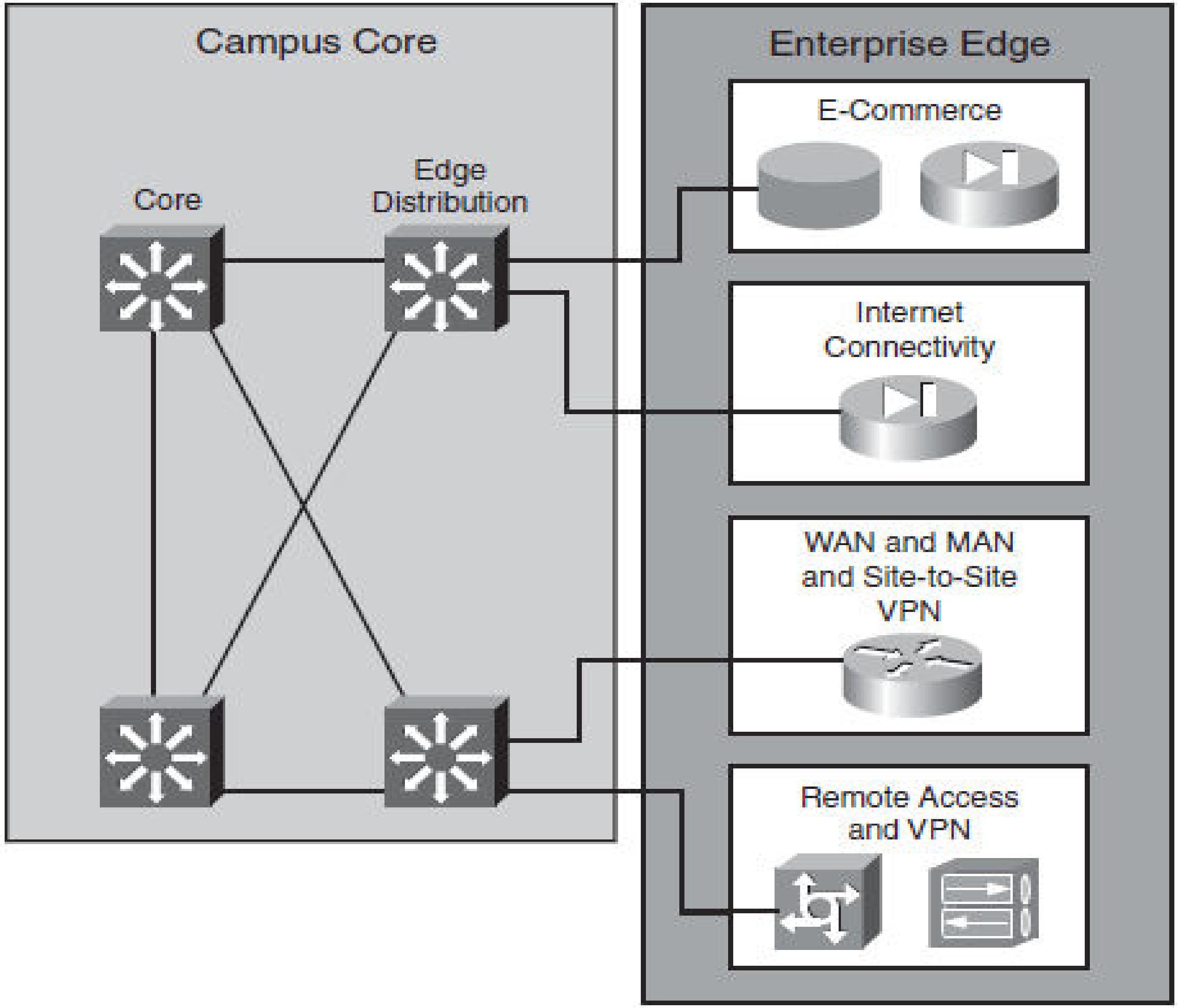
Issues to consider in a Campus Core layer design include the following:

- The performance needed in the Campus Core network.
- The number of high-capacity ports for Building Distribution layer aggregation and connection to the Server Farm module or Enterprise Edge modules.
- High availability and redundancy requirements. To provide adequate redundancy, at least two separate switches (ideally located in different buildings) should be deployed


Building Access
Building Distribution
Campus Core
Small Campus Network
Building Access Switching
Building Distribution/ Campus Core
Medium Campus Network
Building Access Switching
Building Distribution/ Campus Core

Edge Distribution at the Campus Core

Edge Distribution Design



Edge Distribution at the Campus Core

The Edge Distribution multilayer switches filter and route traffic into the Campus Core, aggregate Enterprise Edge connectivity, and provide advanced services.

Switching speed is not as important as security in the Edge Distribution module, which isolates and controls access to devices that are located in the Enterprise Edge modules (for example, servers in an E-commerce module or public servers in an Internet Connectivity module). These servers are closer to the external users and therefore introduce a higher risk to the internal campus. To protect the Campus Core from threats, the switches in the Edge Distribution module must protect the campus from the following attacks

Unauthorized access: All connections from the Edge Distribution module that pass through the Campus Core must be verified against the user and the user’s rights. Filtering mechanisms must provide granular control over specific edge subnets and their capability to reach areas within the campus.

IP spoofing:

Packet sniffers: Packet sniffers are devices that monitor and capture the traffic in the network and might be used by hackers. Packets belonging to the same broadcast domain are vulnerable to capture by packet sniffers, especially if the packets are broadcast or multicast. Because most of the traffic to and from the Edge Distribution module is business-critical, corporations cannot afford this type of security lapse. Multilayer switches can prevent such an occurrence.

Enterprise Network Campus Design:-

An understanding of network scale and knowledge of good structured engineering principles is recommended when discussing network campus design.

Network Requirements:-

When discussing network design, it is useful to categorize networks based on the number of devices serviced:

Small network: Provides services for up to 200 devices.

Medium-size network: Provides services for 200 to 1,000 devices.

Large network: Provides services for 1,000+ devices.

Network designs **vary depending on the size and requirements of the organizations**. For example, the networking infrastructure needs of a small organization with fewer devices will be less complex than the infrastructure of a large organization with a significant number of devices and connections.

- The **Cisco Certified Design Associate (CCDA®)** is an industry-recognized certification for network design engineers, technicians, and support engineers who demonstrate the skills required to design basic campus, data center, security, voice, and wireless networks.

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:-

1.**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.**

2. **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.**

3.**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.

4. **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).

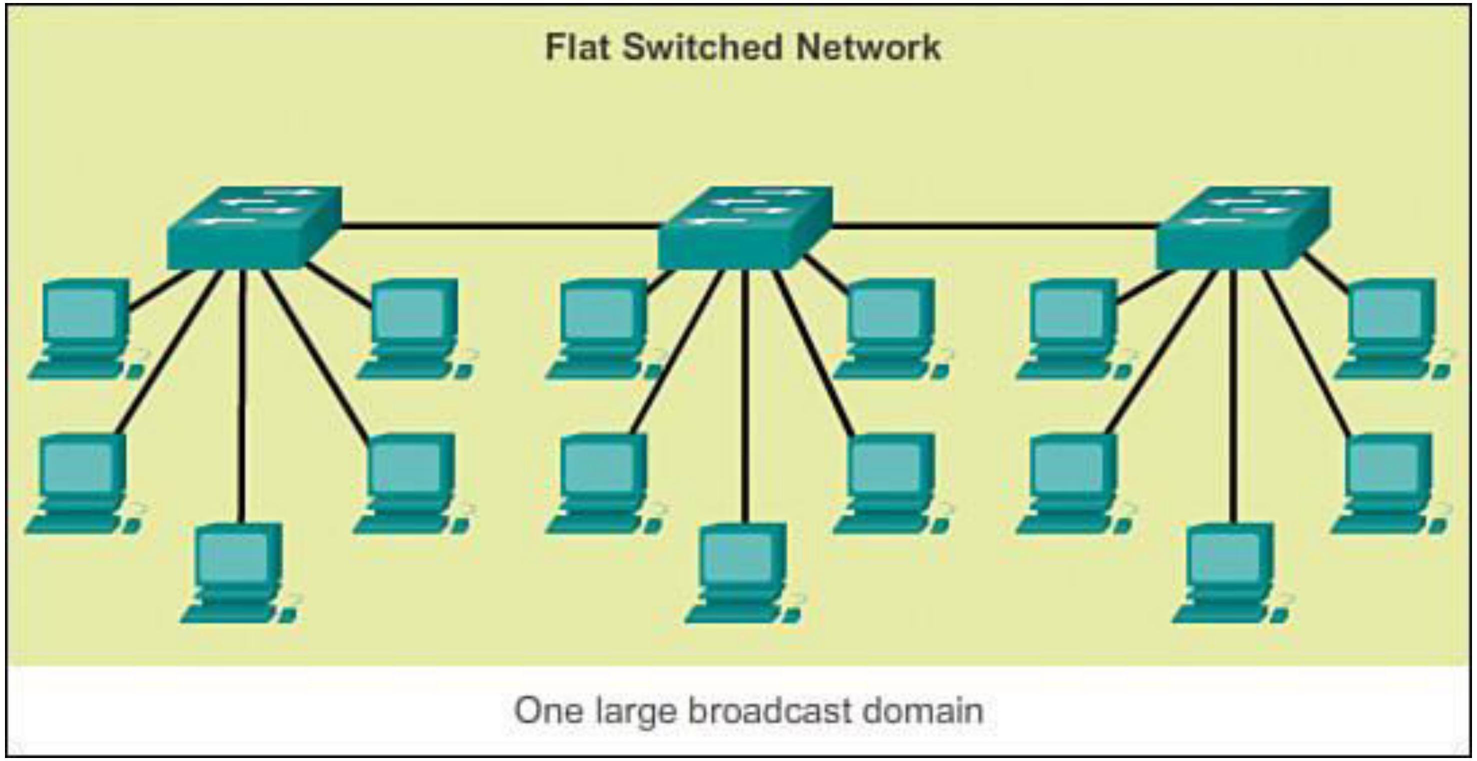
To meet these fundamental design goals, a network must be built on a **hierarchical network architecture** that allows for both flexibility and growth.

Hierarchical Network Design

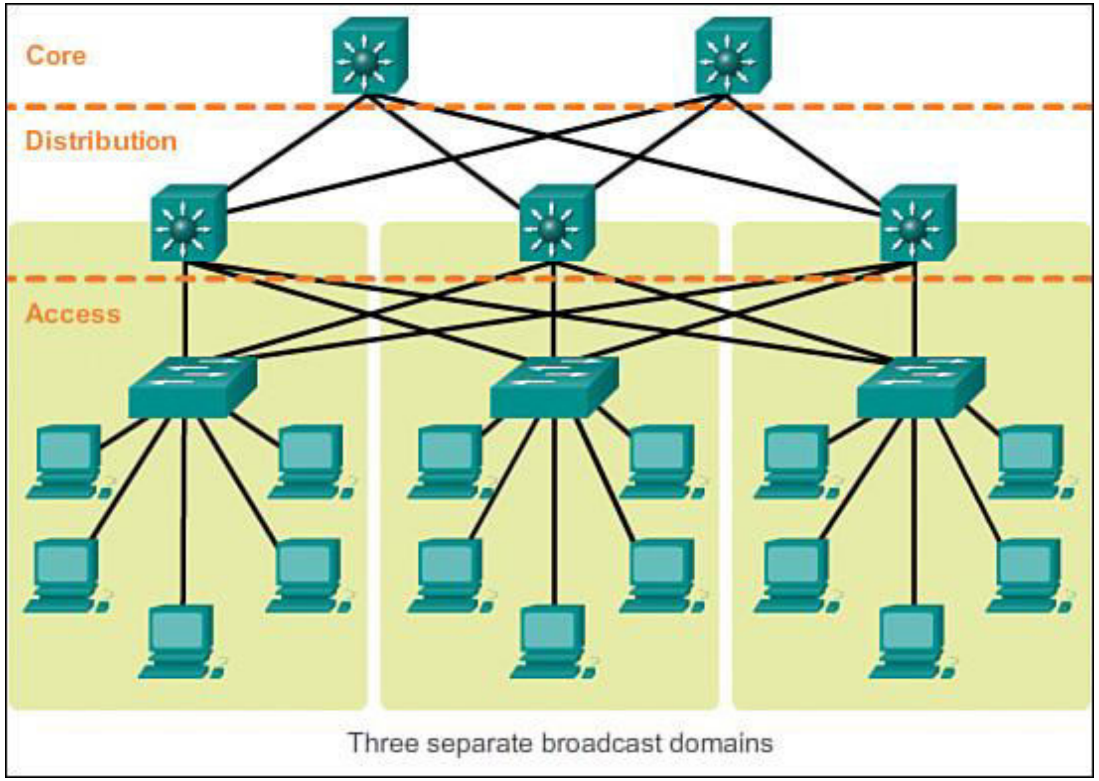
This topic discusses the **three functional layers** of the hierarchical network model: **the access, distribution, and core layers.**

Network Hierarchy

Early networks were deployed in a flat topology as shown in figure

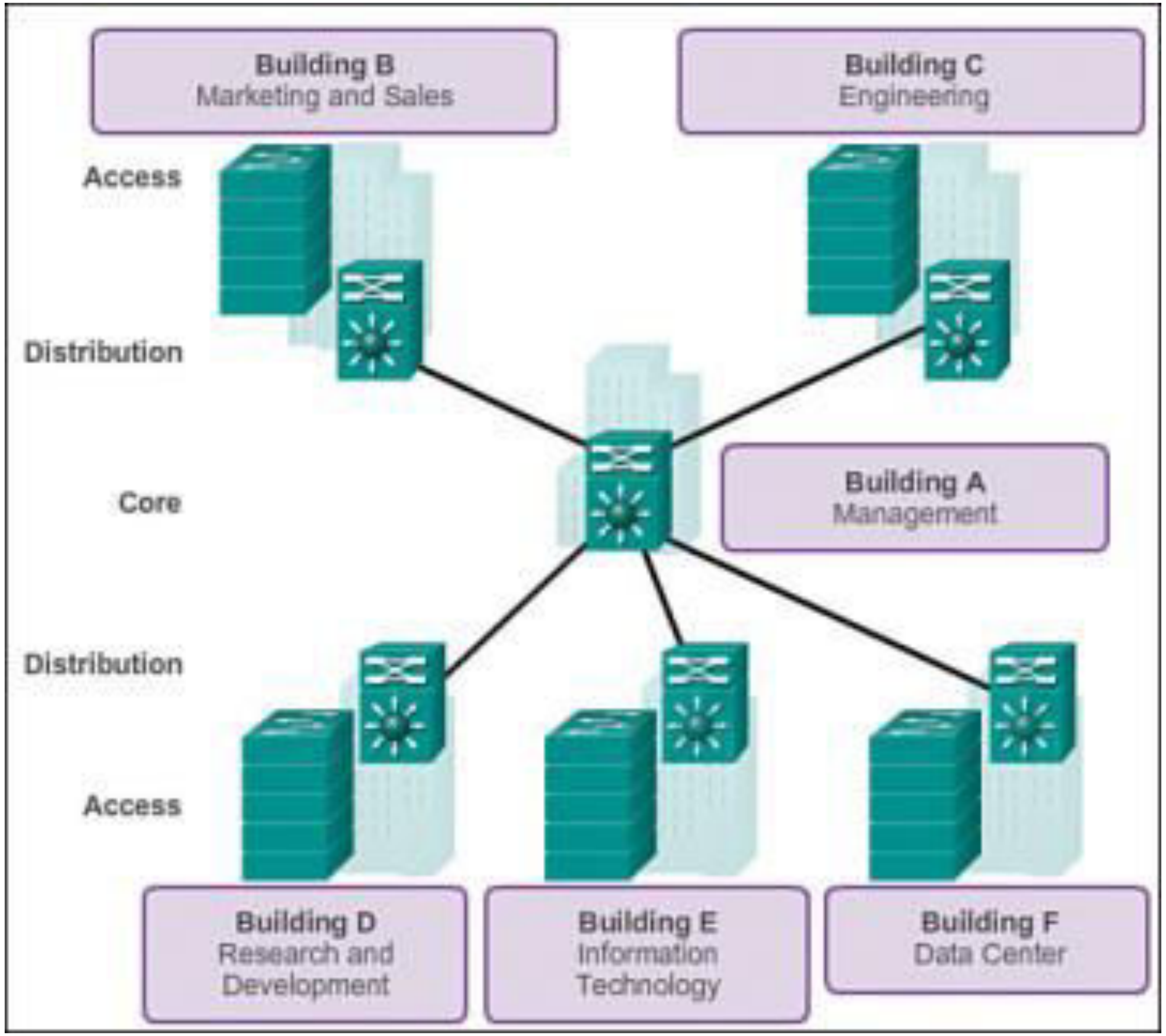


- Hubs and switches were added as more devices needed to be connected.
- A flat network design provided little opportunity to control broadcasts or to filter undesirable traffic.
- As more devices and applications were added to a flat network, response times degraded, making the network unusable.
- A better network design approach was needed. For this reason, organizations now use a hierarchical network design as shown in figure



- 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.

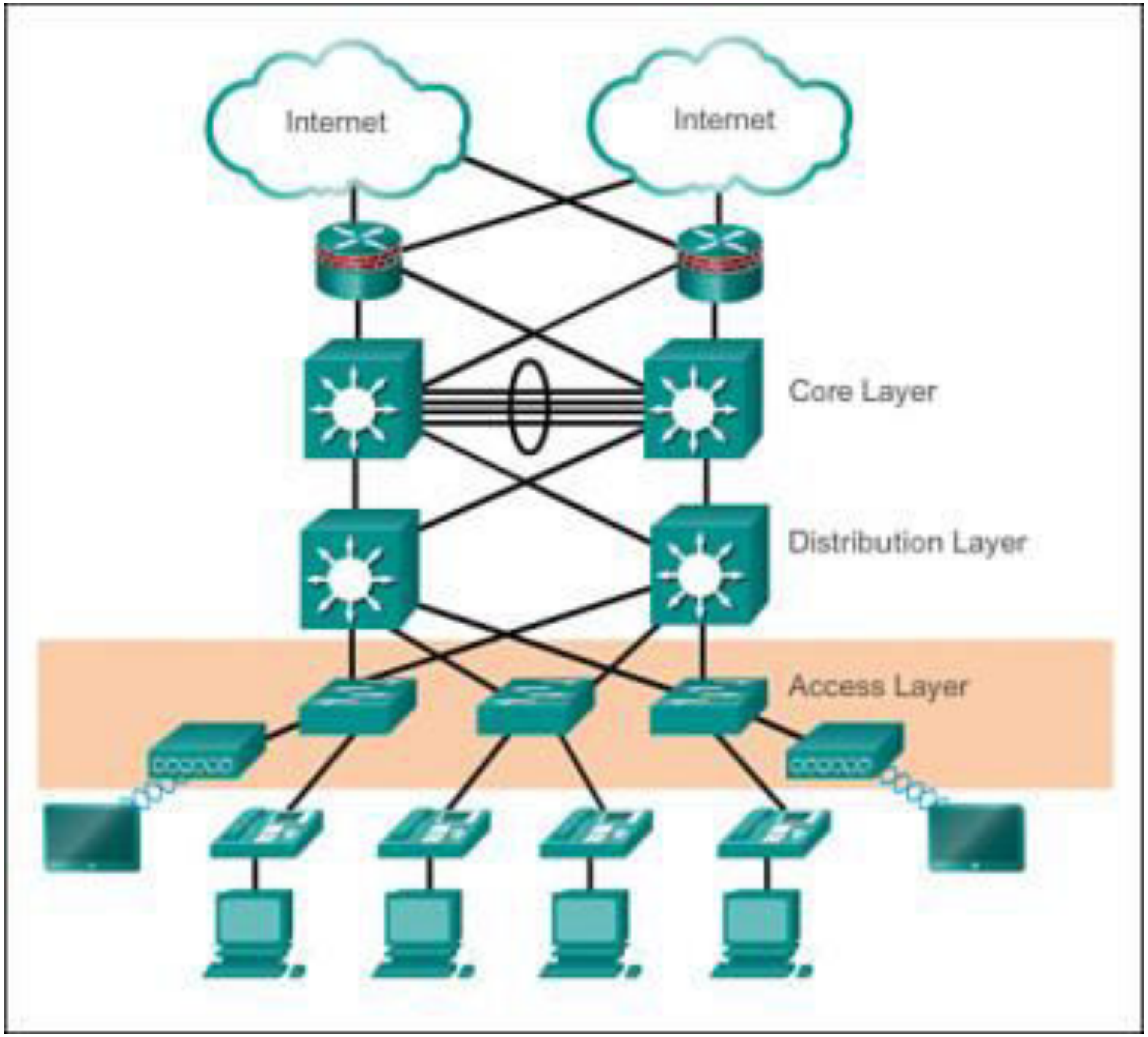
- A typical enterprise hierarchical LAN campus network design includes the following three layers:
- **Access layer**: Provides workgroup/user access to the network
- **Distribution layer**: Provides policy-based connectivity and controls the boundary between the access and core layers
- **Core layer**: Provides fast transport between distribution switches within the enterprise campus



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.

- The access layer serves a number of functions, including
- Layer 2 switching
- High availability
- Port security
- QoS classification and marking and trust boundaries
- Address Resolution Protocol (ARP) inspection
- Virtual access control lists (VACLs)
- Spanning tree


Internet
Internet
Core Layer
Distribution Layer
Access Layer

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.
- 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.
- A distribution layer switch may provide upstream services for many access layer switches.

The distribution layer can provide

- 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.

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.**
- 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.

Considerations at the core layer include

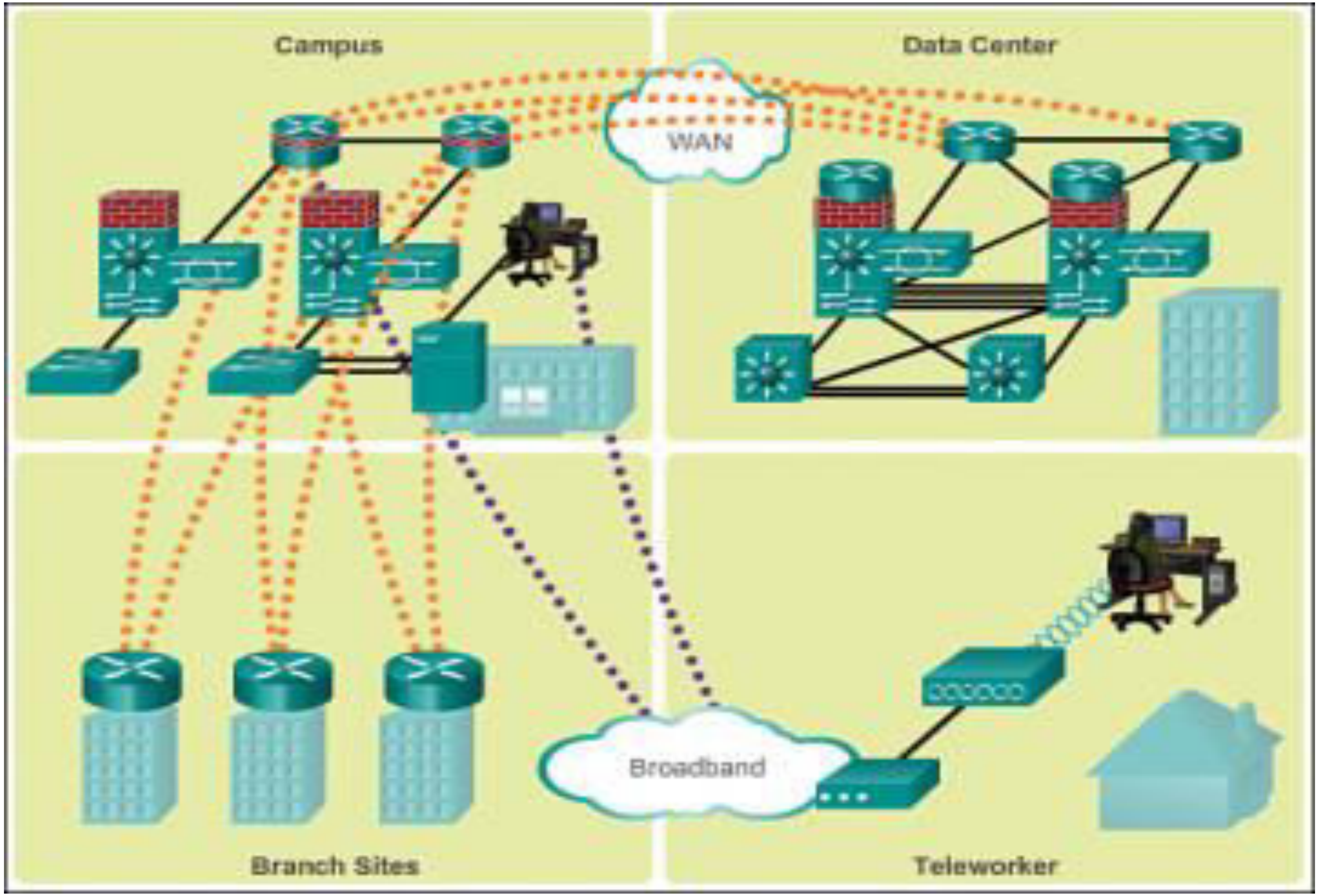
- Providing high-speed switching (i.e., fast transport)
- Providing reliability and fault tolerance
- Scaling by using faster, and not more, equipment
- Avoiding CPU-intensive packet manipulation caused by security, inspection, quality of service (QoS) classification, or other processes

Modular Approach To Network Design:-

The **Cisco Enterprise Architecture** is a **modular approach to network design**. This section identifies enterprise architecture modules that are commonly found in **medium-to-large organizations.**

Modular Design:-

- While the hierarchical network design works well within the campus infrastructure, networks have expanded beyond these borders.
- Networks have become more sophisticated and complex.
- The central campus site now requires connections to branch sites and support for teleworking employees working from home offices or other remote locations.
- Large organizations may also require dedicated connections to offsite data centers.
- As the complexity of the network increased to meet these demands, it became necessary to adjust the network design to one that uses a more modular approach.


Campus
Data Center
WAN
Broadband
Branch Sites
Teleworker

- A *modular network* design separates the network into various functional network modules, each targeting a specific place or purpose in the network.
- The modules represent areas that have different physical or logical connectivity.
- They designate where different functions occur in the network. Using a modular approach has several benefits, including

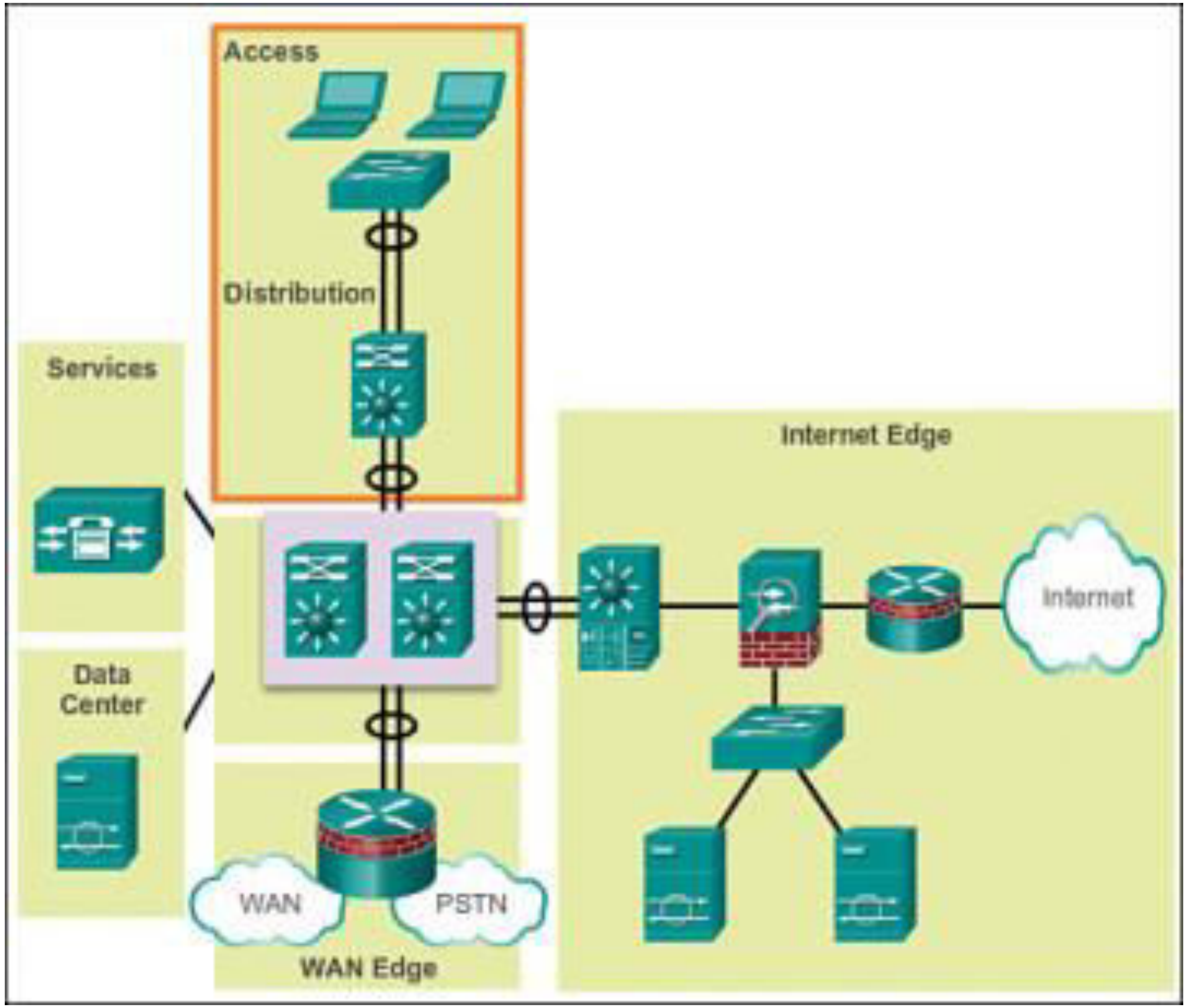
1. Failures that occur within a module can be isolated from the remainder of the network, providing for simpler problem detection and higher overall system availability.
2. Network changes, upgrades, or the introduction of new services can be made in a controlled and staged fashion, allowing greater flexibility in the maintenance and operation of the campus network.
3. When a specific module no longer has sufficient capacity or is missing a new function or service, it can be updated or replaced by another module that has the same structural role in the overall hierarchical design.
4. Security can be implemented on a modular basis allowing for more granular security control.

Modules in the Enterprise Architecture :-

- A modular approach to network design further divides the three-layer hierarchical design by pulling out specific blocks or modular areas. These basic modules are connected together via the core of the network.

Basic network modules include

- **Access-distribution**: Also called the distribution block, this is the most familiar element and fundamental component of a campus design.



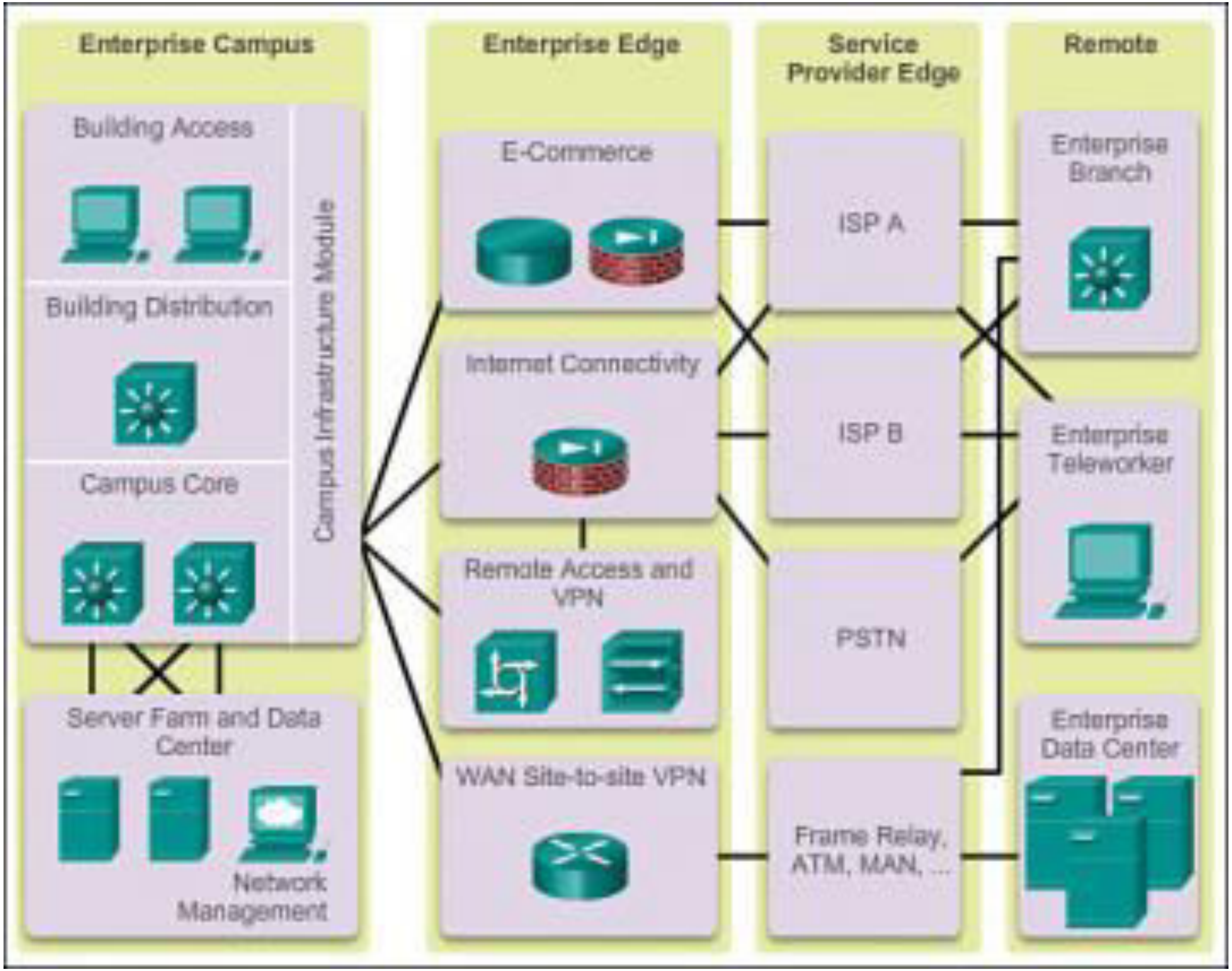
- **Services**: This is a generic block used to identify services such as centralized Lightweight Access Point Protocol (LWAPP) wireless controllers, unified communications services, policy gateways, and more.
- **Data cente**r: Originally called the server farm. This block is responsible for managing and maintaining many data systems that are vital to modern business operations. Employees, partners, and customers rely on data and resources in the data center to effectively create, collaborate, and interact.
- **Enterprise edge**: Consists of the Internet edge and the WAN edge. These blocks offer connectivity to voice, video, and data services outside the enterprise

Cisco Enterprise Architecture Model

- The Cisco Enterprise Architecture is a modular approach to network design. This topic discusses the enterprise campus module, enterprise edge module, and the service provider edge module.

Cisco Enterprise Architecture Model

- To accommodate the need for modularity in network design, Cisco developed the Cisco Enterprise Architecture model.
- This model provides all the benefits of the hierarchical network design on the campus infrastructure, and facilitates the design of larger, more scalable networks.
- The Cisco Enterprise Architecture model separates the enterprise network into functional areas that are referred to as modules.
- The modularity that is built in to the architecture allows flexibility in network design and facilitates implementation and troubleshooting.

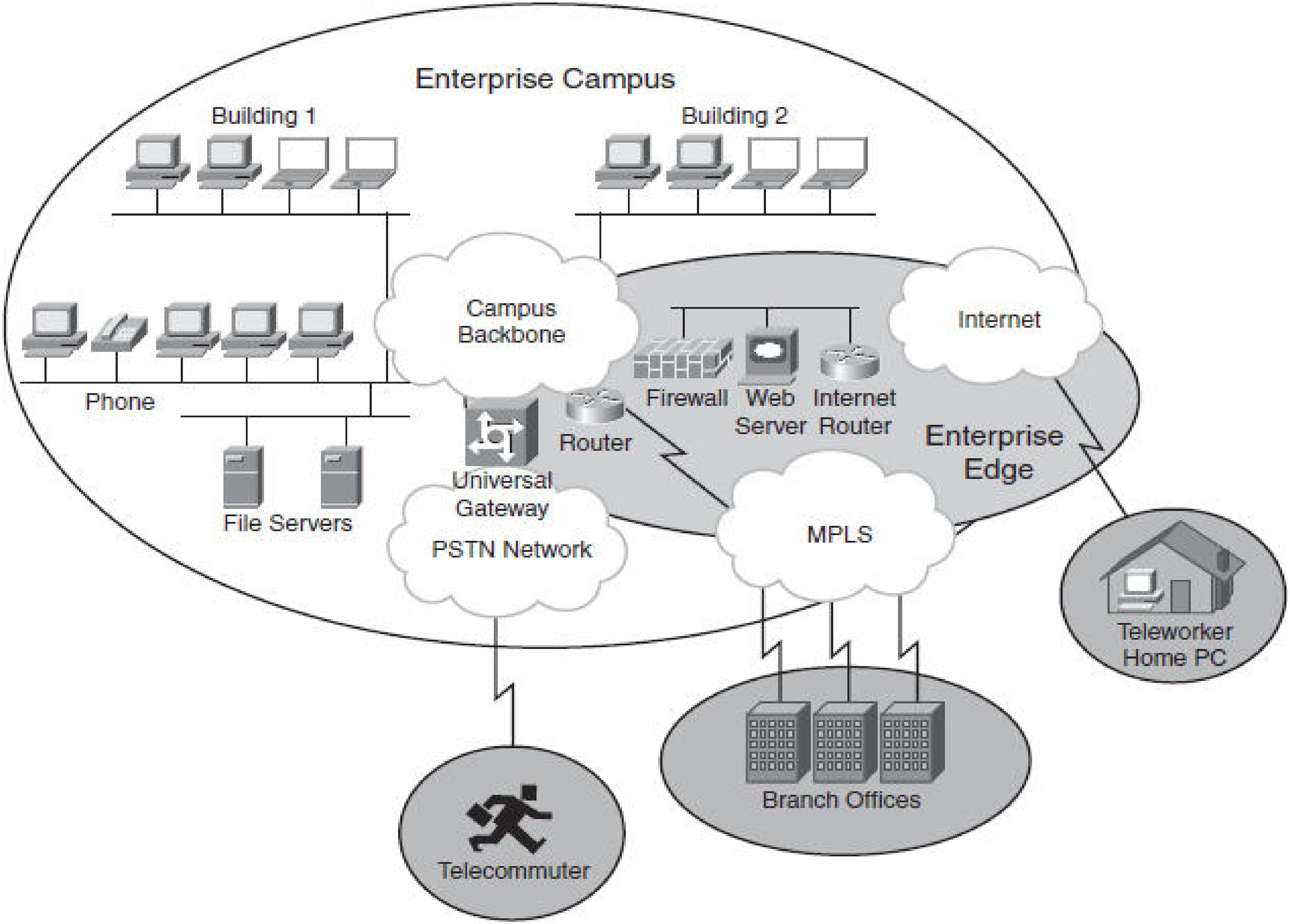

Enterprise Campus
Enterprise Edge
Service Provider Edge
Remote
Building Access
Building Distribution
Campus Core
Campus Infrastructure Module
Server Farm and Data Center
Network Management
E-Commerce
Internet Connectivity
Remote Access and VPN
WAN Site-to-site VPN
ISP A
ISP B
PSTN
Frame Relay, ATM, MAN, ...
Enterprise Branch
Enterprise Teleworker
Enterprise Data Center

As shown in Figure, the following are the primary Cisco Enterprise Architecture modules:

- Enterprise campus
- Enterprise edge
- Service provider edge

Connected to the service provider edge are the remote modules, including

- Enterprise branch
- Enterprise teleworker
- Enterprise data center

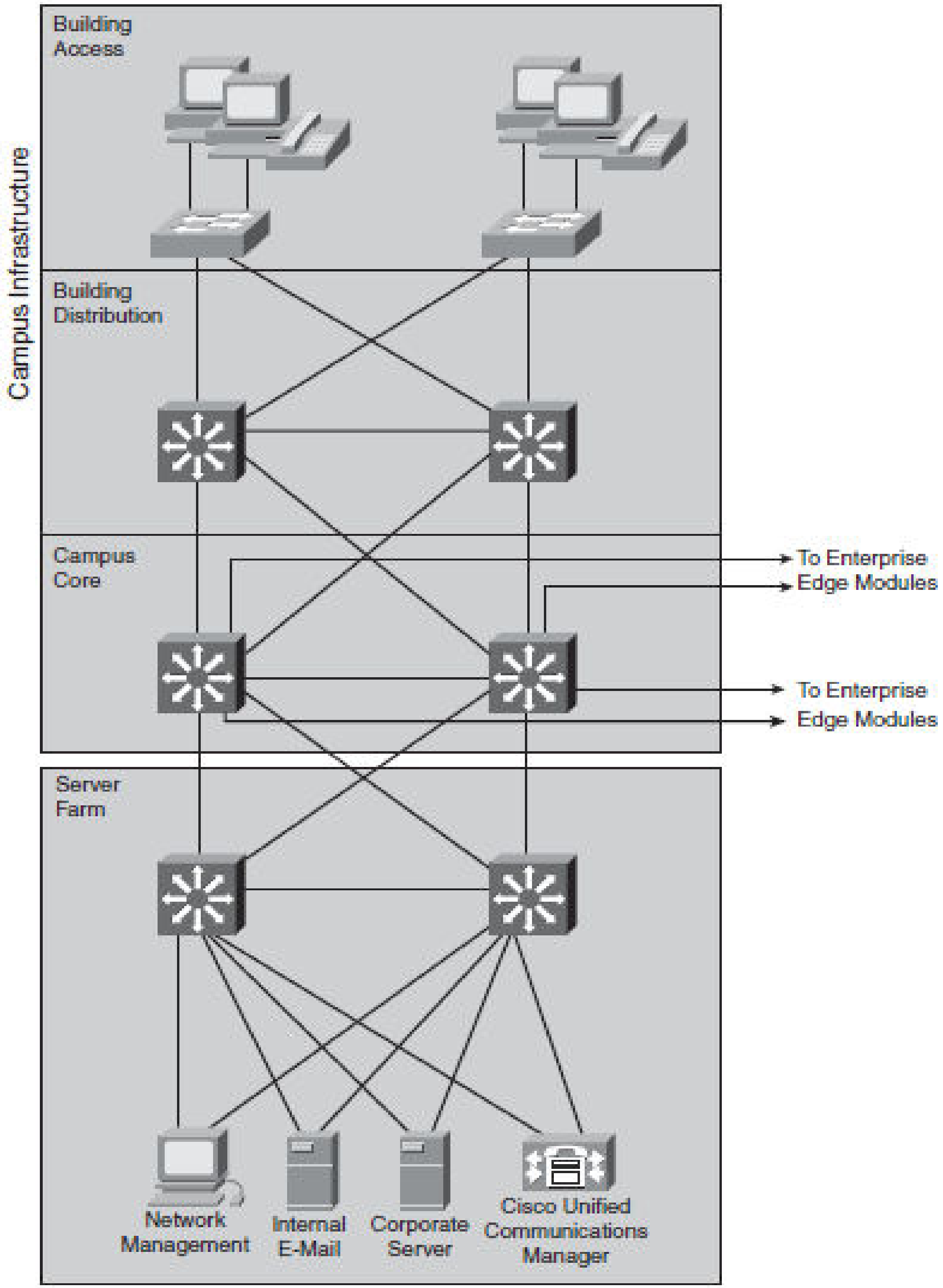

Enterprise Campus
Building 1
Building 2
Campus Backbone
Phone
File Servers
Universal Gateway
Router
Firewall
Web Server
Internet Router
Internet
Enterprise Edge
MPLS
PSTN Network
Teleworker Home PC
Branch Offices
Telecommuter

Cisco Enterprise Campus

- A campus network is a building or group of buildings connected into one enterprise network that consists of many LANs.
- A campus is generally limited to a fixed geographic area, but it can span several neighboring buildings (for example, an industrial complex or business park environment). Regional offices, HOs, and mobile workers may need to connect to the central campus for data and information.
- The enterprise campus module describes the recommended methods to create a scalable network while addressing the needs of campus-style business operations.
- The architecture is modular and can easily expand to include additional campus buildings or floors as the enterprise grows.

The **enterprise campus module** consists of the following submodules:

- ✓ Building access
- ✓ Building distribution
- ✓ Campus core
- ✓ Data center



- The enterprise campus module architecture provides the enterprise with high availability through a resilient multilayer design, redundant hardware and software features, and automatic procedures for reconfiguring network paths when failures occur.
- Integrated security protects against and mitigates the impact of worms, viruses, and other attacks on the network, even at the switch port level.
- A high-capacity, centralized data center module can provide internal server resources to users.
- The data center module typically also supports network management services for the enterprise, including monitoring, logging, troubleshooting, and other common management features from end to end.
- The data center submodule typically contains internal email and corporate servers that provide application, file, print, email, and Domain Name System (DNS) services to internal users.

- Follow these guidelines for creating the modules within an Enterprise Campus functional area:

Step 1 Select modules within the campus that act as buildings with access and distribution layers.

Step 2 Determine the locations and the number of access switches and their uplinks to distribution layer switches.

Step 3 Select the appropriate distribution layer switches, taking into account the number of access layer switches and end users. Use at least two distribution layer switches for redundancy.

Step 4 Consider two uplink connections from each access layer switch to the two distribution layer switches.

Step 5 Determine where servers are or will be located, and design the Server Farm module with at least two distribution layer switches that connect all servers for full redundancy. Include out-of-band network management connections to all critical devices in the campus network.

Step 6 Design the Campus Infrastructure module’s Campus Core layer using at least two switches and provide for the expected traffic volume between modules.

Step 7 Interconnect all modules of the Enterprise Campus with the Campus

Infrastructure module’s Campus Core layer in a redundant manner

- ***Cisco Enterprise Edge:***-

The enterprise edge module provides connectivity for voice, video, and data services outside the enterprise. This module often functions as a liaison between the enterprise campus module and the other modules.

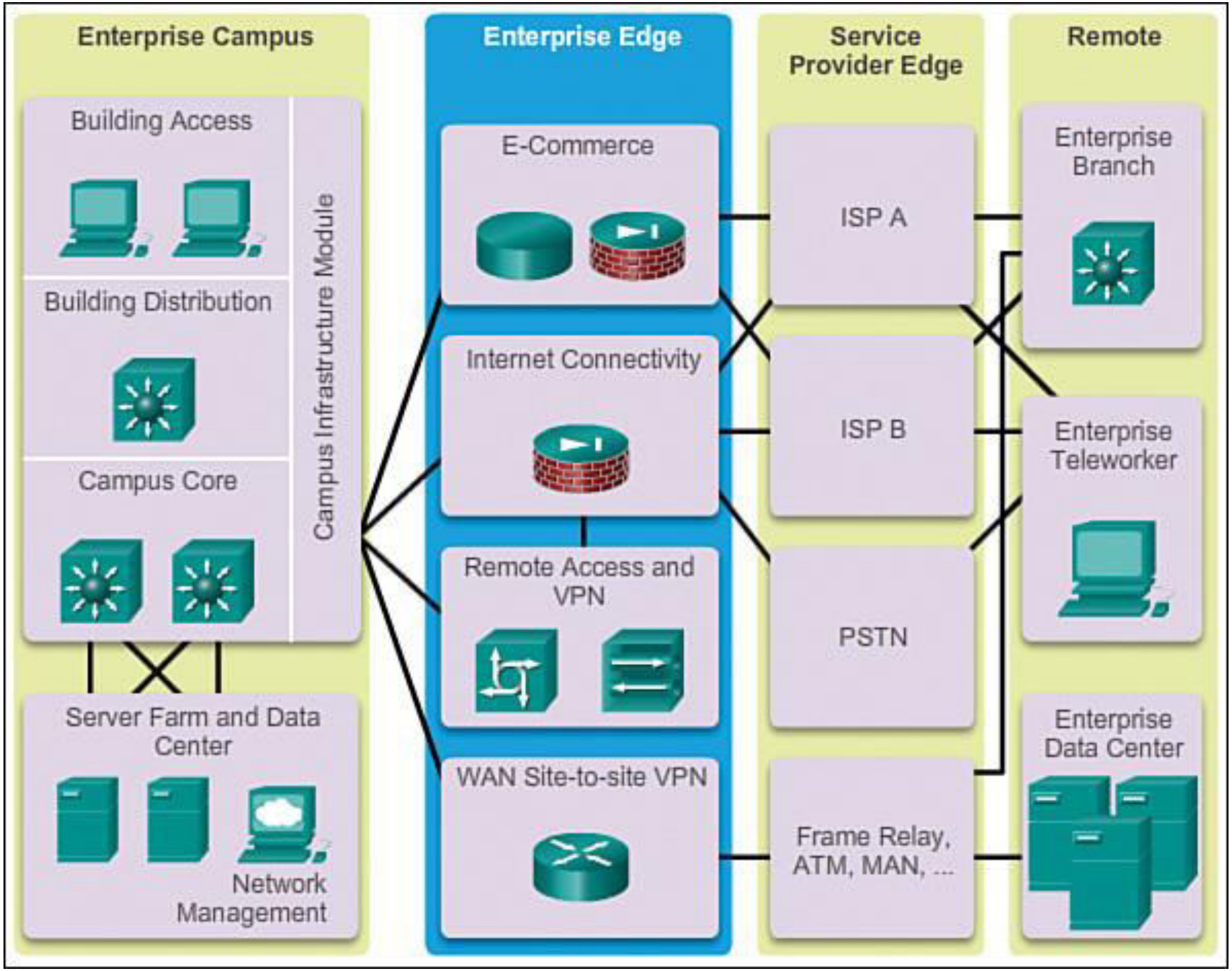
As shown in Figure the enterprise edge module consists of submodules providing

✓E-commerce services

✓Internet connectivity

✓Remote access and VPN access

✓WAN site-to-site VPN access


Enterprise Campus
Building Access
Building Distribution
Campus Core
Campus Infrastructure Module
Server Farm and Data Center
Network Management
Enterprise Edge
E-Commerce
Internet Connectivity
Remote Access and VPN
WAN Site-to-site VPN
Service Provider Edge
ISP A
ISP B
PSTN
Frame Relay, ATM, MAN, ...
Remote
Enterprise Branch
Enterprise Teleworker
Enterprise Data Center

✓E-commerce networks and servers:

1. The e-commerce submodule enables enterprises to support e-commerce applications through the Internet.

2. It uses the high-availability designs of the data center module.

3. Devices located in the e-commerce submodule include web, application, and database servers; firewall and firewall routers; and network intrusion prevention systems (IPS).

✓Internet connectivity and demilitarized zone (DMZ):

1. The Internet submodule of the enterprise edge provides internal users with secure connectivity to Internet services such as public servers, email, and DNS.

2. Connectivity to one or several Internet service providers (ISPs) is also provided.

3.Components of this submodule include firewall and firewall routers, Internet edge routers, FTP and HTTP servers, SMTP relay servers, and DNS servers.

✓Remote access and VPN:

1. The VPN/remote access submodule of the enterprise edge provides remote-access termination services, including authentication for remote users and sites.

2. Components of this submodule include firewalls, dial-in access concentrators, Cisco Adaptive Security Appliances (ASA), and network intrusion prevention system (IPS) appliances.

✓WAN:

1. The WAN submodule uses various WAN technologies for routing traffic between remote sites and the central site.

2.Enterprise WAN links include technologies such as Multiprotocol Label Switching (MPLS), Metro Ethernet, leased lines, Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH), PPP, Frame Relay, ATM, cable, digital subscriber line (DSL), and wireless.

- ***Service Provider Edge***

Enterprises use service providers (SPs) to link to other sites. As shown in Figure the SP edge module can include

✓Internet service providers (ISPs)

✓WAN services such as Frame Relay, ATM, and MAN

✓Public switched telephone network (PSTN) services

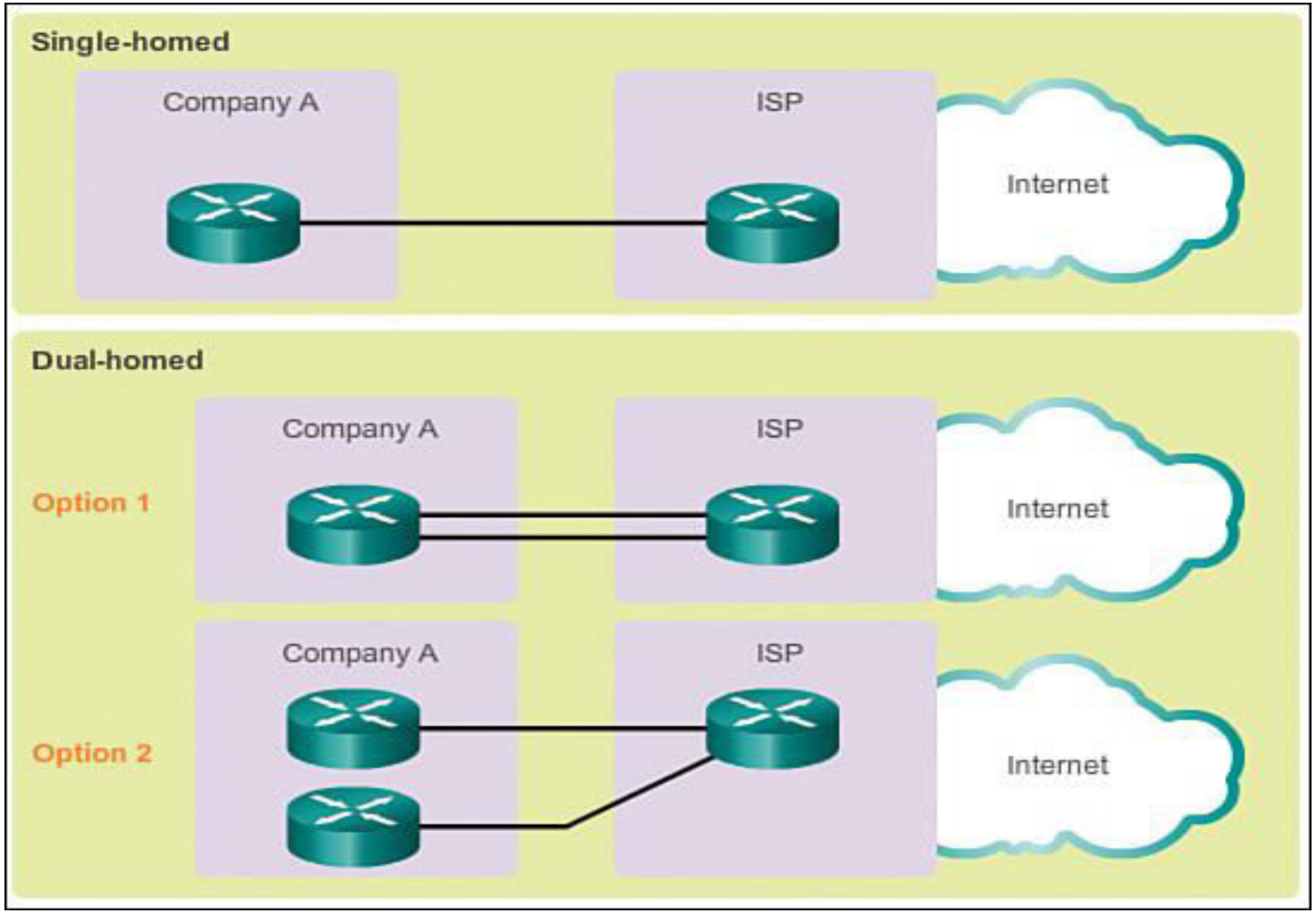
The SP edge provides connectivity between the enterprise campus module to the remote enterprise data center, enterprise branch, and enterprise teleworker modules.

- The SP edge module Spans across large geographic areas in a cost effective manner
- Converges voice, video, and data services over a single IP communications network
- Supports QoS and service level agreements
- Supports security using VPNs (IPsec / MPLS) over Layer 2 and Layer 3 WANs

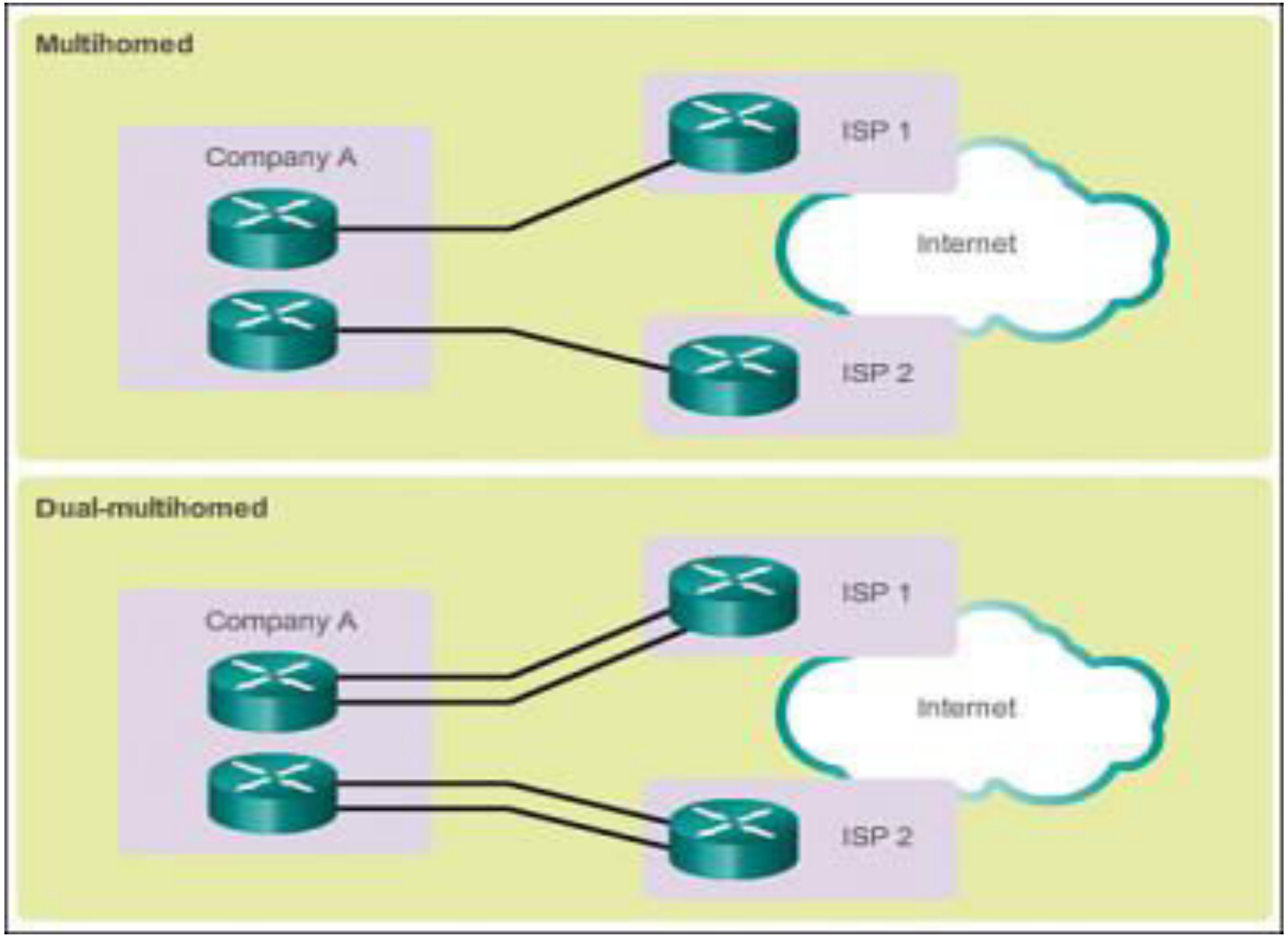
When acquiring Internet services from an ISP, redundancy or failover should be considered. Redundant Internet connections vary depending if the enterprise is connecting to a single ISP or multiple ISPs.

Single-homed: A single connection to an ISP

Dual-homed: Two or more connections to a single ISP



- Alternatively, it is possible to set up redundancy using multiple ISPs, as shown in
- Multihomed: Connections to two or more ISPs
- Dual-multihomed: Multiple connections to two or more ISPs



- ***Remote Functional Area***

Enterprise Branch

- The enterprise branch module includes remote branches that allow employees to work at noncampus locations.
- These locations are typically responsible for providing security, telephony, and mobility options to employees, as well as general connectivity into the campus network and the different components located inside the enterprise campus.
- The enterprise branch module allows enterprises to extend head-office applications and services, such as security, Cisco Unified Communications, and advanced application performance, to the remote branches.
- The edge device connecting the remote site to the central site varies depending on the needs and size of the site.

- Large remote sites may use high-end Cisco Catalyst switches, while smaller sites may use an ISR G2 router.
- These remote sites rely on the SP edge to provide services and applications from the main site.

Enterprise Teleworker

- The enterprise teleworker module is responsible for providing connectivity for workers who operate out of different geographically dispersed locations, including home offices, hotels, or customer/client sites.
- The teleworker module recommends that mobile users connect to the Internet using the services of a local ISP, such as cable modem or DSL.
- VPN services can then be used to secure communications between the mobile worker and central campus.
- Integrated security- and identity-based networking services enable the enterprise to extend campus security policies to the teleworker.
- Staff can securely log in to the network over the VPN and gain access to authorized applications and services from a single cost-effective platform.

Enterprise Teleworker

- The enterprise teleworker module is responsible for providing connectivity for workers who operate out of different geographically dispersed locations, including home offices, hotels, or customer/client sites.
- The teleworker module recommends that mobile users connect to the Internet using the services of a local ISP, such as cable modem or DSL.
- VPN services can then be used to secure communications between the mobile worker and central campus.
- Integrated security- and identity-based networking services enable the enterprise to extend campus security policies to the teleworker.
- Staff can securely log in to the network over the VPN and gain access to authorized applications and services from a single cost-effective platform.

Enterprise Data Center

- The enterprise data center module is a data center with all of the same functional options as a campus data center, but exists at a remote location.
- This provides an added layer of security as the offsite data center can provide disaster recovery and business continuance services for the enterprise.
- High-end switches such as the Cisco Nexus series switch use fast WAN services such as Metro Ethernet (MetroE) to connect the enterprise campus to the remote enterprise data center.
- Redundant data centers provide backup using synchronous and asynchronous data and application replication.
- Additionally, the network and devices offer server and application load balancing to maximize performance.
- This solution allows the enterprise to scale without major changes to the infrastructure.

Services Within Modular Network

- ✓Businesses that operate large enterprise networks strive to create an enterprise-wide networked infrastructure and interactive services to serve as a solid foundation for business and collaborative applications.
- ✓This section explores some of the interactive services with respect to the modules that form the Cisco Enterprise Architecture.

Interactive Serives

- ✓Since the inception of packet-based communications, networks have always offered a forwarding service. Forwarding is the fundamental activity within an internetwork.
- ✓In IP, this forwarding service was built on the assumption that end nodes in the network were intelligent, and that the network core did not have intelligence.
- ✓With advances in networking software and hardware, the network can offer an increasingly rich, intelligent set of mechanisms for forwarding information.
- ✓ Interactive services add intelligence to the network infrastructure, beyond simply moving a datagram between two points.

Interactive Serives

✓Security services: Ensure that all aspects of the network are secure, from devices connecting to the network to secured transport to data theft prevention

✓Mobility services: Allow users to access network resources regardless of their physical location

✓Storage services: Provide distributed and virtual storage across the infrastructure

✓Voice and collaboration services: Deliver the foundation by which voice can be carried across the network, such as security and high availability

✓Compute services: Connect and virtualize compute resources based on the application

✓Identity services: Map resources and policies to the user and device

Interactive Serives

- ✓Examples of network services imbedded in the infrastructure services include the following:

- ✓Network management: Includes LAN management for advanced management of multilayer switches; routed WAN management for monitoring, traffic management, and access control to administer the routed infrastructure of multiservice networks; service management for managing and monitoring service level agreements (SLAs); and VPN security management for optimizing VPN performance and security administration.
- ✓High availability: Ensures end-to-end availability for services, clients, and sessions. Implementation includes reliable, fault-tolerant network devices to automatically identify and overcome failures, and resilient network technologies.

Interactive Serives

✓QoS: Manages the delay, delay variation (jitter), bandwidth availability, and packet loss parameters of a network to meet the diverse needs of voice, video, and data applications. QoS features provide value-added functionality, such as network-based application recognition for classifying traffic on an application basis, Cisco IOS IP SLAs (previously called the service assurance agent) for end-to-end QoS measurements, Resource Reservation Protocol signaling for admission control and reservation of resources, and a variety of configurable queue insertion and servicing functions.

✓IP multicasting: Provides bandwidth-conserving technology that reduces network traffic by delivering a single stream of information intended for many recipients through the transport network. Multicasting enables distribution of videoconferencing, corporate communications, distance learning, software, and other applications. Multicast packets are replicated only as necessary by Cisco routers enabled with Protocol Independent Multicast and other supporting multicast protocols that result in the most efficient delivery of data to multiple receivers.