CCNA Discovery 4.0 Designing and Supporting Computer Networks

Creating the Network Design– Chapter 5

Cisco | Networking Academy®
Mind Wide Open™

Objectives

- Analyze the business goals and technical requirements to produce the required design.
- Design the Core, Distribution and Access Layer topologies for a campus network.
- Design the WAN connectivity module and remote worker support.
- Design a wireless network topology.
- Incorporate security into the network design.

Analyzing Business goals and technical requirements

- Determining how to design a network to meet business goals is a multistep process. The designer usually follows these steps:
- Step 1: List the business goals that must be met by the new design.
- Step 2: Determine what changes or additions are necessary for the business to meet its goals.
- Step 3: Decide what technical requirements are necessary to implement each change.
- Step 4: Determine how the design can address each of the technical requirements.
- Step 5: Decide which design elements must be present in the final design.

Analyzing Business goals and technical requirements

- Dealing with Constraints
- The Design Requirements document includes a list of constraints. Usually, when constraints affect the design, compromises must be made. The network designer explores all possible alternatives and selects the best ones to include in the design.
- Making Trade-offs
- A trade-off is an exchange of one benefit or advantage for another benefit that is determined to be more desirable. Network design constraints often force trade-offs between the ideal design and a design that is realistically achievable.

Analyzing Business goals and technical requirements

- Trade-offs between the benefits of an ideal solution and the reality of cost or time constraints are common. It is the job of the designer to minimize the effects of these trade-offs on the main goals of scalability, availability, security, and manageability.
- An example of a trade-off in the stadium network design is a budget limitation that prevents a connection to a secondary Internet service provider (ISP). Because of this limitation, an alternative strategy must be designed to meet the availability requirements for the e-commerce servers.

Analyzing Business goals and technical requirements

Stadium Network Project Constraints

Constraint	Gathered Information	Designer's Notes
Budget	• No plans to fund redundancy at the access-layer. Must also reuse sixteen existing 2960-48TT switches • New cable runs are not funded, except for fiber to connect new wireless access points.	Since the 2960s only support Layer 2 services, Layer 3 wiring closets will not be possible. The two pairs of fiber to each closet can support a connection to a pair of distribution switches.
Policy	• The management guideline was to use ISP managed VPNs across the Internet for low cost remote connectivity. (This is under review.)	Since the QoS and SLA support needed for the business applications is not possible through the local ISP, need to investigate alternate WAN technologies.
Schedule	• The time frame for implementing a major change is approximately 4 months, the time until the primary sports season starts.	Need to consider the time required for the installation and turn-up of any new circuits and equipment.
Personnel	• There is no plan to add additional staff.	Currently understaffed for the planned network expansion with only one network administrator, three network technicians, and one manager. Staff needs immediate training in wireless and IP telephony. Look to reduce complexity.

Requirements for scalability

- The stadium management anticipates significant growth in certain areas of the network. They do not expect the number of wired connections to increase rapidly. The stadium management plans to add at least two new remote office sites. This expansion increases the number of users by 50 percent, to approximately 750 users.
- The scalability requirements received from the stadium management are significant:

Requirements for scalability

- 50 percent increase in the number of total users (LAN and WAN)
- 75 percent increase in the number of wireless users
- 75 percent increase in the number of online transactions serviced by the stadium e-commerce servers
- 100 percent increase in the number of remote sites
- Addition of IP phones, and the incorporation of the video network, adding 350 end devices

Requirements for scalability

Existing
wireless AP

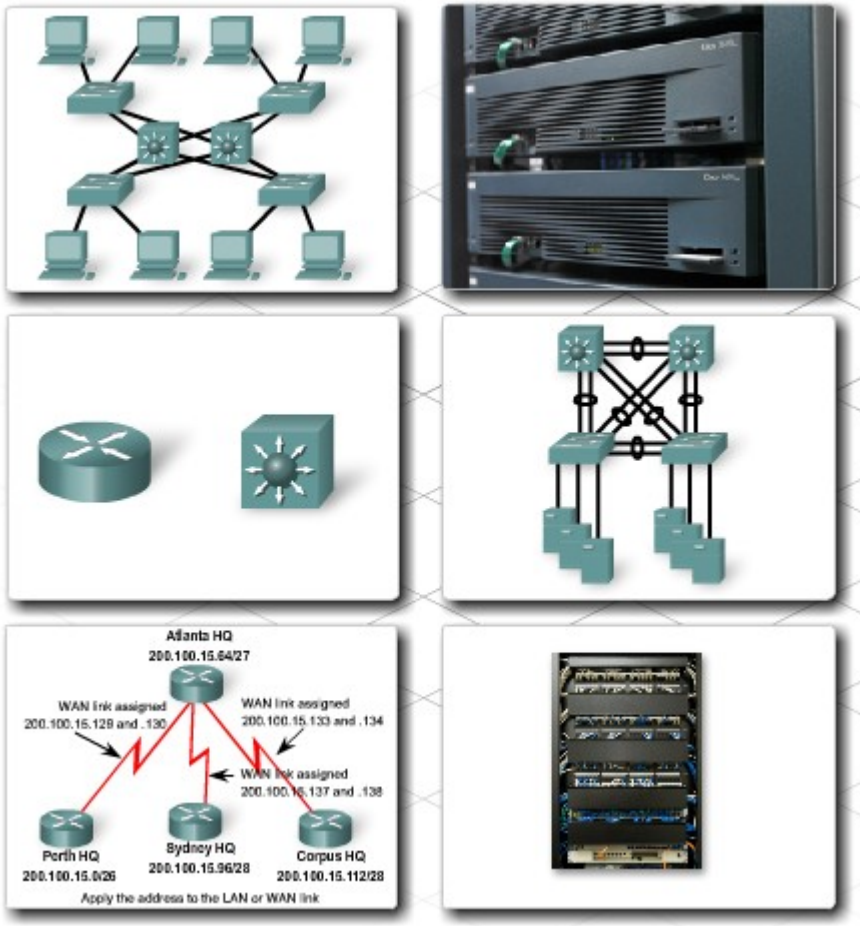
Planned
Wireless AP

Requirements for scalability

- To support this rapid growth, the network designer develops a strategy to enable the network to scale effectively and easily. Included in the strategy are the following recommendations:
- Design Access Layer modules that can be added as necessary without affecting the design of the Distribution and Core Layers.
- Use expandable, modular equipment or clustered devices that can be easily upgraded to increase capabilities.

Requirements for scalability

- Choose routers or multilayer switches to limit broadcasts and filter other undesirable traffic from the network.
- Plan to use multiple links between equipment, using either EtherChannel or equal cost load balancing, to increase bandwidth.
- Create an IP address strategy that is hierarchical and that supports summarization.
- When possible, keep VLANs local to the wiring closet.



Requirements for Availability

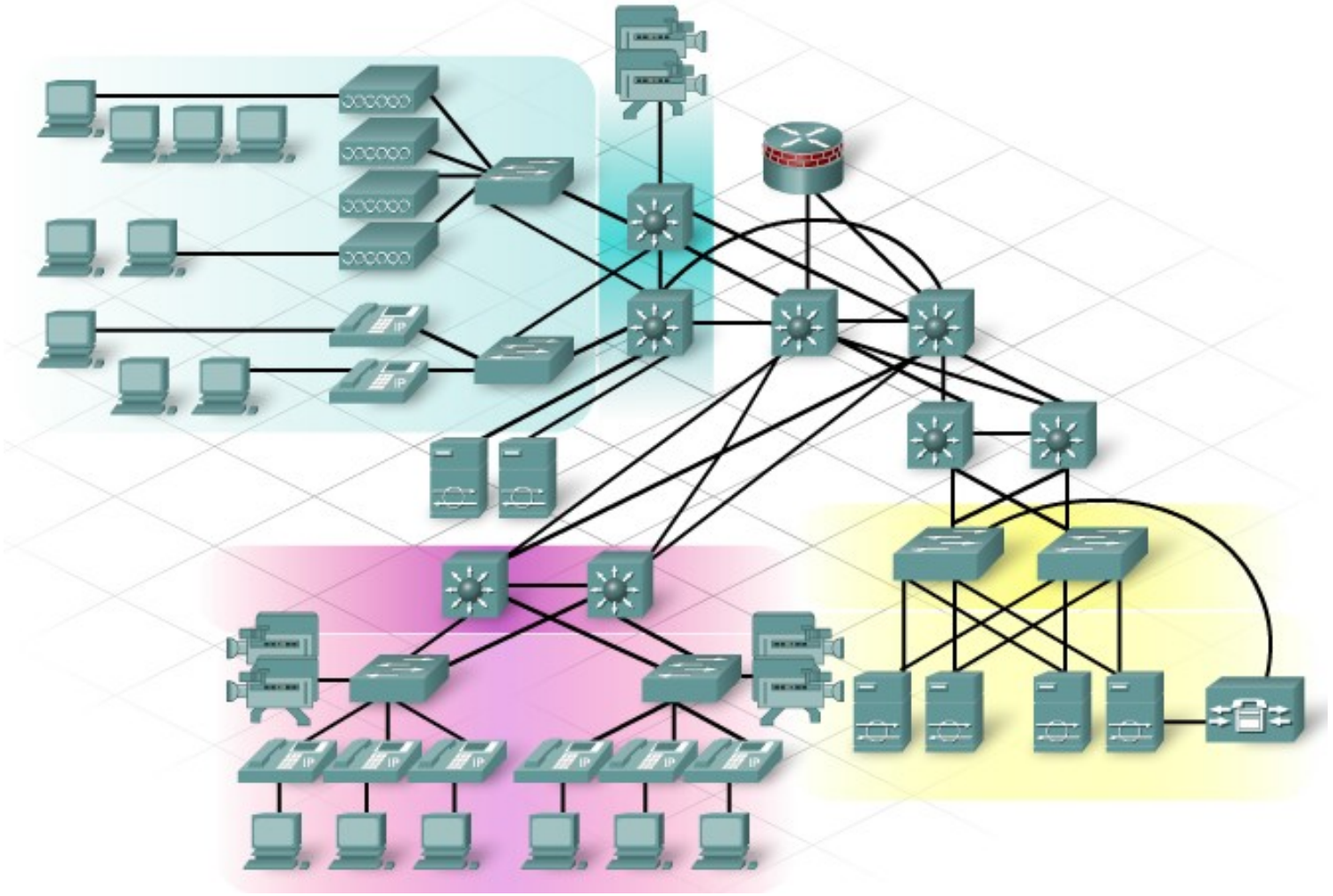
On the stadium network, the planned e-commerce, security, and IP telephony systems rely on the underlying network being available 24 hours a day, 7 days a week.

Incomplete website transactions can cause the stadium management to lose revenue. If the security monitoring becomes unavailable, the safety of the stadium customers can be endangered. In the event that the telephone system is down, vital communications are lost.

Requirements for Availability

- The network designer must develop a strategy for availability that provides the maximum protection from failure and that is not too expensive to implement. To provide the nearly 100 percent uptime requirement of the network applications, the designer must implement high availability and redundancy characteristics in the new design.

Requirements for Availability



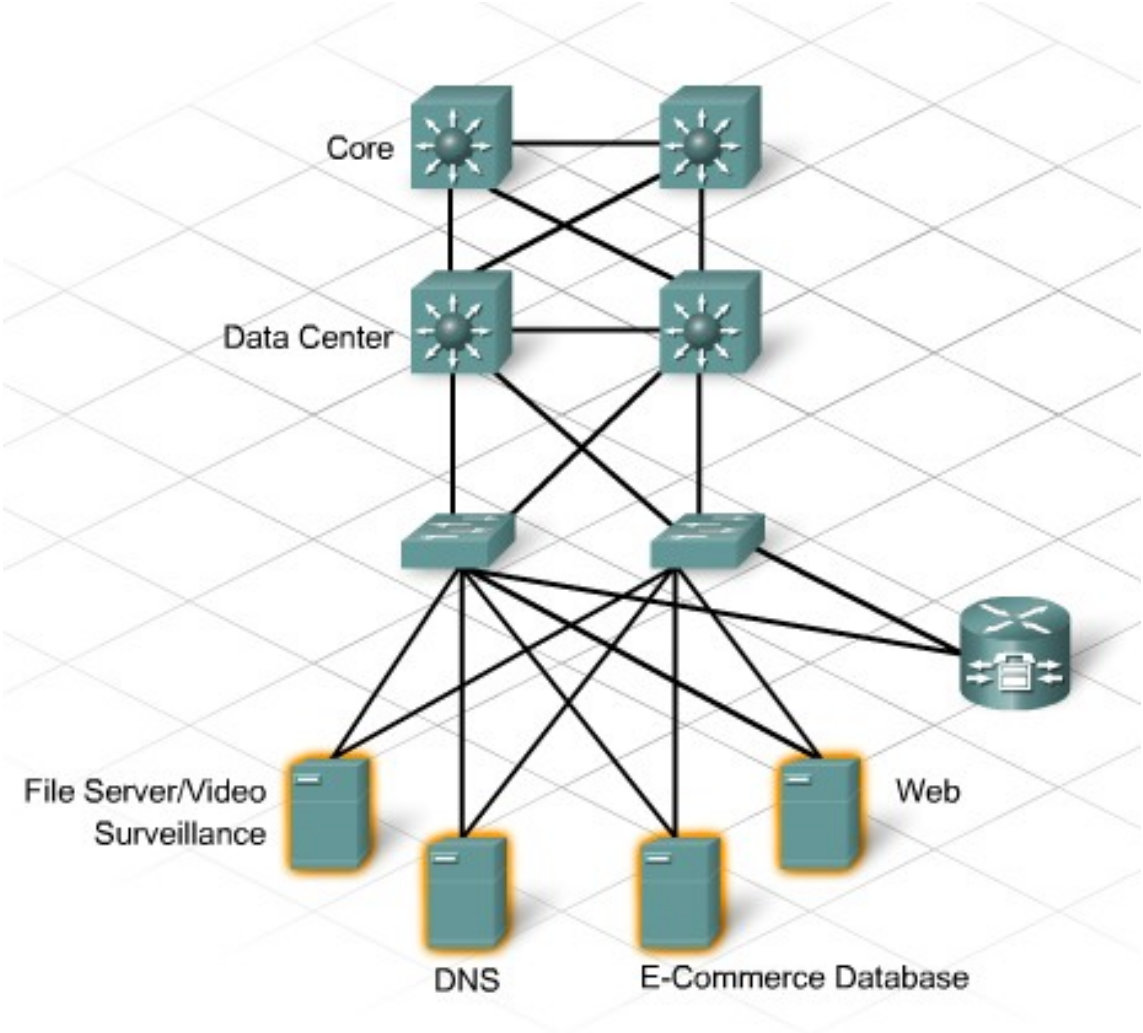
Requirements for Availability

- Availability for E-Commerce
- An unreliable website can quickly become a support problem and even discourage customers from making transactions. To ensure reliability for e-commerce, use the following recommended practices:
- Dual connect the servers on two different Access Layer switches.
- Provide redundant connections at the Distribution Layer.

Requirements for Availability

- Provide secondary DNS servers co-located at the ISP.
- Include additional monitoring locally and through the Internet for devices in the critical path.
- Where possible, include redundant modules and power supplies in critical pieces of equipment.
- Provide UPS and generator power backup.
- Choose a routing protocol strategy that ensures fast convergence and reliable operation.
- Investigate options to provide an additional Internet service provider (ISP) or redundant connectivity to the single ISP

Requirements for Availability



Requirements for Availability

- The Security Monitoring System
- The servers that maintain the video files and the security management software have the same availability requirements as the e-commerce servers. The following additional measures are needed for the cameras and surveillance equipment:
- Redundant cameras in critical areas that are connected to separate switches to limit the affect of a failure
- Power over Ethernet (PoE) to the cameras, with UPS and/or generator backup

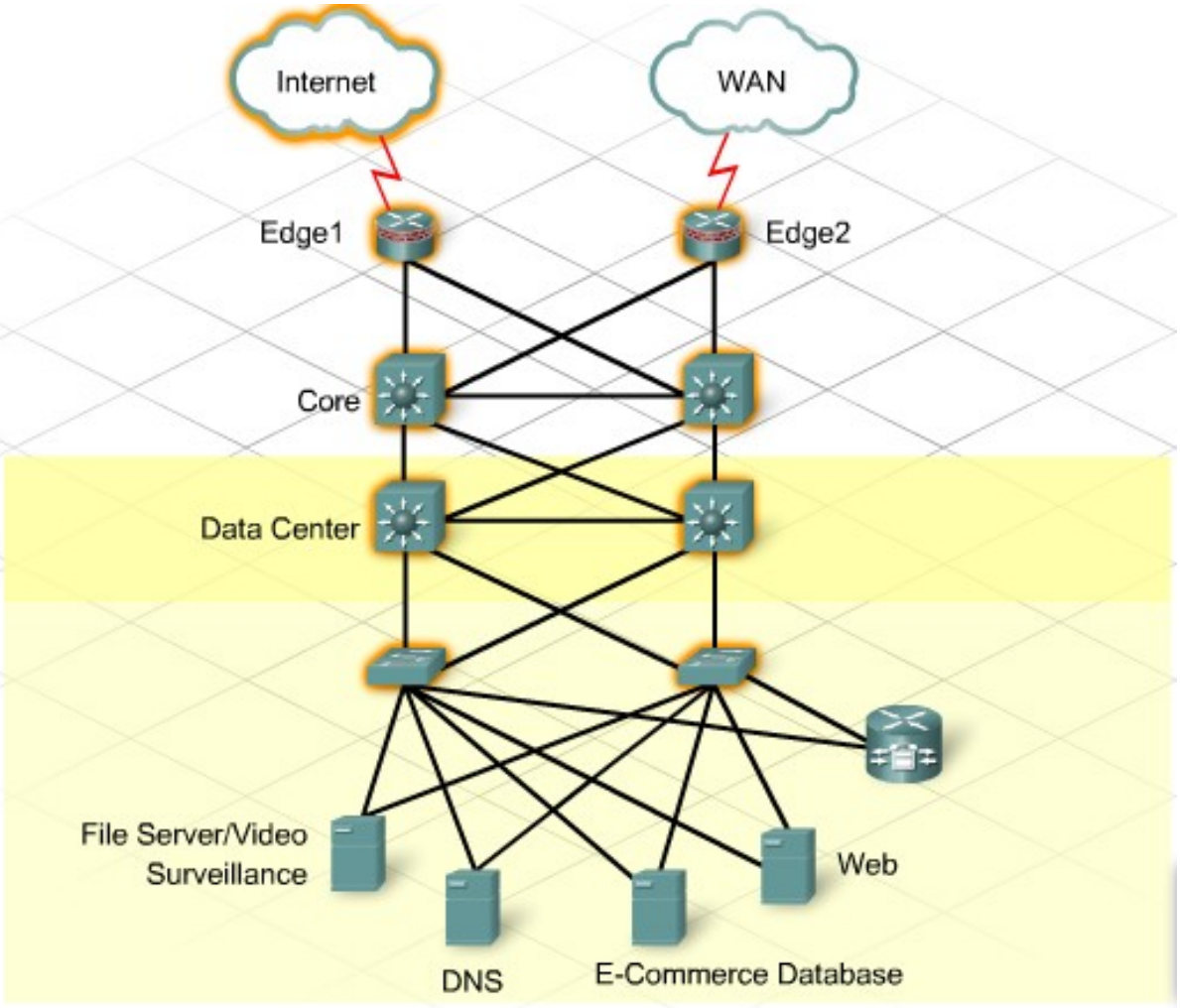
Requirements for Availability

- The IP Telephone System
- Although the installation of the new IP telephone system is outside the scope of this network design project, it is still necessary for the network designer to consider the availability requirements in the design. The designer focuses on the following requirements for providing redundancy and high availability on the Access Layer switches:

Requirements for Availability

- Implement Layer 3 connectivity between the Access Layer and Distribution Layer devices when possible.
- Provide redundant power and UPS backup.
- Create redundant paths from the Access Layer to the Core Layer.
- Reduce the size of failure domains.
- When possible, select equipment that can support redundant components.
- Use a fast, converging routing protocol, such as EIGRP

Requirements for Availability



Requirement for network performance

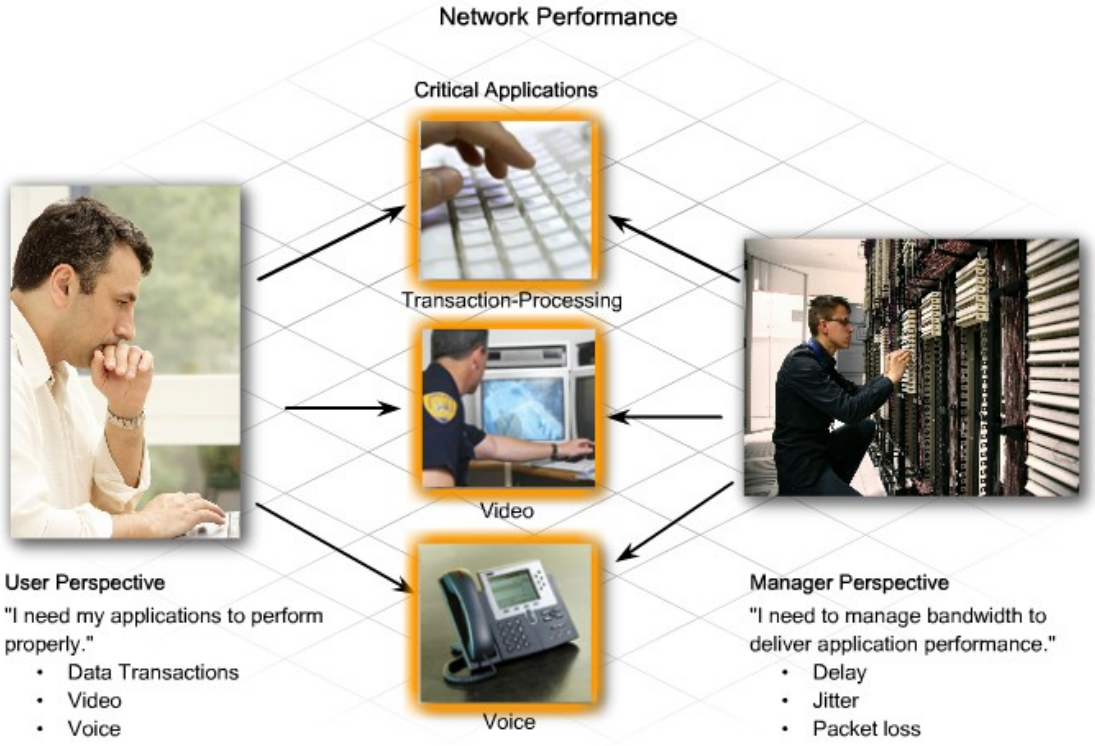
- Converged networks, such as the network being designed for the stadium, carry a combination of data, voice, and video traffic. Each type of traffic has unique service requirements.
- Characteristic features of applications on a typical converged network include:
- Packets of various sizes
- Distinct sets of protocols
- Different tolerances to delay and jitter

Requirement for network performance

- Sometimes the service requirements of one application conflict with the service requirements of another, resulting in performance problems. When this situation occurs, frustrated users call the help desk to report that their application is slow.
- Even skilled, experienced IT professionals struggle to maintain high application performance. Deploying new applications and services without disrupting existing ones is difficult.

Requirement for network performance

- On the new stadium network, three applications have specific performance requirements that must be addressed:
- Transaction-Processing
- Video Distribution and Monitoring
- IP Telephone Voice Quality



Requirement for network performance

- The network designer creates a list of the design goals and considerations that could affect the performance of these high-priority applications.
- Goal: Improve transaction-processing time to less than 3 seconds.
- Reduce the network diameter.
- Restrict unwanted traffic and broadcasts.
- Provide high-bandwidth paths to key servers.
- Recommend additional high-speed storage or content servers.

Requirement for network performance

- Goal: Provide high-quality voice and streaming video.
- Design VLAN and traffic classification strategy.
- Keep the paths from server to end-points short.
- Reduce the number of times traffic is filtered or processed.
- Increase WAN site bandwidth and improve connectivity.
- Determine QoS strategy and traffic priorities.
- Identify areas where bottlenecks might occur and deploy a QoS strategy.

Requirements for security

- Security is the one area of network design where trade-offs should not be made. Although it may be necessary to find lower cost or less streamlined ways to provide a secure network, it is never acceptable to disregard security in order to add other network capabilities.
- A network risk assessment identifies the areas where a network is most vulnerable. Networks that contain highly confidential or critical information often have unique security considerations. Organizations do risk assessments as part of their overall business continuity and disaster recovery planning.

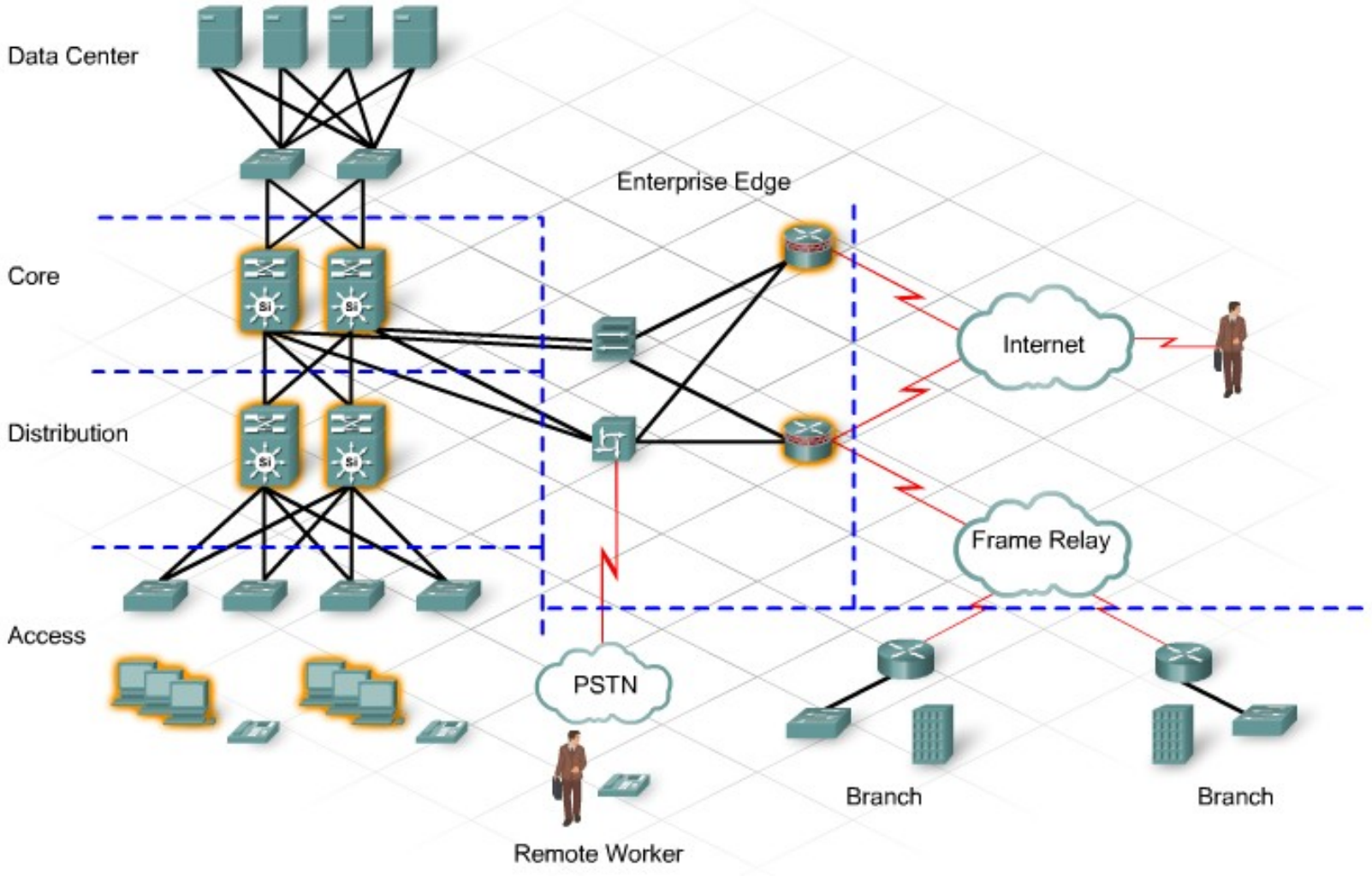
Requirements for security

- Most networks benefit from standard recommended practices when it comes to deploying security. Recommended security practices include:
- Use firewalls to separate all levels of the secured corporate network from other unsecured networks, such as the Internet. Configure firewalls to monitor and control the traffic, based on a written security policy.
- Create secured communications by using VPNs to encrypt information before it is sent through third party or unprotected networks.

Requirements for security

- Prevent network intrusions and attacks by deploying intrusion prevention systems. These systems scan the network for harmful or malicious behavior and alert network managers.
- Control Internet threats by employing defenses to protect content and users from viruses, spyware, and spam.
- Manage endpoint security to protect the network by verifying the identity of each user before granting access.
- Ensure that physical security measures are in place to prevent unauthorized access to network devices and facilities.
- Secure wireless APs and deploy wireless management solutions.

Requirements for security



Making Network Design Tradeoffs

- After the network designer lists all the elements that need to be present in the stadium upgrade design, some hard decisions must be made. Unfortunately, few networks can be designed without considering:
- The cost of the network
- The difficulty of implementation
- The future support requirements
- The StadiumCompany has placed some constraints on the network upgrade that require the designer to evaluate different design options. It may be necessary to make trade-offs in some areas to accommodate these constraints.

Making Network Design Tradeoffs

- The primary business goal of the StadiumCompany is to improve the atmosphere and safety for the thousands of people who attend stadium events. Network improvements that directly affect how the network supports this goal must be a top priority for the designer when making design trade-offs.
- Supporting the business goals may lead to decisions that eliminate or complicate other desirable or necessary improvements. For example, adding wireless access to improve the customer experience in the luxury boxes and restaurant may decrease server security unless the guest access is isolated from the internal network.

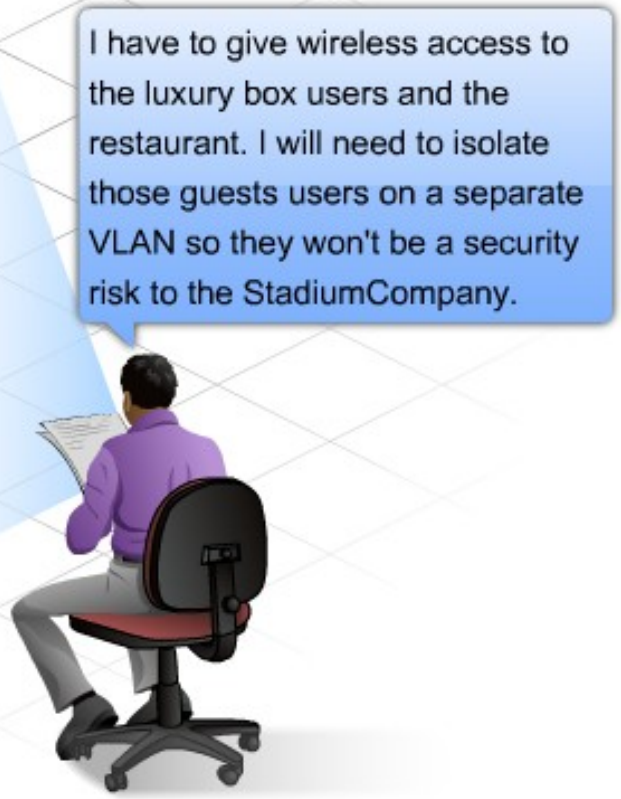
Making Network Design Tradeoffs

1. Provide better atmosphere and safety for people attending events.

2. Reduce costs by consolidating the separate voice, video, and data networks.

3. Provide better customer service by improving the access to the website for viewing of schedules, purchasing and printing of tickets, and purchasing of merchandise.

4. Support the growth of the StadiumCompany as it expands and add new types of entertainment, new partners, and new vendors.

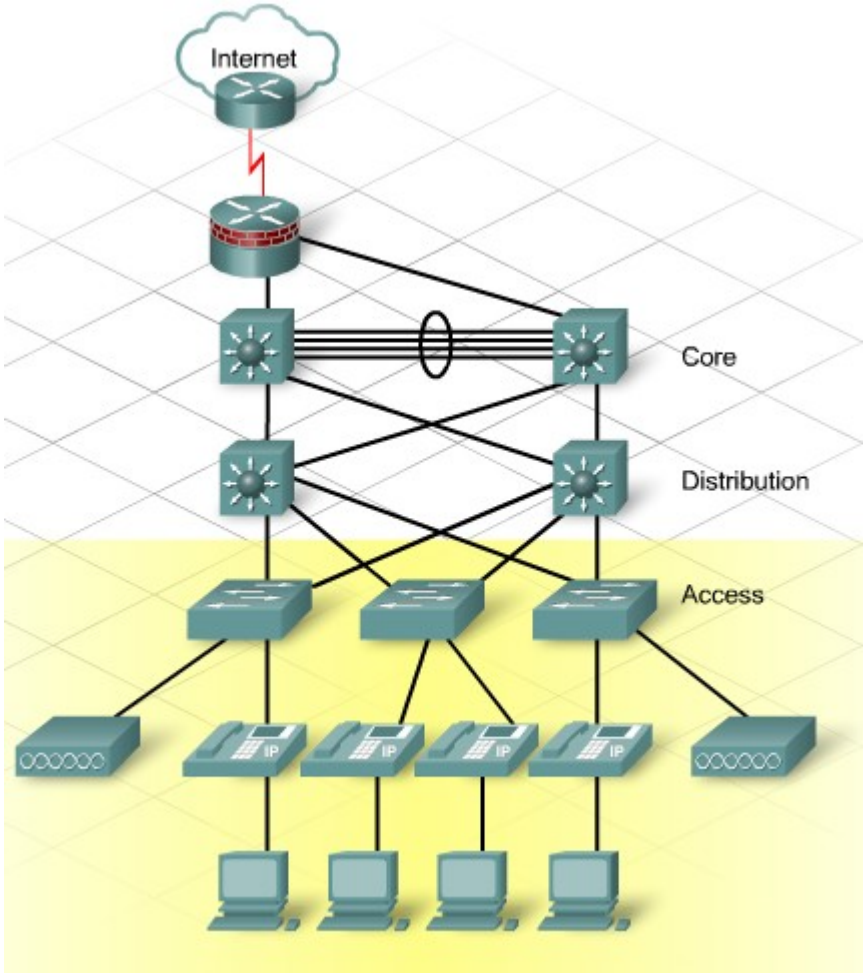


Designing an Access Layer Topology

- Access Layer Requirements
- The designer creates the following list of Access Layer network requirements for the new network:
- Provide connectivity for existing network devices and add wireless access and IP telephones.
- Create VLANs to separate voice, security surveillance monitoring, wireless access, and normal data devices.
- Restrict VLANs to wiring closets, with the exception of the wireless VLAN, to support future roaming requirements.

Designing an Access Layer Topology

Provide redundant links to the Distribution Layer network.
Use the 16 existing 2960 switches where possible.
Provide Power over Ethernet (PoE) to IP phones and wireless access points, if possible.
Provide QoS classification and marking capabilities.

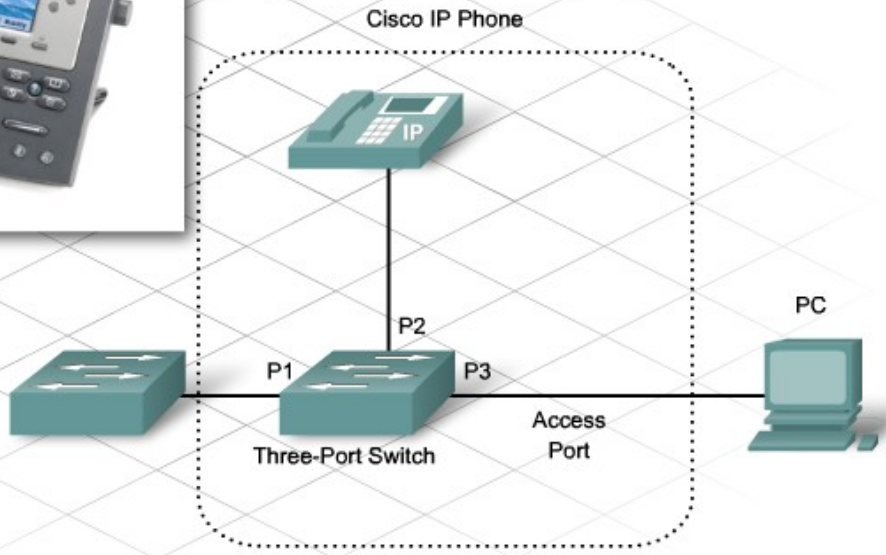


Designing an Access Layer Topology

- An increase in the number of hosts does not always necessitate an equal increase in the number of devices and ports. For example, IP phones and other devices include an embedded switch that permits a PC to be plugged directly into the phone. This switch reduces the number of ports needed in the wiring closet to connect the additional devices. Assuming that over 50 percent of the IP phones also connect PC devices, adding more data connections may not require the addition of a new switch to the wiring closet.

Designing an Access Layer Topology

- IP Phones have three ports:
- Port 1 is an external port that connects to the switch or another VoIP device.
- Port 2 is an internal 10/100 interface that carries the IP phone traffic.
- Port 3 is an external access port that connects to a PC or another device.



Designing an Access Layer Topology

- The 16 existing 2960 switches are to be used in the Access Layer to provide end-user connectivity. The network designer must ensure that the 2960 switch is suitable for the new network.
- 2960 Switch Capabilities
- These switches are fixed configuration 10/100 Ethernet switches with two 10/100/1000 uplink ports. The 2960 can support most of the following requirements of the Access Laver network:

Designing an Access Layer Topology

- Scalability - The 2960 supports Cisco switch clustering; therefore, new switches can easily be added to support additional connectivity.
- Availability - The 2960 supports redundant power supplies. Redundant switch management is available when the switches are configured in a cluster. Two switches can be configured as the command switches. If one fails, the rest of the cluster can still function. Classification and marking capabilities are also available in this model.

Designing an Access Layer Topology

- Security - Port security and other switch security options are available.
- Manageability - The switches support Simple Network Management Protocol (SNMP). They can be managed in-band and out-of-band. The 2960 supports the standard Cisco IOS software command set, as well as Cisco Network Assistant GUI configuration and management tools.

Designing an Access Layer Topology

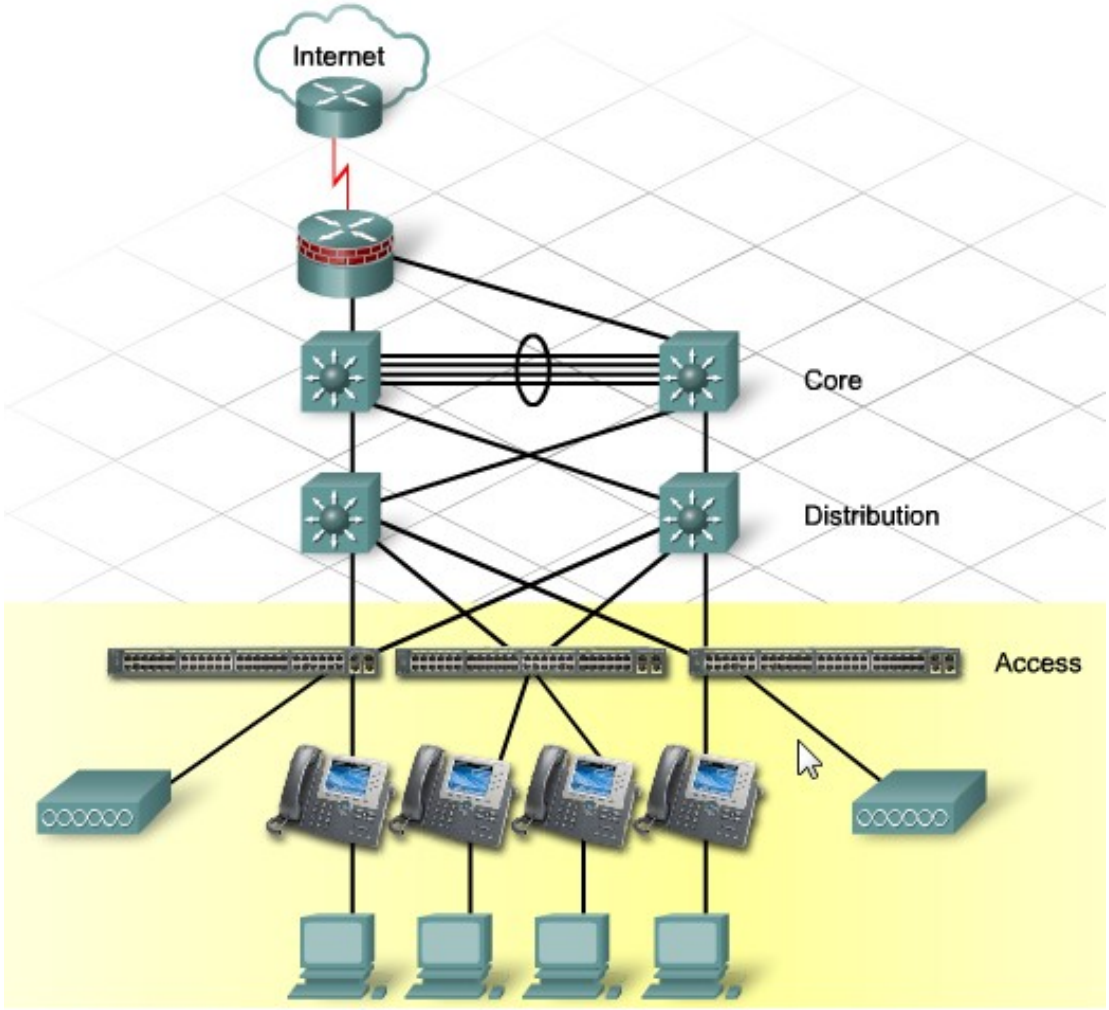
Designing an Access Layer Topology

- Limitations of the Existing Equipment
- The 2960 switch has certain limitations in the new network design. The current 2960 switches in the stadium network need additional transceivers to support the fiber uplinks. Because only two fiber connections are available to each wiring closet, multiple 2960 switches must be clustered to share the uplinks. The 2960 is a Layer 2 switch; therefore, the network designer is limited to providing Layer 2 functionality at the Access Layer.

Designing an Access Layer Topology

- Power Requirements
- Although the 2960 switch does not support PoE, it does support voice VLAN capability. It may be necessary to use powered patch panels to provide power to the IP phones until the switches are replaced in the future.
- UPS units provide backup power for the switches and the powered patch panels. The designer recommends the purchase of a generator to provide power to critical areas of the Access Laver.

Designing an Access Layer Topology

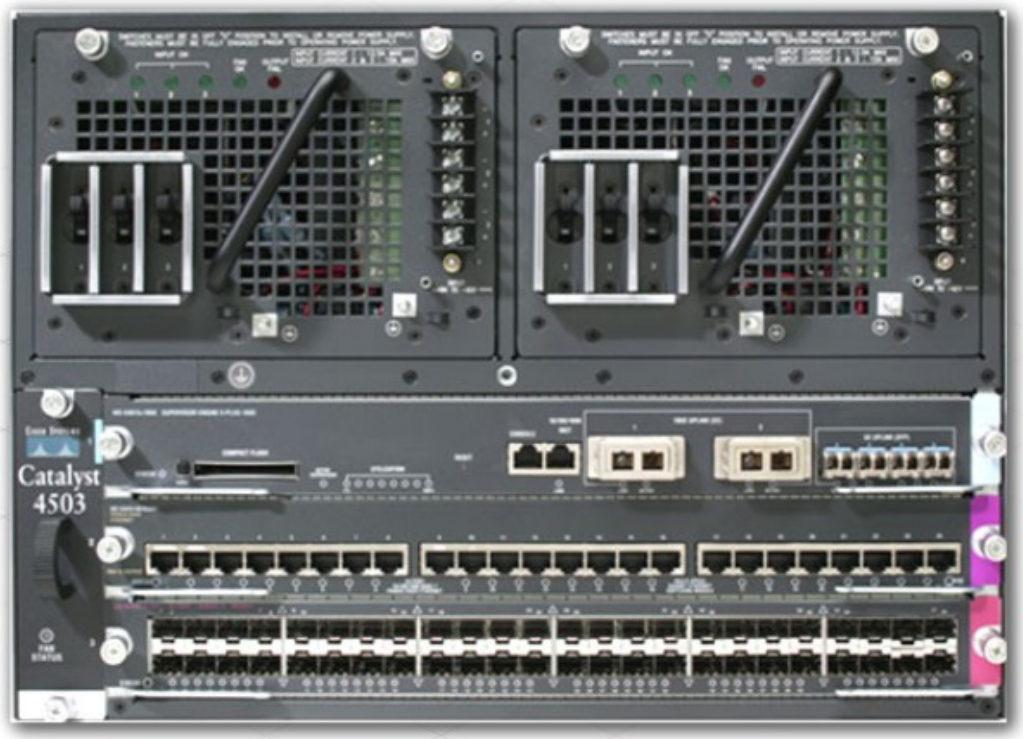


Designing Distribution Layer Topology

- Distribution Layer Requirements
- The network designer creates the following list of Distribution Layer requirements for the new network:
- Provide redundant components and links to minimize the effect of a failure.
- Support high-density routing. Each of the 16 wiring closets in the stadium may eventually have more than one uplink to the Distribution Layer switches.
- Provide traffic filtering capabilities.
- Implement QoS mechanisms.
- Provide high-bandwidth connectivity.
- Implement a fast-converging routing protocol.
- Aggregate traffic and perform route summarization.

Designing Distribution Layer Topology

Multilayer switches are an appropriate choice for meeting these requirements. They provide high port density and support the necessary routing capabilities. The Distribution Layer design includes connectivity for the LAN users, server farm, and enterprise edge distribution. Six multilayer switches need to be purchased to provide the required support.



Designing Distribution Layer Topology

- Design Constraints
- The limited amount of fiber connectivity to the wiring closets is the only design constraint that limits the Distribution Layer. The two fiber pairs that connect the wiring closets limit the number of switches that can be redundantly connected to the Distribution Layer equipment. Because all of the fiber terminates in a central location, much of the Distribution Layer equipment must be installed in the new data center.

Designing Distribution Layer Topology

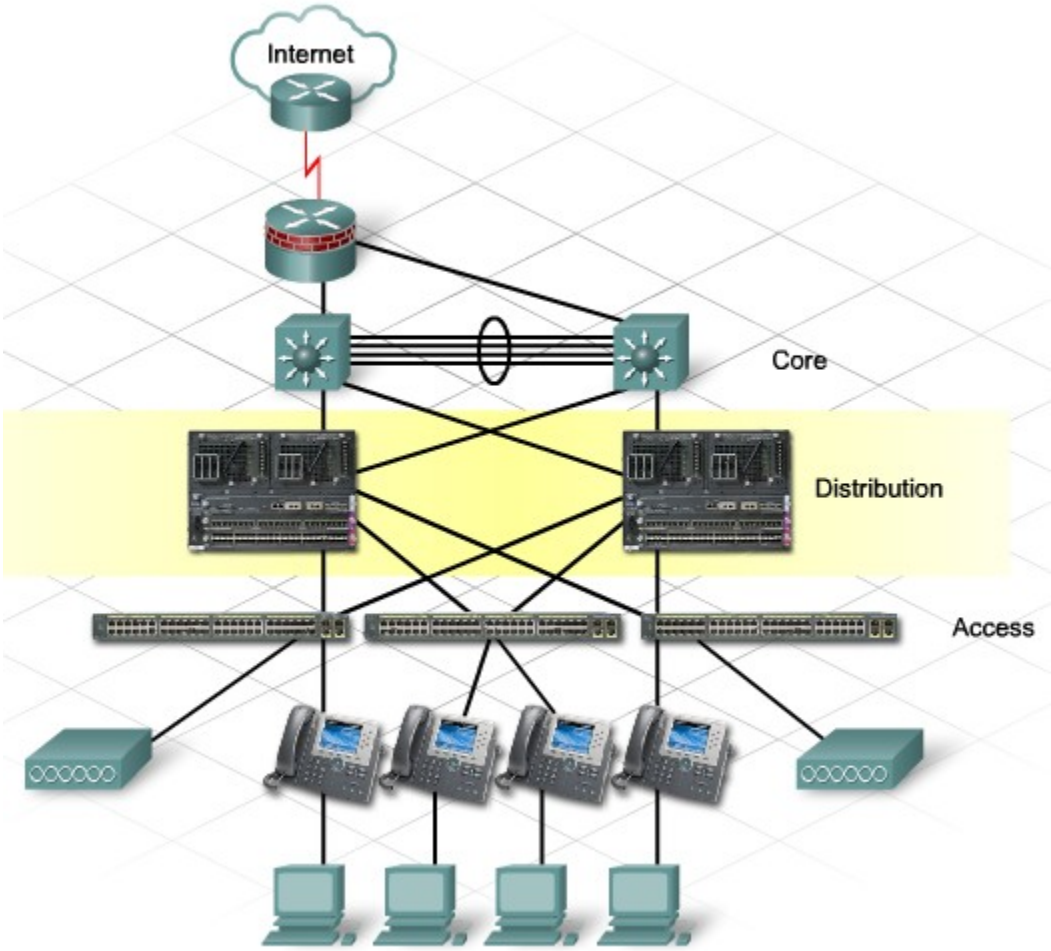
- Multilayer Switch Capabilities
- Using Multilayer switches at the Distribution Layer meets the stadium design technical requirements:
- Scalability - The modular multilayer switches support additional fiber and copper ports. Using routing at the Distribution Layer avoids many Layer 2 Spanning Tree Protocol (STP) reconfiguration issues. New switch blocks can be added without affecting the existing topology.

Designing Distribution Layer Topology

- Availability - The midrange multilayer switches support redundant power supplies and fans. More importantly, they support redundant management modules and fast failover technology. If one management module fails, the secondary module takes over, with no perceptible loss of connectivity. The Layer 3 switched design makes the best use of network links by efficient load balancing of the routed traffic. Routing protocols can be configured to converge as fast as STP or faster. Route summarization can occur at the Distribution Layer, reducing the impact of an Access Layer device or link failure on the Core Layer routing.

Designing Distribution Layer Topology

- Security - Access-list filtering, port security, and firewall feature sets are available on the multilayer switch Cisco IOS. Additional security features prevent unauthorized or unwanted network traffic.
- Manageability - The switches support SNMP. They can be managed both in-band and out-of-band.



Designing Core Layer Topology

- The Core Layer of the stadium LAN must provide high-speed connectivity and high availability. Both the local and remote stadium networks depend on the Core switches for connectivity.
- Core Layer Requirements
- Design requirements for the Core Layer network include:
- High-speed connectivity to the Distribution Layer switches
- 24 X 7 availability
- Routed interconnections between Core devices
- High-speed redundant links between Core switches and between the Core and Distribution Laver devices

Designing Core Layer Topology

- The Core Layer design requires high-speed, lower-density, multilayer switching. In the new design, the Core Layer network for the stadium can be implemented on two powerful multilayer switches.
- The Core Layer is reserved for high-speed traffic switching; therefore, little or no packet filtering is done at this layer.
- In a small business environment, the Distribution and the Core Layers are frequently combined. This may be referred to as a collapsed Core or a collapsed backbone.

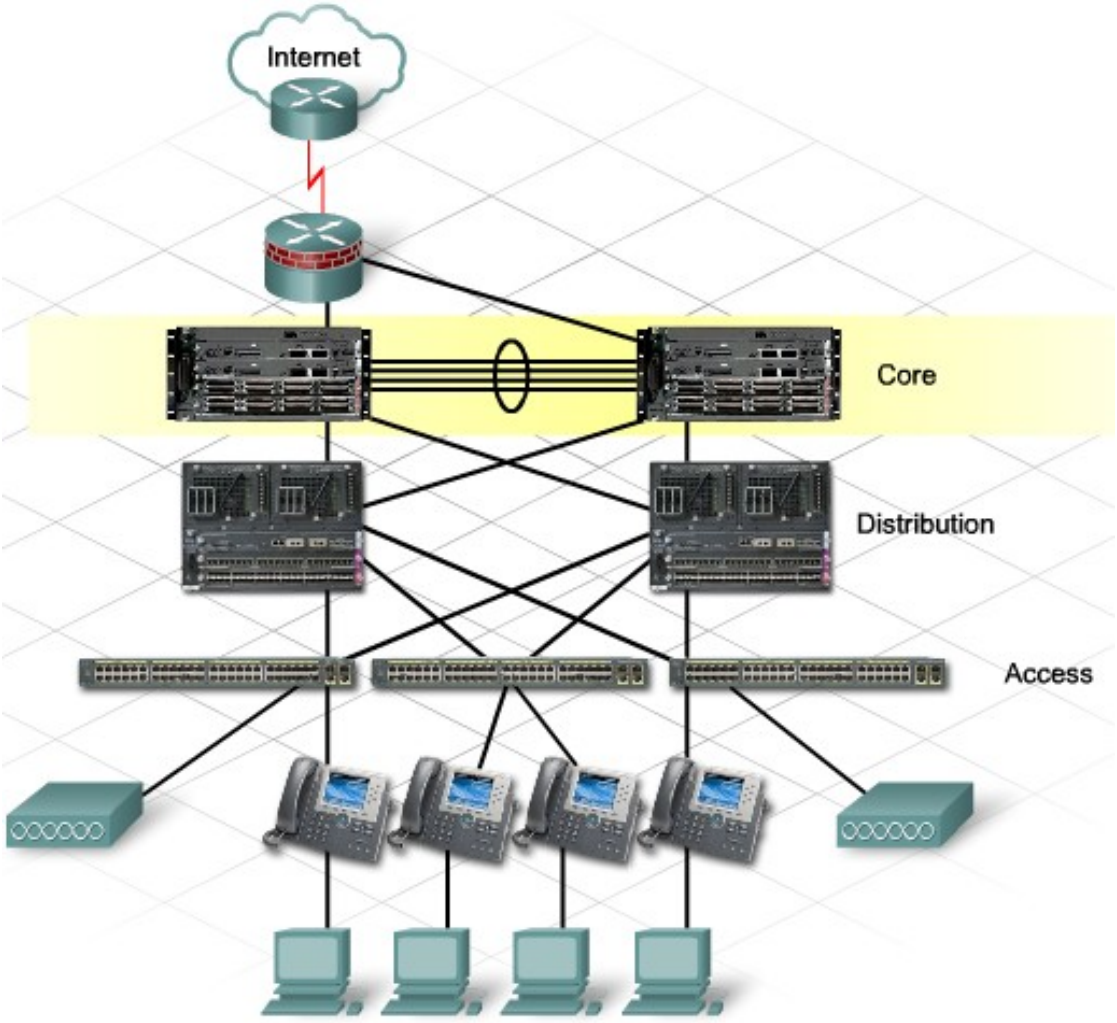
Designing Core Layer Topology

- High Availability
- The top priority at the Core Layer of the network is high availablity. The network designer needs to consider any measures that can be taken to improve reliability and uptime.
- Redundant links between the Core Layer and the Distribution Layer should be established. Installing redundant components and taking additional measures to provide redundant air conditioning, power, and services to the Core Layer devices should be implemented wherever possible.

Designing Core Layer Topology

- Using a Layer 3 routing protocol such as EIGRP or OSPF at the Core Layer can decrease the time it takes to recover from a link failure. Routed connections between the Core Layer switches can provide equal cost load balancing as well as rapid recovery.
- Speed
- The next priority at the Core Layer is speed. Almost all of the stadium network traffic must travel through the Core Layer devices. High-speed interfaces, fiber connectivity, and technologies such as EtherChannel can provide enough bandwidth to support the traffic level and let the network grow in the future.

Designing Core Layer Topology



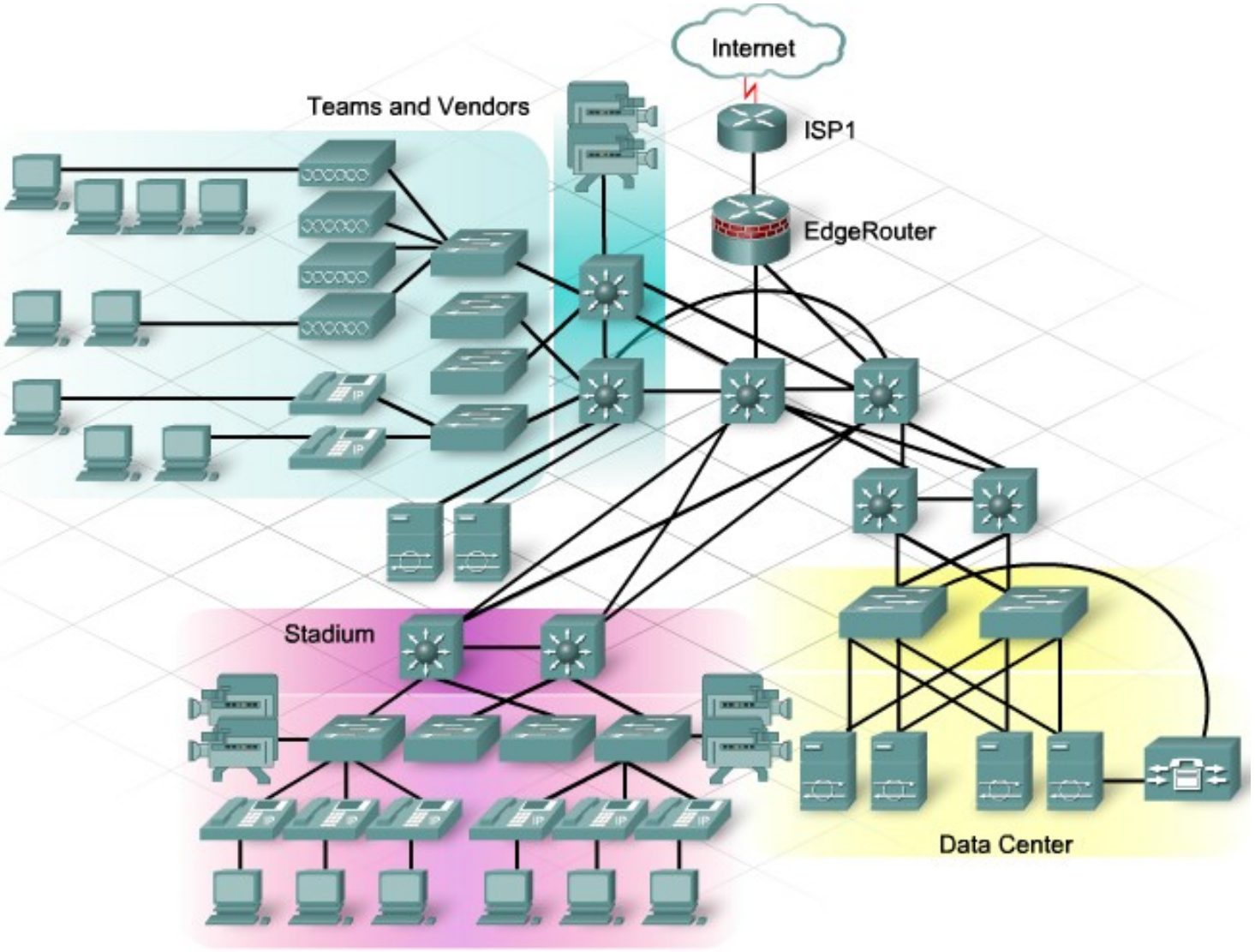
Creating the logical network Diagram for the WAN

- Creating the Logical LAN Diagram
- The final step in the preliminary LAN network design is to create the logical diagram for the new stadium network. This diagram shows how all of the various layers and devices interconnect.
- In the new stadium LAN, each of the 16 wiring closets contains at least one 2960 switch. Because there are three distinct modules in the stadium network, six Distribution Layer switches aggregate and route traffic between the Access Layer and the Core Layer.

Creating the logical network Diagram for the WAN

- The Core Layer consists of two high-end multilayer switches with redundancy. They are connected to the Distribution Layer and to each other with gigabit links.
- The network designer makes notes on the network diagram to indicate where the servers and IP services are located. After completing the wired campus LAN design, the designer then plans the portion of the network that supports remote connectivity into the stadium LAN.

Creating the logical network Diagram for the WAN



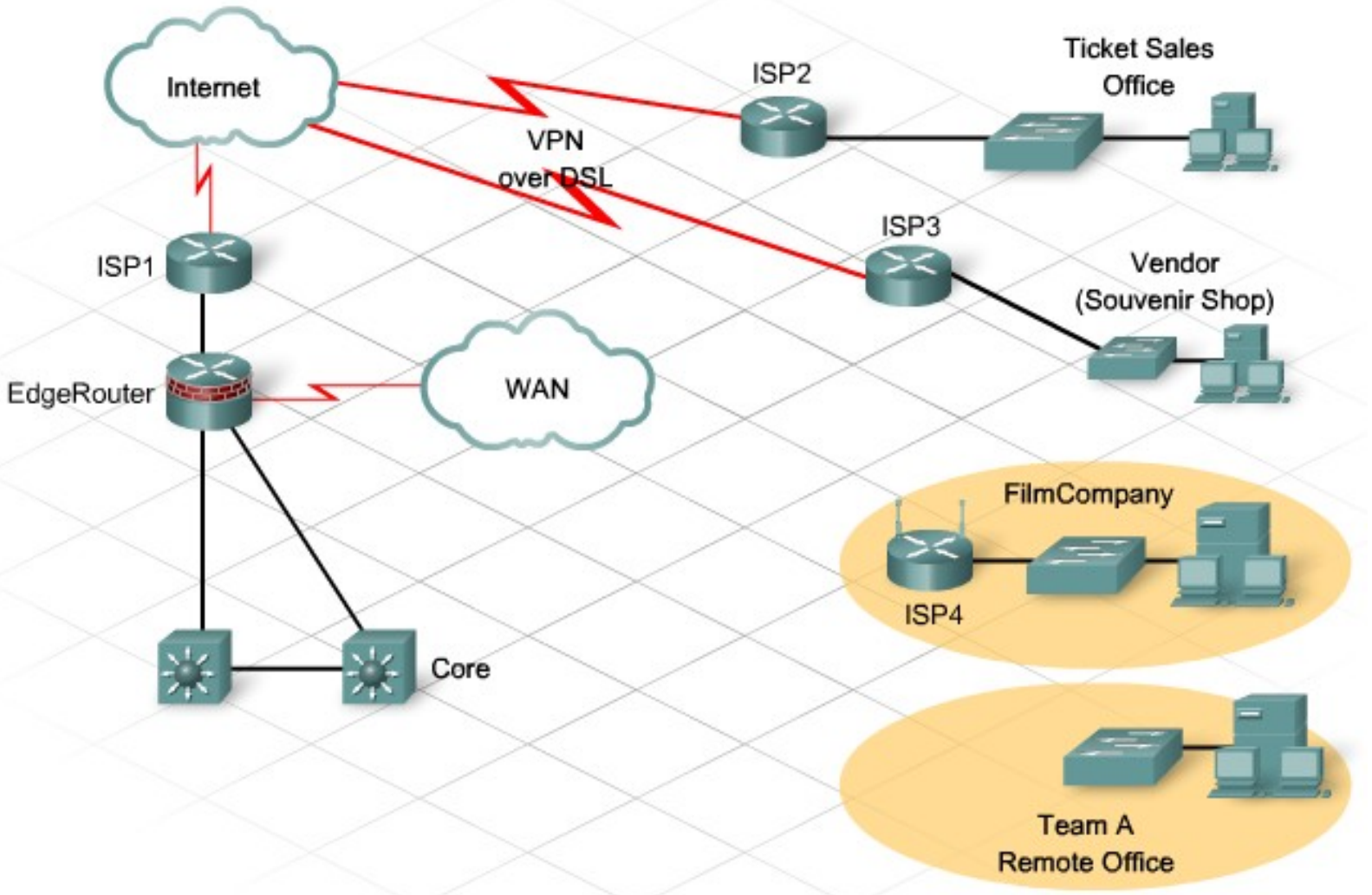
Determining Connectivity for the remote sites

- At the enterprise edge, the stadium network connects to the Internet via DSL provided by a local ISP. ISP-managed routers are located at the stadium connected to the EdgeRouter of the StadiumCompany.
- Extending Services to Remote Locations
- The two existing remote locations, a ticketing office located in the downtown area and a souvenir shop in a local shopping mall, use the same ISP provider as the main stadium site. The ISP also provides a managed VPN service to them. These connections provide the remote sites with access to the databases located on servers in the stadium management offices.

Determining Connectivity for the remote sites

- One of the high-priority goals of the new stadium network is to extend the voice and video network to the remote locations. There are two additional remote connections planned:
- A film production company, hired to provide video during and after events, needs to connect to the stadium network to exchange files.
- A sports team that currently leases space in the stadium is expanding to a remote office location. The team needs access to the same network resources that it uses on the stadium LAN.

Determining Connectivity for the remote sites



Determining Connectivity for the remote sites

- Adding New WAN Connections
- The network designer realizes that dedicated WAN connections are required to meet these new goals. A RFQ is sent to the Telecommunications Service Providers (TSPs) in the area to determine the cost and availability of WAN services.
- Because the stadium is located outside the city limits, the choices for WAN connectivity are limited to point-to-point T1 and Frame Relay. These services are available to both the stadium and the remote locations through a local TSP.

Determining Connectivity for the remote sites

- Although the point-to-point T1 service offers the most control over the quality of service available to the WAN sites, the Frame Relay service is less expensive. The network designer recommends that the stadium use Frame Relay to connect to the remote sites until a MetroEthernet or other high-speed service becomes available in the area.

Determining Connectivity for the remote sites

Options	Description	Advantages	Disadvantages	Bandwidth range	Sample protocols used
Circuit switching	A dedicated circuit path is created between end points. Best example is dialup connections.	Less expensive	Call Setup	28 Kbps to 144 Kbps	PPP, ISDN
Packet switching	Devices transport packets via a shared single point-to-point or point-to-multipoint link across a carrier internetwork. Variable length packets are transmitted over Permanent Virtual Circuits (PVC) or Switched Virtual Circuits (SVC).	Flexible bandwidth, less expensive	Shared media across link	56 Kbps to 45 Mbps	Frame Relay
Leased line	Point-to-Point connection between two computers or Local Area Networks(LANs).	Most Secure	Expensive	56 Kbps to 45 Mbps	PPP, HDLC, SDLC
Cell relay	Similar to packet switching, but uses fixed length cells instead of variable length packets. Data is divided into fixed-length cells and then transported across virtual circuits.	Best for simultaneous use of voice and data	Overhead can be considerable	1.54 Mbps to 622 Mbps	ATM

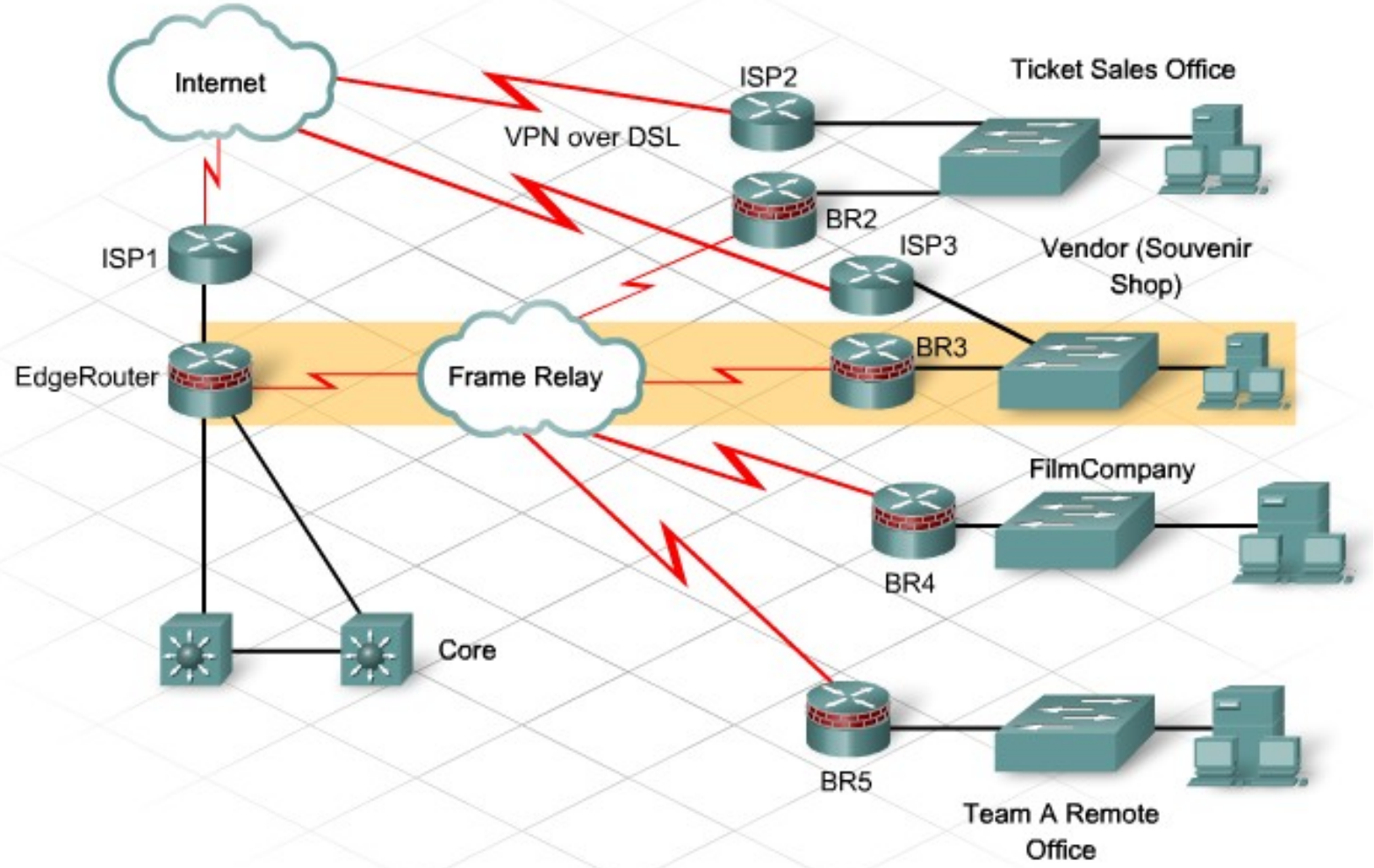
Determining Connectivity for the remote sites

- An advantage of using a Frame Relay connection over point-to-point T1 connections is that a single physical connection to the TSP can provide connectivity from the stadium to multiple remote site locations.
- Frame Relay Connection Types
- Frame Relay networks transfer data using one of these two connection types:

Determining Connectivity for the remote sites

- Switched Virtual Circuits (SVCs)-are temporary connections created for each data transfer and then terminated when the data transfer is complete.
- Permanent Virtual Circuits (PVCs)-are permanent connections. This type of connection is to be provided between the stadium network and the remote WAN sites.
- After discussions with stadium management, the NetworkingCompany staff decides to install a Frame Relay connection from the stadium to the souvenir shop as a pilot to test the dedicated WAN connectivitv.

Determining Connectivity for the remote sites



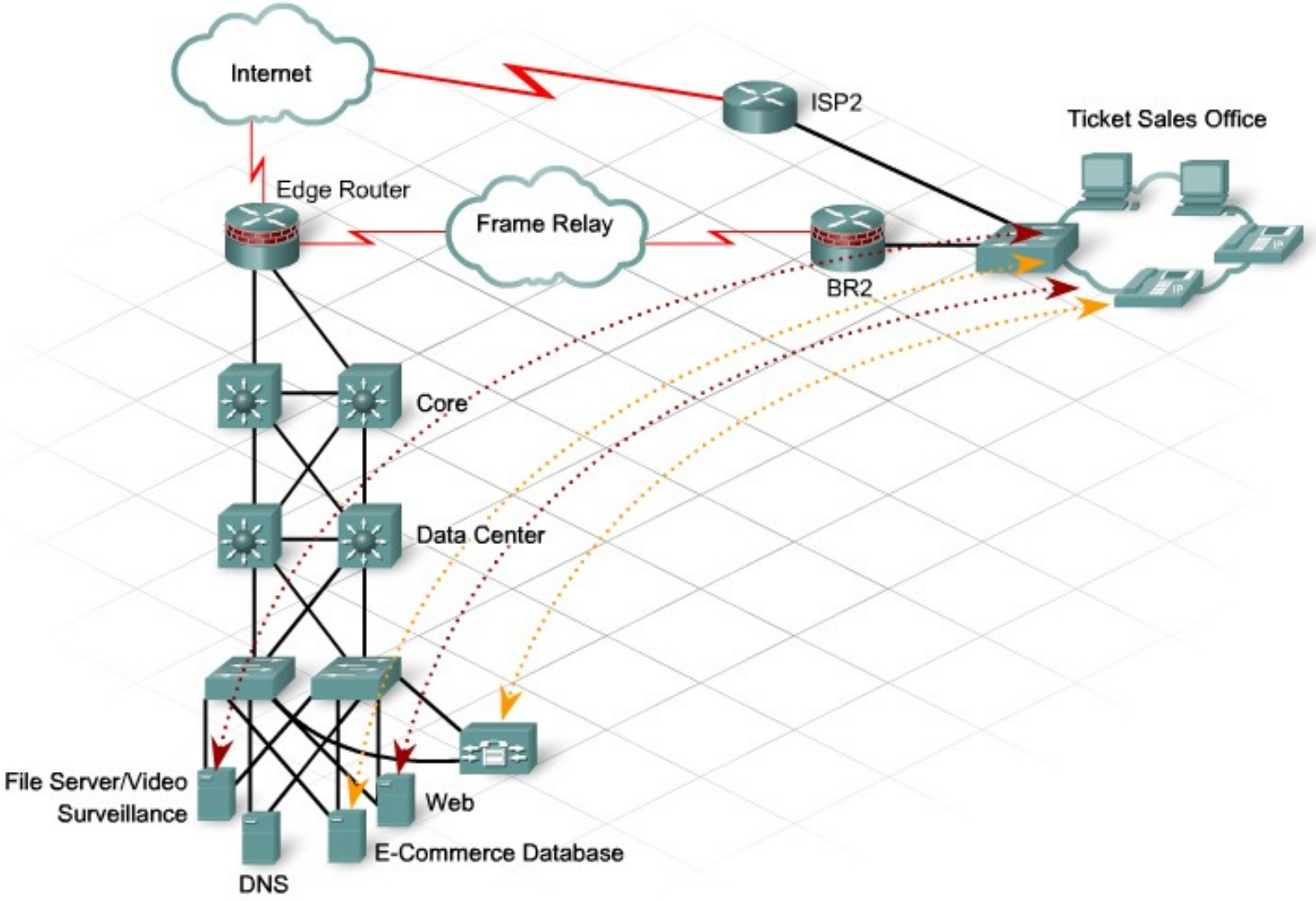
Defining Traffic Patterns and application support

- Network Services for Remote Sites
- When determining the physical method for connecting the remote sites to the main stadium network, the network designer must also analyze how workers at the remote sites expect to use the network services. The remote sites have some applications in common and some requirements that are unique. Services needed by the remote sites include:
- Access to the e-commerce and database services
- IP telephony
- Video surveillance and monitoring

Defining Traffic Patterns and application support

- In addition, the new remote team office requires access to the team payroll and accounting server located at the stadium.
- The FilmCompany employees need to be able to remotely monitor the video screens throughout the stadium and transfer video files to the stadium web servers.
- The designer makes a chart of the traffic flows from each WAN connection through the network to the various service locations.

Defining Traffic Patterns and application support



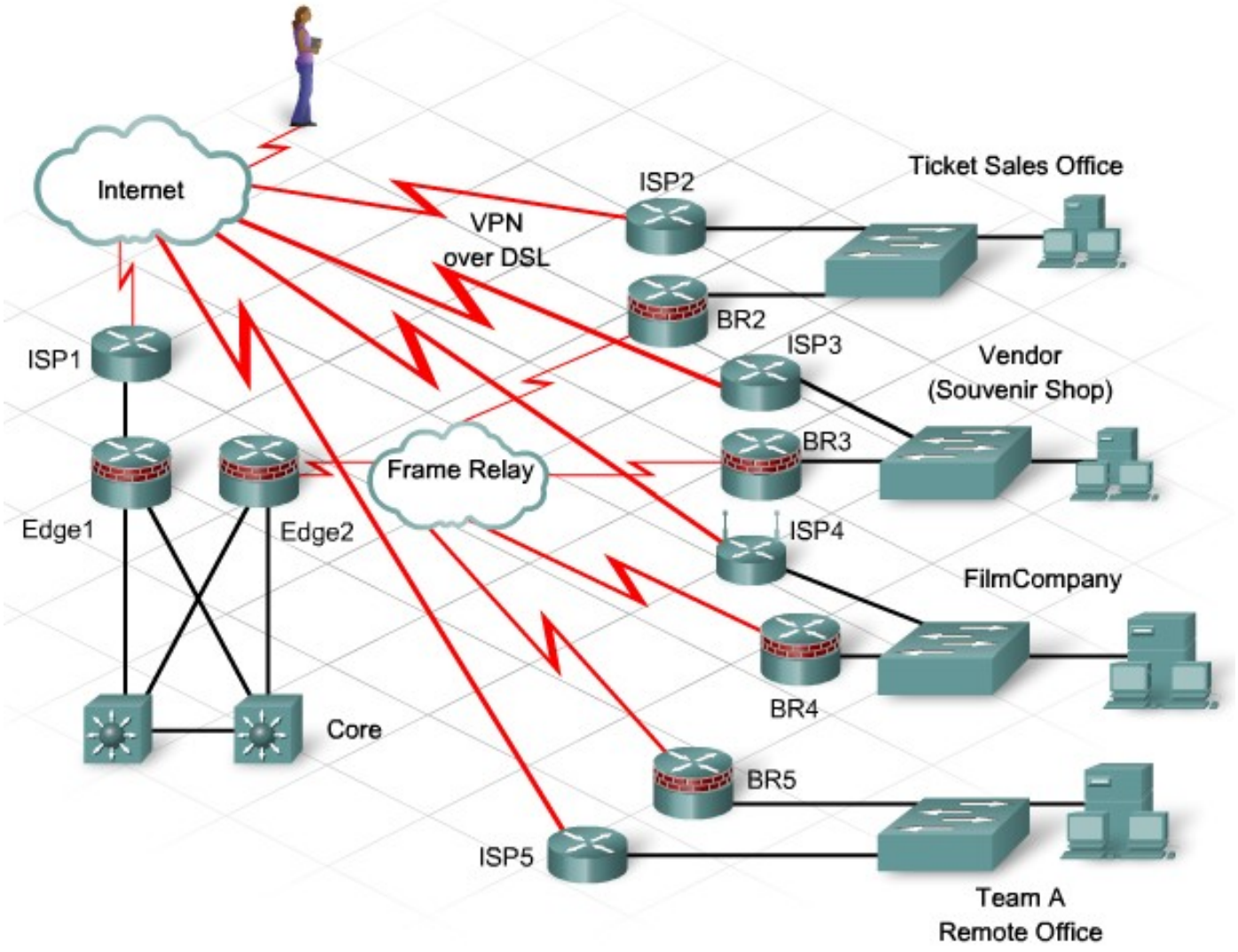
Designing VPN and End point Connectivity Options

- Backing up the Frame Relay Link
- The ticket sales office and the souvenir shop connect back to the stadium network using site-to-site VPNs through the Internet. The routers at the stadium and remote sites that provide end-points for each VPN are owned and managed by the ISP. The network designer plans to use these VPN connections as a backup to the Frame Relay dedicated connections, in the event that the Frame Relay link fails. The designer recommends a backup link from each of the two new sites as well. A second edge router at the main site is planned for redundancy.

Designing VPN and End point Connectivity Options

- Supporting Remote Workers
- The stadium management would also like to support remote workers who occasionally work from home or from other remote sites. The sports team personnel, for example, need to be able to access the team server securely when traveling. Client VPN access can be provided through the same ISP-managed service. The designer recommends that the stadium management investigate this option. They agree to contact the ISP to discuss the upgrade.

Designing VPN and End point Connectivity Options



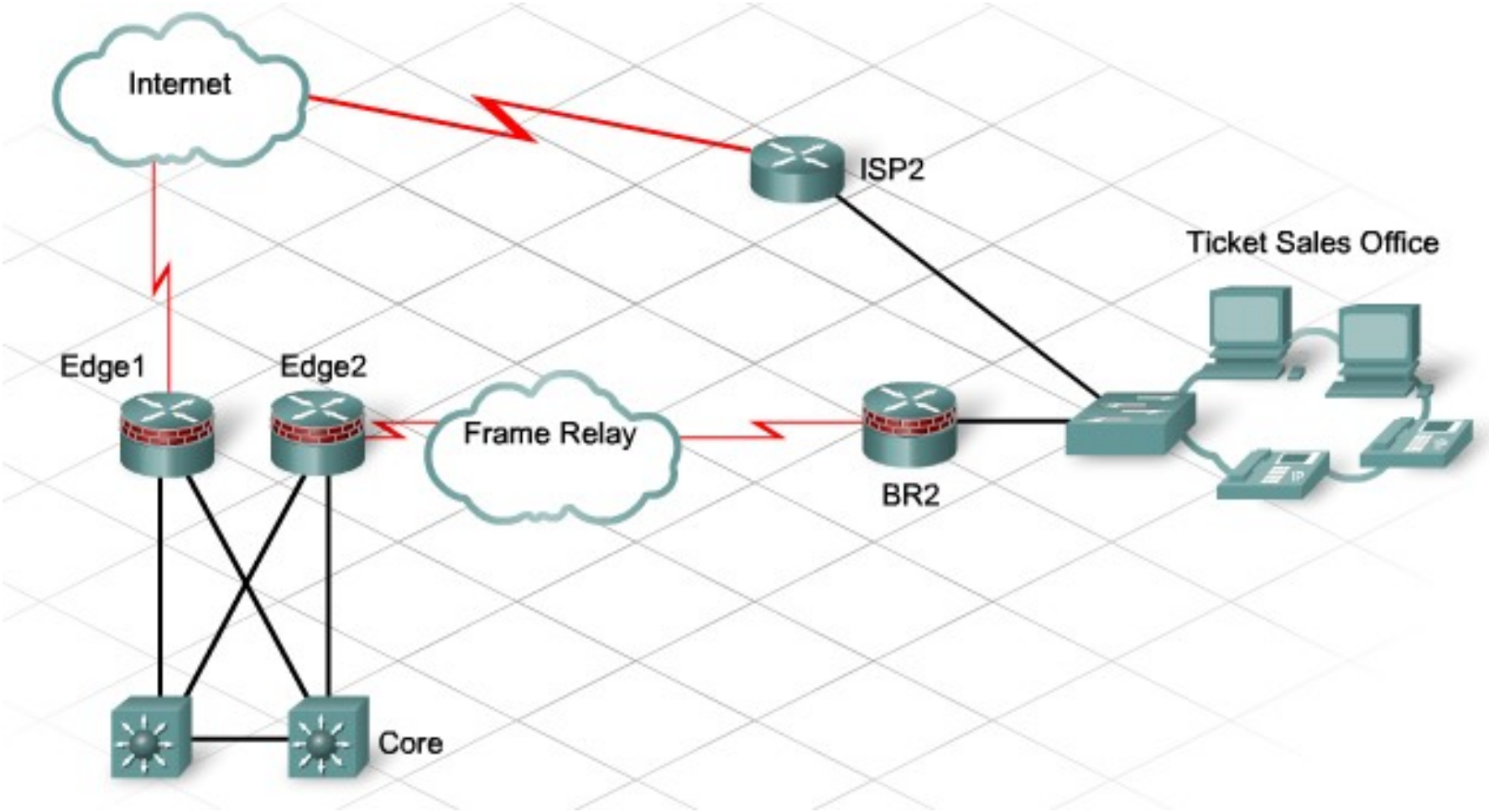
Creating the logical Network design for WAN

- Routing and IP Addressing
- In the existing network, the WAN sites use only the VPN to connect back to the stadium. Simple static routes are sufficient to ensure connectivity. DHCP addressing is provided to the remote site LANs by the ISP-managed services router.
- Providing both VPN and dedicated WAN connections to each site requires that the network designer carefully choose the IP address ranges that are used for each site. It may be necessary to change the address ranges for the remote sites.

Creating the logical Network design for WAN

The addition of the new WAN connection to each of the sites increases the number of possible paths to the stadium network from one to two. As a result, static routing may not be the best method used to ensure connectivity to the services on the stadium LAN. It may be necessary to use a dynamic routing protocol to enable the remote LANs to maintain connectivity in the event of a Frame Relay link failure. The network designer makes a note of this, so that it is considered when the stadium routing protocol implementation is designed.

Creating the logical Network design for WAN



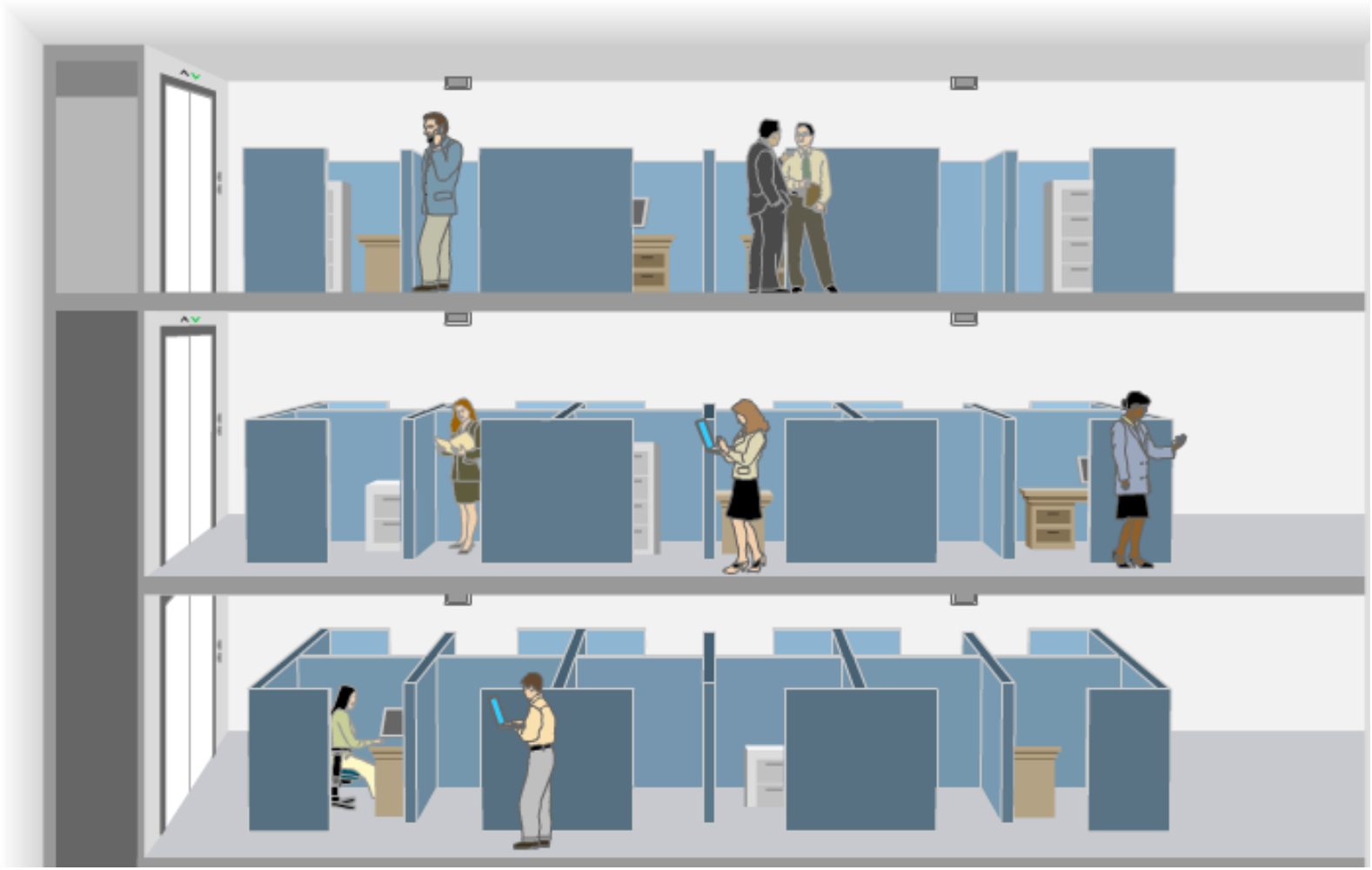
Designing Coverage options and mobility

- Adding Wireless Network Coverage
- A primary goal of the new design is to add wireless network coverage to the network.
- In response to requests from the local media, the stadium management added an inexpensive wireless AP to provide wireless Internet in the press box. Some employees also purchased wireless access routers, providing low-grade wireless coverage in the team offices. These types of devices are not robust enough for an enterprise LAN wireless implementation.

Designing Coverage options and mobility

- Wireless Network Coverage
- To meet the goals for the new stadium network design, wireless coverage is necessary in four identified areas:
- Press box
- Team lounge areas
- Stadium restaurant
- Luxury suites located around the stadium
- The two existing wireless APs need to be replaced with more manageable devices. Some areas require guest wireless access.

Designing Coverage options and mobility



Play 5.4.1

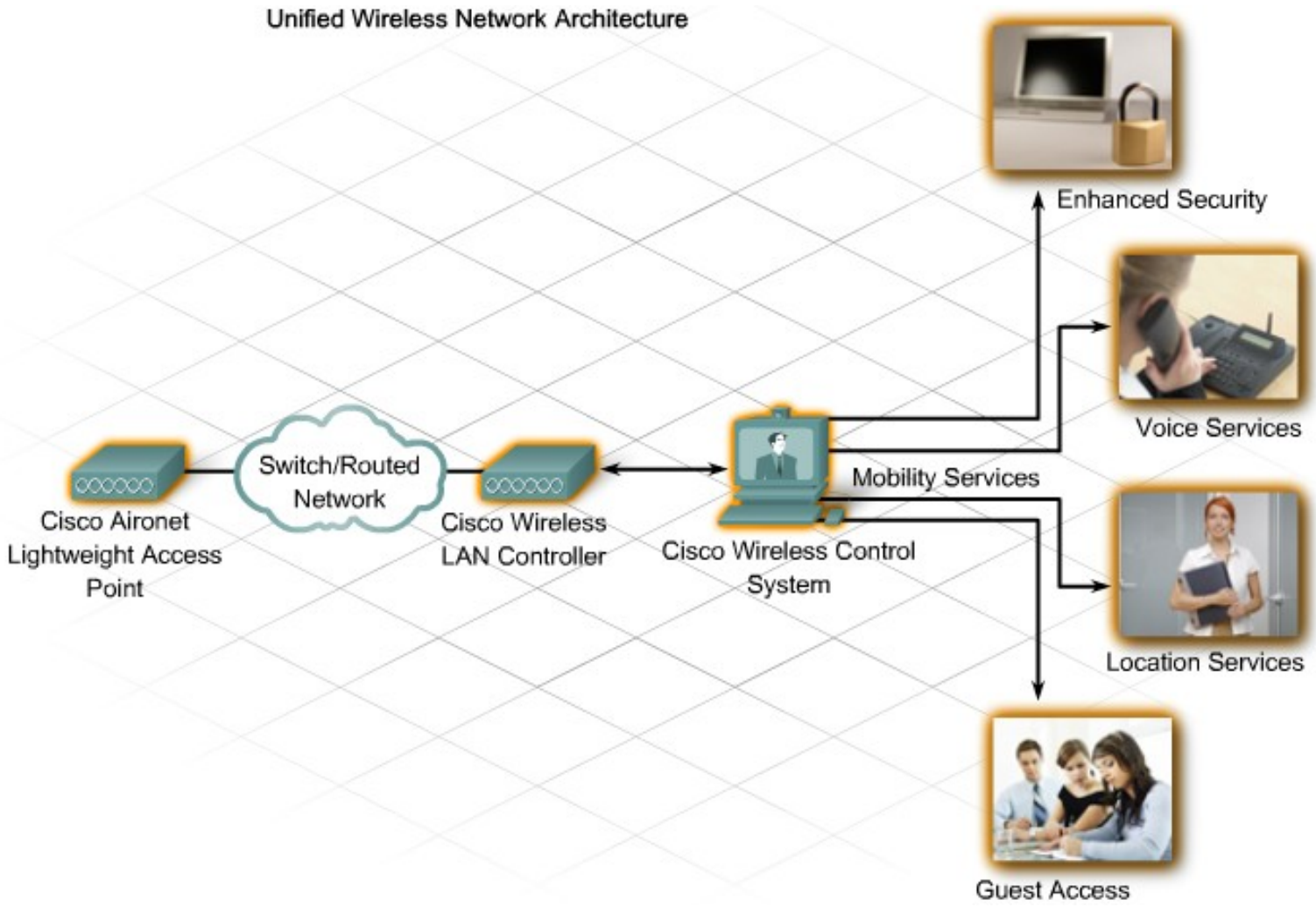
Designing Coverage options and mobility

- Unified Wireless and Wired Solutions
- Integration of the new wireless network with the wired stadium LAN simplifies management and makes use of the security and redundancy of the Ethernet infrastructure.
- Standalone APs connected to the Ethernet switches in the wiring closet can provide the necessary wireless coverage to the four previously identified areas in the stadium. Limited wireless roaming can be supported by creating wireless VLANs that span the network and wireless coverage areas that overlap.

Designing Coverage options and mobility

- Although this solution meets the current stadium network goals, the network designer recommends that the stadium purchase Lightweight Access Points LAPs and wireless LAN controllers to support the wireless requirements. LAPs are not standalone devices; they rely on the wireless controller for configuration and security information.
- Unified wireless network solutions that include wireless control system software offer advanced features, such as centralized management and multiple service levels for different user and client types. These systems allow different levels of QoS and security for different types of wireless use.

Designing Coverage options and mobility



Designing Coverage options and mobility

- The wireless solution proposed by the network designer meets the following requirements for the stadium network upgrade:
- Scalability - New LAPs can be added easily and managed centrally.
- Availability - APs can automatically increase their signal strength if one AP fails.

Designing Coverage options and mobility

- Security - Enterprise-wide security policies apply to all layers of a wireless network, from the radio layer through the MAC Layer and into the Network Layer. This solution makes it easier to provide uniformly enforced security, QoS, and user policies. These policies address the specific capabilities of different classes of devices, such as handheld scanners, PDAs, and notebook computers. Security policies also provide discovery and mitigation of DoS attacks, and detection and denial of rogue APs. These functions occur across an entire managed WLAN.

Designing Coverage options and mobility

- Manageability - The solution provides dynamic, system-wide RF management, including features that aid smooth wireless operations, such as dynamic channel assignment, transmit power control, and load balancing. The single graphical interface for enterprise-wide policies includes VLANs, security, and QoS.

Designing Coverage options and mobility

Lightweight Access Points

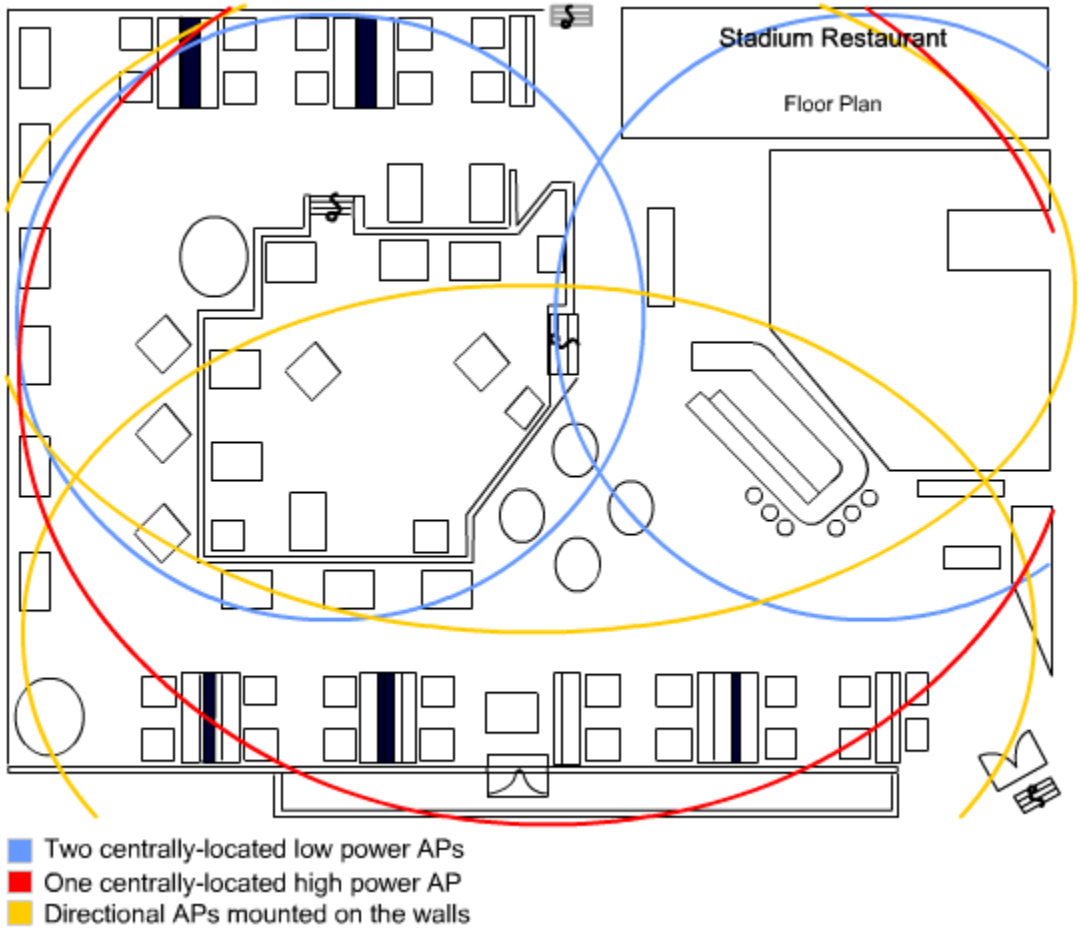
Wireless Controllers

Designing Coverage options and mobility

- The results of the stadium wireless site survey indicate that the restaurant requires at least two APs to provide high-quality wireless coverage.
- The network designer determines that to contain the wireless signal within the restaurant, it is best to mount directional APs against the two outside walls.
- The site survey did not uncover any issues that would cause wireless interference within the eating areas. However, the kitchen area microwave oven may cause interference near the bar.

Designing Coverage options and mobility

- Each of the 20 luxury suites located around the stadium requires a single, ceiling-mounted, low-power AP in the center of room.
- The press box currently has a single standalone AP that does not have adequate coverage. Two new lightweight APs are recommended.



Redundancy and resiliency in a wireless Network

- Availability Considerations
- The availability of a wireless connection is dependent on the following factors:
- Location of the AP
- Signal strength of the AP
- Number of users sharing the AP connectivity
- Wireless networks using standalone APs usually have the APs configured and deployed with the channel and power statically set. The channel and power settings are determined by the network designer.

Redundancy and resiliency in a wireless Network

- Dynamic Reconfiguration
- In contrast to the autonomous APs, wireless LAN controllers automatically determine the signal strength that exists between lightweight APs within the same network. These controllers can use this information to create a dynamic, optimal RF topology for the network.
- When a Cisco LAP boots, it immediately looks for a wireless LAN controller within the network. When it detects a wireless LAN controller, the AP sends out encrypted neighbor messages that include the MAC address and signal strength of any neighboring APs.

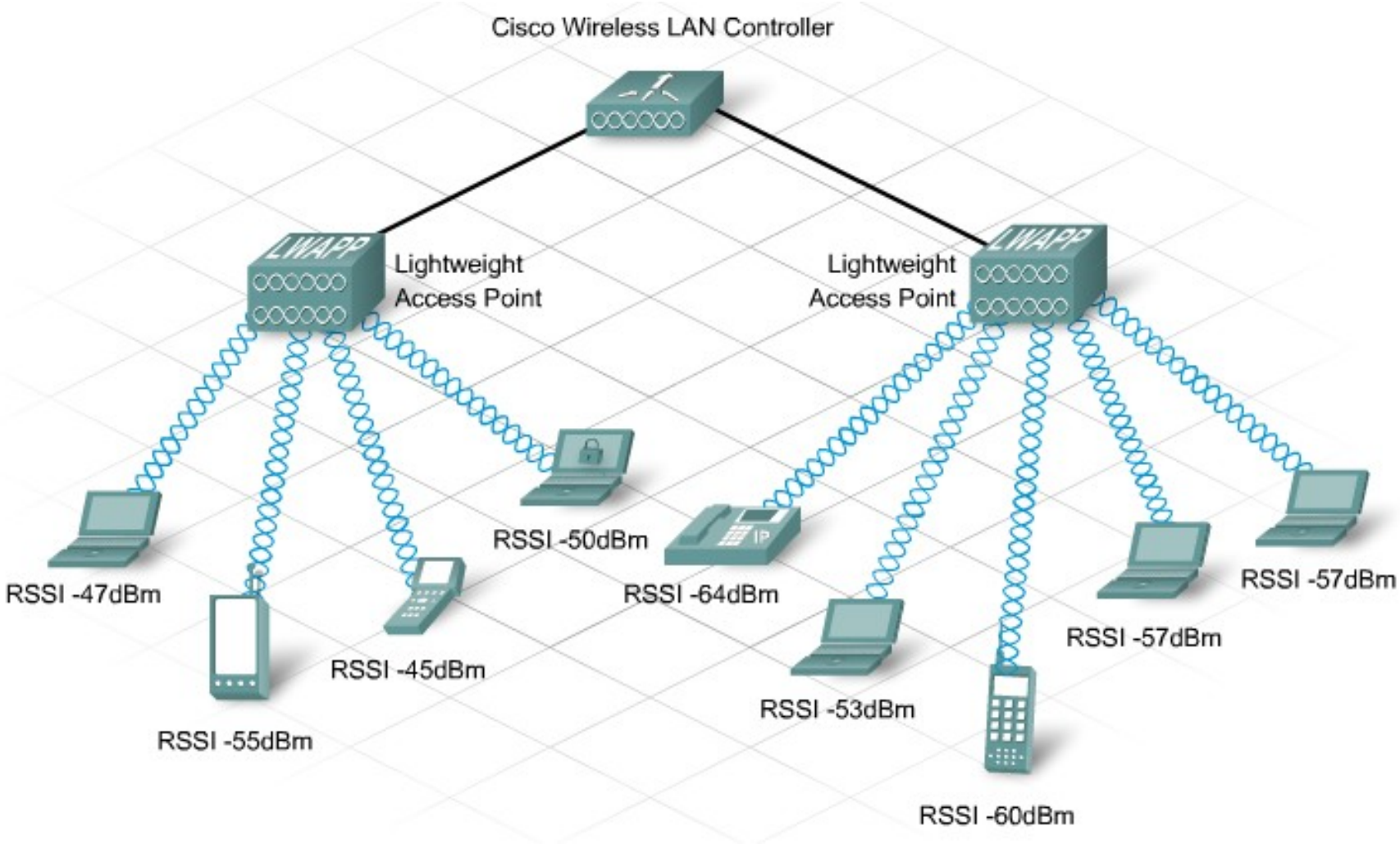
Redundancy and resiliency in a wireless Network

- Centralization Load Balances Users
- Through encrypted over-the-air messages, Cisco wireless LAN controllers detect the entire network. These controllers also detect signal strength between APs. When a client looks for an AP to connect to, a probe is sent to the controller from each AP that hears the request from the client. The controller determines which AP responds to the request from the client, taking into account the signal strength of the client and signal-to-noise ratio.

Redundancy and resiliency in a wireless Network

- For example, an adjacent AP may provide an equivalent service but at a lower signal strength. The controller determines which AP should respond to the probe from the client, based on its signal strength, or Receiver Signal Strength Indicator (RSSI).
- These measures improve the availability of wireless services within the WLAN. Wireless controllers centrally located in the data center benefit from the high availability and redundant connections contained in the wired LAN.

Redundancy and resiliency in a wireless Network



Creating the Logical Network Design for a WAN

- IP Addressing in a WLAN
- The network designer must also consider the IP addressing structure when planning wireless roaming in a WLAN. In the case of standalone APs, a single VLAN is created and extended to all of the wiring closets to connect the APs in the same Layer 3 IP network. However, if a large number of wireless users connect to the network, broadcasts become a problem. The network is no longer scalable.

Creating the Logical Network Design for a WAN

- Layer 3 Roaming
- When using the wireless controllers and lightweight APs, Layer 3 roaming can be introduced into a network. It is not necessary to extend VLANs to all of the APs in the network to keep a flat wireless subnet.
- With the wireless controller, the lightweight APs are installed in the normal subnet infrastructure and are given an IP address that is local to the subnet to which they are deployed. All traffic that comes from wireless clients is placed into a packet that is tunneled through the underlying network to the wireless LAN controller.

Creating the Logical Network Design for a WAN

Play 5.4.4

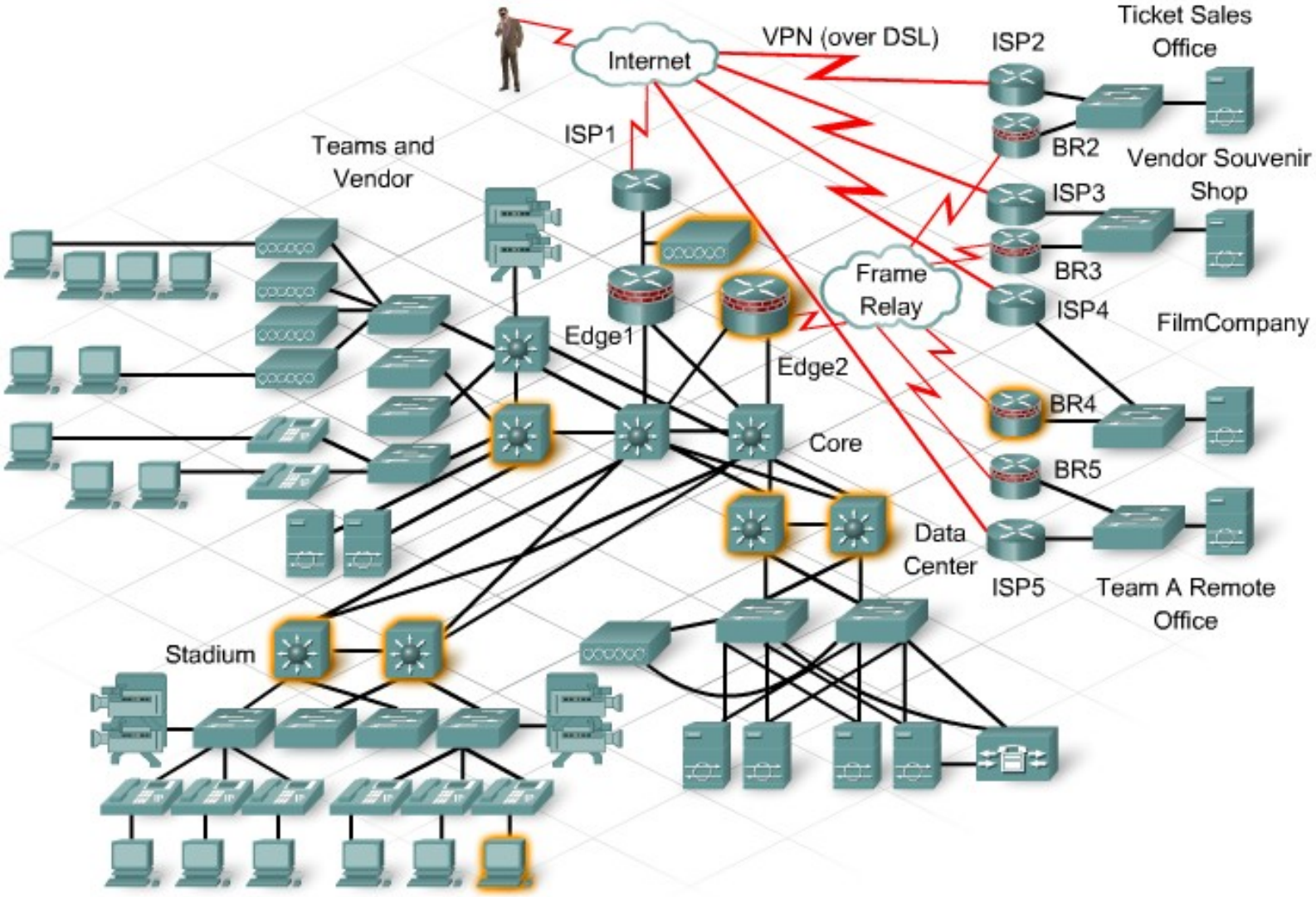
Placing security functions and appliances

- Threats to networks can come in many different forms, and from both internal and external sources. Simply placing a firewall at the enterprise edge does not ensure network security. The network designer must identify which data and communications are at risk and what the potential sources of attacks are. Security services then need to be placed at appropriate points throughout the network design to prevent likely attacks.

Placing security functions and appliances

- The e-commerce servers on the stadium network contain customer information that may include credit card and banking details. Users access these servers from within the stadium network and through the Internet.
- The stadium management and team administrative servers contain personnel and payroll information. These servers, and the infrastructure that transports the data they contain, must be secured adequately to protect this information from unauthorized use.
- Security measures relating to the stadium wireless network need to be considered as well.

Placing security functions and appliances



Placing security functions and appliances

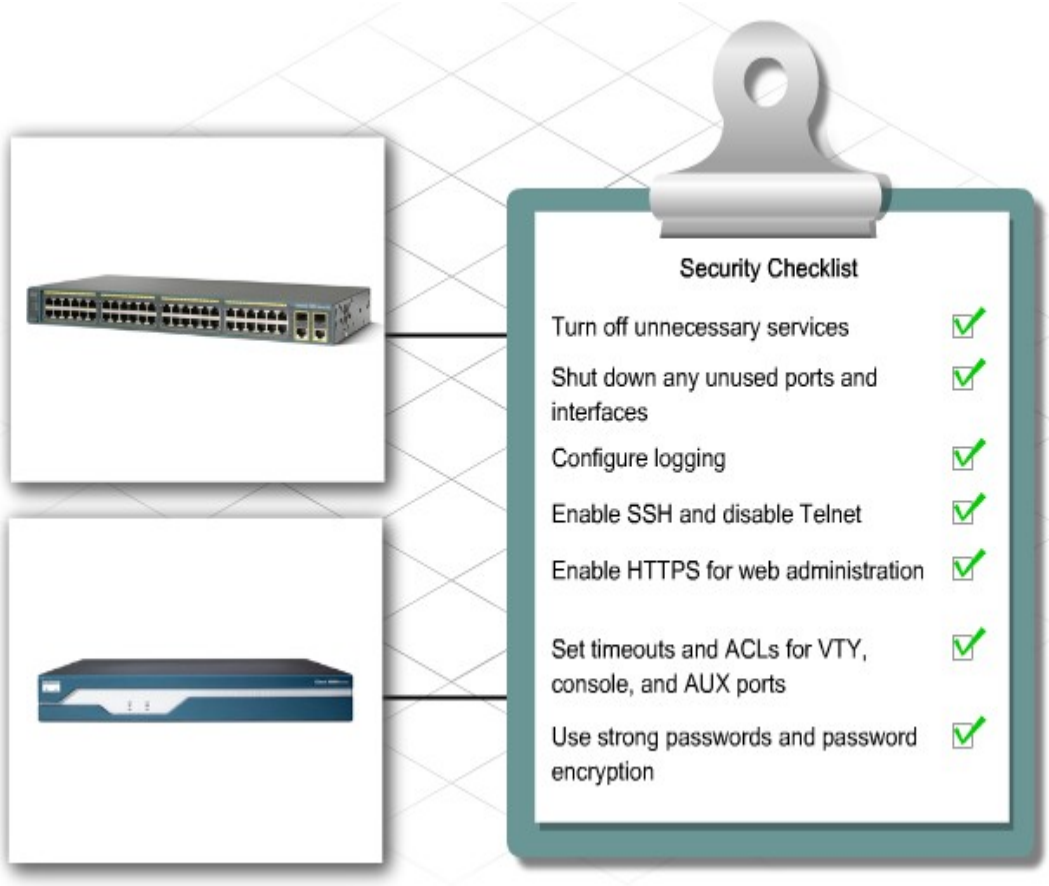
- Security services help protect the devices and the network from intrusion, tampering, altering of data, and disruption of services through Denial of Service (DoS) attacks. The primary categories of security services include:
- Infrastructure protection
- Secure connectivity
- Threat detection, defense, and mitigation

Placing security functions and appliances

- Infrastructure Protection
- Network security begins with securing the network devices themselves. This involves securing Cisco IOS software-based routers, switches, and appliances from direct as well as indirect attacks. This protection helps to ensure availability of the network for data transport.
- Secure Connectivity
- It is critical to prevent unauthorized users from accessing the network. This can be done by ensuring that the physical network is secure, and by requiring authentication to gain access to wireless services.

Placing security functions and appliances

- Threat Detection, Defense, and Mitigation
- Firewalls, IDS, IPS and ACLs provide protection from threats and attackers. ACLs and firewall rules filter traffic to permit only desirable traffic through the network.

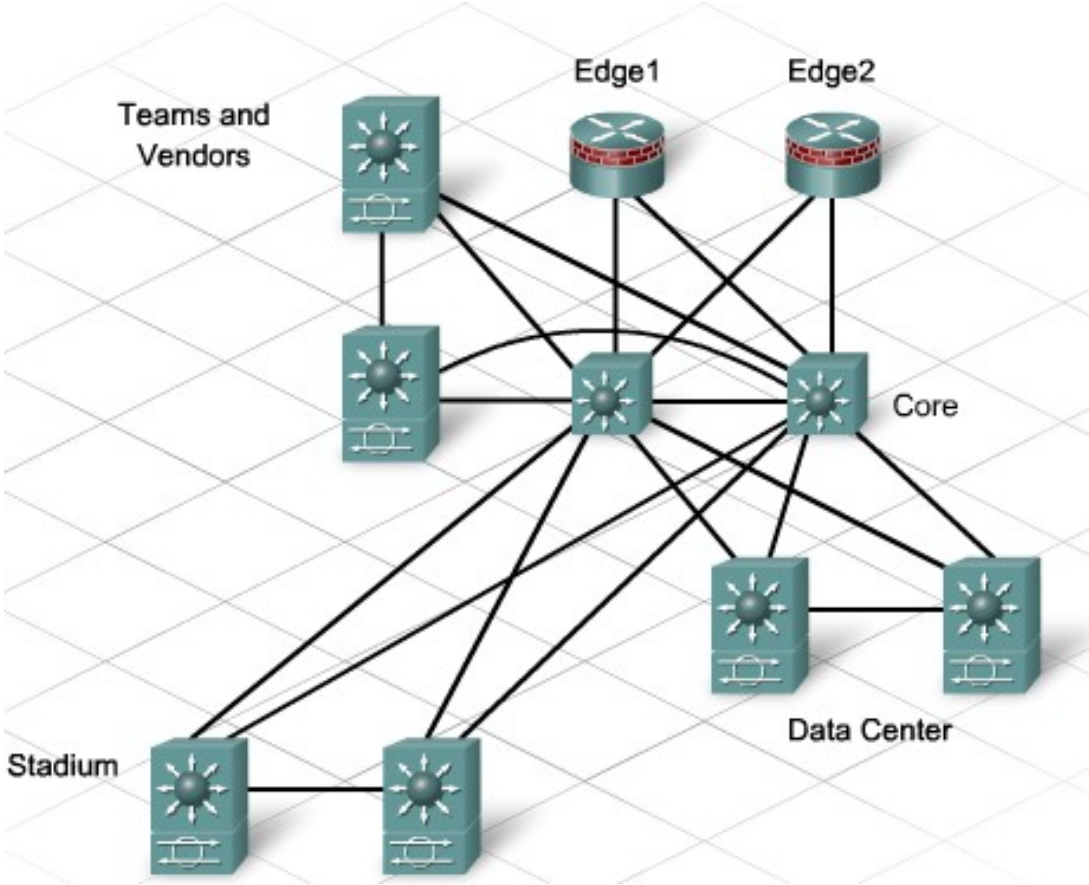


Placing security functions and appliances

- Implementing Security Services
- Security services are not effective if they are not implemented at the correct locations throughout the network. Firewalls and filters placed at the enterprise edge do not protect servers from attacks from within the LAN. The network designer analyzes the traffic flow diagrams that were created earlier that show:
- Resources that are accessed by internal users
- Resources that are accessed by external users
- Paths that this access takes through the network

Placing security functions and appliances

- Using Integrated Services
- Wherever possible, the network designer uses integrated services, such as IOS-based firewall features and IDS modules to eliminate the need for additional security devices. In a larger network, it is necessary to use separate devices because the additional processing can cause routers and switches to become overloaded.



Implementing Access Control List and Filters

- The network designer works with the stadium IT staff to define the firewall rule sets to be implemented in the stadium network upgrade.
- Examples of firewall rule sets include these statements:
- Deny all inbound traffic with network addresses matching internal-registered IP addresses - Inbound traffic should not originate from network addresses matching internal addresses.
- Deny all inbound traffic to server external addresses - This rule includes denying server translated addresses, with the exception of permitted ports.

Implementing Access Control List and Filters

- Deny all inbound ICMP echo request traffic - This rule prevents internal network hosts from receiving ping requests generated from outside the trusted network.
- Deny all inbound Microsoft Domain Local Broadcasts, Active Directory, and SQL server ports - Microsoft domain traffic should be carried over VPN connections.
- Allow DNS (UDP 53) to DNS server - Permit external DNS lookups.
- Allow web traffic (TCP 80/443) from any external address to the web server address range.

Implementing Access Control List and Filters

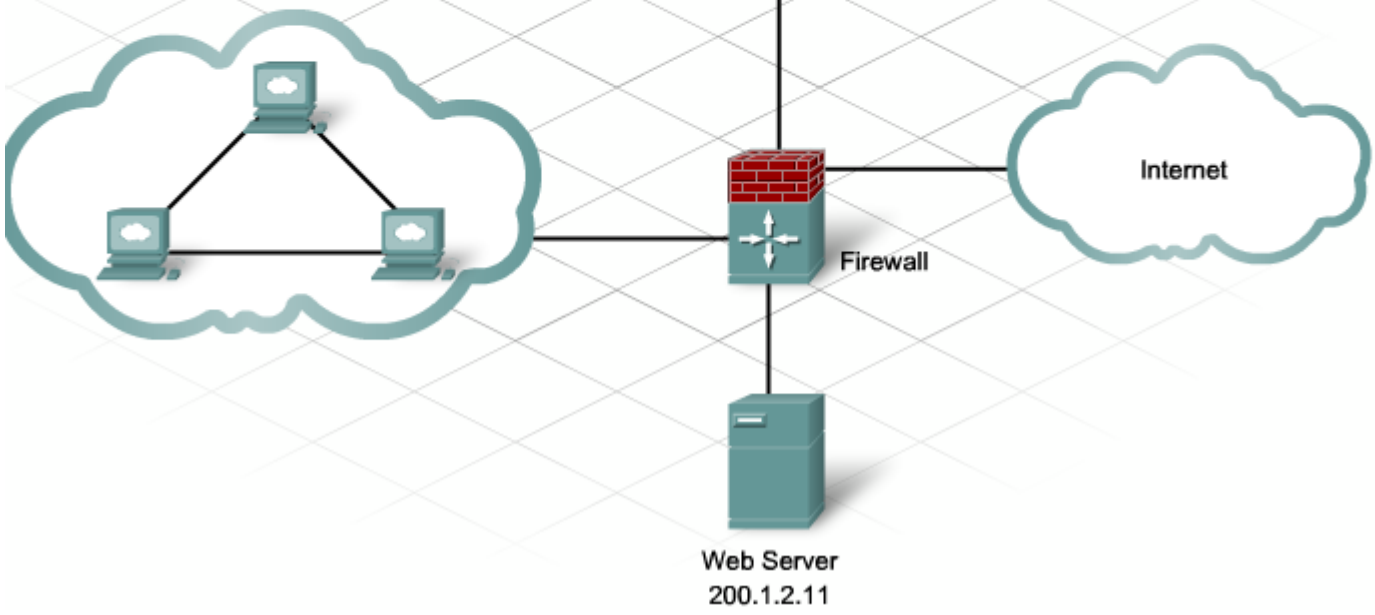
- Allow traffic (TCP 21) to FTP server address ranges - If FTP services are provided to external users, this rule permits access to the FTP server. As a reminder, when using FTP services, user account and password information is transmitted in clear text. Use of passive FTP (PASV) negotiates a random data port versus the use of TCP port 20.
- Allow traffic (TCP 25) to SMTP server - Permit external SMTP users and servers access to internal SMTP mail server.
- Allow traffic (TCP 143) to internal IMAP server - Permit external IMAP clients access to internal IMAP server.

Implementing Access Control List and Filters

Firewall Rule:
Deny all inbound traffic from the Internet to a Web Server except on the permitted ports.

Access Control List statements:

```
access-list 112 permit tcp any host 200.1.2.11 eq www
access-list 112 permit tcp any host 200.1.2.11 eq ftp
access-list 112 permit tcp any host 200.1.2.11 eq 7000
access-list 112 permit tcp any host 200.1.2.11 eq 1755
access-list 112 permit tcp any host 200.1.2.11 eq 1720
access-list 112 deny ip any host 200.1.2.11 log
```



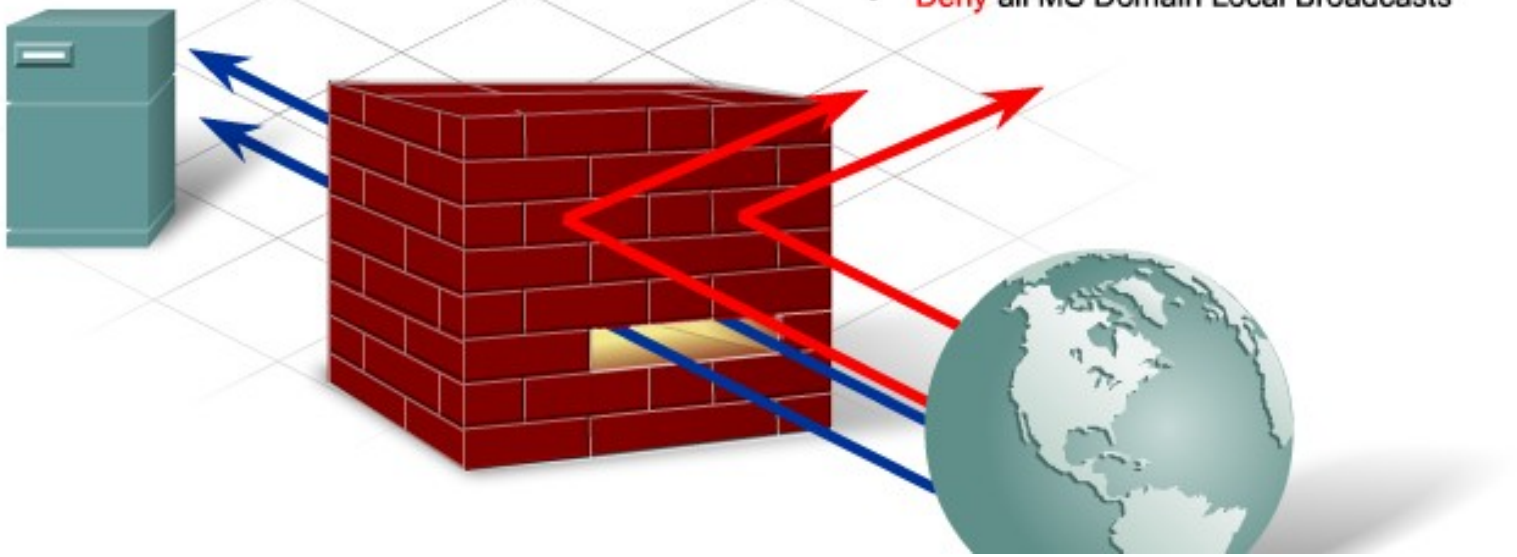
Implementing Access Control List and Filters

- The security policies of the stadium management dictate user and group permissions to resources. The designer also complies with the recommended practices defined by the server operating system vendors. These practices help to identify and filter traffic that is known to be malicious.
- When designing firewall rule sets and ACLs, the general policy is to deny all traffic that is either not specifically authorized or is not in response to a permitted inquiry.

Implementing Access Control List and Filters

- Allow web traffic from any external address to the web server
- Allow traffic to FTP server
- Allow traffic to SMTP server
- Allow traffic to internal IMAP server

- Deny all inbound traffic with network addresses matching internal-registered IP addresses
- Deny all inbound traffic to server external addresses
- Deny all inbound ICMP echo request traffic
- Deny all inbound MS Active Directory
- Deny all inbound MS SQL server ports
- Deny all MS Domain Local Broadcasts



Implementing Access Control List and Filters

- Rule Sets and Access Control Lists
- Firewall rule sets are used to create the ACL statements that are implemented on the routers and firewall appliances. Each firewall rule set may require more than one ACL statement and may require both inbound and outbound placement.

Updating the Logical Network Design Documentation

- The design documentation includes all firewall rule sets and ACLs and defines where they are implemented. Rule set statements become part of the stadium management security policy documentation.
- Documenting the firewall rule sets and the ACL placement offers these benefits:
- Provides evidence that the security policy is implemented on the network
- Ensures that when changes are necessary, all instances of a permit or deny condition are known and evaluated
- Assists in troubleshooting problems with access to applications or segments of the network