CCNA Discovery 4.0 Designing and Supporting Computer Networks

Introducing Network Design Concepts– Chapter 1

Cisco | Networking Academy®
Mind Wide Open™

Objectives

- Review the benefits of a hierarchical network design.
- Explain the design methodology used by network designers.
- Describe the various design considerations at each area of the network:
  - The Core, Distribution and Access Layers
  - The network Enterprise Edge
  - The Data Center Server Farm
  - Remote Worker Support
  - Enterprise Wireless

Network Design Overview

Computers and information networks are critical to the success of businesses, both large and small. They connect people, support applications and services, and provide access to the resources that keep the businesses running. To meet the daily requirements of businesses, networks themselves are becoming quite complex.

Network Design Overview (cont.)

Network Requirements

Today, the Internet-based economy often demands around-the-clock customer service. This means that business networks must be available nearly 100 percent of the time. They must be smart enough to automatically protect against unexpected security incidents.

Building a Good Network

Good networks do not happen by accident. They are the result of hard work by network designers and technicians, who identify network requirements and select the best solutions to meet the needs of a business.

Network Design Overview (cont.)

Step 1

Verify the business and technical needs.

Step 2

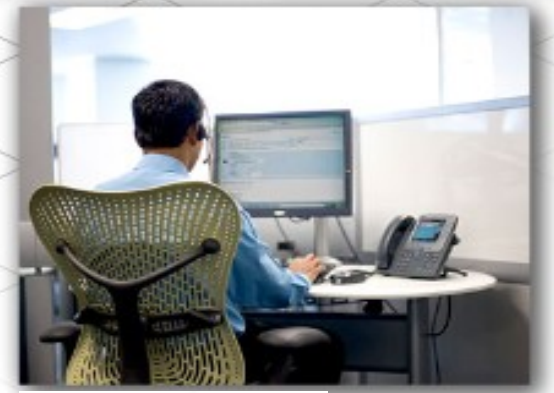
Determine the features and functions

Step 3

Perform a network readiness assessment.

Step 4

Create a solution and site acceptance test plan.



Step 5

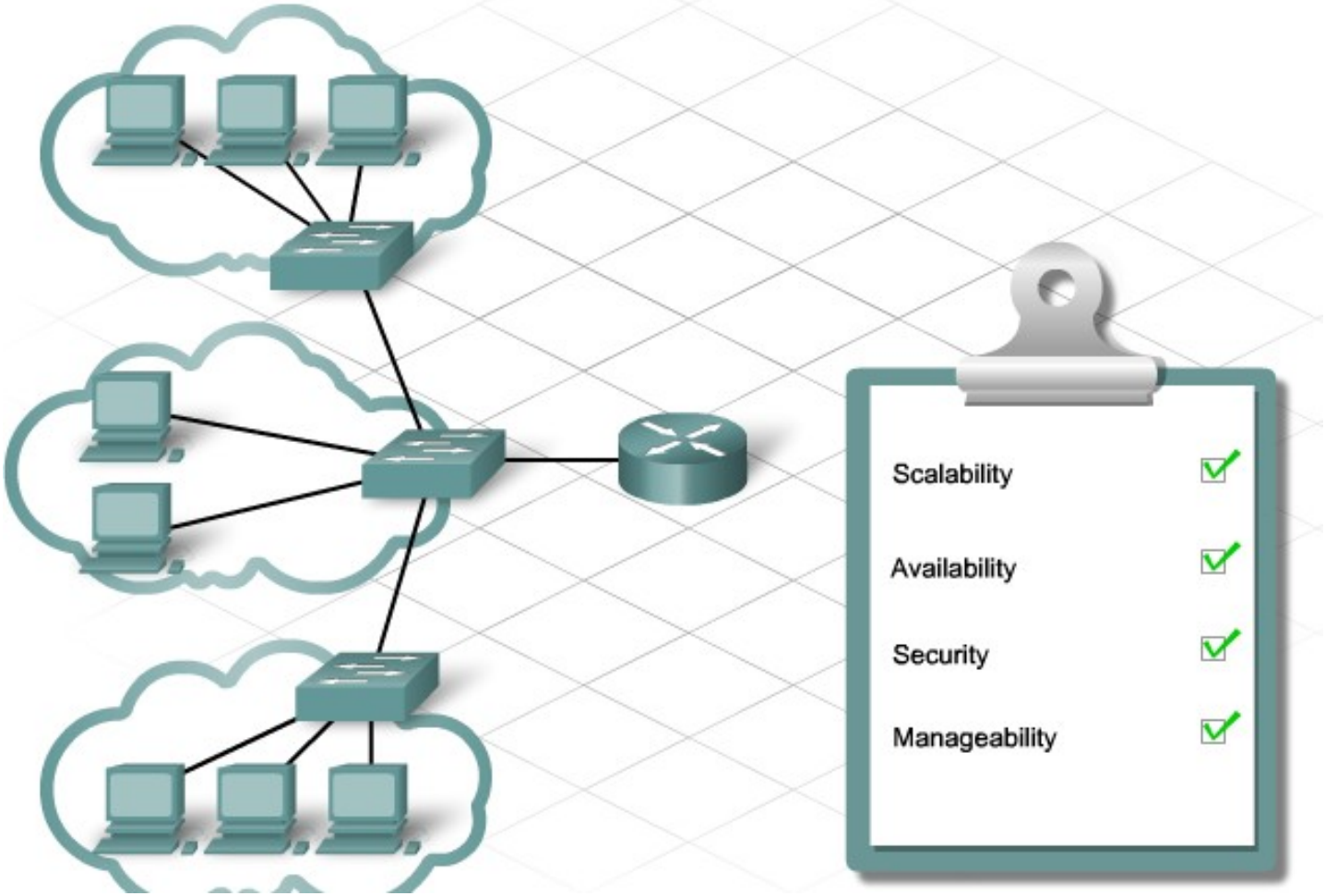
Create a project plan.

Network Design Overview (cont.)

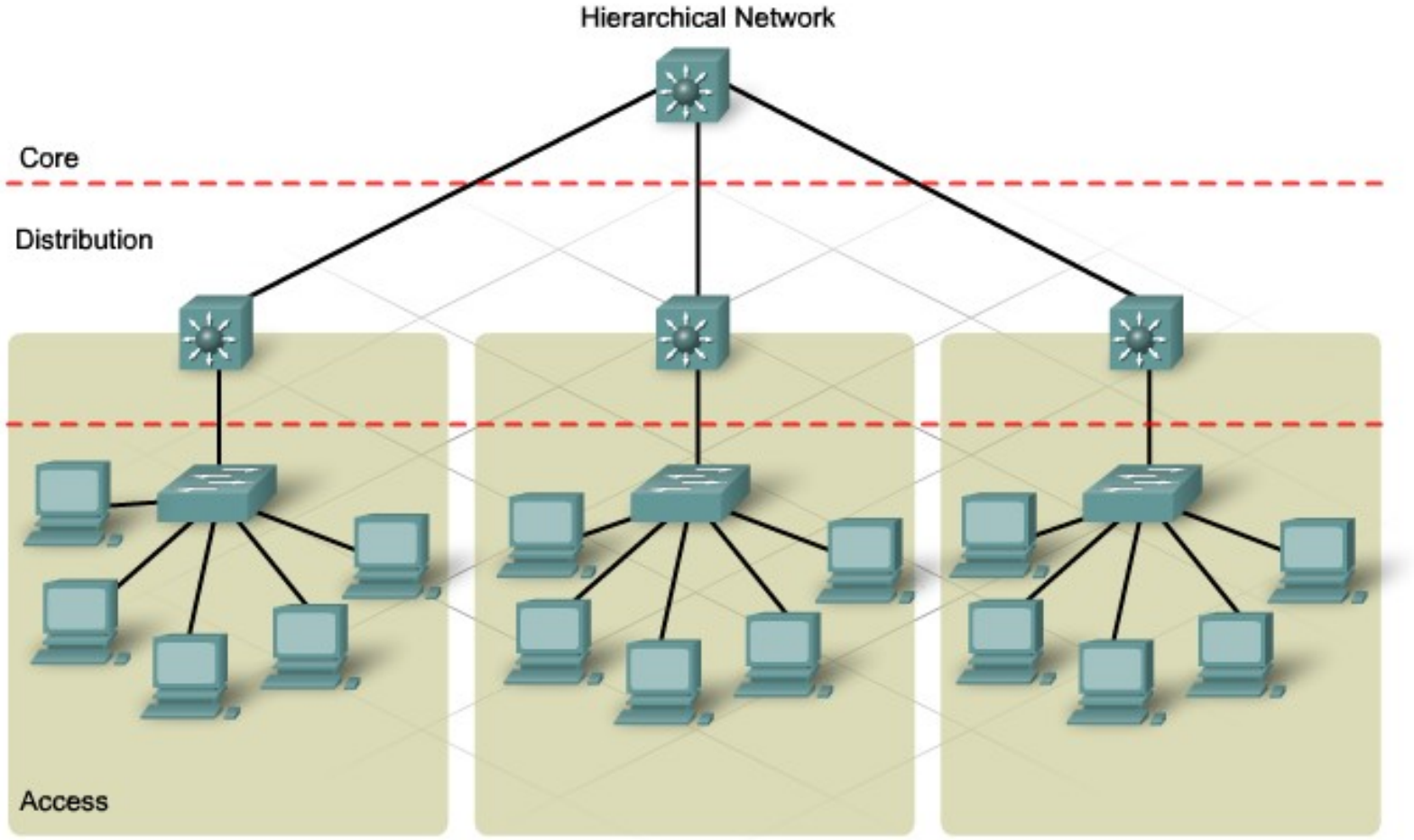
Network Requirements

- The network should stay up all the time, even in the event of failed links, equipment failure, and overloaded conditions.
- The network should reliably deliver applications and provide reasonable response times from any host to any host.
- The network should be secure. It should protect the data that is transmitted over it, as well as data stored on the devices that connect to it.
- The network should be easy to modify to adapt to network growth and general business changes.
- Because failures occasionally occur, troubleshooting should be easy. Finding and fixing a problem should not be too time-consuming.

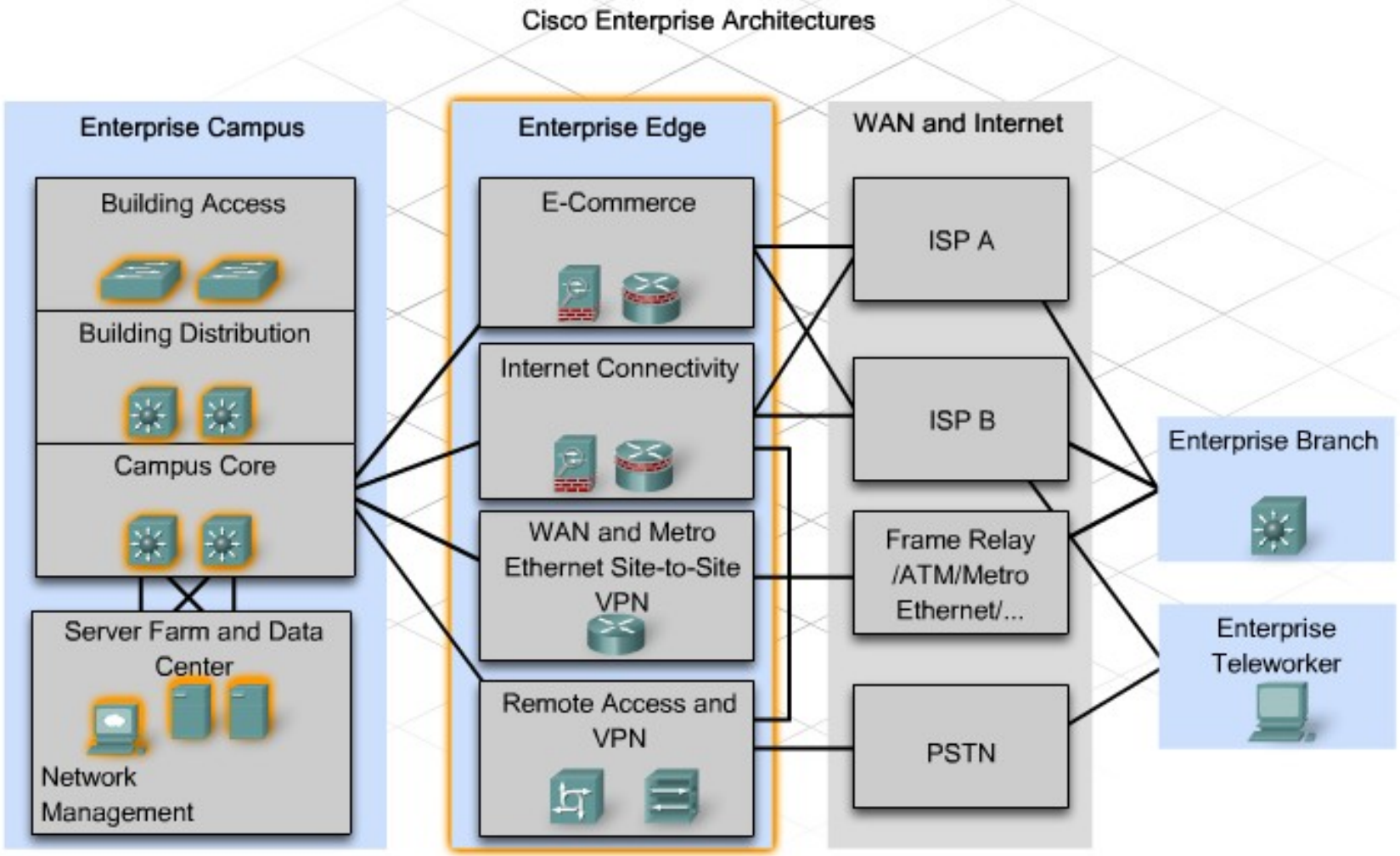
Network Design Overview



The benefits of Hierarchical Network Design



The benefits of Hierarchical Network Design



The benefits of Hierarchical Network Design

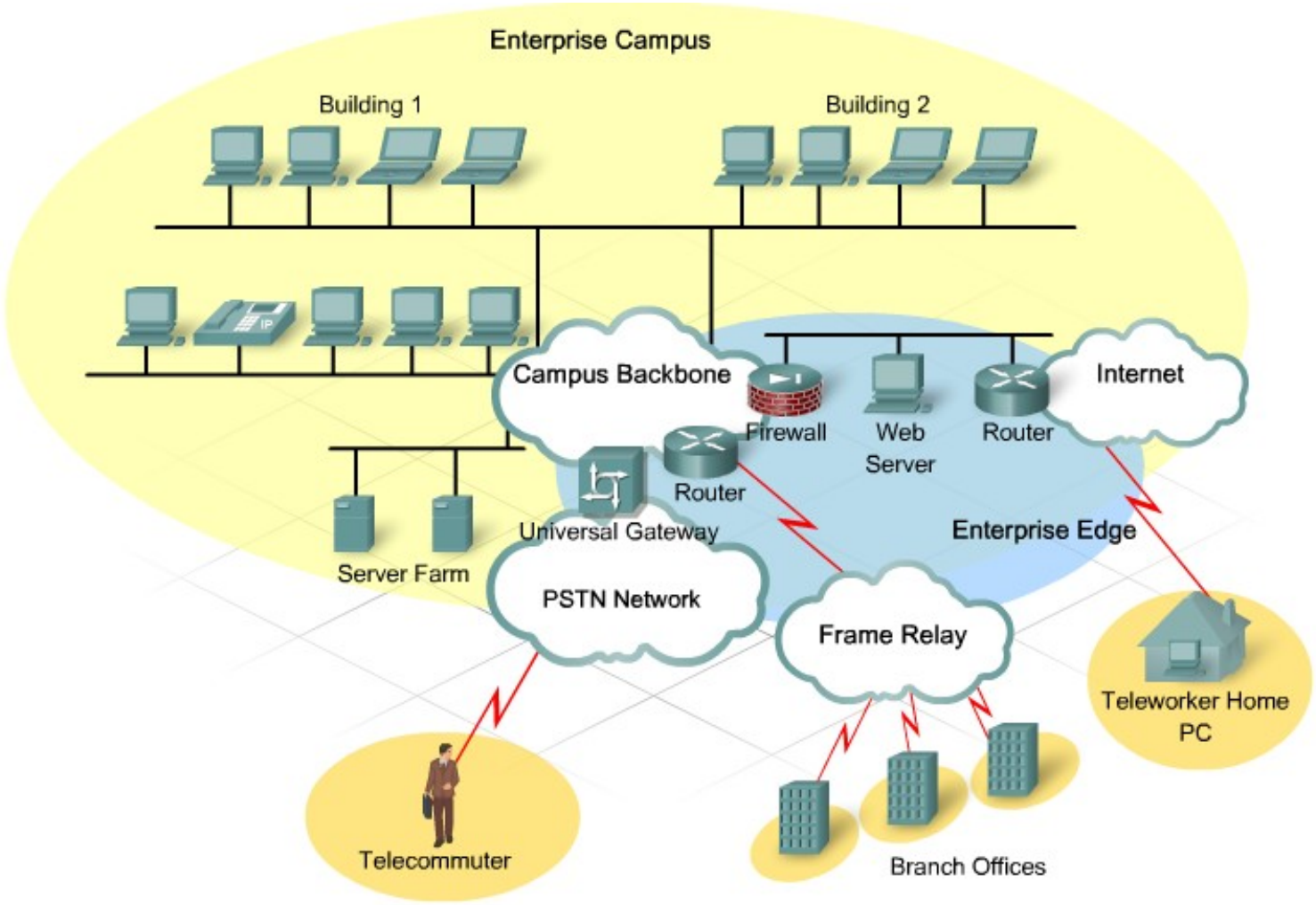
Core Layer	Distribution Layer	Access Layer
✓ Provides redundancy and fast convergence between other network layers or modules	✓ Aggregates access devices and supports routing, access control, and QoS	✓ Provides network connectivity for hosts and end devices

Enterprise Campus	Server Farm	Enterprise Edge
✓ Provides network support for all enterprise services within a campus	✓ Protects server resources with reliable, high-speed connectivity	✓ Extends enterprise services to remote sites and provides connectivity to external sites using QoS, policy enforcement, service levels, and security

The benefits of Hierarchical Network Design

Enterprise Campus - This area contains the network elements required for independent operation within a single campus or branch location.
Server Farm - A component of the enterprise campus, the data center server farm protects the server resources and provides redundant, reliable high-speed connectivity.
Enterprise Edge - As traffic comes into the campus network, this area filters traffic from the external resources and routes it into the enterprise network. It contains all the elements required for efficient and secure communication between the enterprise campus and remote locations, remote users, and the Internet.

The benefits of Hierarchical Network Design



The benefits of Hierarchical Network Design

The modular framework of the **Cisco Enterprise Architectures has the following design advantages:**

- It creates a deterministic network with clearly defined boundaries between modules. This provides clear demarcation points so that the network designer knows exactly where the traffic originates and where it flows.
- It eases the design task by making each module independent.
- It provides scalability by allowing enterprises to add modules easily. As network complexity grows, the designer can add new functional modules.
- It enables the designer to add services and solutions without changing the underlying network design.

Network Design Methodologies

Large network design projects are normally divided into three distinct steps:

Step 1: Identify the network requirements.

Step 2: Characterize the existing network.

Step 3: Design the network topology and solutions

Network Design Methodologies

Impacting the Entire Network

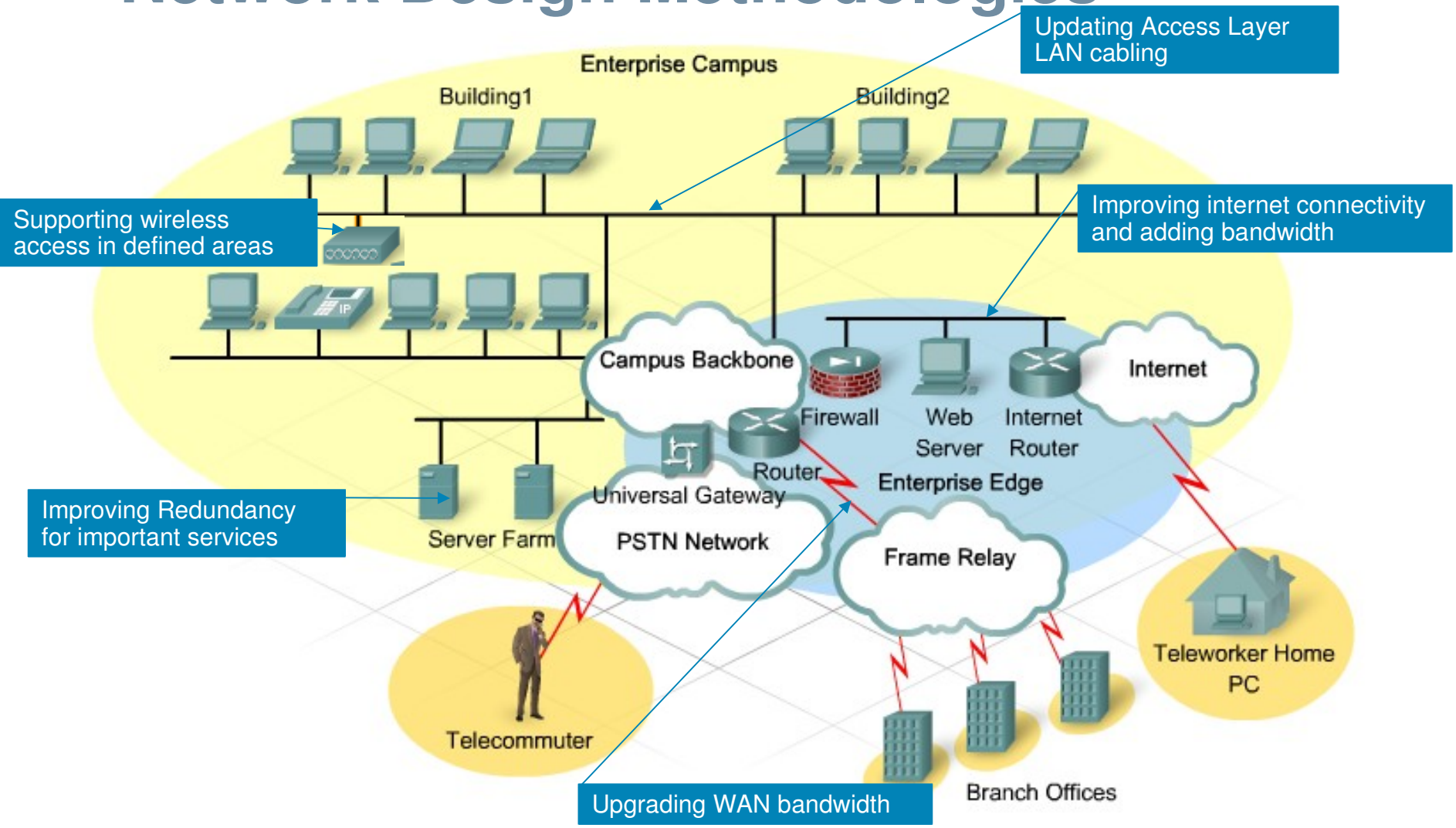
- Network requirements that impact the entire network include:
- Adding new network applications and making major changes to existing applications, such as database or DNS structure changes
- Improving the efficiency of network addressing or routing protocol changes
- Integrating new security measures
- Adding new network services, such as voice traffic, content networking, and storage networking
- Relocating servers to a data center server farm

Network Design Methodologies

Impacting a Portion of the Network

- Requirements that may only affect a portion of the network include:
- Improving Internet connectivity and adding bandwidth
- Updating Access Layer LAN cabling
- Providing redundancy for key services
- Supporting wireless access in defined areas
- Upgrading WAN bandwidth

Network Design Methodologies

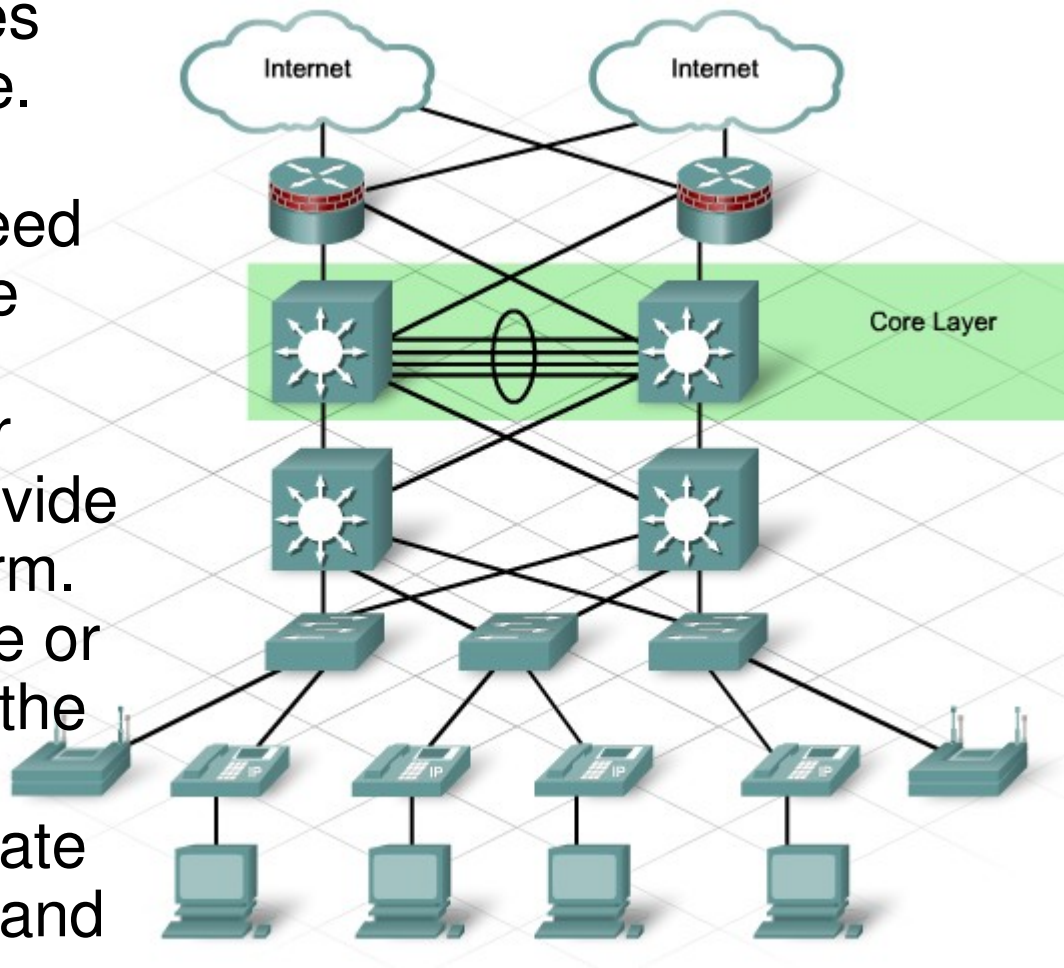


Network Design Methodologies

Proposed Design Change	Project Scope: Entire Network	Project Scope: Portions of the Network
Add server farm bandwidth		✓
Add IP telephony	✓	
Provide Core Layer redundancy		✓
Add a wireless access point		✓
Add new security policies	✓	
Upgrade WAN bandwidth		✓
Routing Protocol Change	✓	
Centralize servers and services	✓	

What happens at the Core Layer?

The Core Layer is sometimes called the network backbone. Routers and switches at the Core Layer provide high-speed connectivity. In an enterprise LAN, the Core Layer may connect multiple buildings or multiple sites, as well as provide connectivity to the server farm. The Core Layer includes one or more links to the devices at the enterprise edge in order to support Internet, Virtual Private Networks (VPNs), extranet, and WAN access.



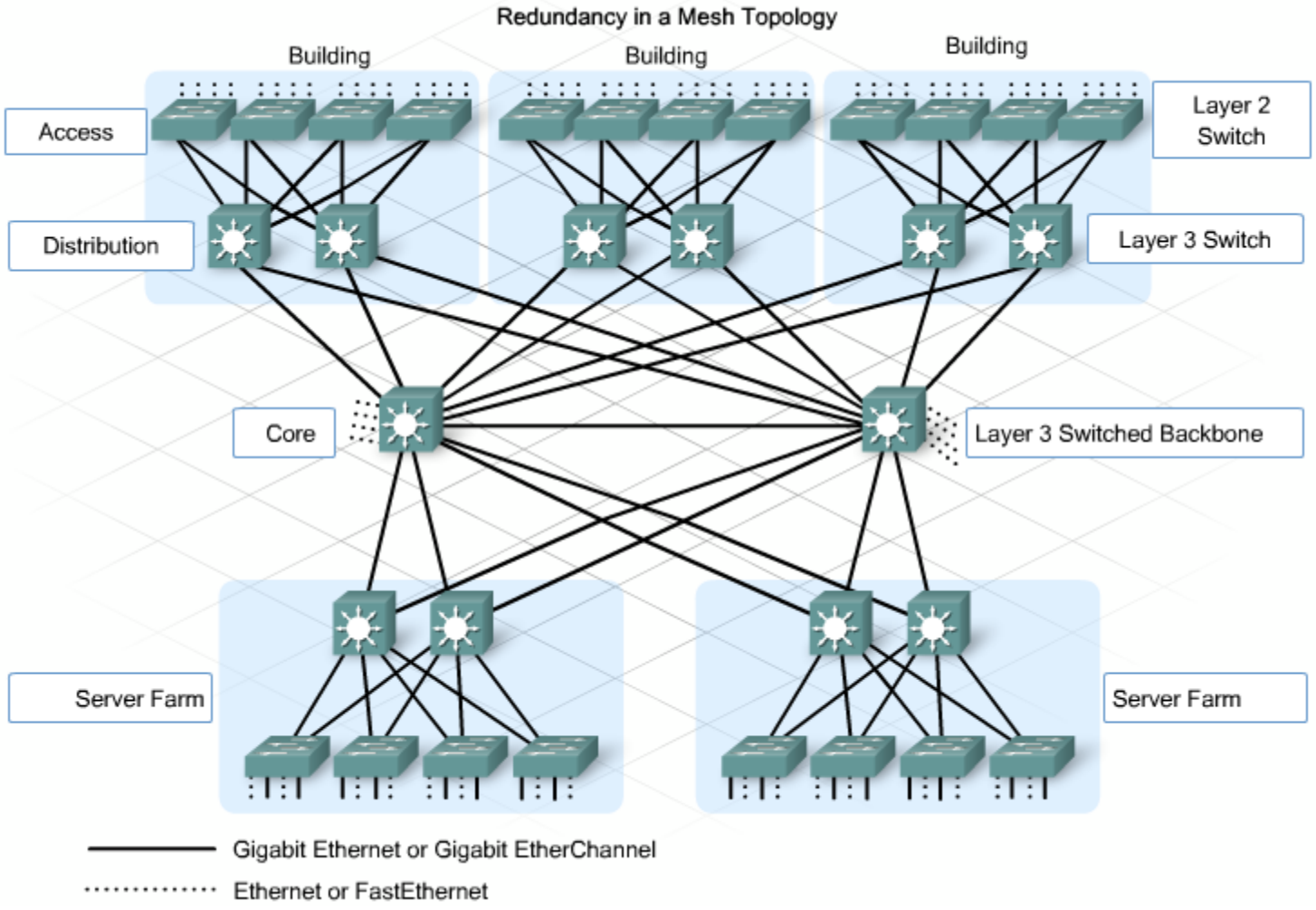
What happens at the Core Layer?

- Goals of the Core Layer
  - The Core Layer design enables the efficient, high-speed transfer of data between one section of the network and another. The primary design goals at the Core Layer are to:
  - Provide 100% uptime
  - Maximize throughput
  - Facilitate network growth

What happens at the Core Layer?

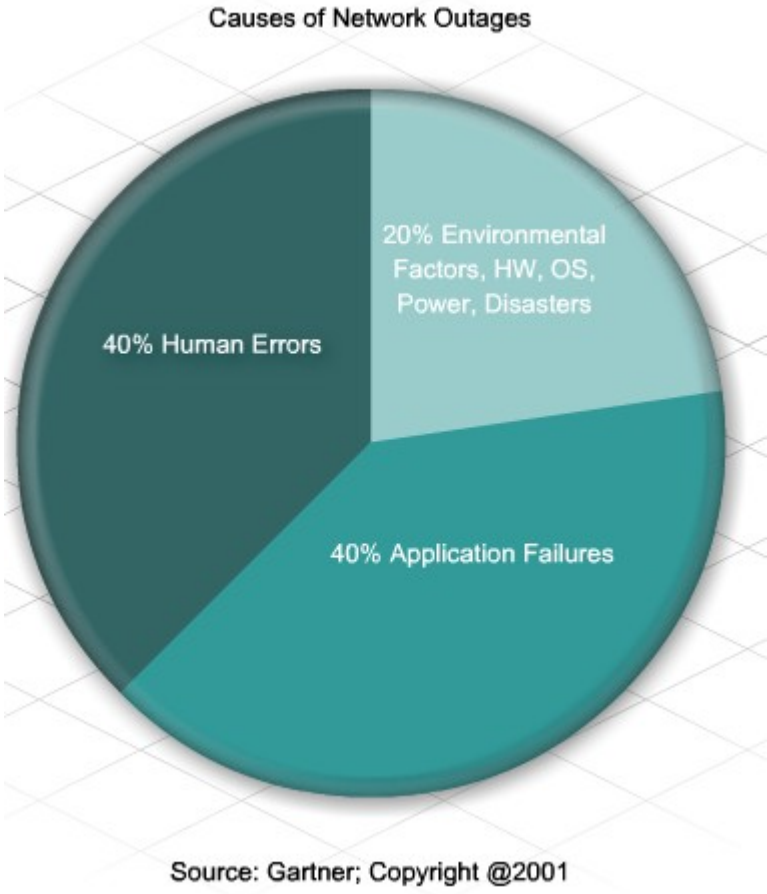
- Core Layer Technologies
  - Technologies used at the Core Layer include:
  - Routers or multilayer switches that combine routing and switching in the same device
  - Redundancy and load balancing
  - High-speed and aggregate links
  - Routing protocols that scale well and converge quickly, such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) protocol

What happens at the Core Layer?



Network Traffic Prioritization

- Preventing Failures
  - The network designer must strive to provide a network that is resistant to failures and can recover quickly in the event of a failure. Core routers and switches can contain:
    - Dual power supplies and fans
    - A modular chassis-based design
    - Additional management modules



Network Traffic Prioritization

- Redundant components increase the cost, but they are usually well worth the investment. Core layer devices should have hot-swappable components whenever possible. Using these components reduces repair time and disruption to network services.
- Larger enterprises often install generators and large UPS devices. These devices prevent minor power outages from causing large-scale network failures.

Network Traffic Prioritization

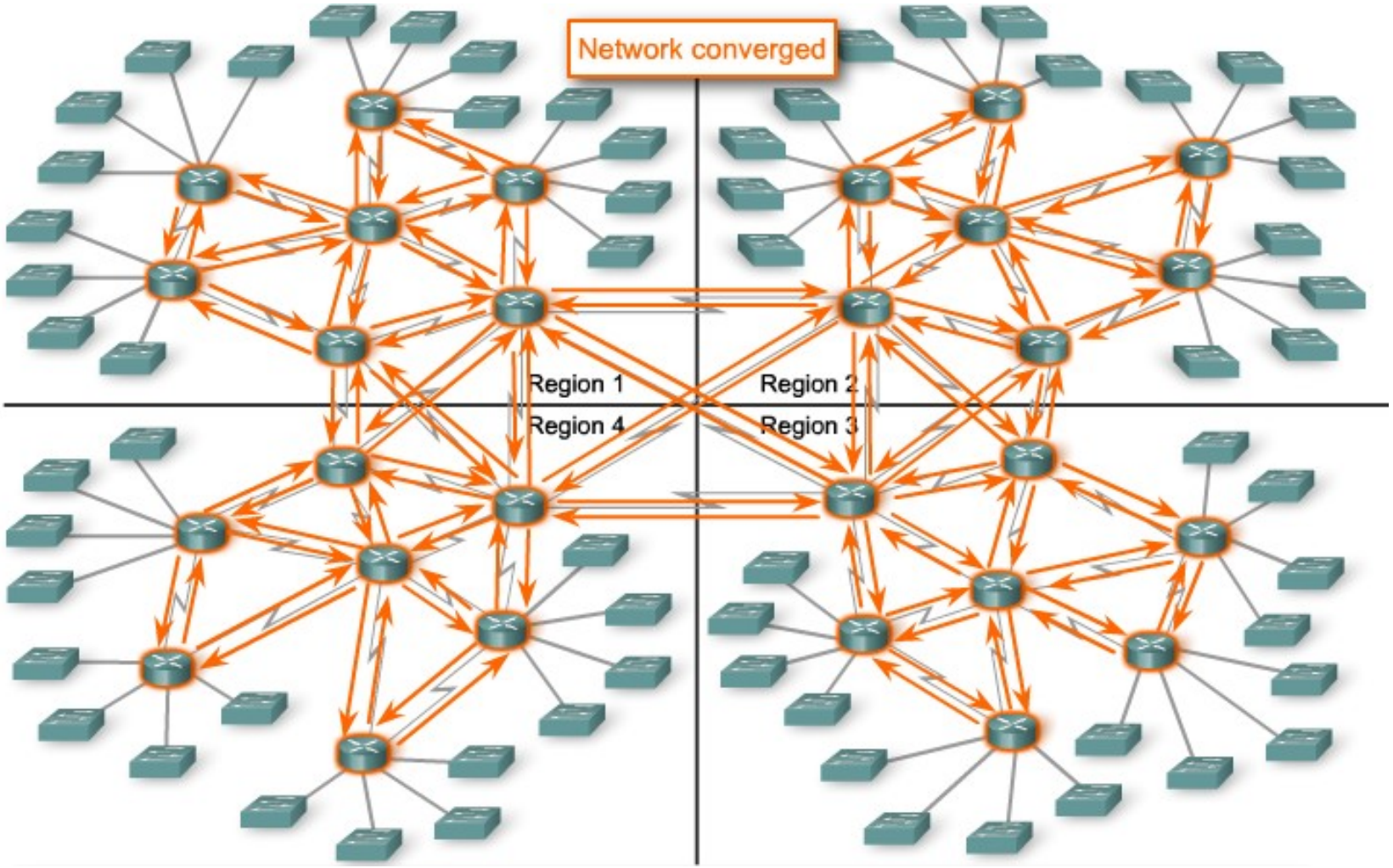
- **Reducing Human Error**
- Human errors contribute to network failures. Unfortunately, the addition of redundant links and equipment cannot eliminate these factors. Many network failures are the result of poorly planned, untested updates or additions of new equipment. Never make a configuration change on a production network without first testing it in a lab environment!
- Failures at the Core Layer cause widespread outages. It is critical to have written policies and procedures in place to govern how changes are approved, tested, installed, and documented. Plan a back-out strategy to return the network to its previous state if changes are not successful.

Network Convergence

Network convergence occurs when all routers have complete and accurate information about the network. The faster the convergence time, the quicker a network can react to a change in topology. Factors that affect convergence time include:

- The speed at which the routing updates reach all of the routers in the network
- The time that it takes each router to perform the calculation to determine the best paths

Network Convergence



Network Convergence

- Selecting a Routing Protocol

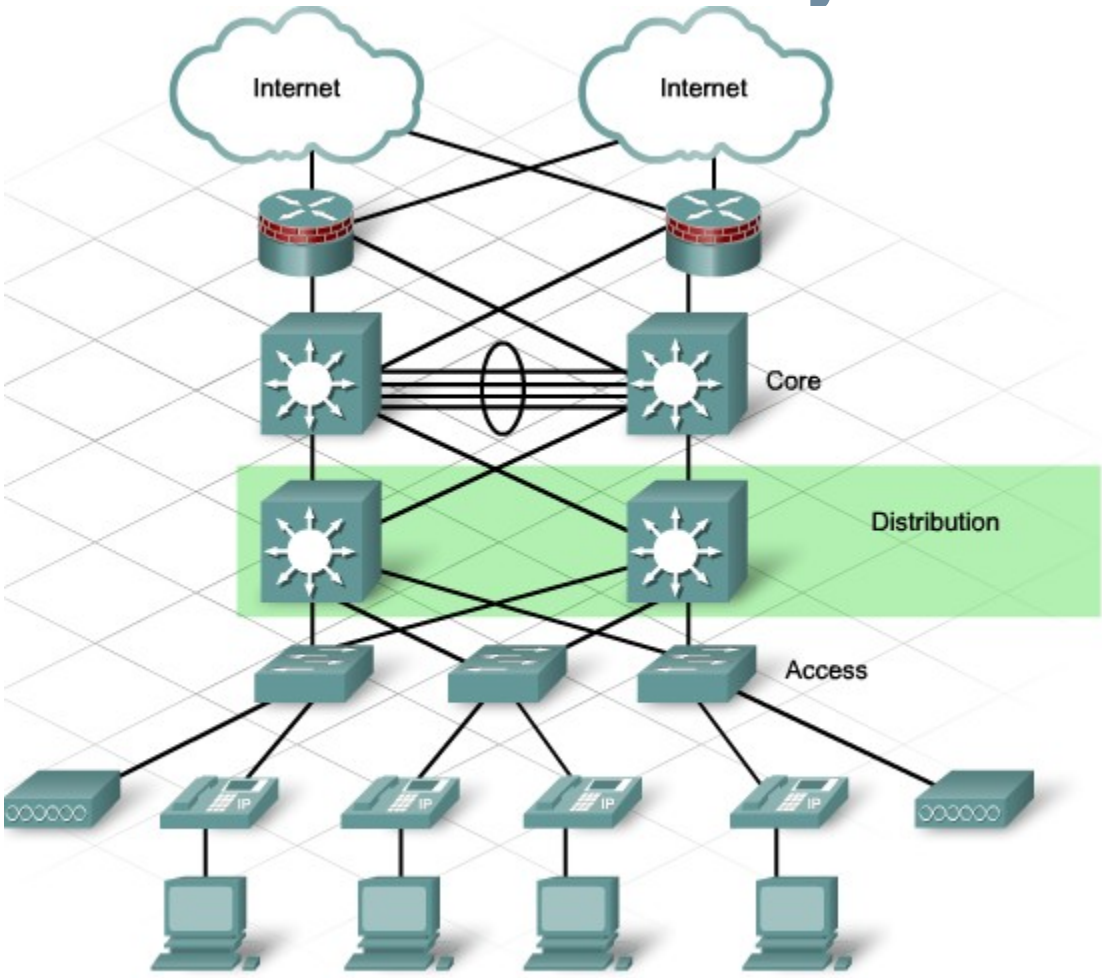
- Most dynamic routing protocols offer acceptable convergence times in small networks. In larger networks, protocols like RIPv2 may converge too slowly to prevent disruption of network services if a link fails. Generally, in a large enterprise network, EIGRP or OSPF provide the most stable routing solution.

Network Convergence

- Design Considerations
- Most networks contain a combination of dynamic and static routes. Network designers need to consider the number of routes required to ensure that all destinations in the network are reachable. Large routing tables can take significant time to converge. The design of network addressing and summarization strategies in all layers affects how well the routing protocol can react to a failure.

What happens at the Distribution Layer?

- The Distribution Layer represents a routing boundary between the Access Layer and the Core Layer. It also serves as a connection point between remote sites and the Core Layer.



What happens at the Distribution Layer?

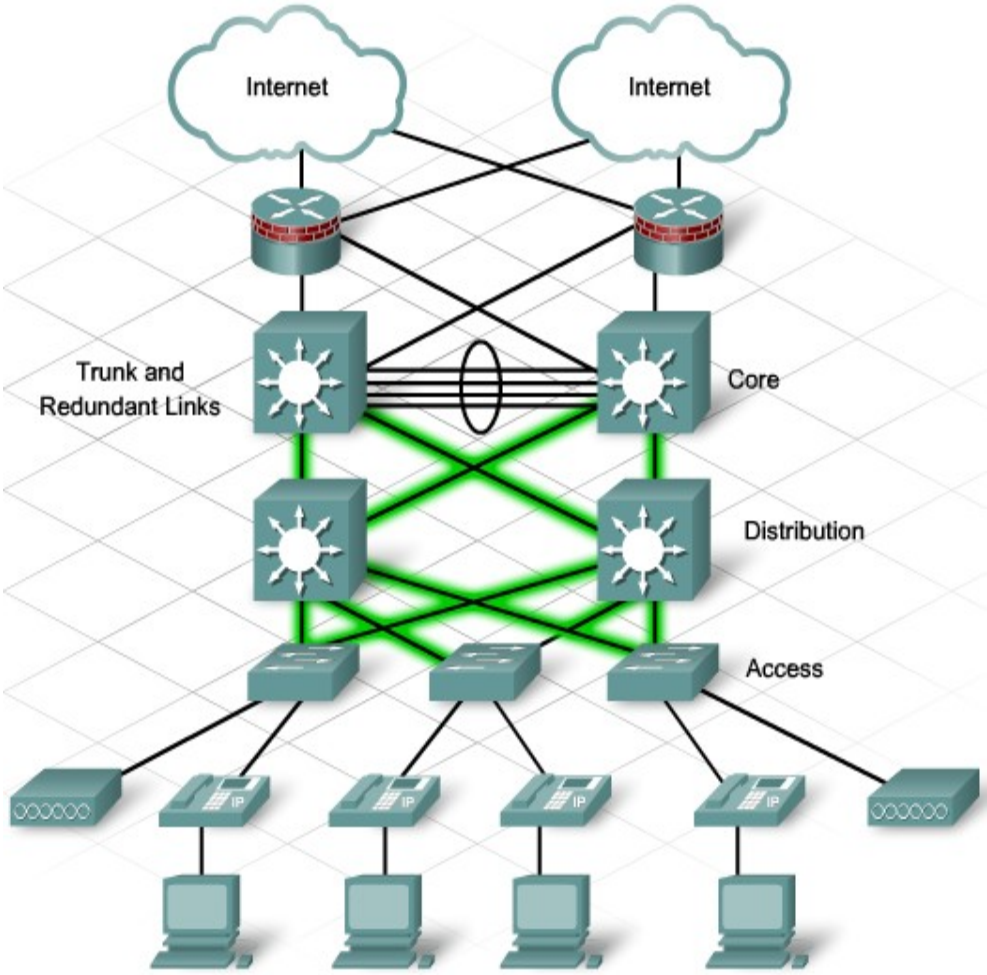
- Distribution Layer Routing
- The Access Layer is commonly built using Layer 2 switching technology. The Distribution Layer is built using Layer 3 devices. Routers or multilayer switches, located at the Distribution Layer, provide many functions that are critical for meeting the goals of the network design.

What happens at the Distribution Layer?

- **These network design goals include:**
- Filtering and managing traffic flows
- Enforcing access control policies
- Summarizing routes before advertising the routes to the Core
- Isolating the Core from Access Layer failures or disruptions
- Routing between Access Layer VLANs

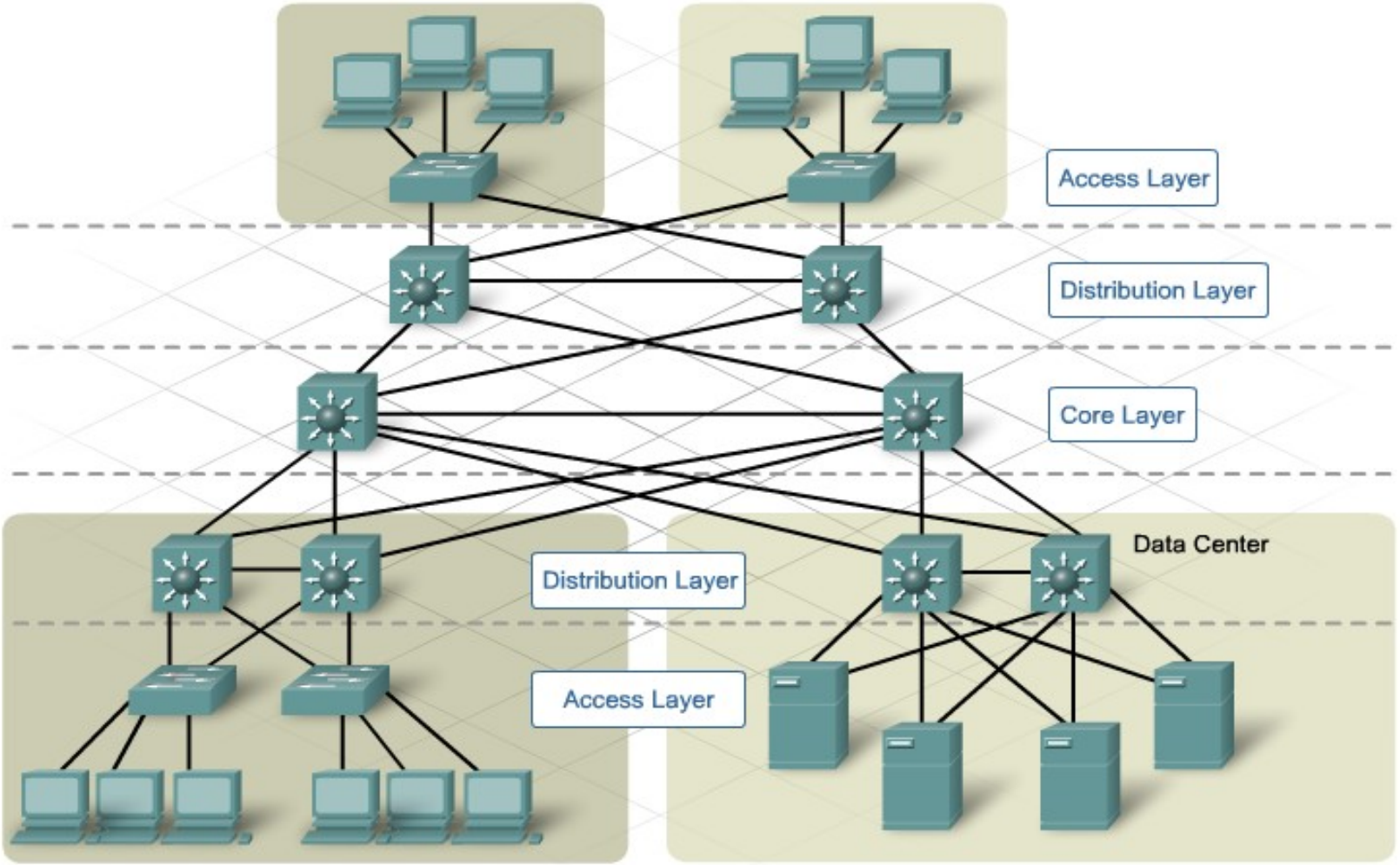
What happens at the Distribution Layer?

- Trunk links are often configured between Access and Distribution Layer networking devices.
- Redundant links exist between devices in the Distribution Layer, the devices can be configured to load balance the traffic across the links.
- Distribution Layer networks are usually wired in a partial mesh topology. This topology provides enough redundant paths to ensure that the network can survive a link or device failure.



Limiting the scope of network failures

A failure domain defines the portion of the network that is affected when either a device or network application fails.



Limiting the scope of network failures

- **Limiting the Size of Failure Domains**
- Because failures at the Core Layer of a network have a large impact, the network designer often concentrates on efforts to prevent failures. These efforts can greatly increase the cost to implement the network. In the hierarchical design model, it is easiest and usually least expensive to control the size of a failure domain in the Distribution Layer. In the Distribution Layer, network errors can be contained to a smaller area, thus affecting fewer users. When using Layer 3 devices at the Distribution Layer, every router functions as a gateway for a limited number of Access Layer users.

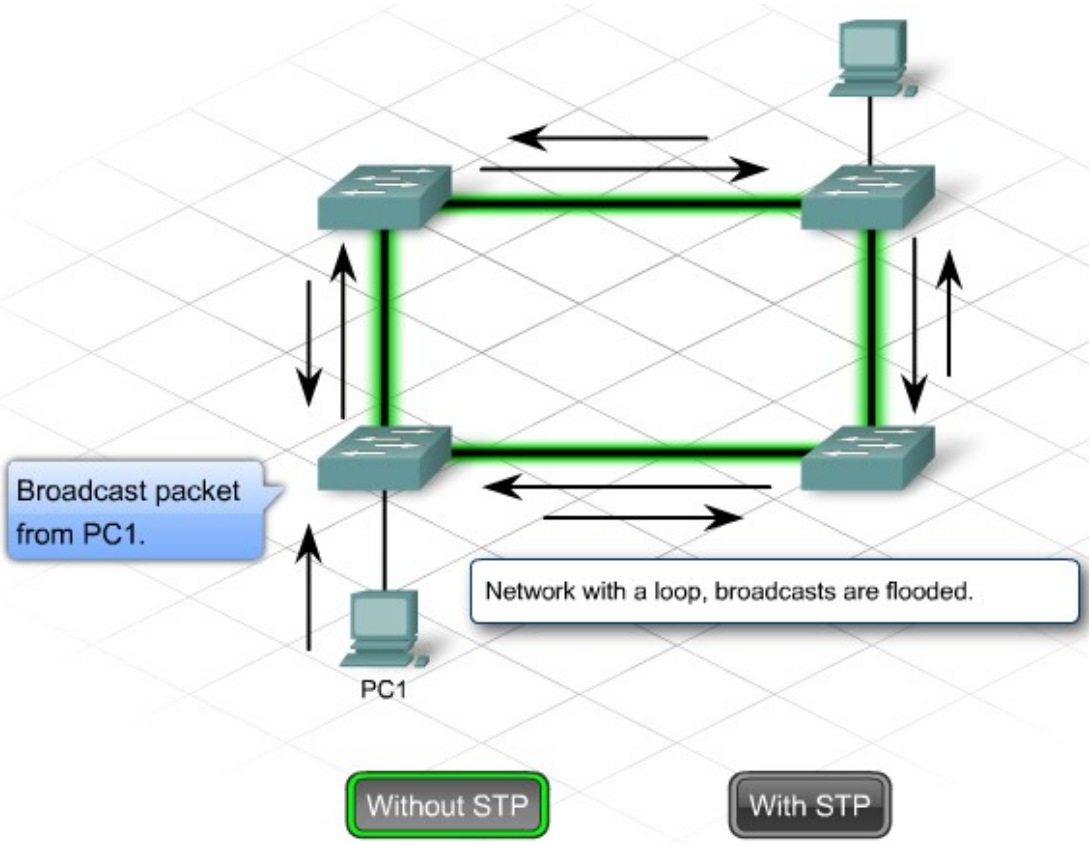
Limiting the scope of network failures

- **Switch Block Deployment**
- Routers, or multilayer switches, are usually deployed in pairs, with Access Layer switches evenly divided between them. This configuration is referred to as a building or departmental switch block. Each switch block acts independently of the others. As a result, the failure of a single device does not cause the network to go down. Even the failure of an entire switch block does not impact a significant number of end users.

Building a redundant Network

Redundancy at the Distribution Layer

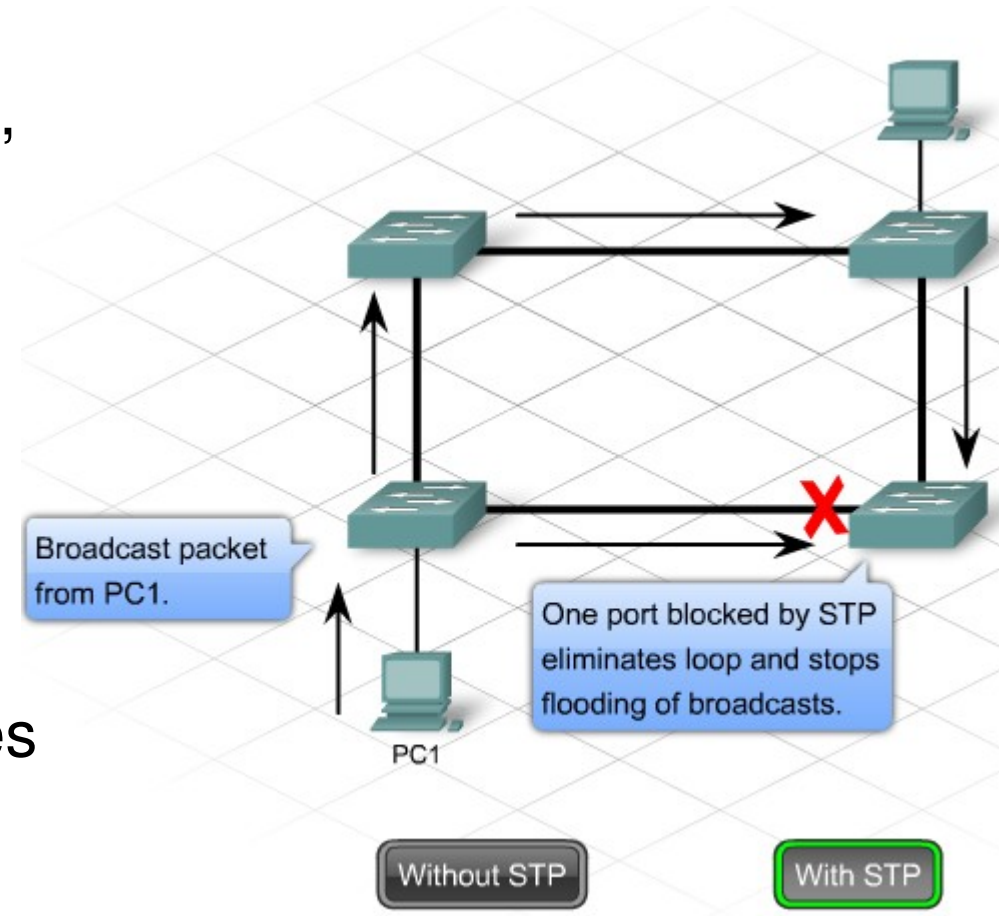
Providing multiple connections to Layer 2 switches can cause unstable behavior in a network unless STP is enabled. Without STP, redundant links in a Layer 2 network can cause broadcast storms. Switches are unable to correctly learn the ports, so traffic ends up being flooded throughout the switch. By disabling one of the links, STP guarantees that only one path is active between two devices.



Building a redundant Network

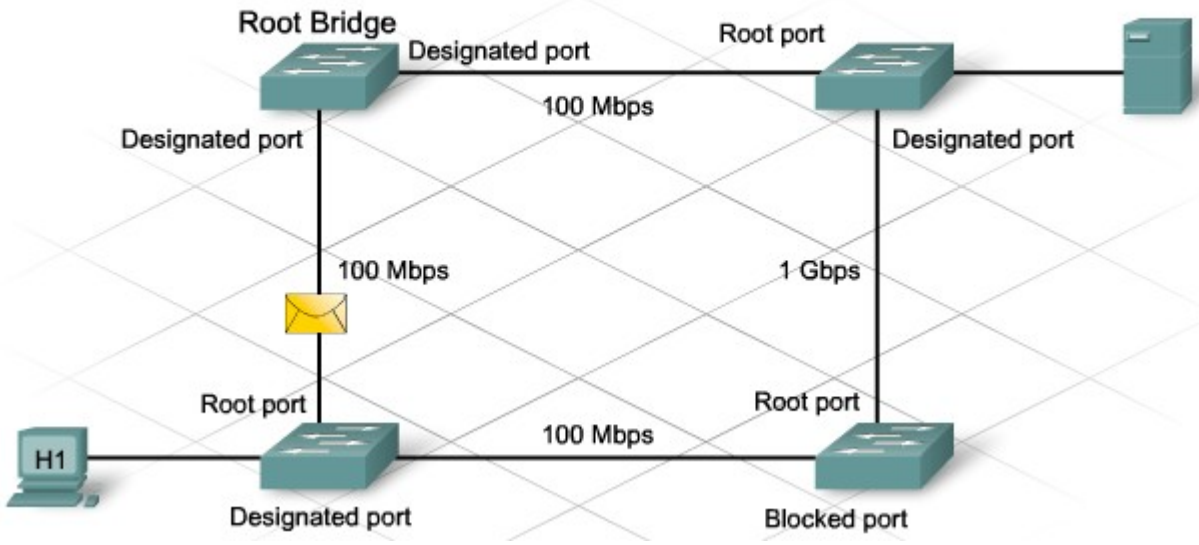
By disabling one of the links, STP guarantees that only one path is active between two devices. If one of the links fails, the switch recalculates the spanning tree topology and automatically begins using the alternate link.

Rapid Spanning Tree Protocol (RSTP), as defined in IEEE 802.1w, builds upon the IEEE 802.1d technology and provides rapid convergence of the spanning tree.



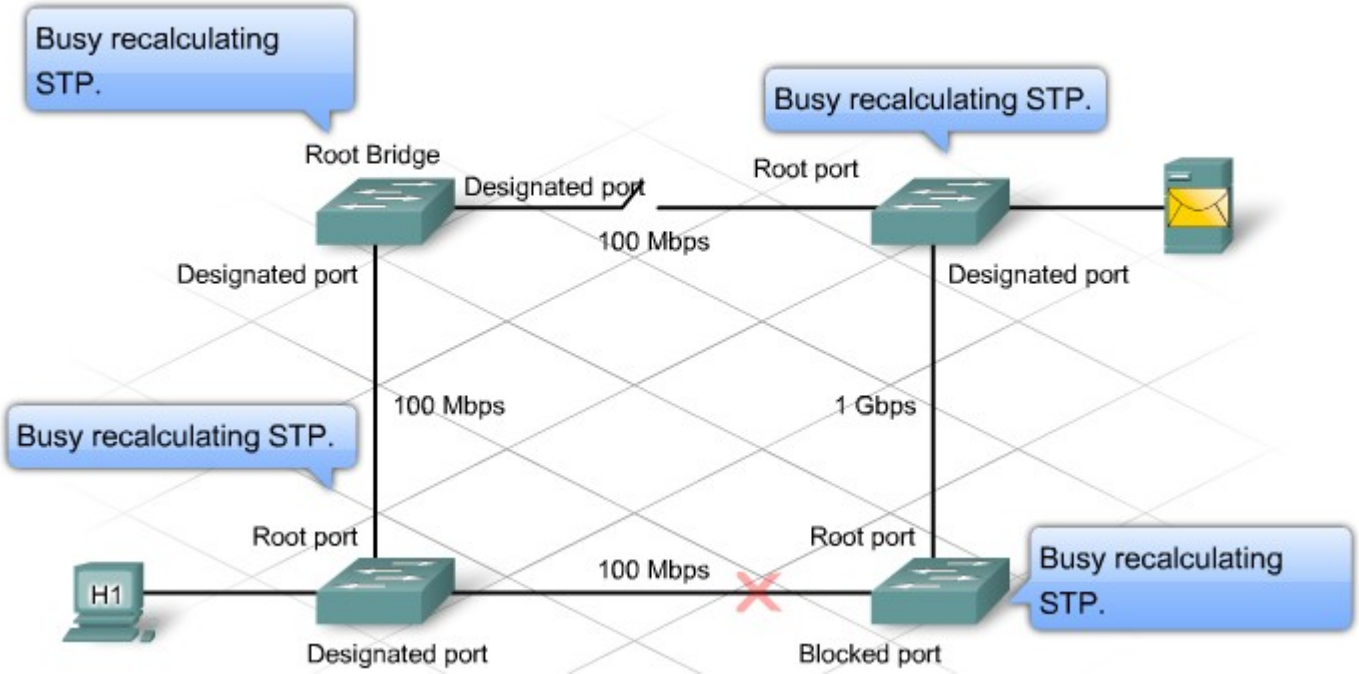
Building a redundant Network

A high volume, enterprise server is connected to a switch port. If that port recalculates because of STP, the server is down for 50 seconds. It would be difficult to imagine the number of transactions lost during that timeframe.



Building a redundant Network

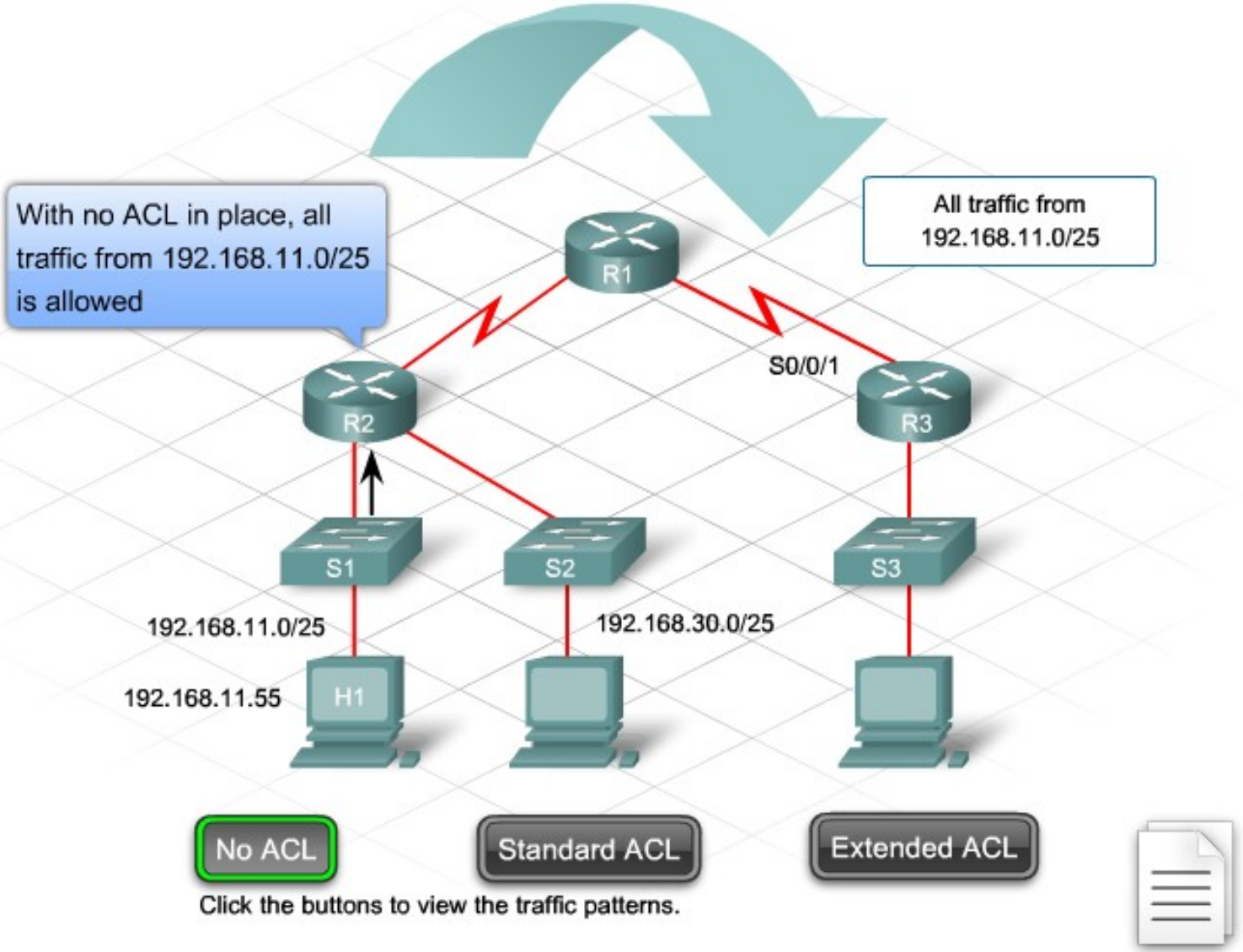
- In a stable network, STP recalculations are infrequent. In an unstable network, it is important to check the switches for stability and configuration changes. One of the most common causes of frequent STP recalculations is a faulty power supply or power feed to a switch. A faulty power supply causes the device to reboot unexpectedly. Controversy



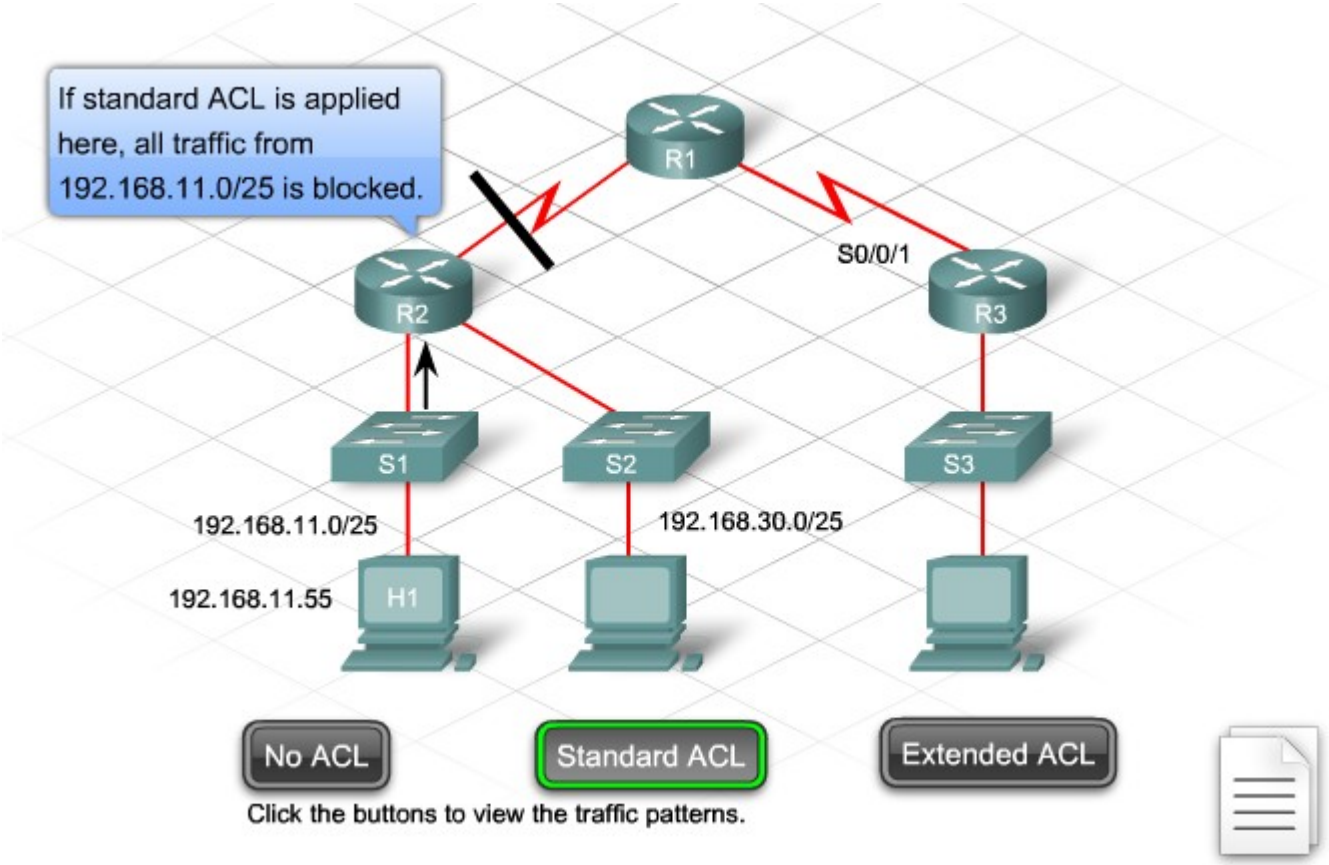
Traffic Filtering at Distribution Layer

- Filtering Network Traffic
- To filter network traffic, the router examines each packet and then either forwards or discards it, based on the conditions specified in the ACL. There are different types of ACLs for different purposes. Standard ACLs filter traffic based on the source address. Extended ACLs can filter based on multiple criteria including:
- Source address
- Destination address
- Protocols
- Port numbers or applications
- Whether the packet is part of an established TCP stream

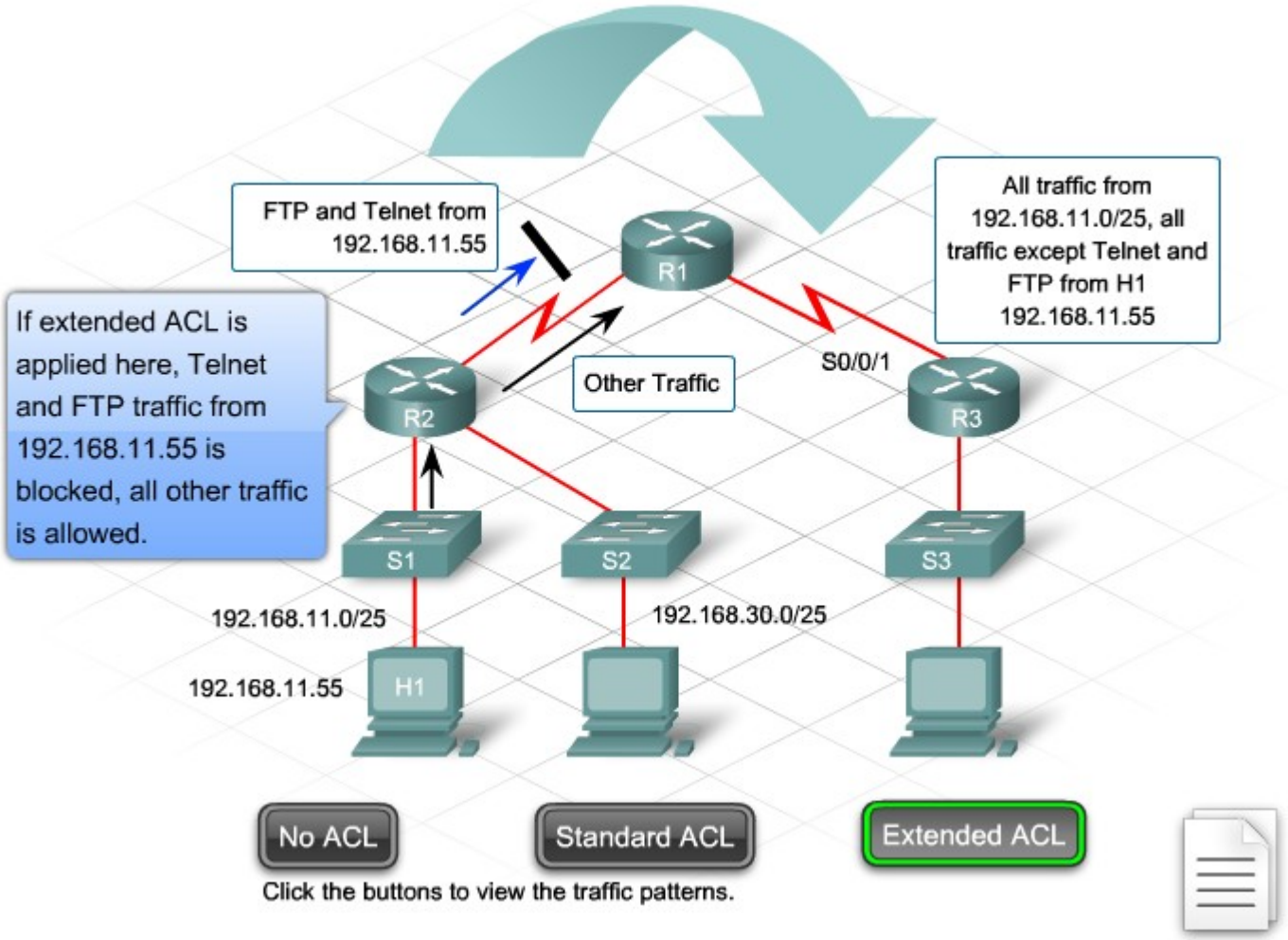
Traffic Filtering at Distribution Layer



Traffic Filtering at Distribution Layer



Traffic Filtering at Distribution Layer



Traffic Filtering at Distribution Layer

- **Complex ACLs**
- Standard and extended ACLs serve as the basis for other, more complex types of ACLs. Using Cisco IOS software, there are three complex ACL features that can be configured: dynamic, reflexive, and time-based.
- **Dynamic ACL** - requires a user to use Telnet to connect to the router and authenticate. Once authenticated, traffic from the user is permitted. Dynamic ACLs are sometimes referred to as "lock and key" because the user is required to login in order to obtain access.

Traffic Filtering at Distribution Layer

- **Reflexive ACL** - allows outbound traffic and then limits inbound traffic to only responses to those permitted requests. This is similar to the established keyword used in extended ACL statements, except that these ACLs can also inspect UDP and ICMP traffic, in addition to TCP.
- **Time-based ACL** - permits and denies specified traffic based on the time of day or day of the week.

Traffic Filtering at Distribution Layer

	A Standard Access List that allows you to permit traffic from 172.16.3.XXX
	A Standard Access List that allows you to deny traffic from 172.16.5.2
	A Standard Access List that allows you to permit traffic from any host
	A Standard Access List that allows you to permit traffic from 172.16.5.5

Traffic Filtering at Distribution Layer

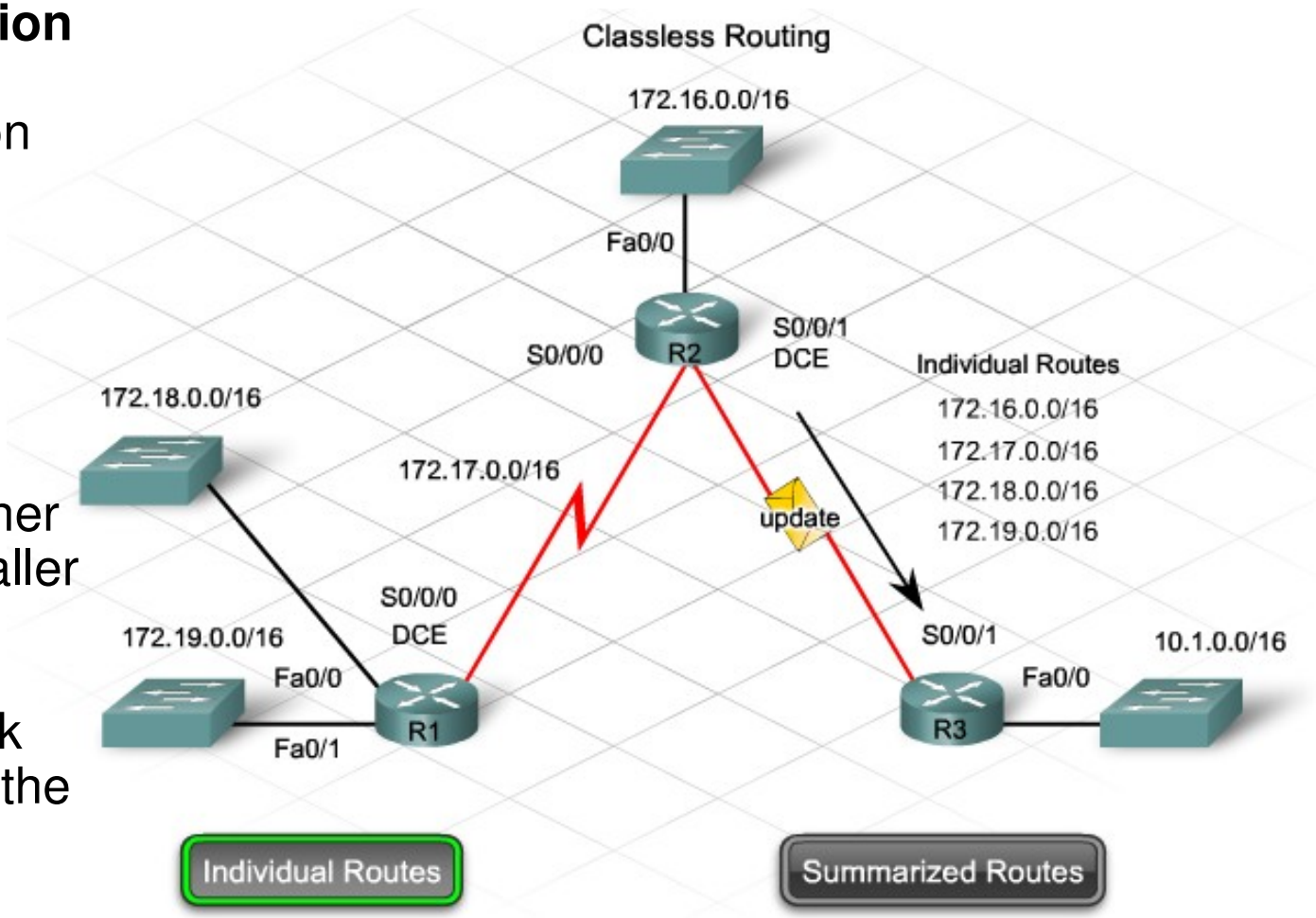
✓ access-list 10 permit 172.16.3.0 0.0.0.255	A Standard Access List that allows you to permit traffic from 172.16.3.XXX
✓ access-list 1 deny 172.16.5.2 0.0.0.0	A Standard Access List that allows you to deny traffic from 172.16.5.2
✓ access-list 10 permit any	A Standard Access List that allows you to permit traffic from any host
✓ access-list 10 permit 172.16.5.5 0.0.0.0	A Standard Access List that allows you to permit traffic from 172.16.5.5

Routing Protocols at the Distribution Layer

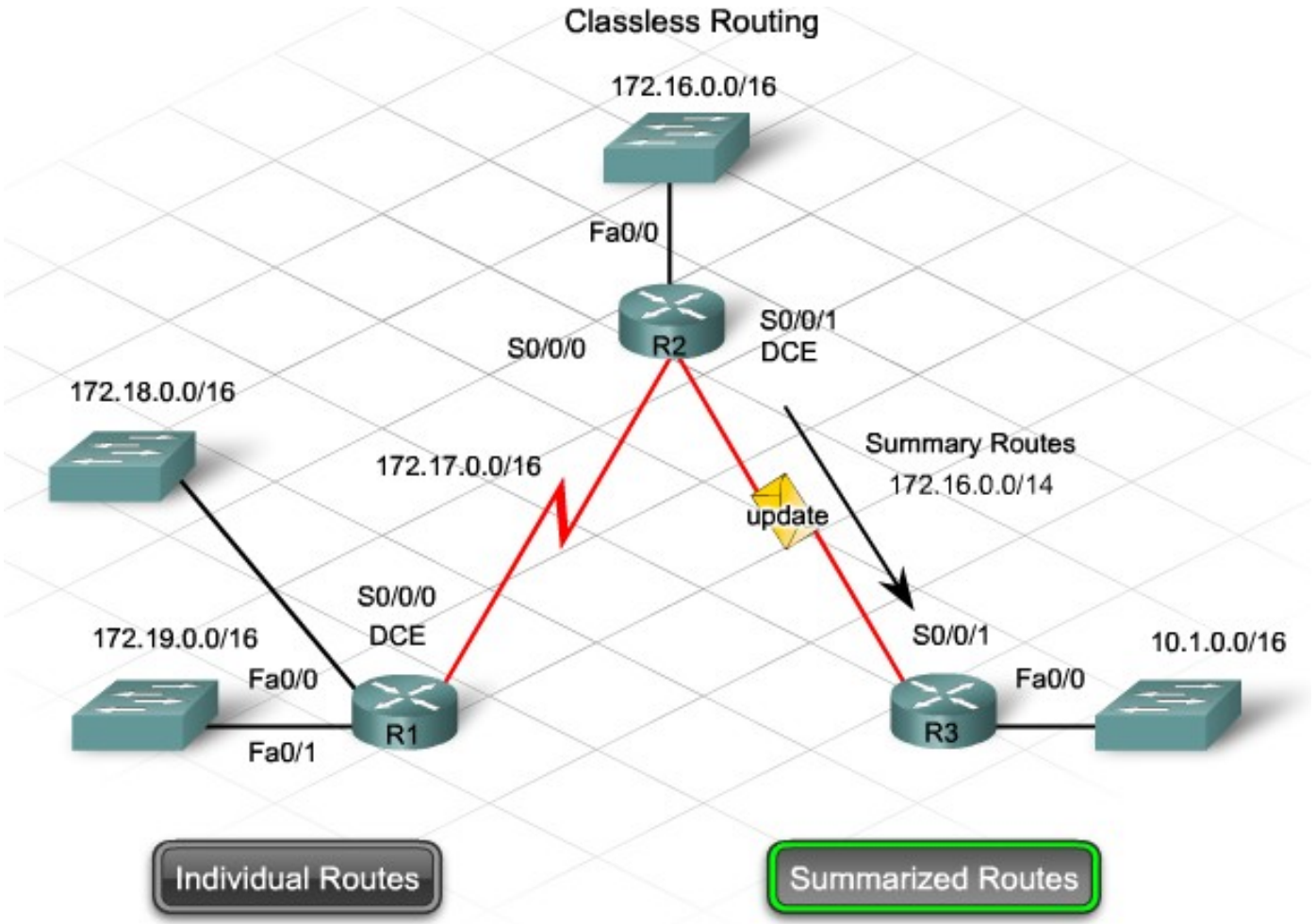
Route Summarization

Route summarization has several advantages for the network, such as:

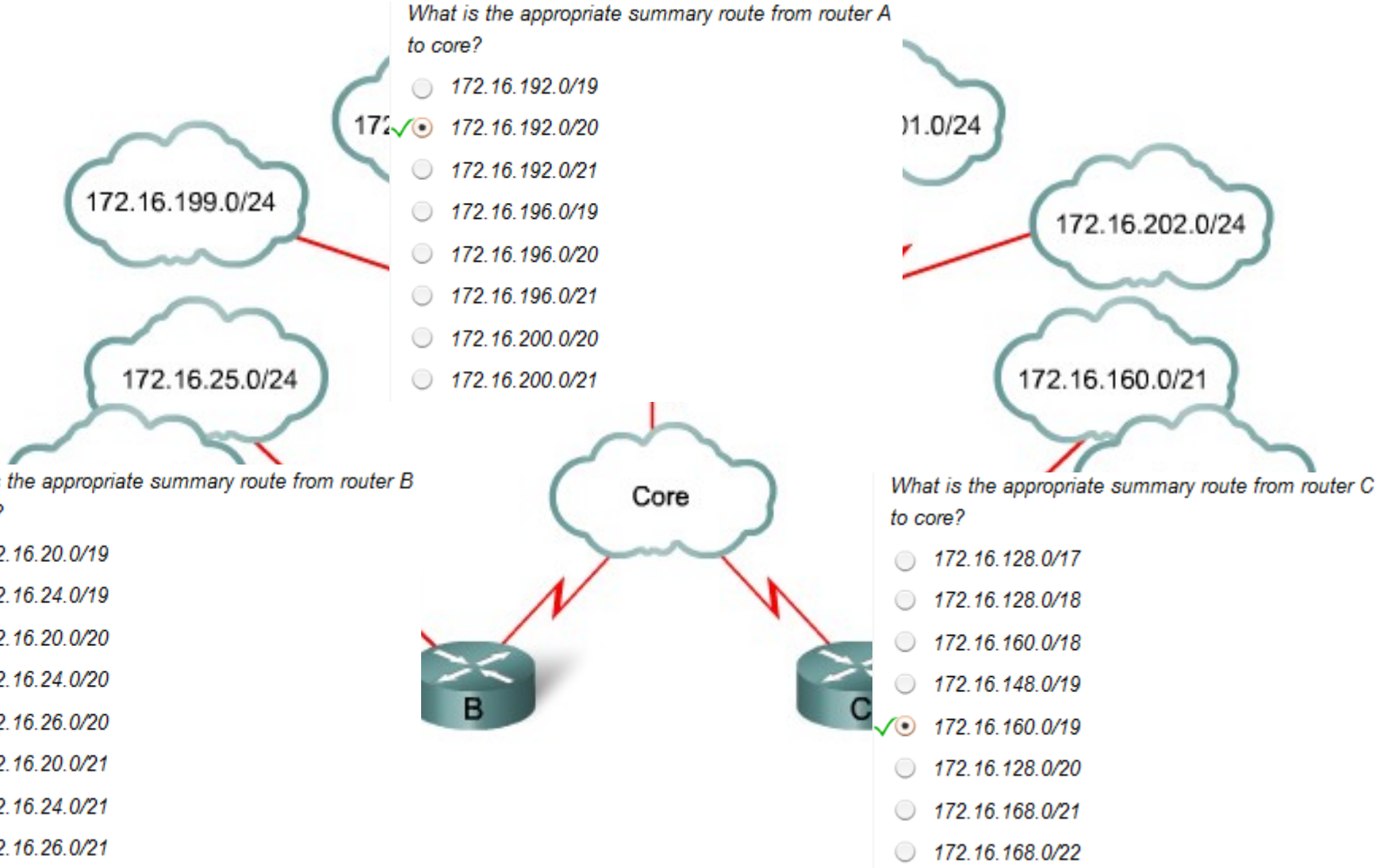
One route in the routing table that represents many other routes, creating smaller routing tables
Less routing update traffic on the network
Lower overhead on the router



Routing Protocols at the Distribution Layer



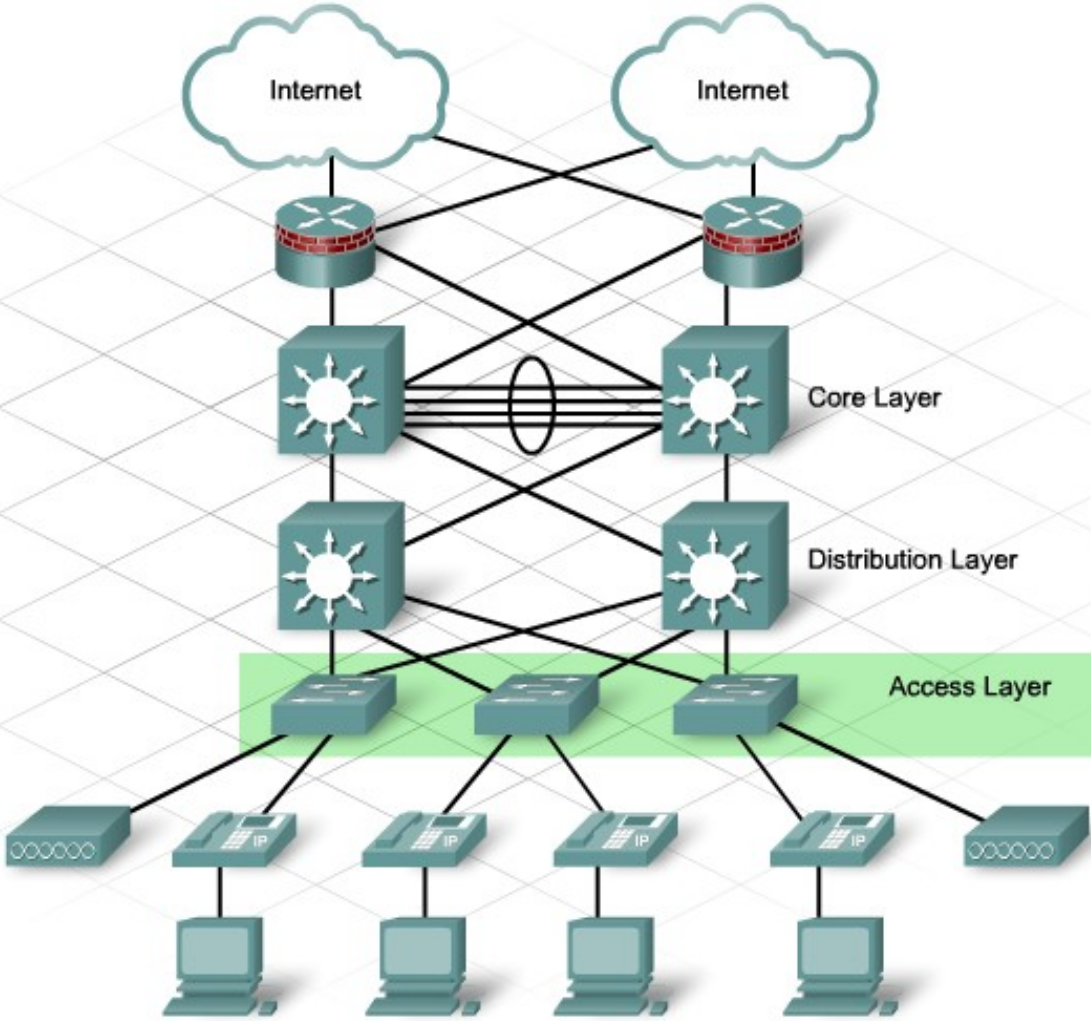
Routing Protocols at the Distribution Layer



What happens at the access layer?

Access Layer Physical Considerations

The Access Layer of the campus infrastructure uses Layer 2 switching technology to provide access into the network. The access can be either through a permanent wired infrastructure or through wireless Access Points. Ethernet over copper wiring poses distance limitations.

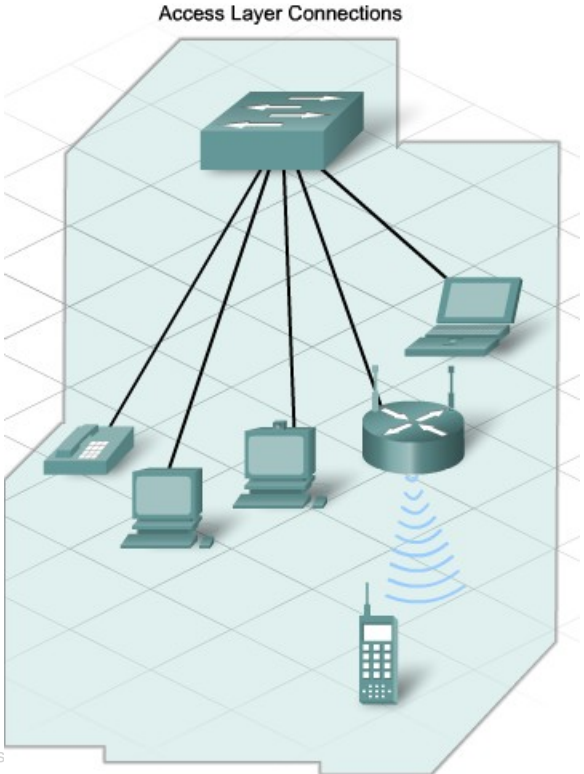


What happens at the access layer?

- **Wiring Closets**
- Wiring closets can be actual closets or small telecommunication rooms that act as the termination point for infrastructure cabling within buildings or within floors of a building. The placement and physical size of the wiring closets depends on network size and expansion plans.
- The wiring closet equipment provides power to end devices such as IP phones and wireless Access Points. Many Access Layer switches have Power-over-Ethernet (PoE) functionality.

What happens at the access layer?

- The Impact of Converged Networking
- The modern computer network consists of more than just personal computers and printers connecting to the Access Layer. Many different devices can connect to an IP network, including:
- IP telephones
- Video cameras
- Video conferencing systems

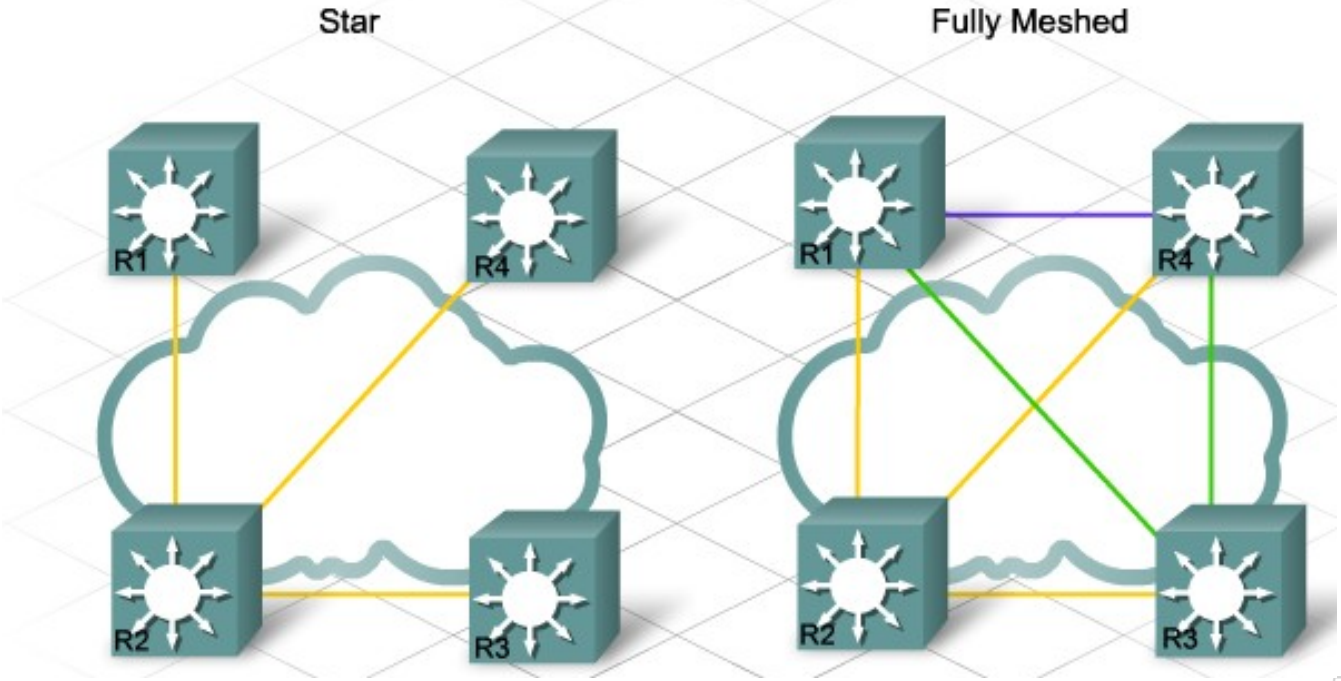


What happens at the access layer?

- Access Layer Management
- Improving the manageability of the Access Layer is a major concern for the network designer.
- Access Layer management is crucial due to:
  - The increase in the number and types of devices connecting at the Access Layer
  - The introduction of wireless access points into the LAN
  - Designing for Manageability
- In addition to providing basic connectivity at the Access Layer, the designer needs to consider:
  - Naming structures
  - VLAN architecture
  - Traffic patterns
  - Prioritization strategies

Network Topologies at Access Layer
Diagram View

Most recent Ethernet networks use a star topology, which is sometimes called a hub and spoke topology. In a star topology, each end device has a direct connection to a single networking device. This single networking device is usually a Layer 2 or multilayer switch.



Network Topologies at Access Layer

- **The disadvantages of a star topology are significant:**
- The central device represents a single point of failure.
- The capabilities of the central device can limit overall performance for access to the network.
- The topology does not recover in the event of a failure when there are no redundant links.
- **Ethernet star topologies usually have a combination of the following wiring:**
- Twisted pair wiring to connect to the individual end devices
- Fiber to interconnect the access switches to the Distribution Layer devices

Network Topologies at Access Layer
Photo View

Star

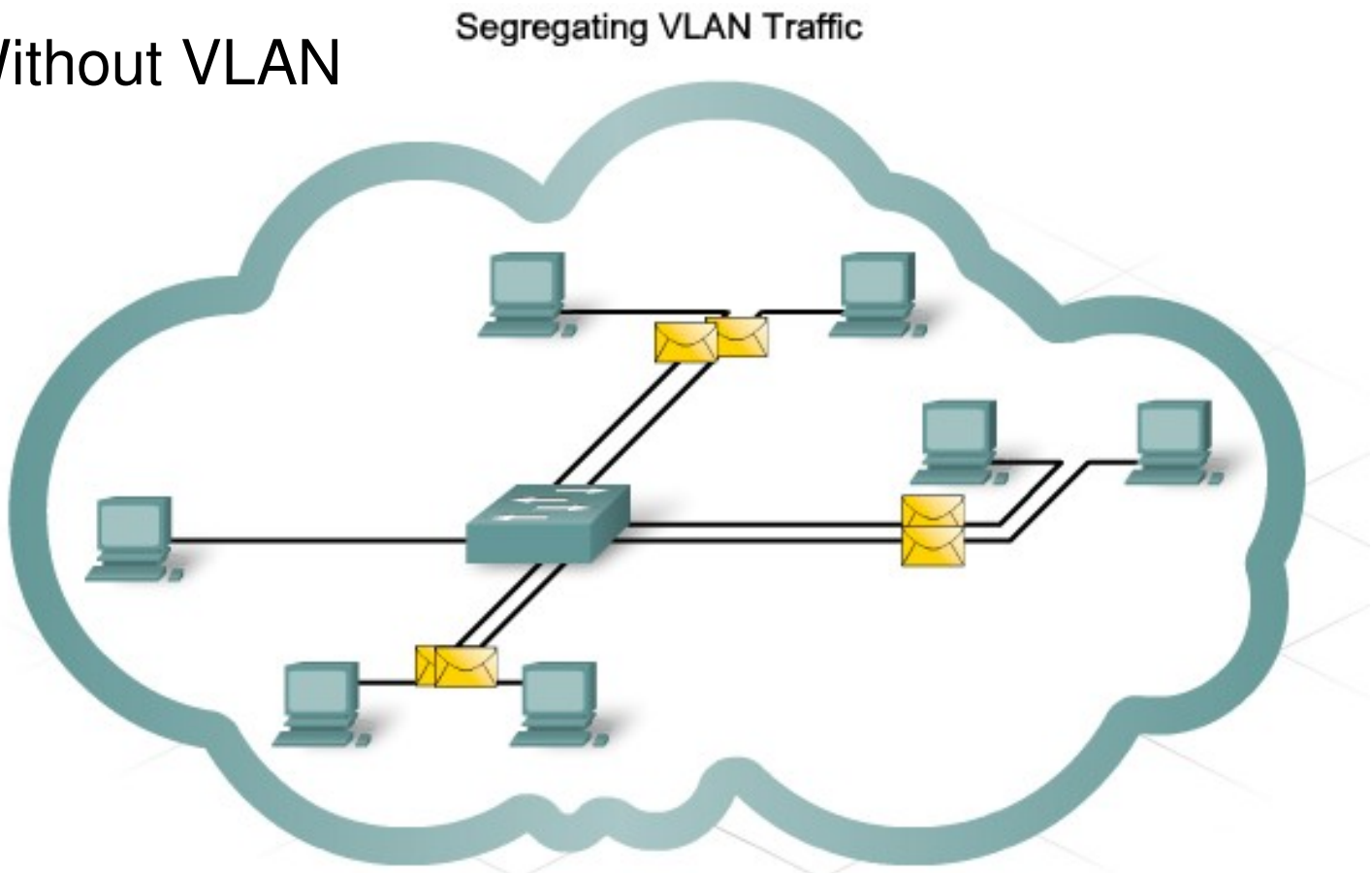
Fully Meshed

How VLANs Segregate Traffic?

- Using VLANs and IP subnets is the most common method for segregating user groups and traffic within the Access Layer network.
- VLANs in the Past
- With the introduction of Layer 2 switching, VLANs were used to create end-to-end workgroup networks. The networks connected across buildings or even across the entire infrastructure. End-to-end VLANs are no longer used in this way. The increased number of users and the volume of network traffic that these users generate is too high to be supported.

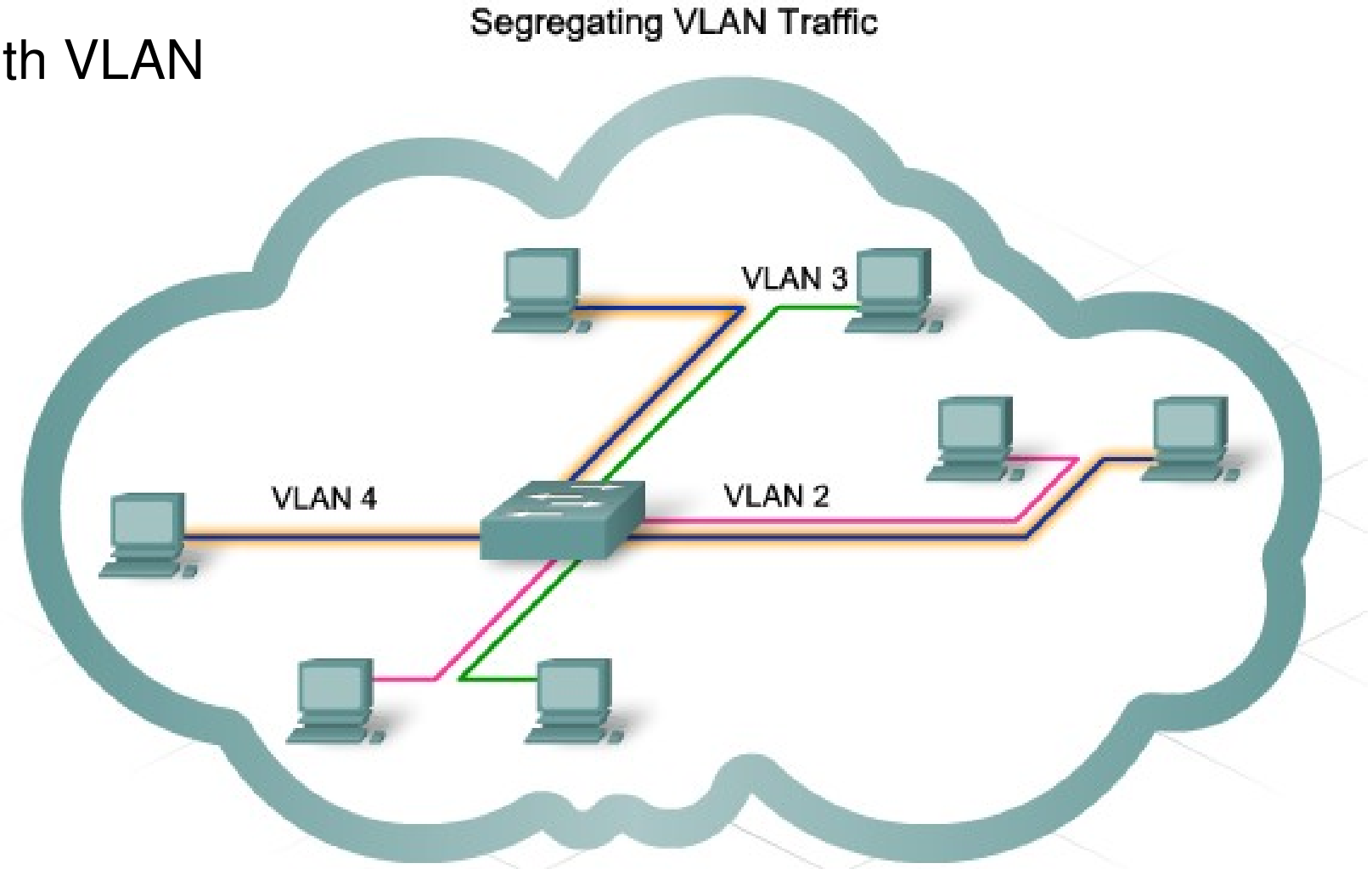
How VLANs Segregate and Control Network Traffic?

Without VLAN



How VLANs Segregate and Control Network Traffic?

With VLAN



How VLANs Segregate and Control Network Traffic?

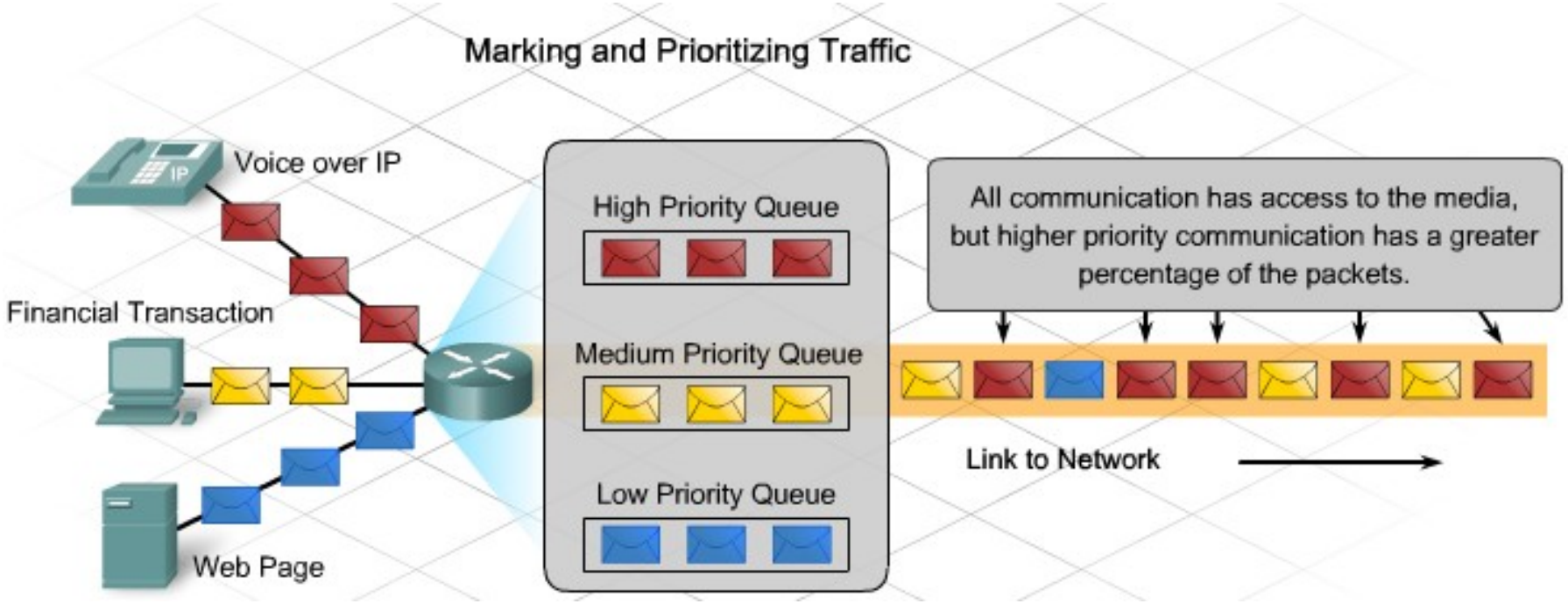
- **VLANs Now**
- Today VLANs are used to separate and classify traffic streams and to control broadcast traffic within a single wiring closet or building. Although large VLANs that span entire networks are no longer recommended, they may be required to support special applications, such as wireless roaming and wireless IP phones.
- The recommended approach is to contain VLANs within a single wiring closet. This approach increases the number of VLANs in a network, which also increases the number of individual IP subnets.

Services at the Network Edge

Providing Quality of Service to Network Applications
Networks must provide secure, predictable, measurable and, at times, guaranteed services. Networks also need mechanisms to control congestion when traffic increases. Congestion is caused when the demand on the network resources exceeds the available capacity.

All networks have limited resources. For this reason, networks need QoS mechanisms. The ability to provide QoS depends on traffic classification and the assigned priority.

Services at the Network Edge



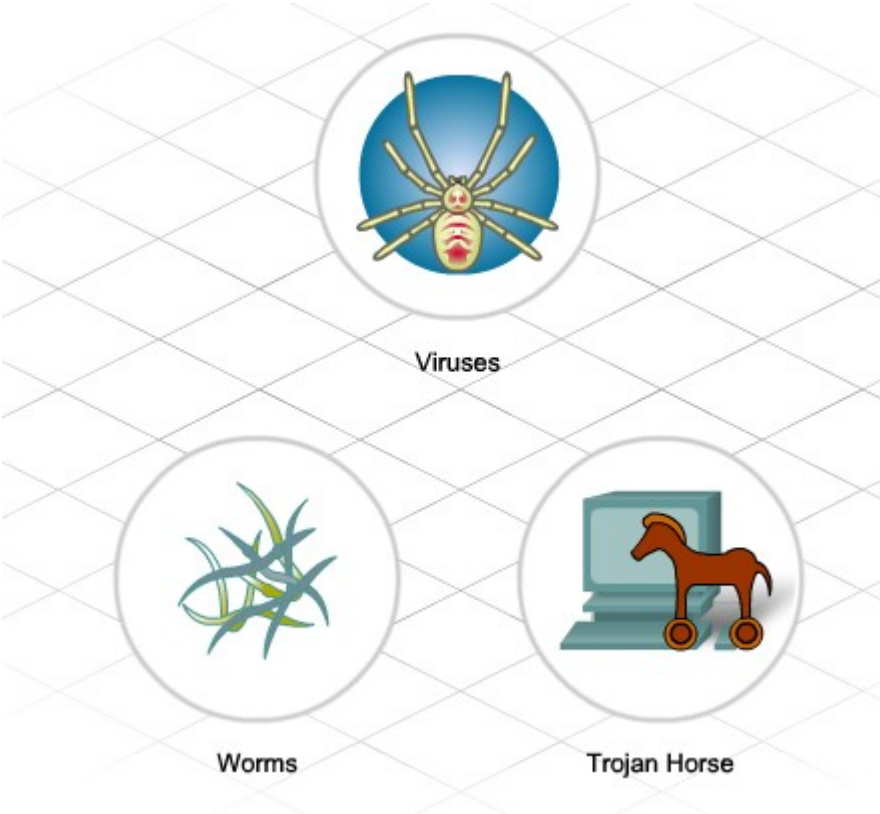
Services at the Network Edge

- Classification
- Before designing QoS strategies, it is necessary to classify applications based on specific delivery requirements. Classifying data at or near the source enables the data to be assigned the appropriate priority as it moves through the entire network. Segregating traffic with similar characteristics into classes, and then marking that traffic, is a function of the network devices at the Access and Distribution Layers. An example of this strategy is to place the voice traffic on an access switch into a single VLAN. The device then marks the traffic originating from the voice VLAN with the highest priority.

Security at the Network Edge

Security Risks at the Access Layer

Many of the security risks that occur at the Access Layer of the network are the result of poorly-secured end devices. User error and carelessness account for a significant number of network security breaches.



Security at the Network Edge

- **How Can the Network Designer Improve Security?**
- Providing adequate security for end devices may not be in the scope of a network design project. Nevertheless, the designer needs to understand the network impact of a security incident, such as a worm or a trojan, at an end device. The designer can then better determine what network security measures to put in place to limit the effects on the network.
- Permitting network access to only known or authenticated devices limits the ability of intruders to enter the network. It is important to apply wireless security measures that follow recommended practices.

Security Measures

- **Providing Physical Security**
- Physical security of a network is very important. Most network intruders gain physical entry at the Access Layer. On some network devices, like routers and switches, physical access can provide the opportunity to change passwords and obtain full access to devices.
- Obvious measures, like locking wiring closets and restricting access to networking devices, are often the most effective ways to prevent security breaches.

Security Measures

In high risk or easily accessible areas, it may be necessary to equip wiring closets with additional security, such as cameras or motion detection devices and alarms.

Security Measures

- **Securing Access Layer Networking Devices**
- The simple measures below can provide additional security to networking devices at the Access Layer:
- Setting strong passwords
- Using SSH to administer devices
- Disabling unused ports
- Switch port security and network access control can ensure that only known and trusted devices have access to the network.

Security Measures

- **Recommended Practice on Security**
- Security risks cannot be eliminated or prevented completely. Effective risk management and assessment can significantly minimize the existing security risks. When considering security measures, it is important to understand that no single product can make an organization secure. True network security comes from a combination of products, services, and procedures as well as a thorough security policy and a commitment to adhere to that policy.

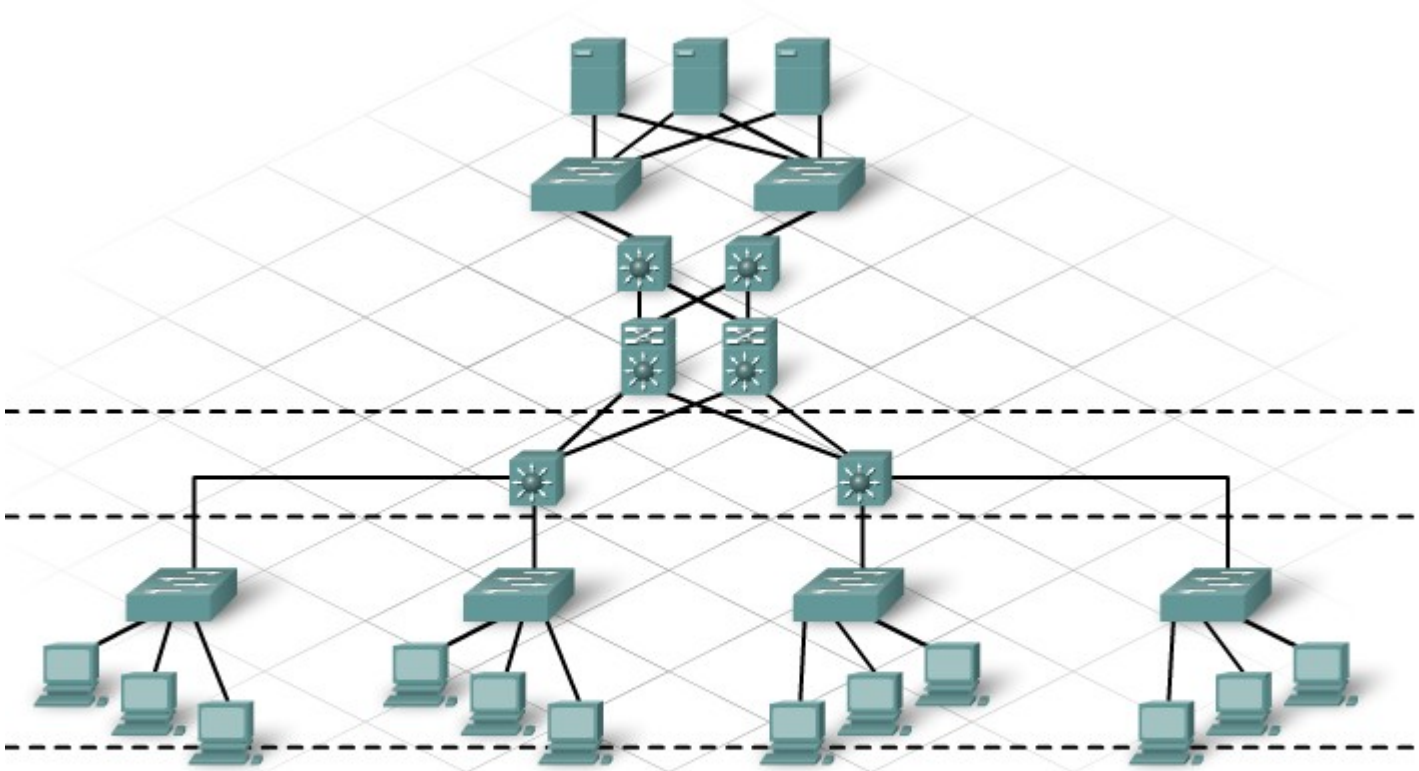
What is a server farm?

- Most enterprise networks provide users with Internet-accessible services, like email and e-commerce. The availability and security of these services is crucial to the success of a business.
- Managing and securing numerous distributed servers at various locations within a business network is difficult. Recommended practice centralizes servers in server farms. Server farms are typically located in computer rooms and data centers.

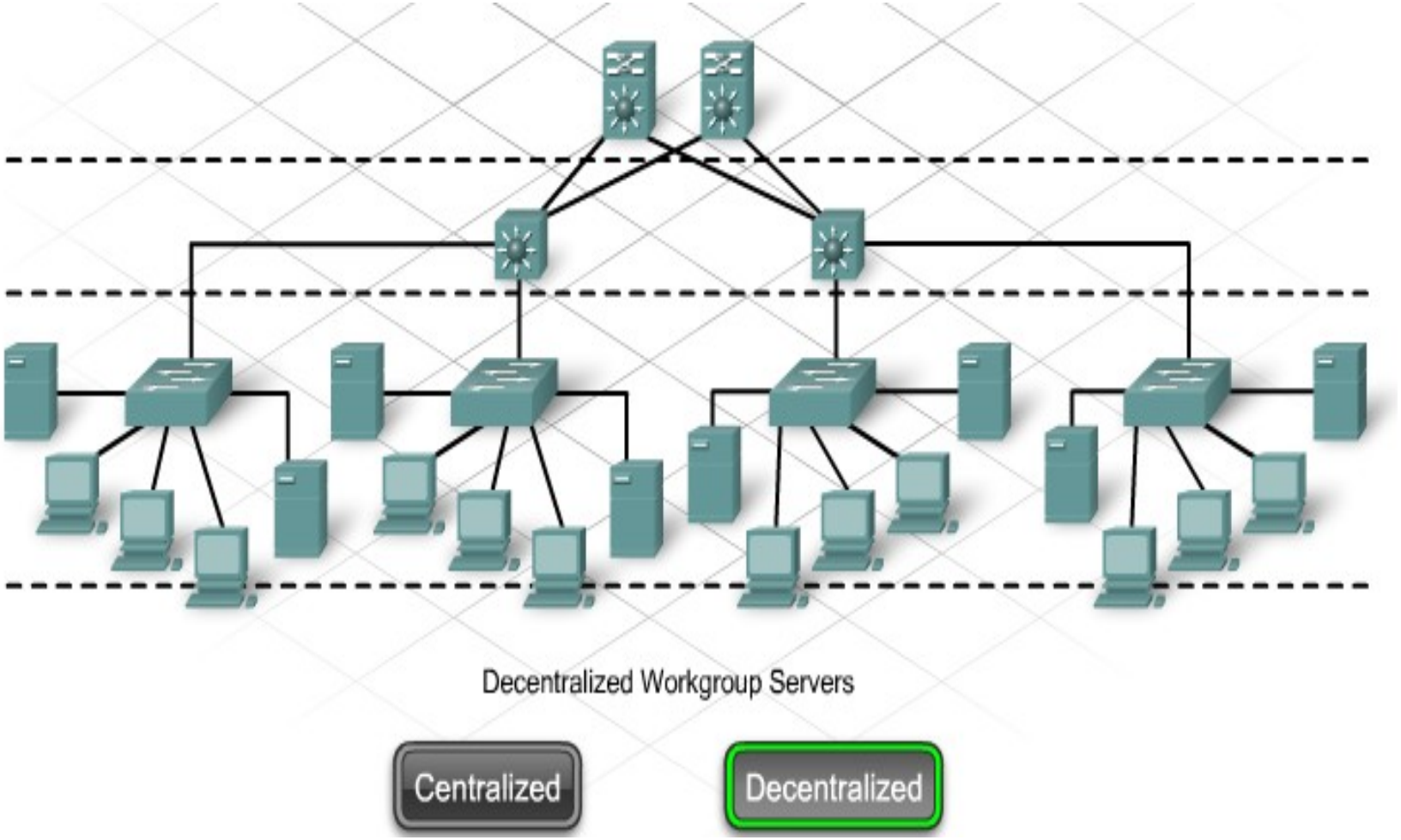
What is a server farm?

- Creating a server farm has the following benefits:
- Network traffic enters and leaves the server farm at a defined point. This arrangement makes it easier to secure, filter, and prioritize traffic.
- Redundant, high-capacity links can be installed to the servers as well as between the server farm network and the main LAN.
- Load balancing and failover can be provided between servers and between networking devices.
- The number of high-capacity switches and security devices is reduced, helping to lower the cost of providing services

What is a server farm?



What is a server farm?



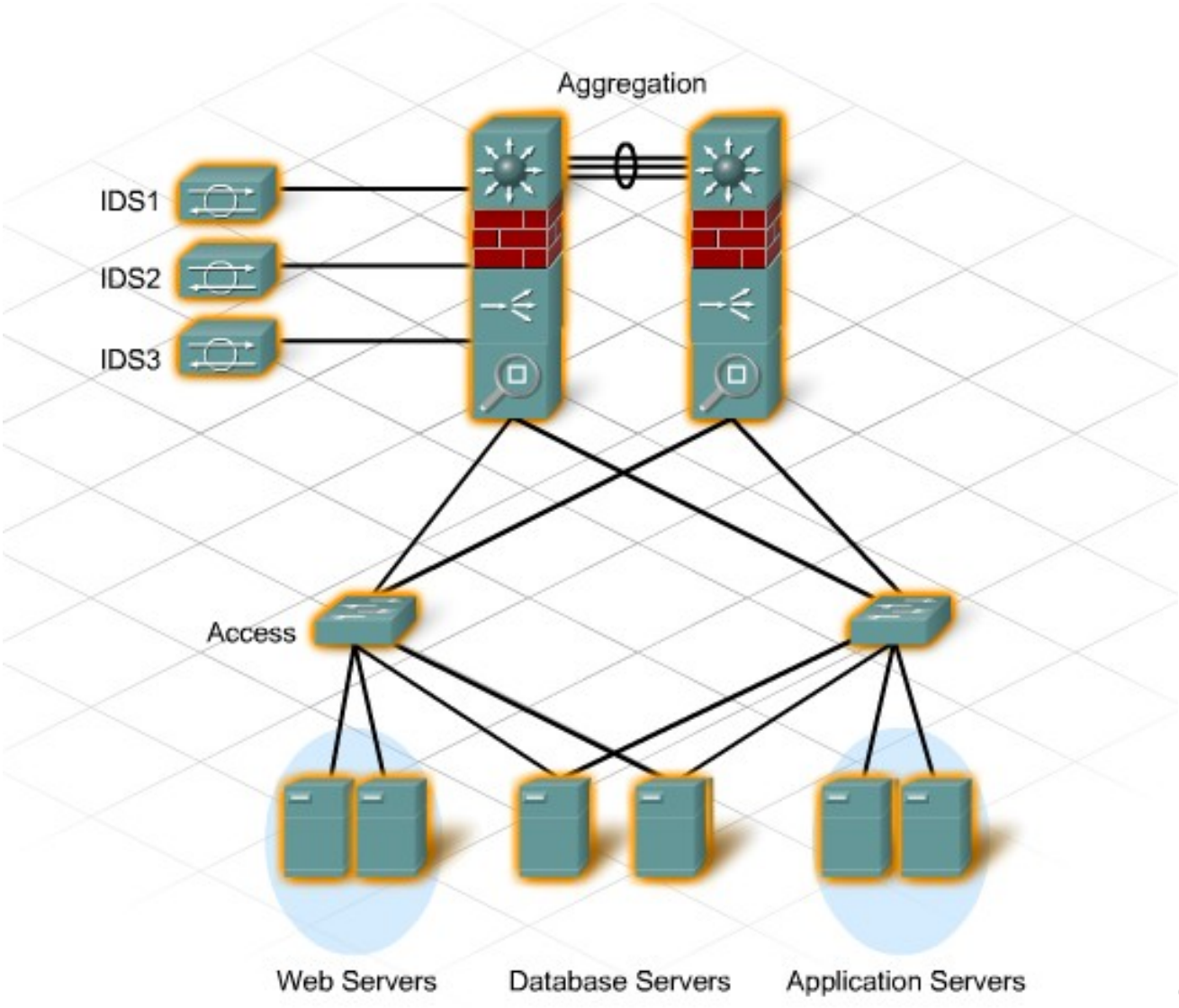
Security, Firewalls and DMZs

- Data center servers can be the target of malicious attacks and must be protected.
- Attacks against server farms can result in lost business for e-commerce and business-to-business applications as well as information theft. Both local area networks (LANs) and storage area networks (SANs) must be secured to reduce the chances of such attacks. Hackers use a variety of tools to inspect networks and to launch intrusion and denial of service (DoS) attacks.

Security, Firewalls and DMZs

- Protecting Server Farms Against Attack
- Firewalls are often deployed to provide a basic level of security when internal and external users attempt to access the Internet via the server farm. Following network products that can be deployed in a server farm:
- Firewalls
- LAN switch security features
- Host-based and network-based intrusion detection and prevention systems
- Load balancers
- Network analysis and management devices

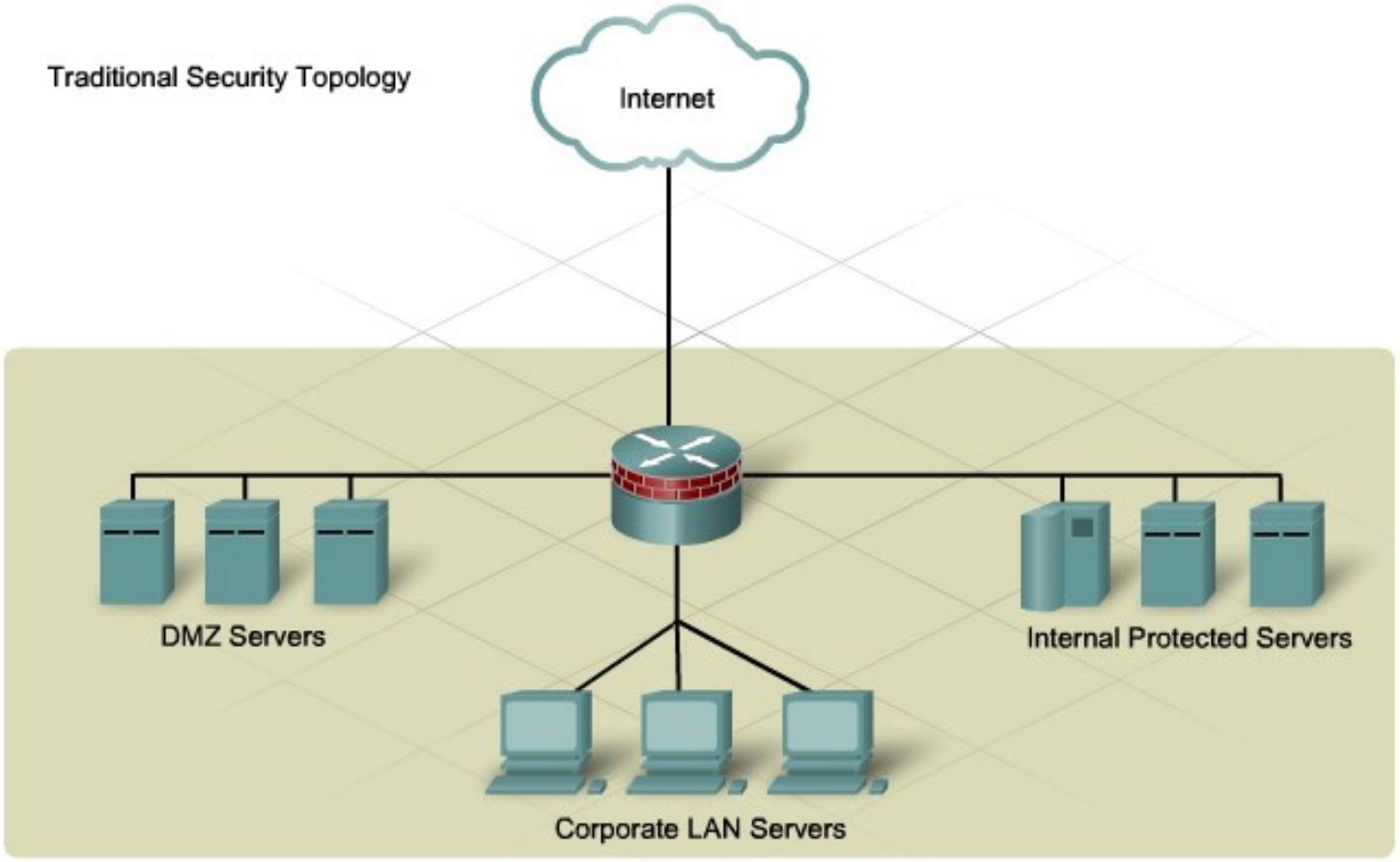
Security, Firewalls and DMZs



Security, Firewalls and DMZs

- **Demilitarized Zones**
- In the traditional network firewall design, servers that needed to be accessed from external networks were located on a demilitarized zone (DMZ). Users accessing these servers from the Internet or other untrusted external networks were prevented from seeing resources located on the internal LAN. LAN users were treated as trusted users and usually had few restrictions imposed when they accessed servers on the DMZ.

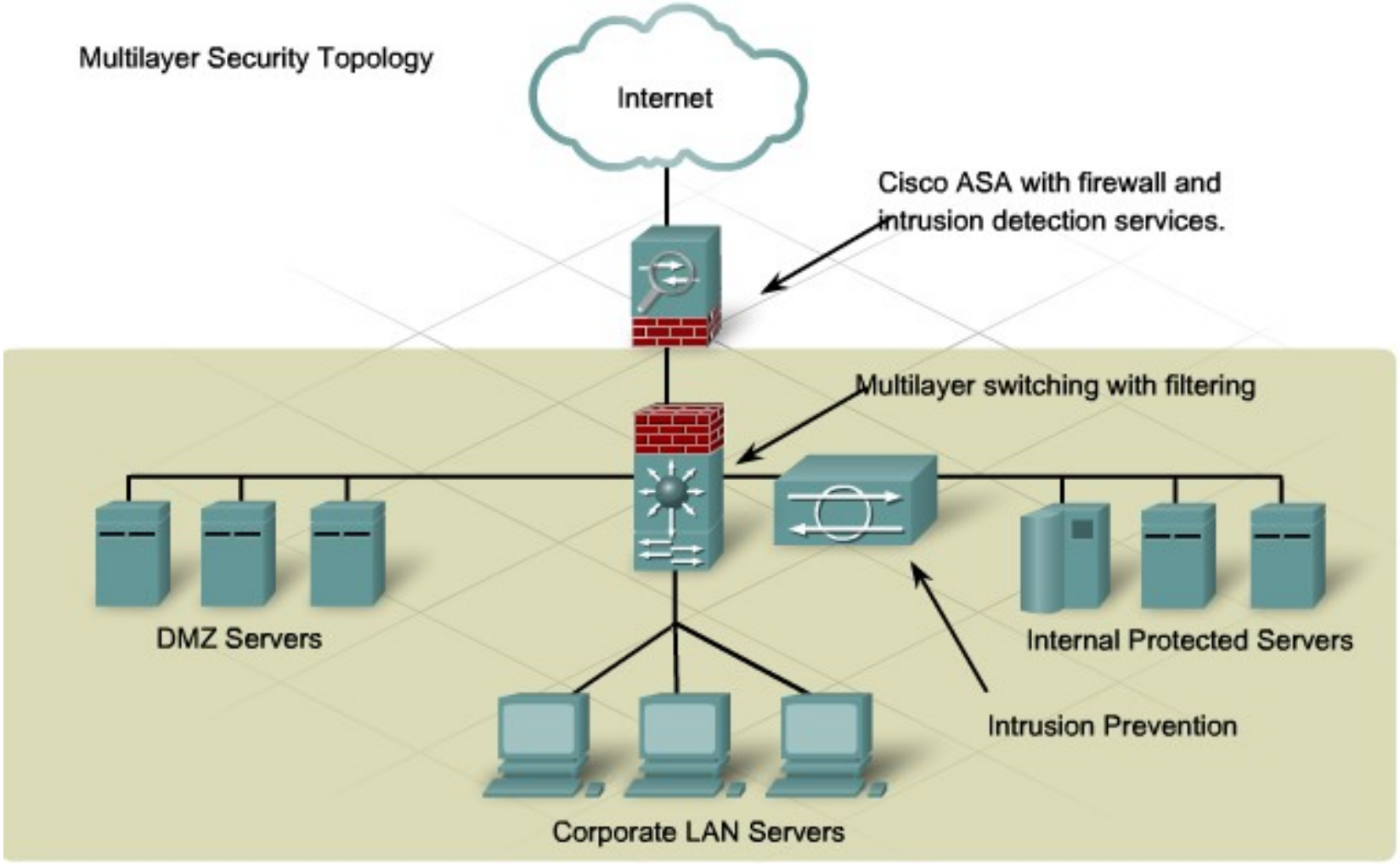
Security, Firewalls and DMZs



Security, Firewalls and DMZs

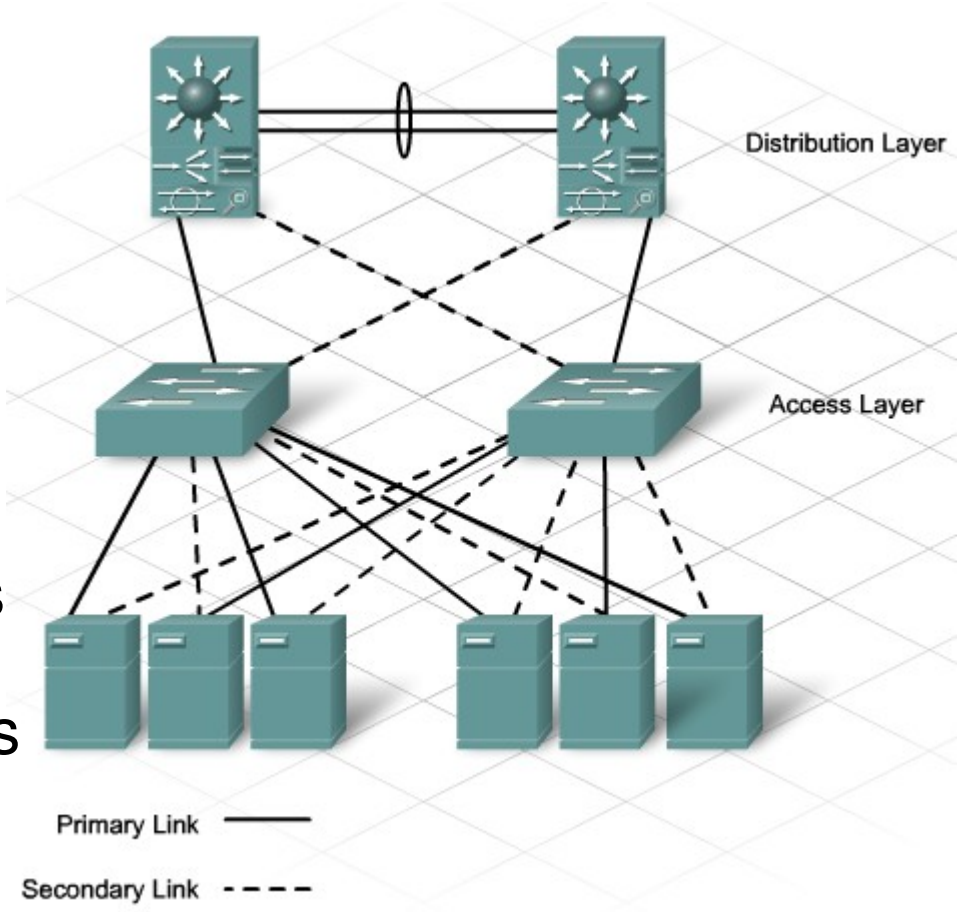
- Protecting Against Internal Attacks
- Attacks originating on the internal network are now more common than attacks from external sources. As a result, the design of server farm security is different from the older DMZ model. A layer of firewall features and intrusion protection is required between the servers and the internal networks, as well as between the servers and the external users. An additional security layer between the servers may also be required.
- The sensitivity of data stored on the servers and contained in the transactions traveling the network determines the appropriate security policy for the design of the server farm.

Security, Firewalls and DMZs



Providing High Availability

In addition to providing an extra layer of security, server farms are usually required to provide high availability for network applications and services. A highly available network is one that eliminates or reduces the potential impact of failures. This protection enables the network to meet requirements for access to applications, systems, and data from anywhere, at any time.



Providing High Availability

- Building in Redundancy
- To achieve high availability, servers are redundantly connected to two separate switches at the Access Layer. This redundancy provides a path from the server to the secondary switch if the primary switch fails. Devices at the Distribution and Core Layers of the server farm network are also redundantly connected. Spanning Tree Protocols, like Rapid Spanning Tree Protocol (RSTP+), manage redundant Layer 2 links. Hot Standby Router Protocol (HSRP) and routing protocols provide support for Layer 3 redundancy and failover.

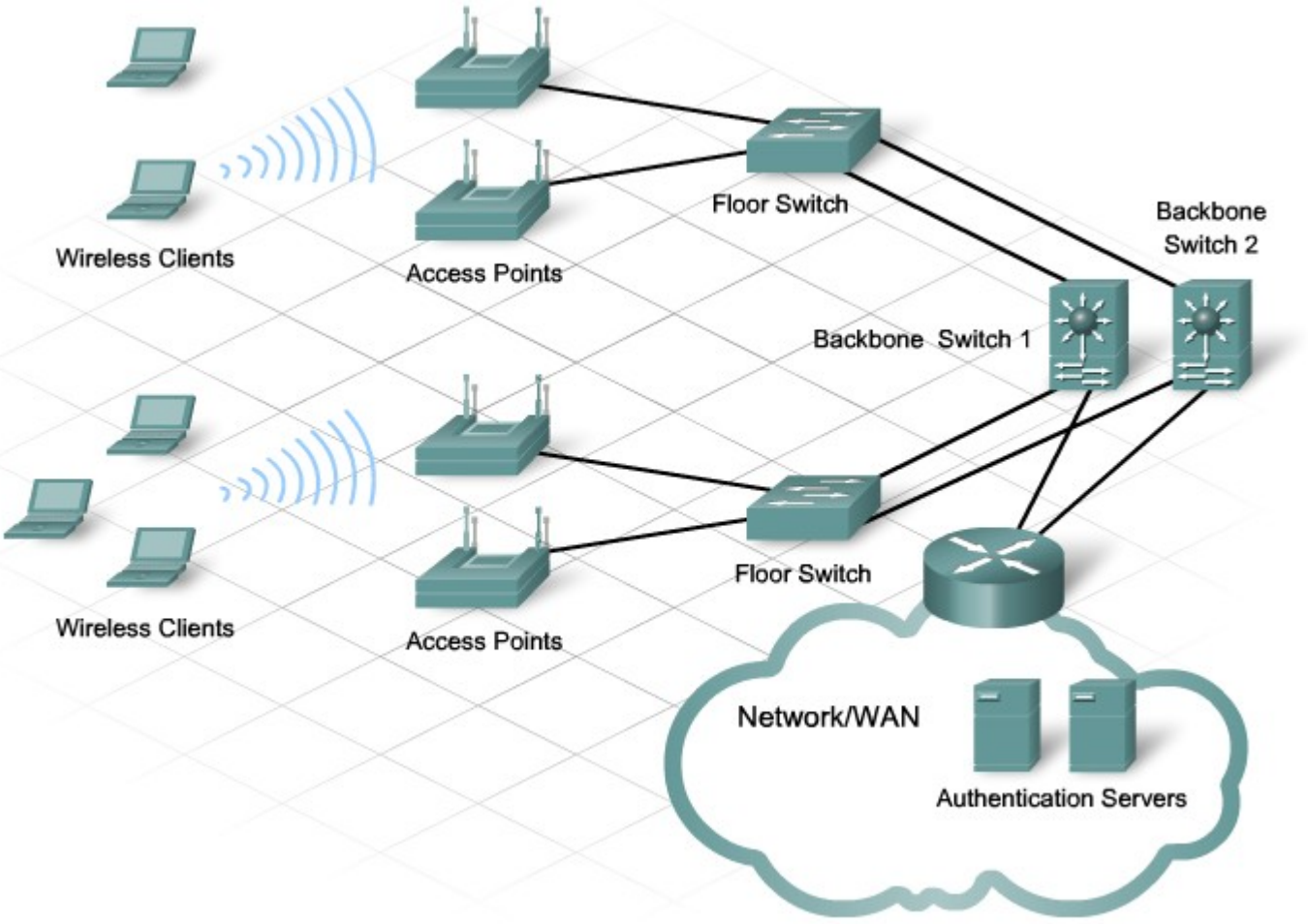
Providing High Availability

- Virtualization
- Many separate logical servers can be located on one physical server. The physical server uses an operating system specifically designed to support multiple virtual images. This feature is known as virtualization. This technology reduces the cost of providing redundant services, load balancing, and failover for critical network services.

Considerations unique to WLAN

- The designer learns about the network requirements by asking the customer questions. The answers to these questions affect how a wireless network is implemented. Examples of some of these questions are:
- Will wireless roaming be required?
- What authentication for users is needed?
- Will open access (hotspots) be provided for the guests?
- Which network services and applications are available to wireless users?
- What encryption technique can be used?
- Are wireless IP telephones planned?
- Which coverage areas need to be supported?
- How many users are in each coverage area?

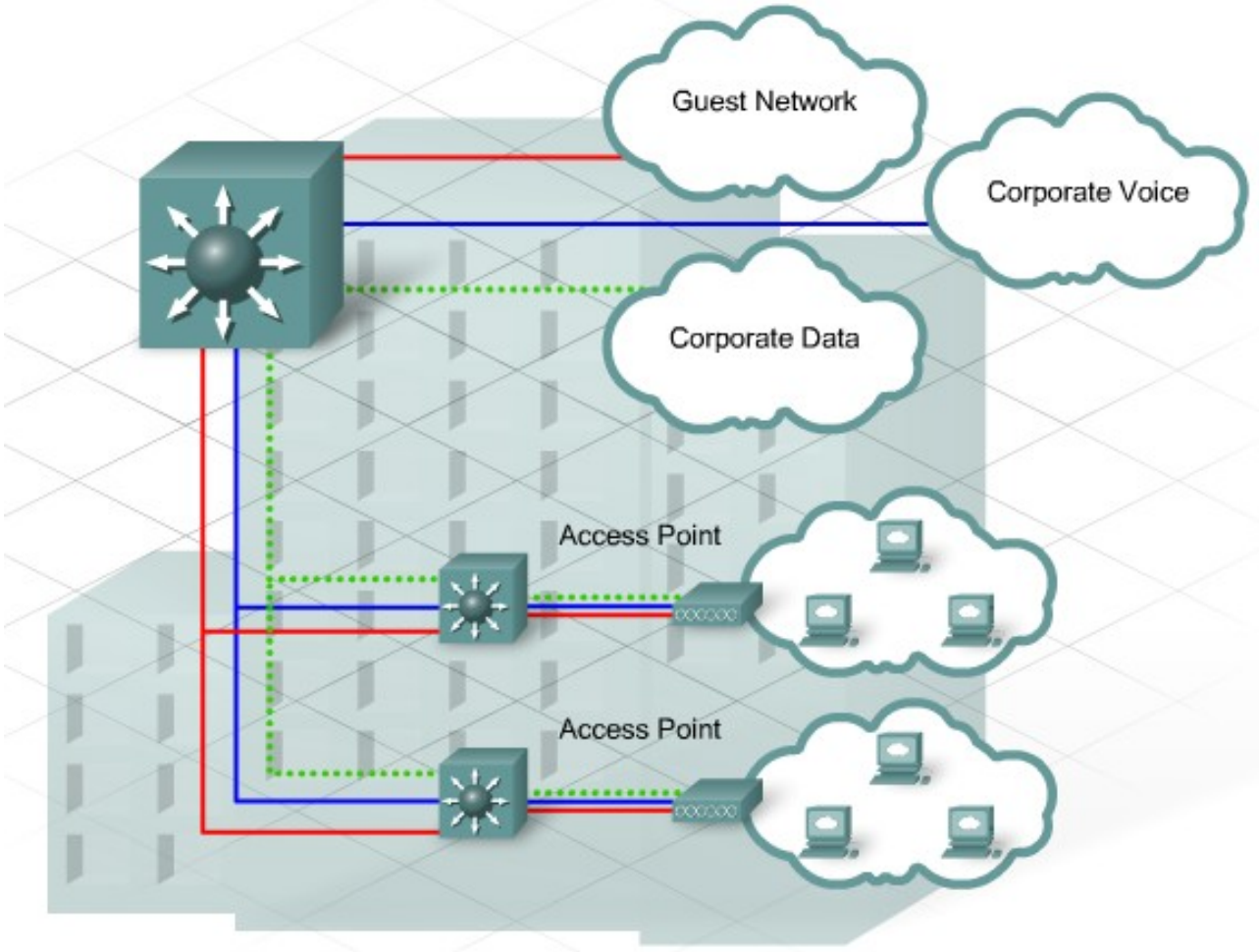
Considerations unique to WLAN



Considerations unique to WLAN

- Physical Network Design
- In typical wireless network designs, most of the effort focuses on the physical coverage areas of the network.
- The network designer conducts a site survey to determine the coverage areas for the network and to find the optimum locations for mounting wireless Access Points. The site survey results help determine the Access Point hardware, types of antennas, and the desired wireless feature sets. The designer determines that roaming between overlapping coverage areas can be supported.

Considerations unique to WLAN



Considerations unique to WLAN

- Logical Network Design
- Designing the logical network usually causes network designers the most difficulty. Customers often want to provide different levels of access to different types of wireless users. In addition, wireless networks must be both easy to use and secure. Resolving both the desired features and the constraints presents many different ways to design and configure wireless LANs.
- An example of a complex wireless network design is a business that needs to offer the following services:
- Open wireless access for their visitors and vendors
- Secured wireless access for their mobile employees
- Reliable connectivity for wireless IP phones

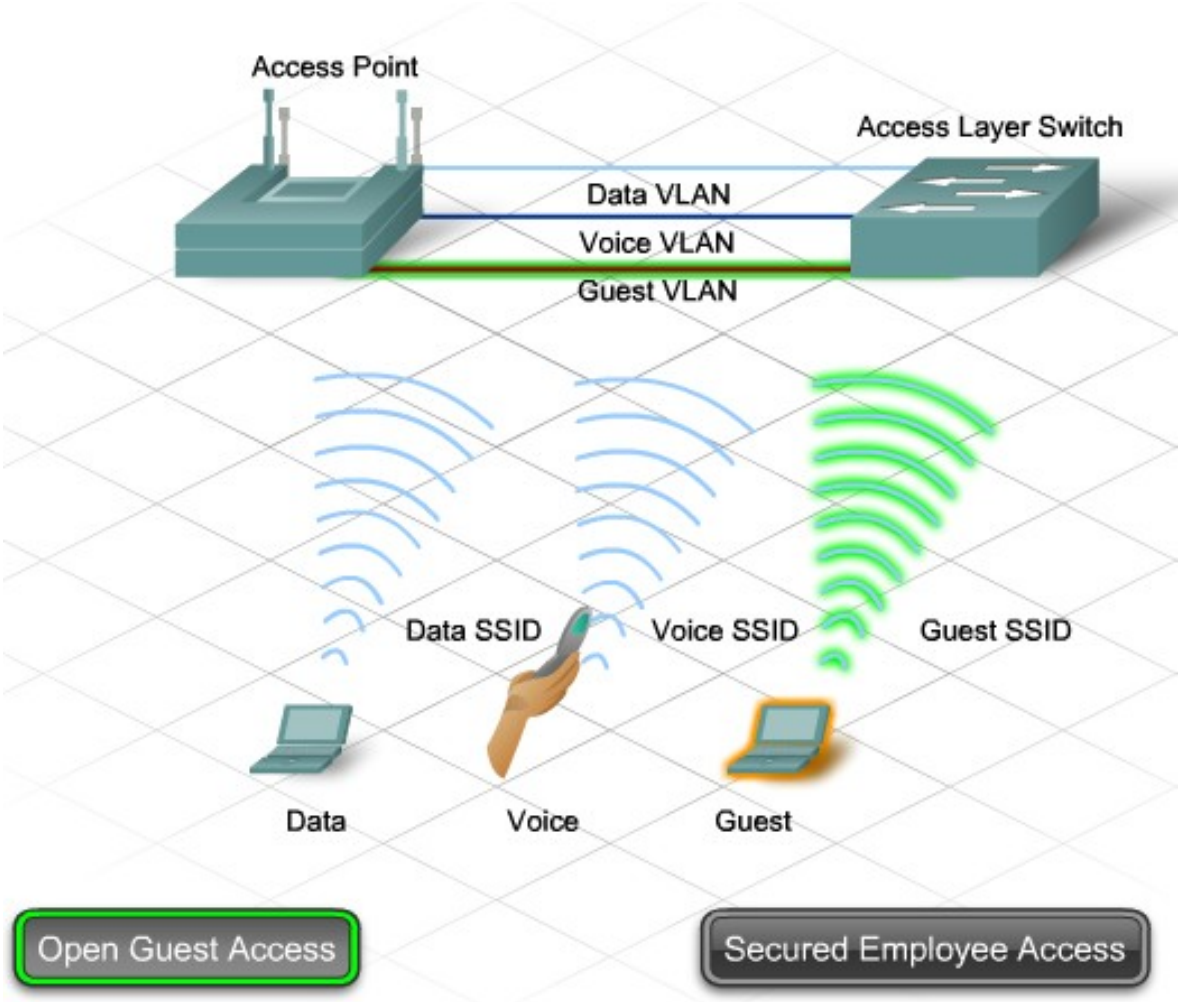
Considerations unique to WLAN

- Open Guest Access
- When visitors and vendors are at a business site, they often require access to email and web sites. This type of access must be convenient to use, and typically is not Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) encrypted. To help guest users connect to the network, the Access Point service set identifier (SSID) is broadcast.
- Many hotspot guest systems use DHCP and a logging server to register and record wireless use. Guest users typically access the wireless network by opening a browser window and agreeing to a specified usage policy.

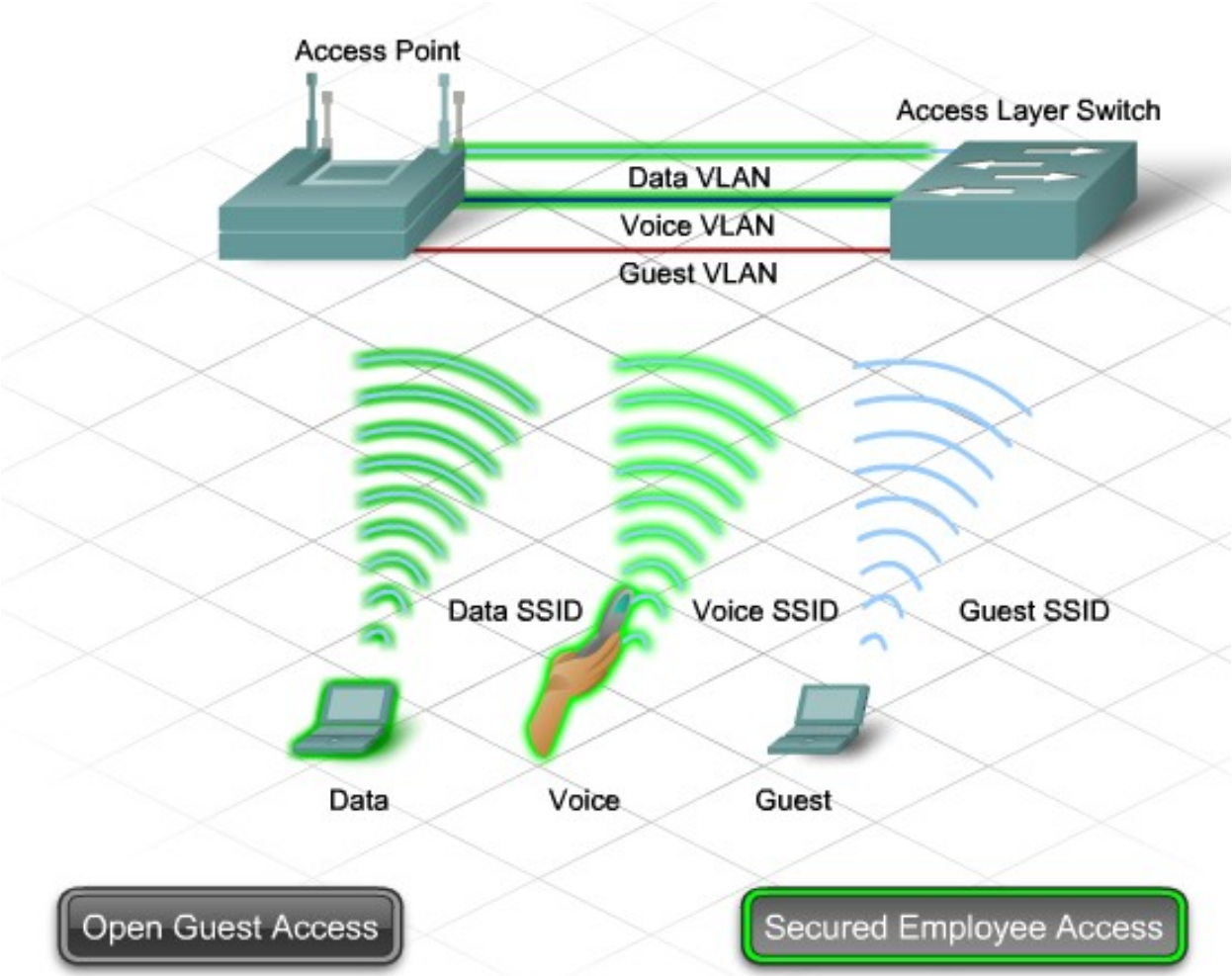
Considerations unique to WLAN

- Secured Employee Access
- Some WLAN devices do not support isolated guest access. To secure employee access, use an entirely separate WLAN infrastructure that does not include guest access. The recommended practice is to separate the internal users on a different VLAN.
- Other wireless implementation recommended practices include:
- Non-broadcast SSID
- Strong encryption
- User authentication
- Virtual Private Network (VPN) tunneling for sensitive data
- Firewall and intrusion prevention
- In areas where secured wireless is restricted to a few devices, MAC address filtering can be used to limit access.

Considerations unique to WLAN



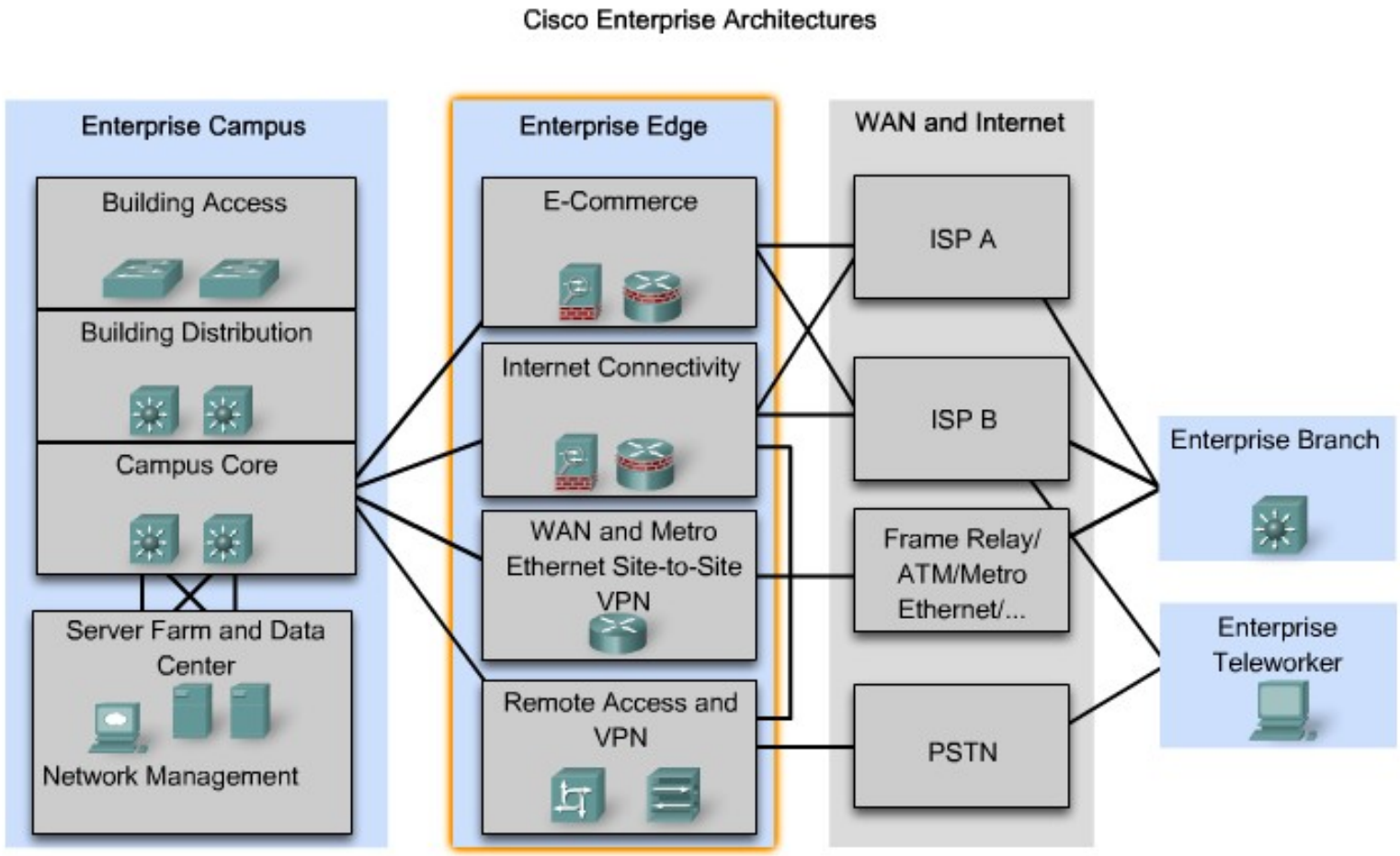
Considerations unique to WLAN



Design Considerations at enterprise edge

- The enterprise edge is the area of the network where the enterprise network connects to external networks. Routers at the enterprise edge provide connectivity between the internal campus infrastructure and the Internet. They also provide connectivity to remote WAN users and services. The design requirements at the enterprise edge differ from those within the campus network.

Design Considerations at enterprise edge



Design Considerations at enterprise edge

- Cost of Bandwidth
- Most campus networks are built on Ethernet technology. However, WAN connectivity at the enterprise edge is usually leased from a third-party telecommunications service provider. Because these leased services can be expensive, the bandwidth available to WAN connections is often significantly less than the bandwidth available in the LAN.
- QoS
- The difference in bandwidth between the LAN and the WAN can create bottlenecks. These bottlenecks cause data to be queued by the edge routers. Anticipating and managing the queuing of data requires a Quality of Service (QoS) strategy. As a result, the design and implementation of WAN links can be complicated.

Design Considerations at enterprise edge

- Security
- Because the users and services accessed through the edge routers are not always known, security requirements at the enterprise edge are critical. Intrusion detection and stateful firewall inspection must be implemented to protect the internal campus network from potential threats.
- Remote Access
- In many cases, the campus LAN services must extend through the enterprise edge to remote offices and workers. This type of access has different requirements than the level of public access provided to users coming into the LAN from the Internet.

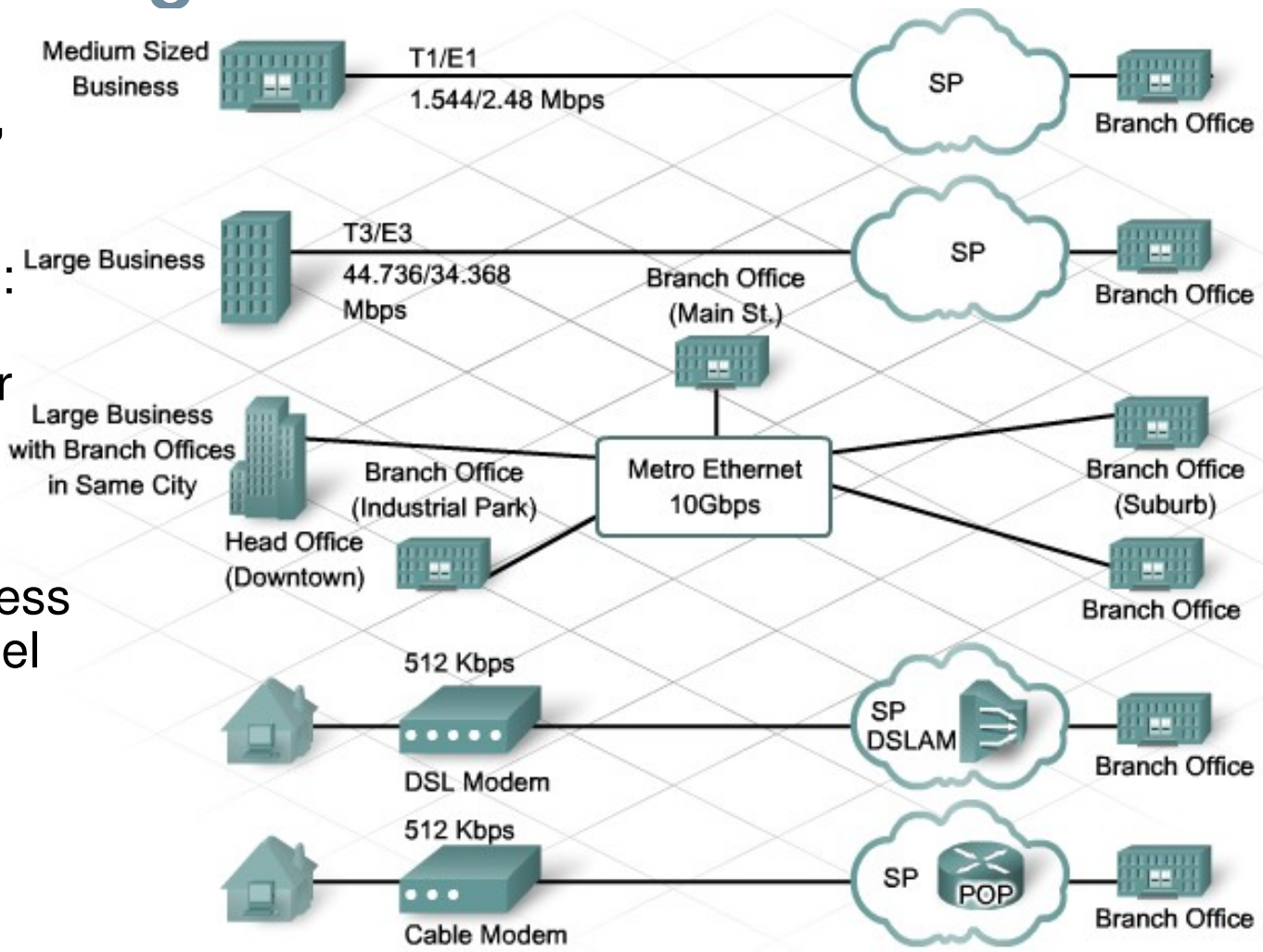
Integrating Remote sites into the network Design

- Designing a network to support branch locations and remote workers requires the network designer to be familiar with the capabilities of the various WAN technologies. Traditional WAN technologies include:
- Leased lines
- Circuit-switched networks
- Packet-switched networks, such as Frame Relay networks
- Cell-switched networks such as Asynchronous Transfer Mode (ATM) networks

Integrating Remote sites into the network Design

In many locations, newer WAN technologies are available, such as:

- Digital Subscriber Line (DSL)
- Metro Ethernet
- Cable modem
- Long-range wireless
- Multiprotocol Label Switching (MPLS)



Integrating Remote sites into the network Design

- In many companies, not every employee works on the main site premises. Employees who work offsite can include:
- Remote workers
- Mobile workers
- Branch employees
- Remote workers usually work one or more days a week from home or from another location. Mobile workers may be constantly traveling to different locations or be permanently deployed at a customer site.

Integrating Remote sites into the network Design

Integrating Remote sites into the network Design

- **Virtual Private Networks**
- One very common connectivity option, especially for remote workers, is a Virtual Private Network (VPN) through the Internet. A VPN is a private network that uses a public network to connect remote sites or users together. Instead of using a dedicated, real-world connection, such as leased lines, a VPN uses virtual connections routed through the Internet from the company private network to the remote router or PC.

- ✓ Enterprise teleworker using router supporting IP telephony and a VPN

- ✓ VPN over DSL

- ✓ VPN over a satellite modem

- ✓ Wireless LAN connected to Internet

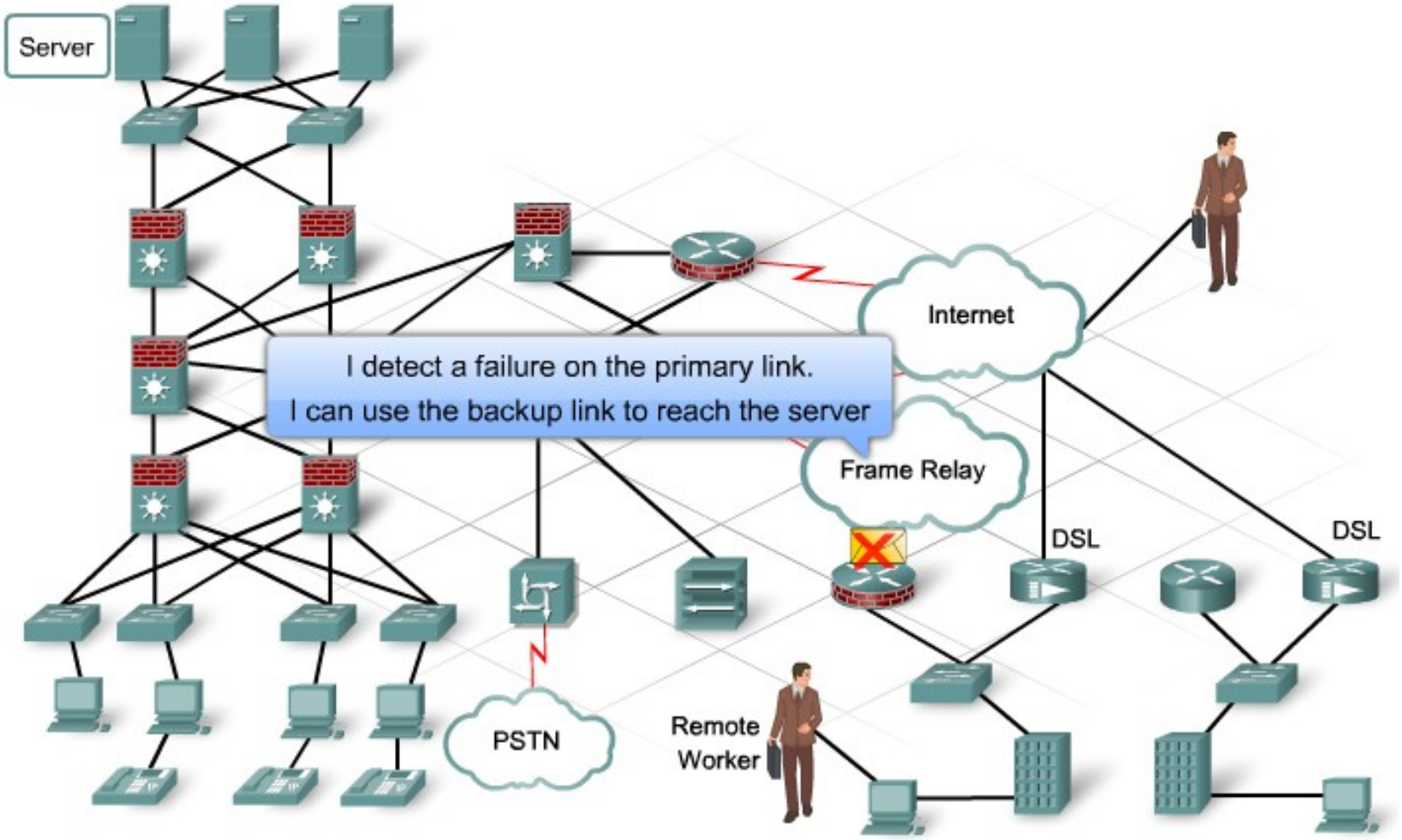
Redundancy and backup links

- Redundancy is required on WAN links and is vitally important to ensure reliable connectivity to remote sites and users.
- Some business applications require that all packets be delivered in a timely fashion. For these applications, dropped connectivity is not an option. Providing redundancy on the WAN and throughout the internetwork ensures high availability for end-to-end applications.
- For a WAN, backup links provide the required redundancy. Backup links often use different technologies than the primary connection. This method ensures that if a failure occurs in one system, it does not necessarily affect the backup system.

Redundancy and backup links

- For example, a business that uses point-to-point WAN connections to remote sites can use VPNs through the Internet as an alternate strategy for redundancy. DSL, ISDN, and dialup modems are other connectivity options used to provide backup links in the event of a WAN failure.
- Load Sharing
- In addition to providing a backup strategy, redundant WAN connections can provide additional bandwidth through load sharing. The backup link can be configured to provide additional bandwidth all of the time or during peak traffic time only.

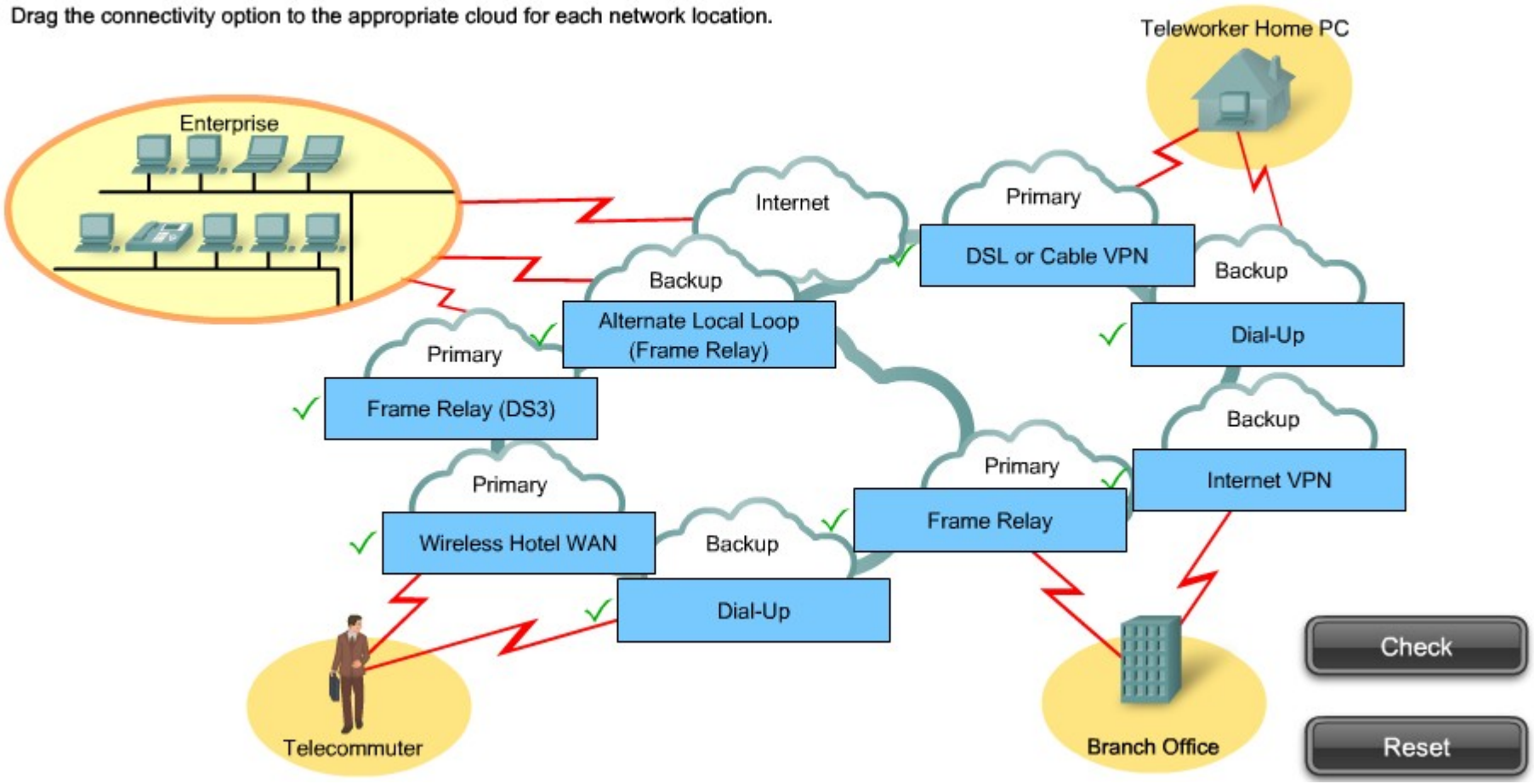
Redundancy and backup links



Redundancy and backup links

Activity

Drag the connectivity option to the appropriate cloud for each network location.



Summary

- Cisco Enterprise Architecture
- Core Layer
- Distribution Layer
- Access Layer