CCNA Discovery 4.0 Designing and Supporting Computer Networks

Identifying Application Impacts on Network Design– Chapter 4

Cisco Networking Academy®
Mind Wide Open™

Objectives

- Explain how the characteristics of various applications affect the design of the network.
- Describe the network requirements of various common applications, including voice and video.
- Explain the need for Quality of Service to support converged networking, and methods to implement it in the network design.
- Diagram the various application traffic flows to determine where bandwidth is needed and where potential bottlenecks exist.

The importance of application performance

- Most people who use network services know very little about the underlying network or network design. Their experience as users is based on how they interact with the applications that run on the network.
- In the case of the sports stadium, network-based applications provide essential services to the fans, the teams, and the management. These services, and the network on which they reside, are among the business-critical elements ensuring that customer and user demands are met.

The importance of application performance

- Gathering statistical information from routers, servers, and other network devices helps determine whether a system is functioning to manufacturer specifications. However, technical considerations alone do not determine success in the marketplace.
- Success depends on how the customer, the suppliers, and the vendors view the performance of the network.

The importance of application performance

- For end users, application performance is based on:
- Availability-Is the application working when they need it?
- Responsiveness-Is the application responding as quickly as expected?
- For example, in the stadium, revenue from ticket sales, concessions, and souvenirs suffers when transaction processes are not available or are taking too long to complete.

The importance of application performance

- Stadium customers rate the convenience of an application by the length of time it takes to complete the transaction. They also expect the application to be available whenever they want to use it.
- Applications for which fast response time is considered critical for the user include:
- Interactive kiosk services
- Point-of-sale ticket machines
- Concession registers

The importance of application performance

- Applications considered critical by stadium personnel include:
- Emergency services
- Voice and video monitoring and transmission
- The measurement of application performance should combine user satisfaction with normal technical metrics, such as throughput on the network, or the number of successful transactions.

The importance of application performance

Characteristics of Different Application Categories

- In an existing network, application characterization helps the network designer to incorporate business goals and technical requirements into the network design.
- The application characterization process involves looking at the following aspects of network applications:
- How the applications work on the network
- The technical requirements of the application
- How applications interact with each other on the network

Characteristics of Different Application Categories

- From the information gathered during the early phases of the design process, the designer determines which applications are considered business-critical.
- The characterization process provides information about network bandwidth usage and response times for specific applications. These parameters influence design decisions, including:
- Selection of the transmission medium
- Estimates of required bandwidth

Characteristics of Different Application Categories

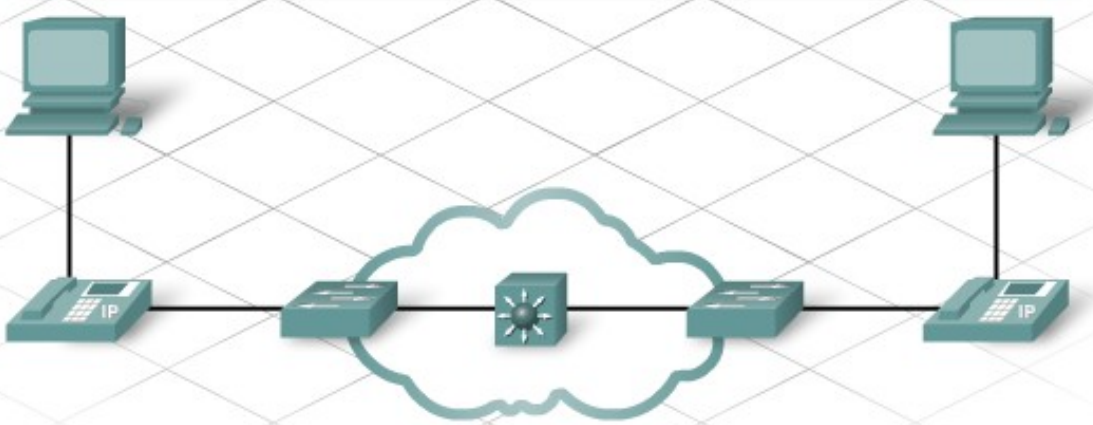
- Traffic from different types of applications results in varying network demands. The network designer recognizes four main types of application communication:

- Client-to-client
- Client-to-distributed server
- Client-to-server farm
- Client-to-enterprise edge

Characteristics of Different Application Categories

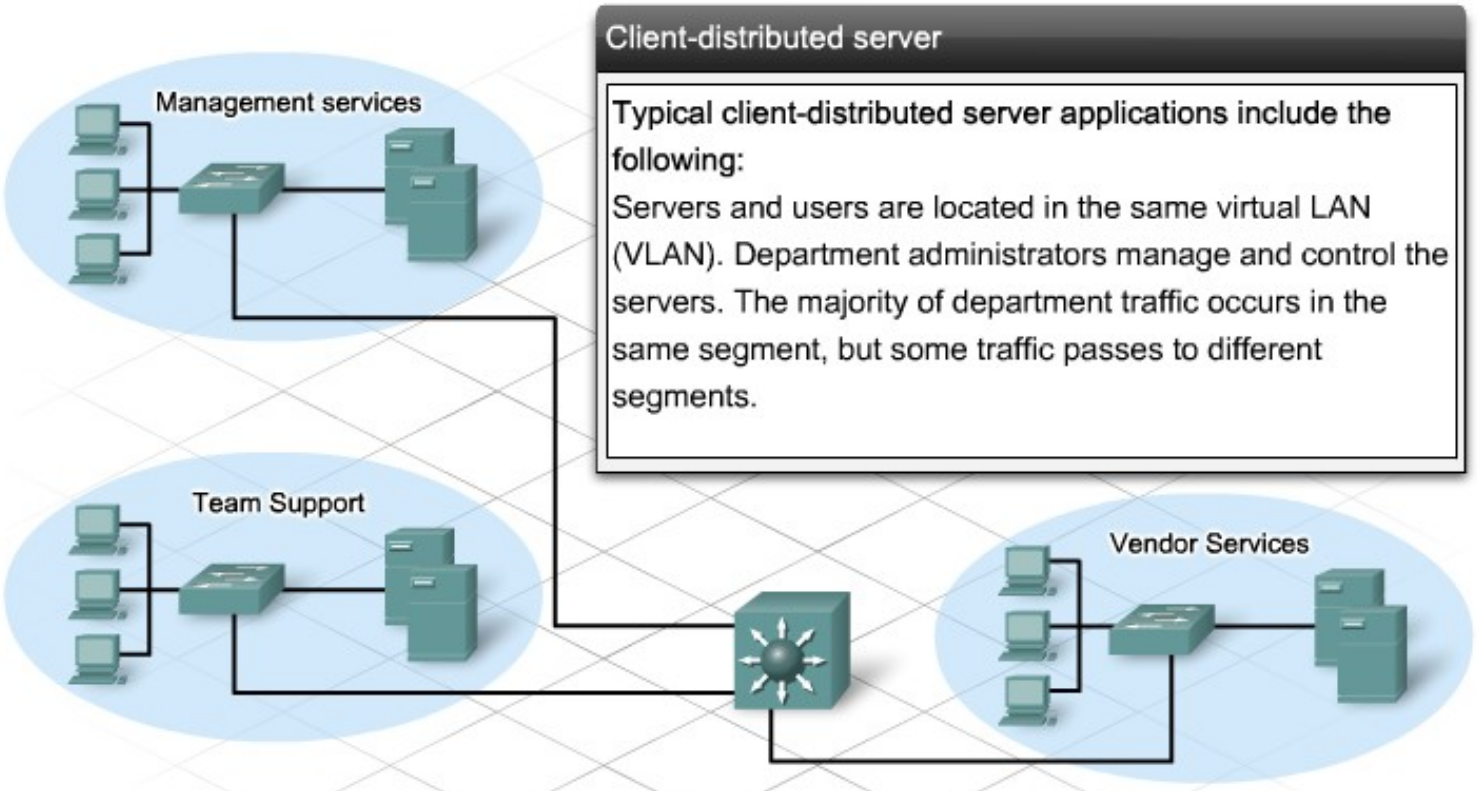
Client-client

Typical client-client applications include the following:
IP telephony - Two peers establish communication with the help of a telephone manager workstation; however, the conversation occurs directly between the two peers when the connection is established.

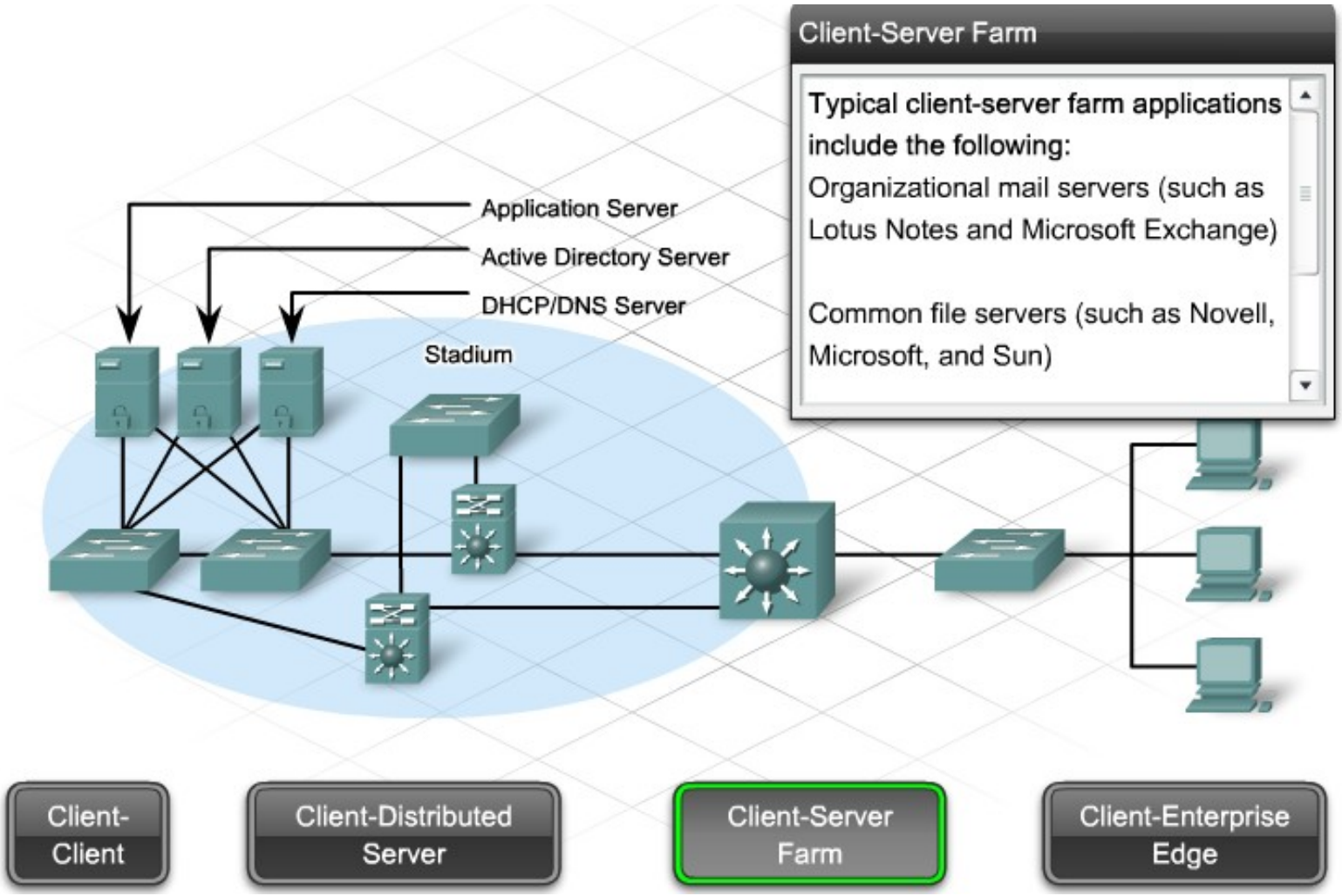


Client-Client | Client-Distributed Server | Client-Server Farm | Client-Enterprise Edge

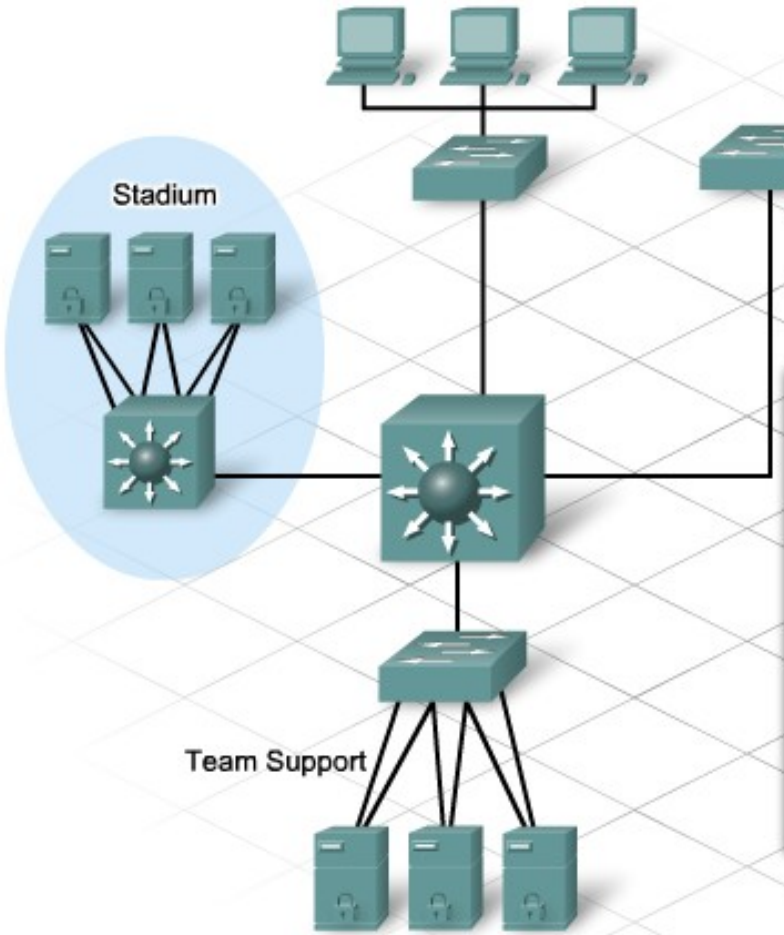
Characteristics of Different Application Categories



Characteristics of Different Application Categories



Characteristics of Different Application Categories



Client-Enterprise Edge

Typical client-enterprise edge applications include the following:

Applications installed on the Enterprise Edge can be crucial to organizational process flow; therefore, any outages can increase costs. Typical Enterprise Edge applications are based on web technologies. Some examples

Client-Client | Client-Distributed Server | Client-Server Farm | Client-Enterprise Edge

Characteristics of Different Application Categories

- On an existing network, the first step in characterizing applications is to gather as much information about the network as possible. This includes gathering information from:

- Organizational input
- Network audit
- Traffic analysis

Characteristics of Different Application Categories

- Organizational Input
- Organizational input consists of existing documentation about the network and verbal input from the stadium personnel. During the early phases of design, obtaining input is easy but not always reliable. For example, application changes such as upgrades or user-installed software may go undocumented or unnoticed.
- Network Audit
- A network audit gathers information about network devices, monitors traffic, and reveals details of the current network configuration.

Characteristics of Different Application Categories

- Traffic Analysis

- Traffic analysis provides information about how the applications and protocols use the network. It can reveal shortcomings in the network. For example, several high-bandwidth applications using the same medium can generate large amounts of traffic. This could be a potential weakness in the current design.

Characteristics of Different Application Categories

- Cisco IOS Software Embedded Tools

- Network-Based Application Recognition (NBAR) is a Cisco utility that conducts audits and traffic analysis. NBAR is a classification engine that recognizes a wide variety of applications. NBAR recognizes web-based and other difficult-to-classify protocols that utilize dynamic TCP and UDP port assignments.

Characteristics of Different Application Categories

- Another tool is Cisco IOS NetFlow. NetFlow efficiently provides a set of services for IP applications. Services include:
- Network traffic accounting
- Usage-based network billing
- Network planning
- Security
- Denial of Service monitoring capabilities
- Network monitoring

Characteristics of Different Application Categories

Sample NBAR Printout

```
Router# show ip nbar protocol-discovery interface FastEthernet 6/0
 FastEthernet6/0
                              Input                     Output
   Protocol                   Packet Count              Packet Count
                              Byte Count                Byte Count
                              5 minute bit rate (bps)   5 minute bit rate (bps)
   ------------------------   ------------------------  ------------------------
   igrp                       316773                    0
                              26340105                  0
                              3000                      0
```

Sample NetFlow Printout

```
Router# show ip cache flow
IP packet size distribution (2381 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .092 .000 .003 .000 .141 .048 .000 .000 .000 .093 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .048 .189 .381 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  22 active, 4074 inactive, 45 added
```

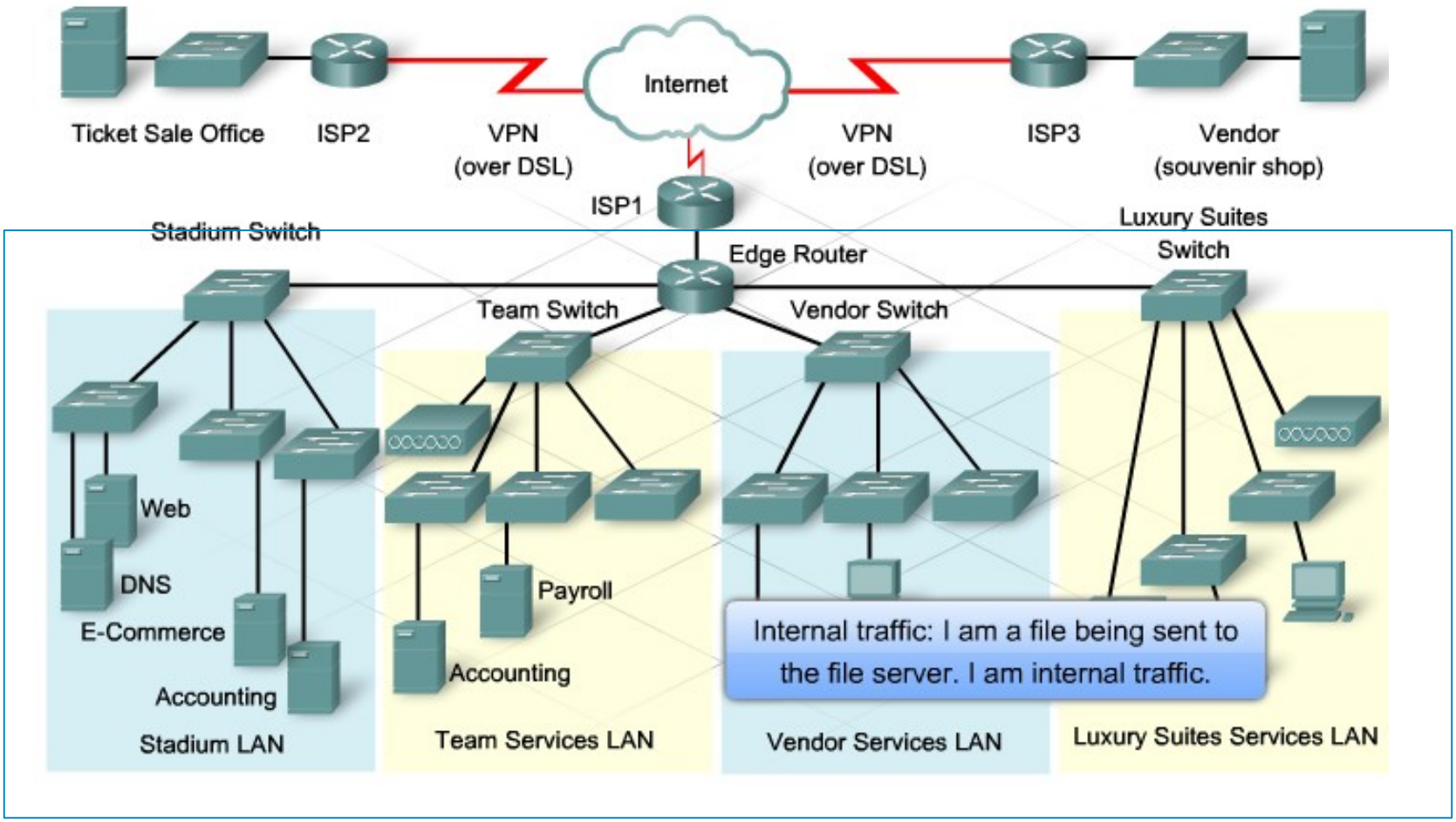
How traffic flow affects network design

- Internal Traffic
- Internal traffic is generated by local hosts and is destined for other hosts within the campus network. Diagramming internal traffic flows can show areas where high bandwidth connections are needed, as well as identify possible bottlenecks where traffic might become congested. These diagrams assist the designer to select the appropriate equipment and infrastructure to support the traffic volumes.

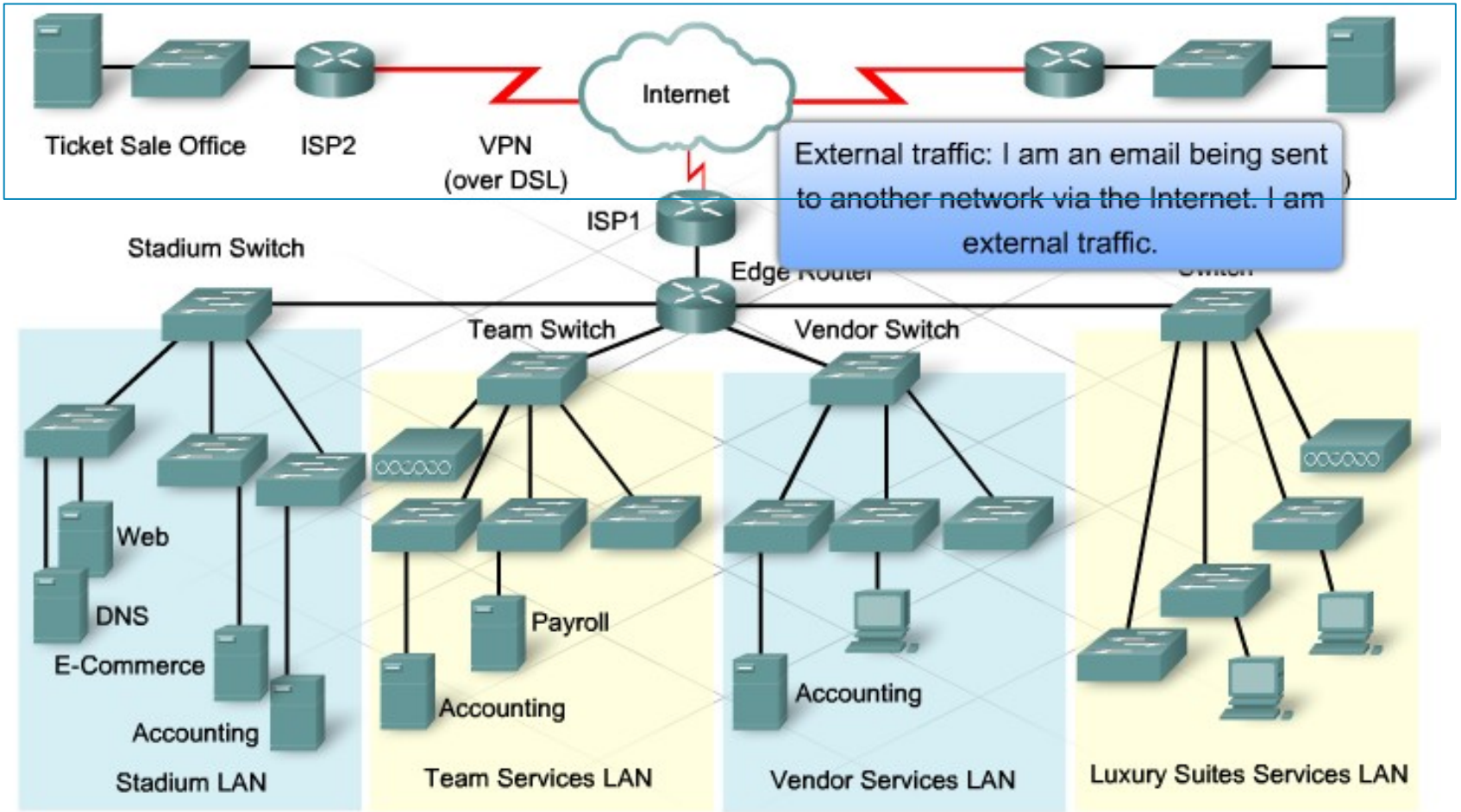
How traffic flow affects network design

- External Traffic
- External traffic is defined as traffic that is initiated by users outside the local network as well as traffic sent to destinations located on remote networks. Some types of external traffic, such as emergency services or financial services, require redundancy and present additional security concerns. The designer diagrams this traffic in order to determine the location of firewalls and DMZ networks, as well as the Internet connectivity requirements.

How traffic flow affects network design
Internal Traffic Flow



How traffic flow affects network design
External Traffic Flow



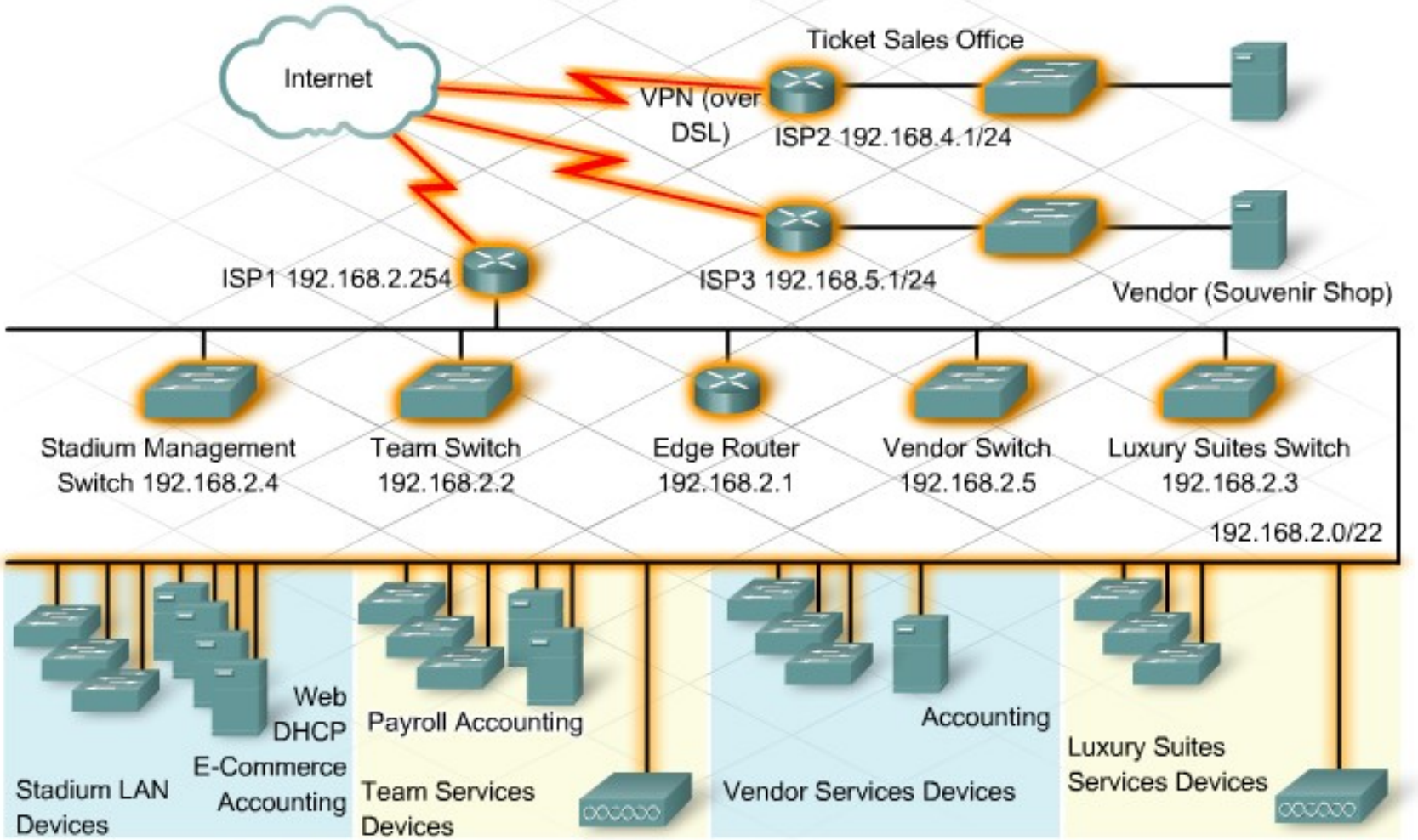
How application characteristics affect network design

- The types of hardware installed on a network affect the performance of an application. A complex network, such as the sports stadium network, contains many different types of hardware. Each of these device types can introduce delay in application response speed to user requests. Delay affects customer satisfaction with the application performance. Hardware delays can be caused by:
- Processing time that a router takes to forward traffic
- Older switches that are not able to handle traffic loads generated by modern applications

How application characteristics affect network design

- One way to ensure high performance is to use the top-down approach. The top-down approach adapts the design of the physical infrastructure to the needs of the network applications. Network devices are chosen only after a thorough technical requirements analysis.
- Network applications on a modern network produce a range of packets. These packets are of various sizes, with distinct sets of protocols, different tolerances to delay, and other characteristics. When the service requirements of these different applications conflict with one another, performance problems can result.

How application characteristics affect network design



How application characteristics affect network design

Which of the following communications are considered the main types of application communications?

	Correct	Incorrect
Client-to-client	✓	
Client-to-Access Point		✓
Client-to-server farm	✓	
Client-to-enterprise edge	✓	
Client-to-switch		✓

Transaction Processing

- Networked applications are now the backbone of business activity. To meet the business goals of the client, the network designer must ensure application performance.
- Some of the more **common application** types include:
- Transaction-processing applications
- Real-time streaming applications
- File transfer and email applications
- HTTP and web applications
- Microsoft domain services

Transaction Processing

- Transaction-Processing Applications
- Transaction-processing is a type of processing in which the computer responds immediately to user requests. Each request generated by the user is a transaction. These transactions can require additional operations to take place in response to the original request. For this reason, application transactions are a unique consideration in network design.
- As an example of a transaction process, consider what happens when a customer purchases tickets online for an event at the sports stadium.

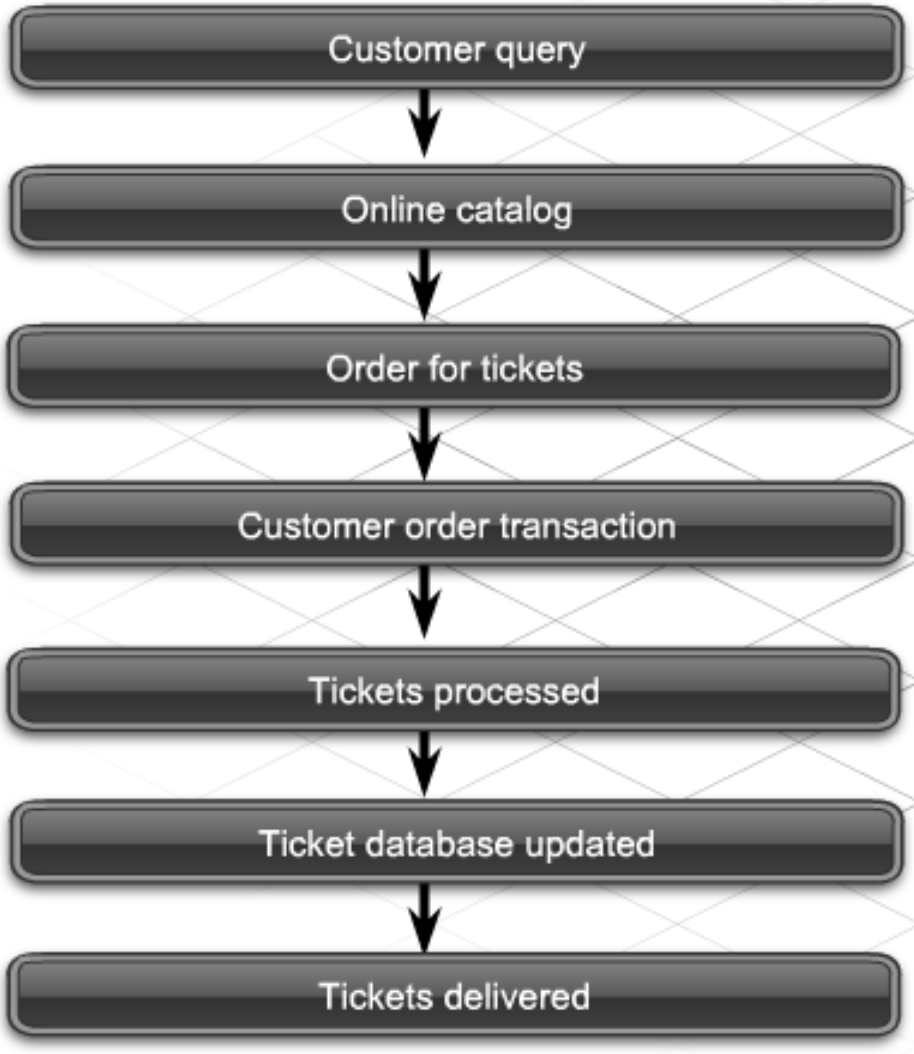
Transaction Processing

- This single transaction generates all the following operations on the network:

- Web traffic from the client to the network
- Database transactions
- Customer order transaction
- Order processing transaction
- Shipping/delivery transaction

Transaction Processing

Transaction Process Example: Purchasing a Ticket Online



Customer query

The customer accesses the online catalog to see if there are tickets available.

Online catalog

Simply viewing the catalog is a transaction that places traffic on the stadium network by accessing the database stored on a server.

Order for tickets

The customer places an order based on what was viewed in the catalog.

Customer order transaction

If tickets are available, the database will begin to process the transaction.

Tickets processed

The database verifies the number of tickets, costs, and prepares the tickets for delivery.

Ticket database updated

The database is updated to ensure proper accountability of available tickets and to accurately support future orders for the remaining tickets.

Tickets delivered

The tickets are shipped to the client or delivered as online tickets that can be printed later.

Transaction Processing

- Not all traffic that enters or exits a network is considered a transaction process. A valid transaction must meet the following criteria:
- It must be atomic.
- It must be consistent.
- It must be isolated.
- It must be durable.

Transaction Processing

- Atomic Transaction
- An atomic transaction guarantees that either all the tasks of a transaction are performed or none of them are. If the transaction is not fully processed, then the entire transaction is void.
- Consistent Transaction
- A consistent transaction ensures that incomplete transactions are not allowed. If an incomplete transaction occurs, the system returns to the state that it was in before the transaction began.

Transaction Processing

- Isolated Transaction
- An isolated transaction is kept secure from all the other transactions on the network. Security is a major network design consideration. Security options include the addition of access control lists (ACLs), encryption, and firewalls to the network topology.

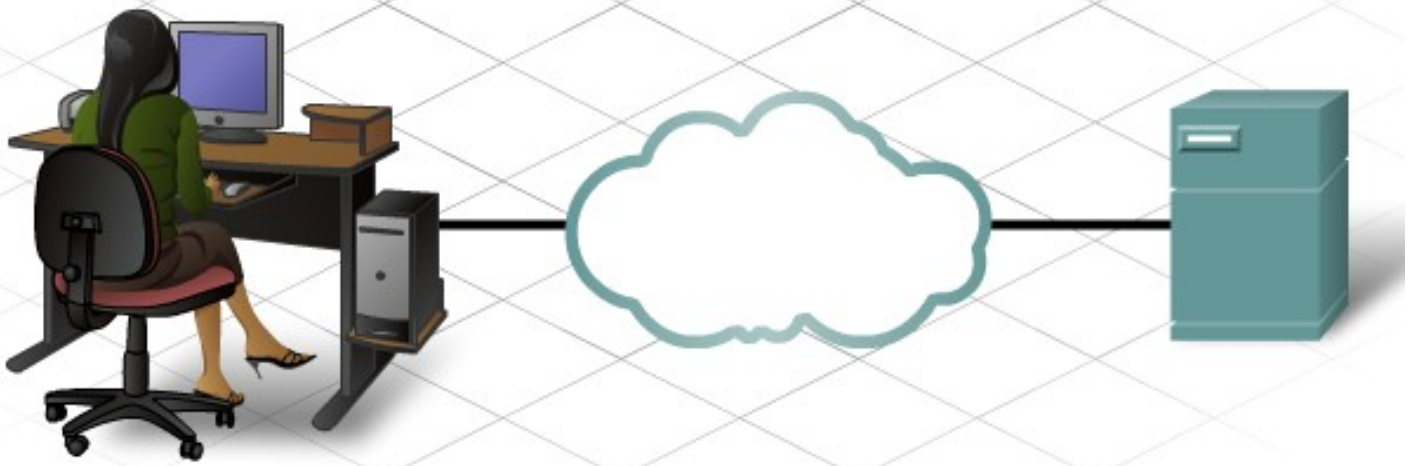
Transaction Processing

- Durable Transaction
- A durable transaction guarantees that once the transaction is completed, the transaction will not be undone - even after a system failure. A durable design for transaction processes requires redundancy at multiple levels. These levels include the Physical Layer connections, servers, switching devices, and routers.

Transaction Processing

Atomic

A customer that purchases tickets online expects the payment to be received and the tickets to be mailed or made available for printing. The database is updated so those tickets are no longer for sale.

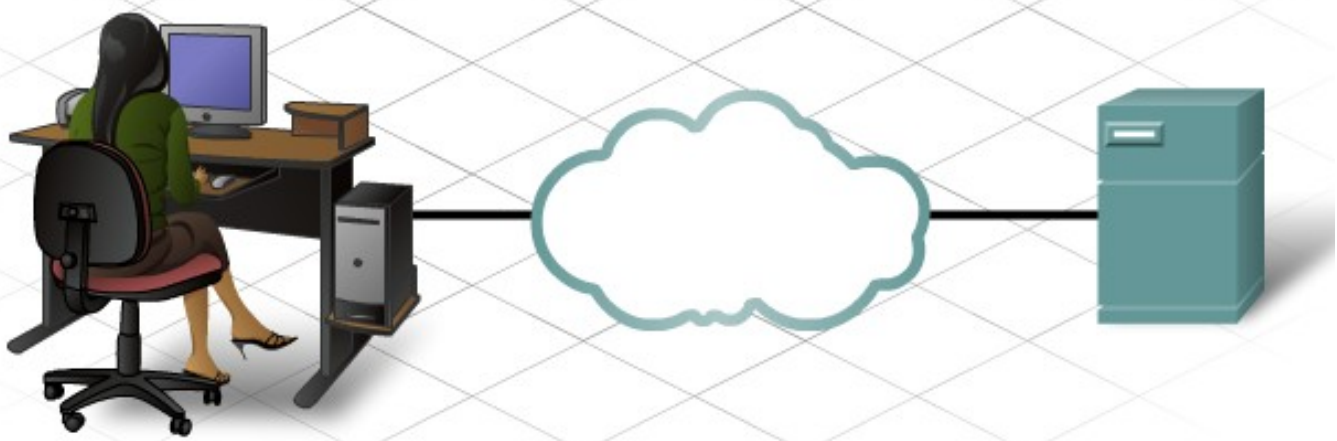


Atomic | Consistent | Isolated | Durable

Transaction Processing

Consistent

If the customer cancels the transaction before it is completed, the customer account is not debited and the database still shows the tickets are available for sale.

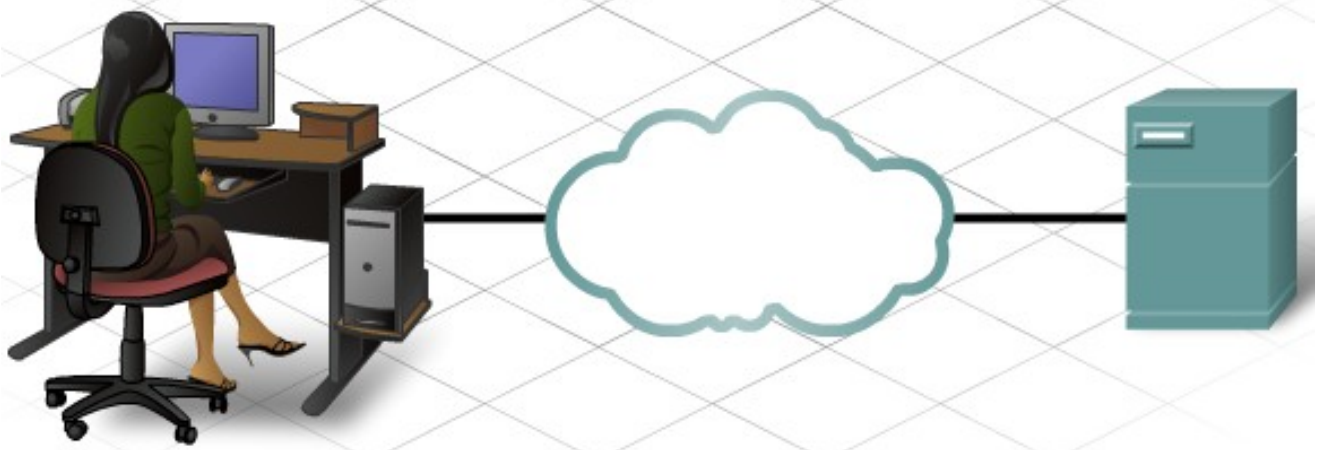


Atomic | Consistent | Isolated | Durable

Transaction Processing

Isolated

The customer must be assured that his or her transactions are secure. For example, the customer's financial details are not visible to other users.

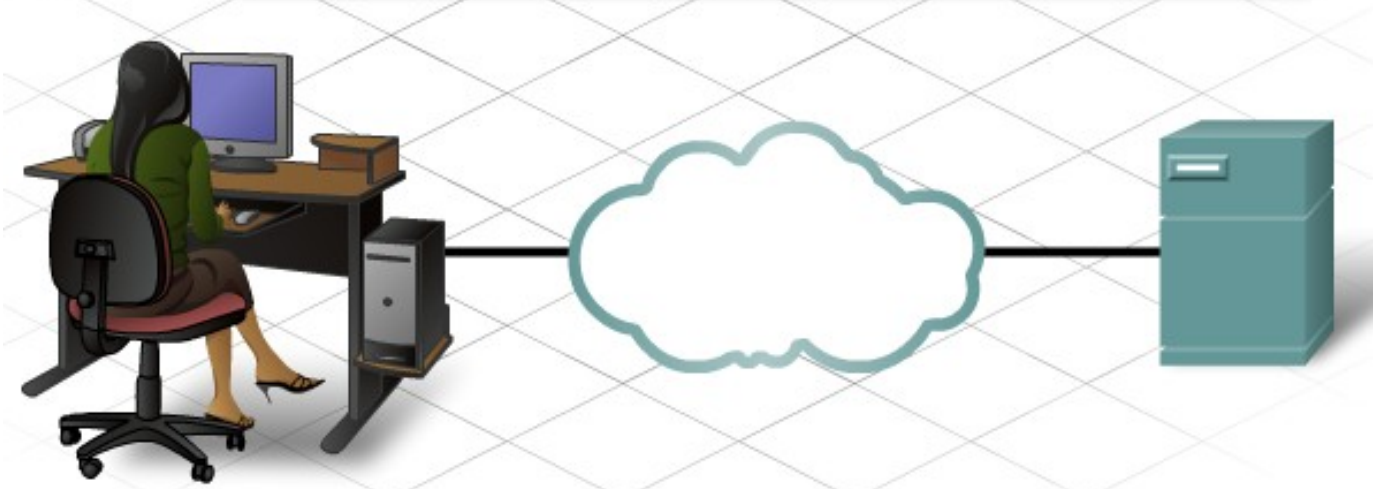


Atomic | Consistent | **Isolated** | Durable

Transaction Processing

Durable

The record of the transaction must be retained even after a system failure, so the tickets are available to the customer and the account is debited correctly.



Atomic | Consistent | Isolated | Durable

Transaction Processing

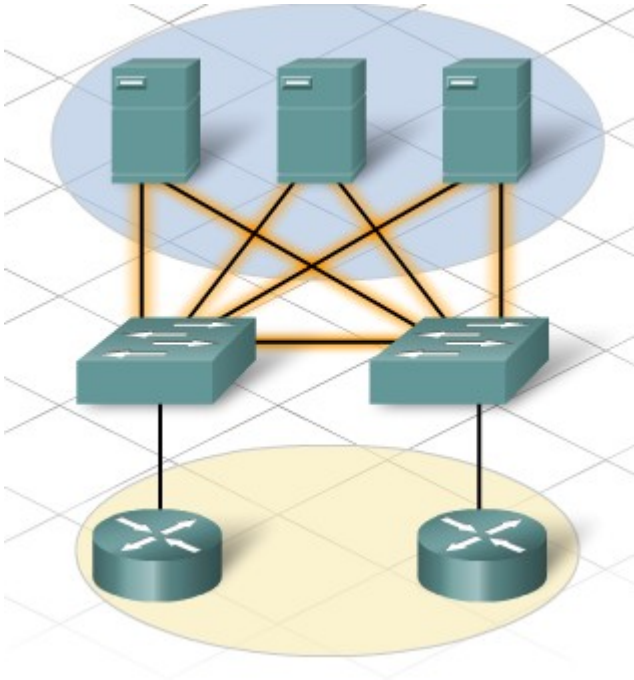
- The network designer evaluates redundancy and security tools that support transaction-processing applications.
- Redundancy
- Incorporating transaction applications requires the designer to consider the impact of each transaction on the network. This process is crucial, because additional cabling or devices may be needed to provide the redundancy or available throughput that these transactions require. Adding redundancy to a network brings the following advantages:
- Reduction or elimination of network downtime
- Increased availability of applications

Transaction Processing

- Networks with redundancy eliminate the problem of single points of failure. If a path or device fails, the redundant path or device can complete the process or transaction. Servers that handle transaction processes have an alternate path to receive or deliver traffic. This helps ensure that the application is available when the customer requests it.
- Network devices can also be configured for redundancy. Two common protocols are:
- Rapid Spanning Tree Protocol (RSTP)
- Hot Standby Routing Protocol (HSRP)

Transaction Processing

- RSTP prevents Layer 2 switching loops that can occur with redundant switches.
- HSRP can provide Layer 3 redundancy in the network. HSRP provides immediate or link-specific failover and a recovery mechanism.
- Redundant links and devices can be implemented in the proposed stadium network design at both the Distribution and Core Layers.



Transaction Processing

- Security
- Security is always a major consideration. It affects not only the transaction processes, but all applications and traffic within an internal network and an external network. Protecting the privacy and integrity of transaction information and the transaction database should be the focus of security considerations. The network designer analyzes the potential for the transaction data to be accessed inappropriately or altered.

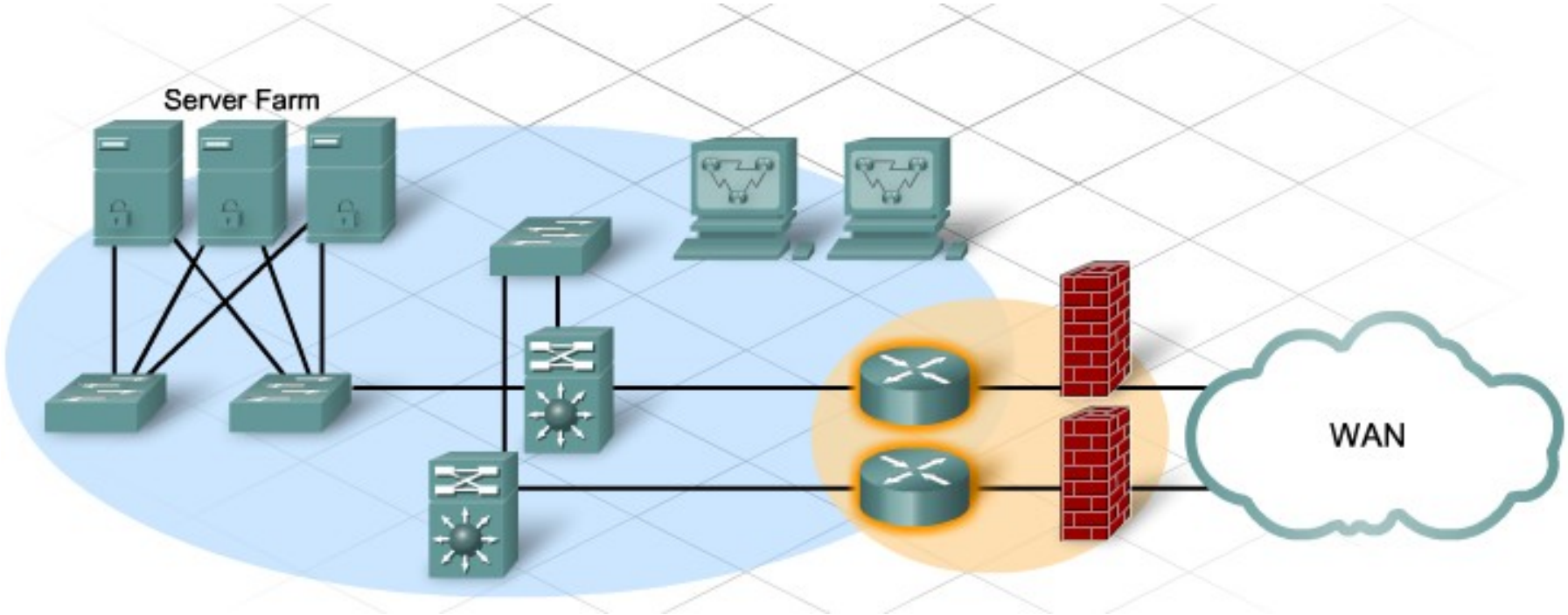
Transaction Processing

- VPNs use a process called tunneling. Tunneling is often referred to as "port forwarding". It is the transmission of data through a public network that is intended for a private network. Tunneling is accomplished by encapsulating the private network data and protocol information within the public network transmission units.
- Intrusion detection systems (IDS) are used to monitor network traffic for suspicious activity. If suspicious activity is detected, an IDS alerts the system or administrator. An IDS can be configured to block the user source IP address from accessing the network.

Transaction Processing

- Firewalls filter traffic based on a set of criteria. The complexity of the firewall configuration can cause delays. The potential impact of delays should be considered in the design of a network.
- ACLs can filter potentially harmful traffic that is trying to enter the network and block specific traffic from exiting the network. These access controls can slow the transaction process. The time-sensitive nature of some transactions should be considered when configuring ACLs.

Transaction Processing



Real-time Streaming and Voice

- Real-time Applications
- When designing the network to accommodate real-time applications, the network designer must consider how the network infrastructure will affect application performance.
- These considerations include the physical elements of the infrastructure:
- Hardware devices and connections
- Network topology
- Phvsical redundancv

Real-time Streaming and Voice

- Logical considerations include how the configuration of QoS and security solutions affect traffic. All of these considerations affect how the designer will implement network solutions, such as IP telephony services.
- Real-time streaming applications present unique requirements for the network design. The only real-time application currently in use in the stadium is video surveillance. IP telephony is included in the proposed network upgrade. Traffic from these applications must be forwarded with the least latency and jitter possible.

Real-time Streaming and Voice

When determining the business goals and technical requirements for the customer, all aspects of the network should be analyzed to ensure proper implementation and support of the real-time applications.

Real-time Streaming and Voice

- Infrastructure
- To support the existing and proposed real-time applications, the infrastructure must accommodate the characteristics of each type of traffic.
- The network designer must determine whether the existing switches and cabling can support the traffic that will be added to the network. Cabling that can support gigabit transmissions should be able to carry the traffic generated and not require any changes to the infrastructure.

Real-time Streaming and Voice

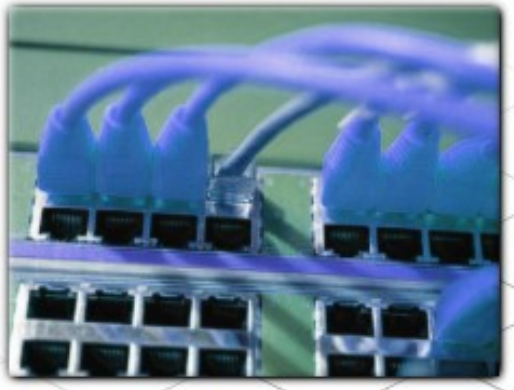
- VoIP
- When introducing VoIP to a network that uses traditional telephones, it is important to remember that VoIP uses voice-enabled routers. These routers convert analog voice from traditional telephone signals into IP packets.
- Once converted into IP packets, the router sends those packets between corresponding locations. Voice-enabled routers must be added to the design.

Real-time Streaming and Voice

- IP Telephony

- In IP telephony, the IP phone itself performs voice-to-IP conversion. Voice-enabled routers are not required within the enterprise network. IP phones can use Cisco Unified Communications Manager as a server for call control and signaling. The stadium network requirements include IP telephony.

Real-time Streaming and Voice



Cable and switch

IP phones

Cisco Unified Communications 500 Series

Real-time Streaming and Voice

- Real-time Video Protocols
- To transport streaming media effectively, the network must be able to support applications that require delay-sensitive delivery. Real-Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP) are two protocols that support this requirement.

Real-time Streaming and Voice

- RTP and RTCP enable control and scalability of the network resources by allowing QoS mechanisms to be incorporated. These QoS mechanisms provide valuable tools for minimizing latency issues for real-time streaming applications. These tools include priority queuing, custom queuing, low latency queuing, and class-based weighted fair queuing.

File Transfer and E-mail

- File transfers put high-volume traffic onto the network. This traffic can have a greater effect on throughput than interactive end-to-end connections. Although file transfers are throughput-intensive, they typically have low response-time requirements.

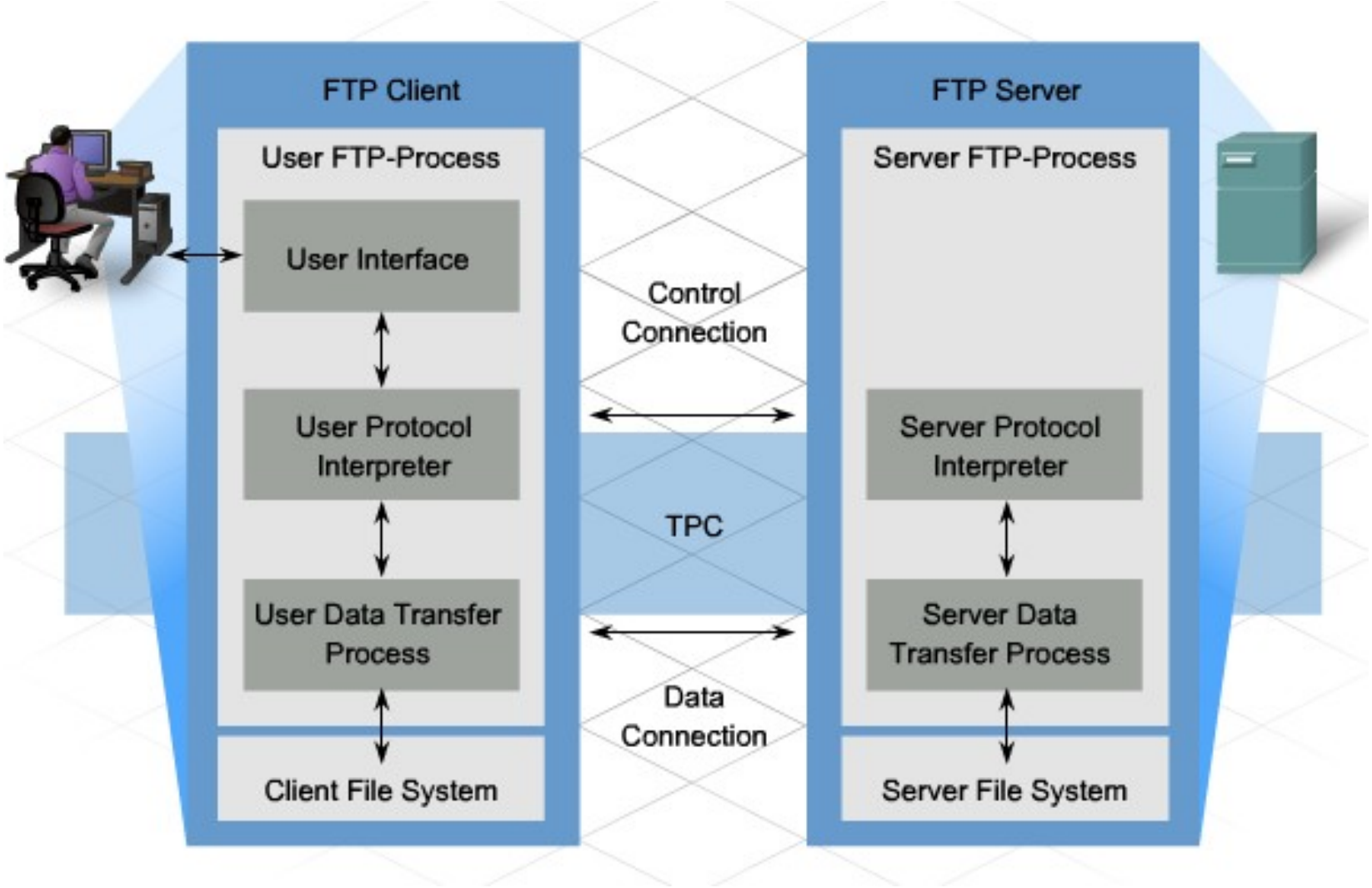
File Transfer and E-mail

- Some of the characteristics of file transfer traffic include:
- Unpredictable bandwidth usage - this type of traffic is usually user initiated and therefore cannot be reliably predicted.
- Large packet size - FTP and other file transfer traffic uses large packet sizes for efficient transfer. These large packets can cause delay for other types of traffic when the network becomes congested.

File Transfer and E-mail

- As part of the initial characterization of the network, it is important to identify the number of users that use file transfers on a regular basis. FTP is not the only type of file transfer traffic usually present on a LAN. Copying files from shared network drives and downloading large files using http have similar characteristics to FTP.
- From this information, the network designer can anticipate the throughput requirements.

File Transfer and E-mail



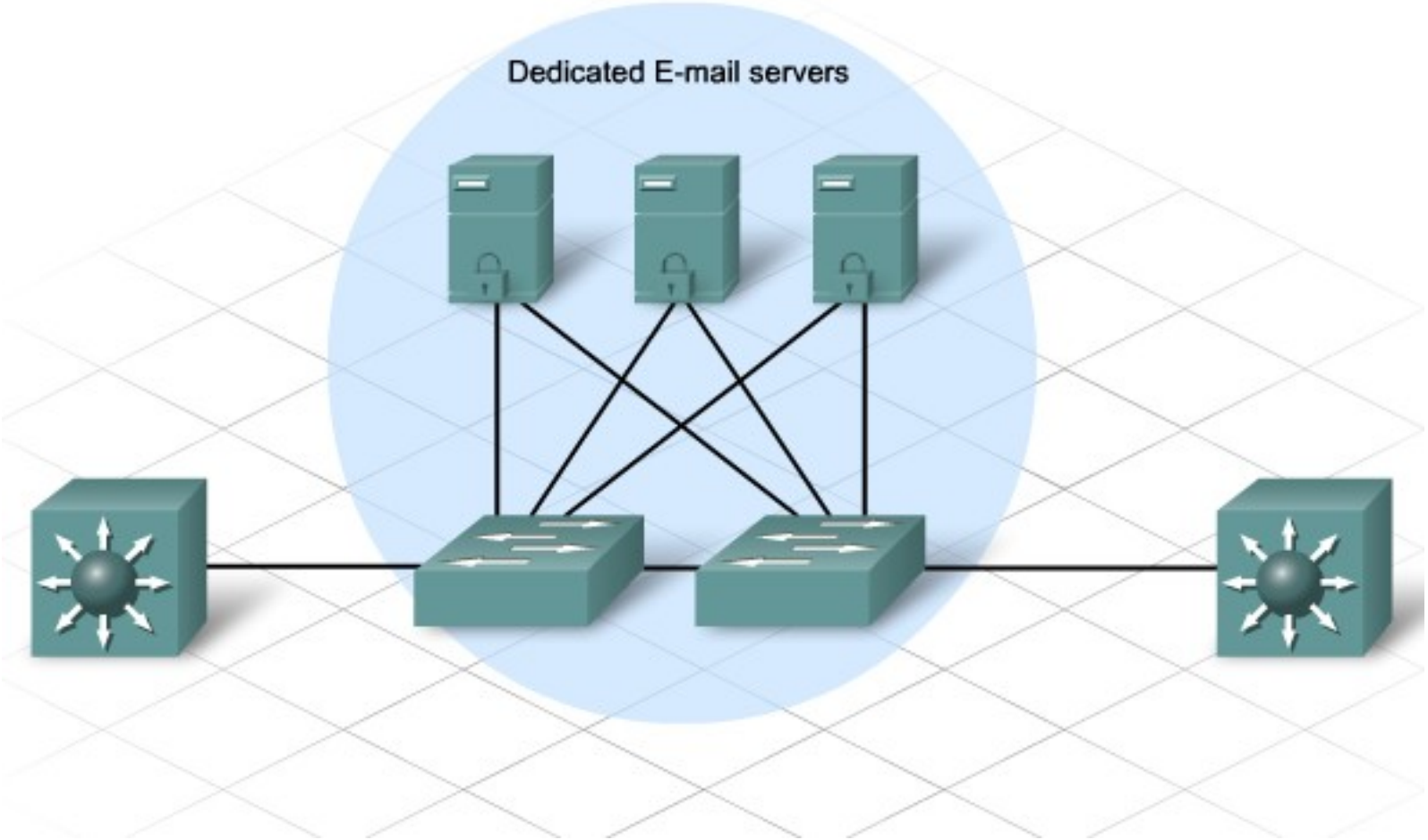
File Transfer and E-mail

- Email
- Email is one of the most popular network services. With its simplicity and speed, email has revolutionized how people communicate. Yet, to run on a computer or other end device, email requires several applications and services. Two common Application Layer protocols are Post Office Protocol (POP) and Simple Mail Transfer Protocol (SMTP).

File Transfer and E-mail

- Email Client Processes
- Email users typically access their email service using an application called an email client. The email client enables users to compose and send messages, then places received messages into the user's mailbox.
- Email Server Processes
- The email server also transfers and delivers mail to the email client.
- Although a single email does not generate significant traffic, it is possible for mass emails to be transmitted that inundate the network or servers with traffic.

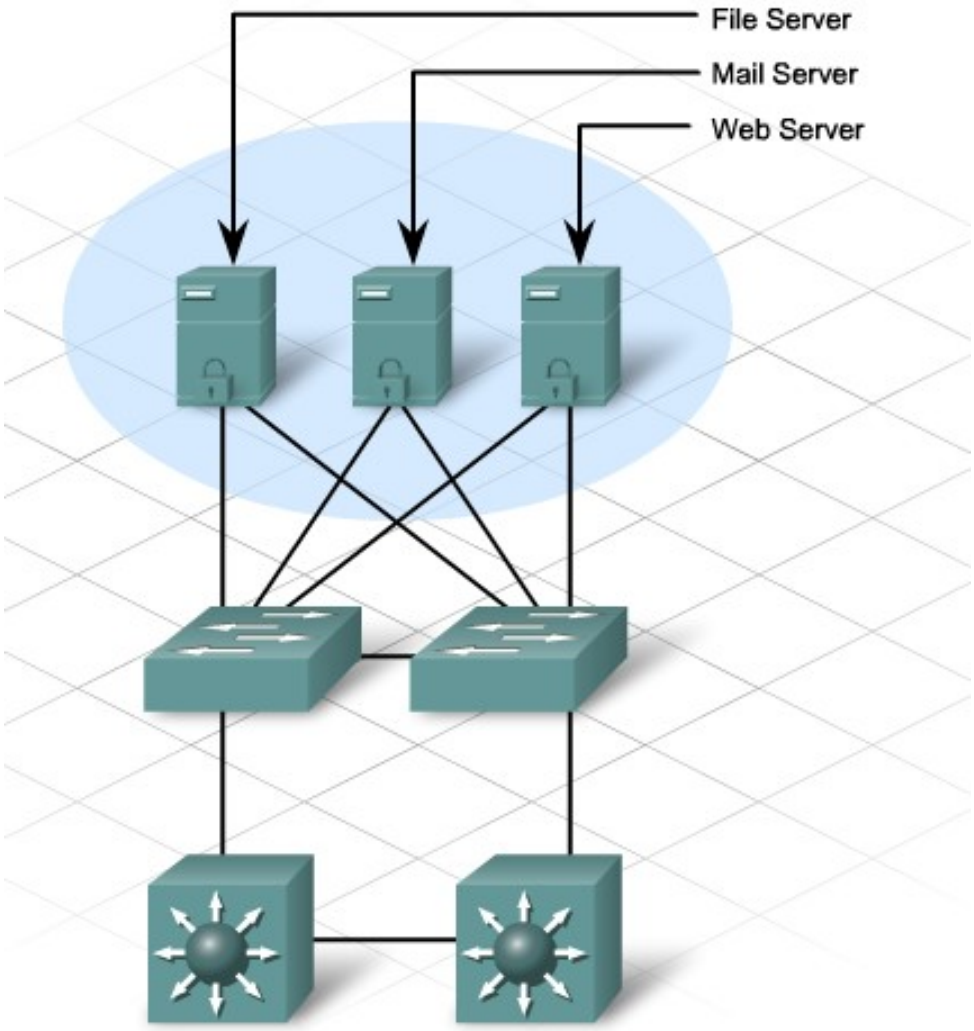
File Transfer and E-mail



File Transfer and E-mail

- Supporting File Transfer and Email Applications
- Customers expect immediate access to their emails and to the files that they are sharing or updating.
- To help ensure this availability, the network designer takes the following steps:
- Securing file and mail servers in a centralized location, such as a server farm.
- Protecting the location from unauthorized access by physical and logical security measures.
- Creating redundancy in the server farm that ensures that if one device fails, all files are not lost.
- Configuring redundant paths to the servers.

File Transfer and E-mail



HTTP and Web Traffic

- HTTP and Web Traffic
- Hypertext Transfer Protocol (HTTP) is one of the protocols in the TCP/IP suite that was originally developed to publish and retrieve web pages. It is now used for distributed collaborative information systems. HTTP is used across the World Wide Web for data transfer. It is one of the most widely used application protocols.
- HTTP specifies a request/response protocol between a client, typically a web browser, and a server.

HTTP and Web Traffic

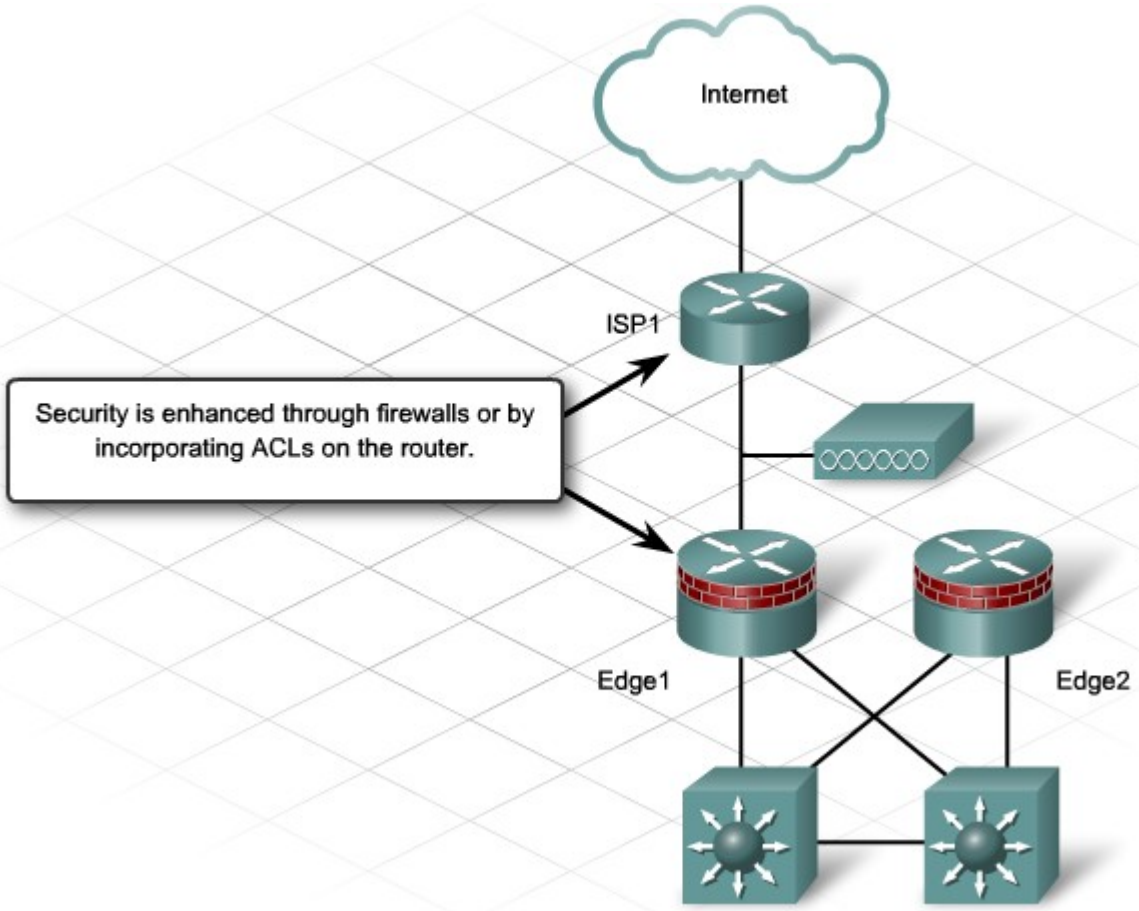
- When a client sends a request message to a server, the HTTP protocol defines the message types used by the client. The protocol also specifies the message types that the server uses to respond.
- This process would appear to be a minor consideration in the design process. However, if the server that is being accessed is used for e-commerce or to store customer information, the security and redundancy issues become even more important.

HTTP and Web Traffic

- Network Media
- To support HTTP and web traffic, it is necessary to have Layer 3 devices that can control the internal and external traffic flows. In a network audit, the inbound traffic should be considered part of the network baseline testing.
- Redundancy
- Servers usually have redundant components and power sources. They may be equipped with two or more NICs connected to separate switches.

HTTP and Web Traffic

- Security
- Security features such as ACLs, firewalls, and IDS, are also used to prevent unauthorized traffic from being sent in to or out of the protected networks. As with the other application servers, the HTTP server should be located at the ISP or in the centralized server farm for added physical security and redundancy.



Microsoft Domain Services

- The stadium uses Microsoft Active Directory Services. Therefore, the network designer must consider both server-to-server and server-to-client communications. Microsoft servers support many different types of services that rely on high speed communications between the servers themselves. These services, such as Active Directory replication, must be considered when relocating servers during a network redesign.

Microsoft Domain Services

- Ports used by Microsoft Domain Services
- Microsoft servers and clients communicate with each other using a set of TCP and UDP ports. These ports are used for various Microsoft services, including authentication and authorization. Many Microsoft-specific services generate local broadcast packets on these ports, as well as unicast requests. Common TCP and UDP ports that must be open for Microsoft Domain Services to operate correctly include:

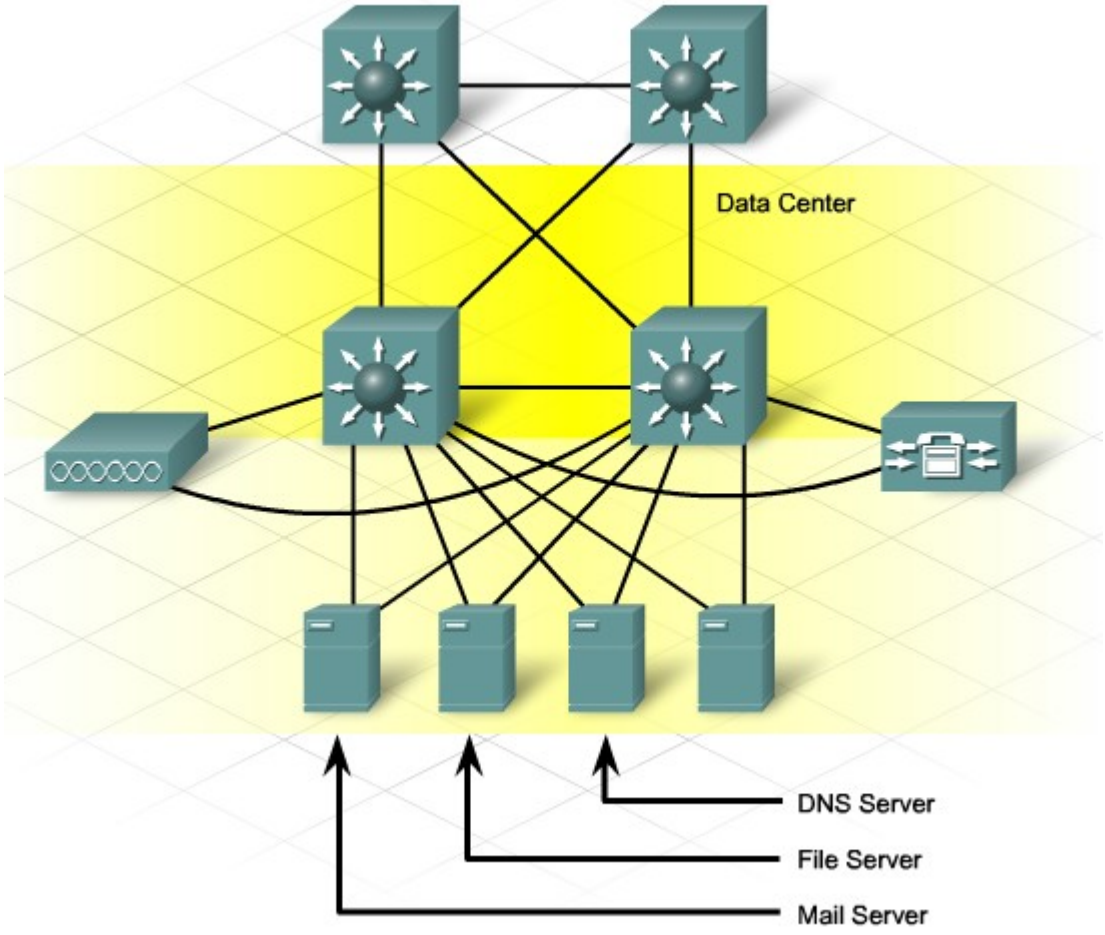
Microsoft Domain Services

- UDP 53 - DNS Services
- UDP 67 - DHCP
- UDP 123 - Windows Time Service
- TCP 135 - Remote Procedure Call (RPC)
- UDP 137 - NetBIOS Name Resolution
- UDP 138 - NetBIOS Datagram Service
- TCP 139 - NetBIOS Session Service
- TCP 389 and UDP 389 - LDAP Service
- TCP 445 - Server Message Blocks (SMB)
- TCP 1433 - Microsoft SQL over TCP
- Active Directory and DNS

Microsoft Domain Services

- Active Directory and DNS
- When a Microsoft Windows 2003 Server is installed in a network, there is very tight integration between Active Directory Services and DNS. Active Directory requires DNS to locate domain controllers, which provide authentication and authorization services. Windows 2003 Domain Controllers must be DNS servers as well. This DNS service can provide the main DNS for an organization, or may be in addition to Internet DNS services located on non-Windows servers

Microsoft Domain Services



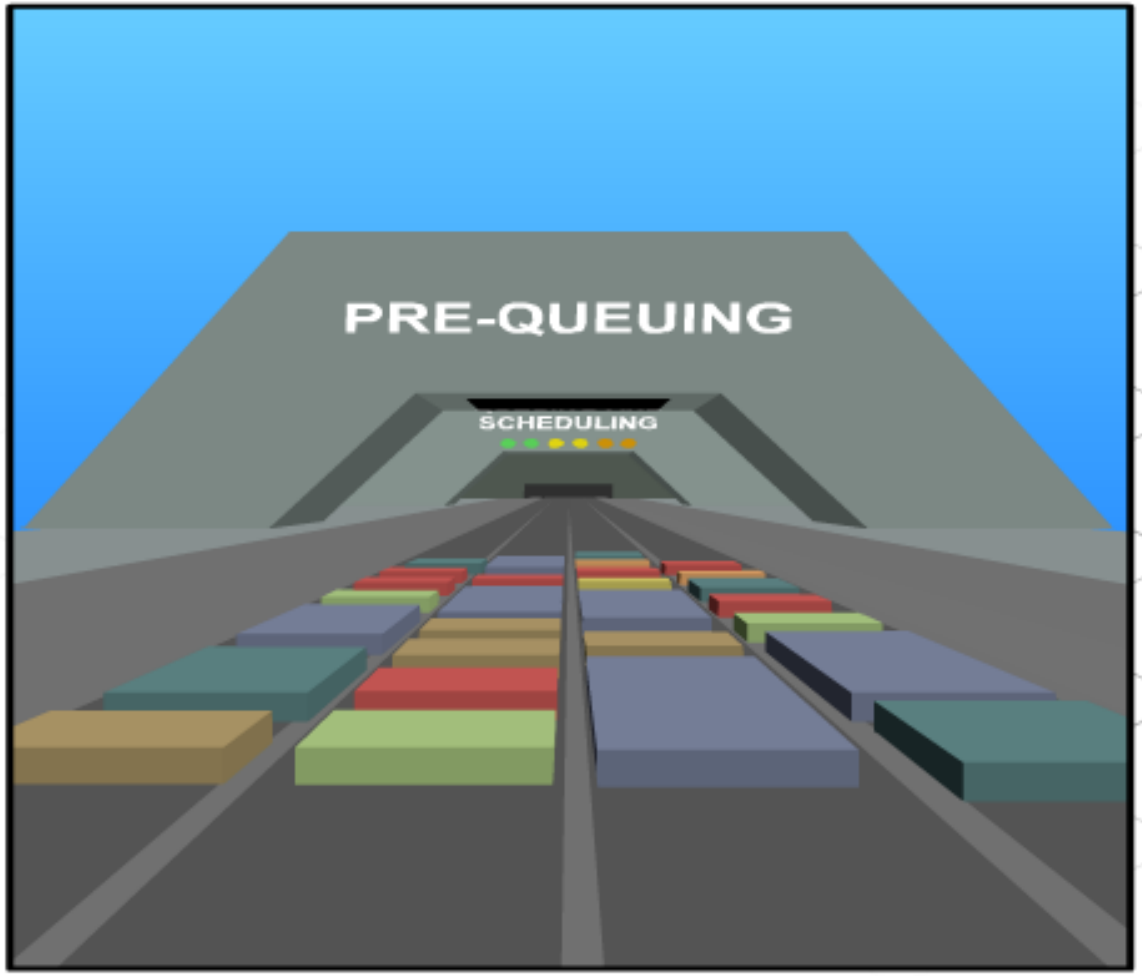
What is Quality of Service and why is it needed?

- Quality of Service (QoS) refers to the capability of a network to provide preferential service to selected network traffic. The primary goal of QoS is to provide priority, including dedicated bandwidth, controlled jitter and latency, and reduced packet loss.
- When creating QoS policies for an organization, it is important to focus on which traffic needs preferential treatment.

What is Quality of Service and why is it needed?

- Users perceive service quality based on two criteria:
- The speed with which the network reacts to their requests
- The availability of the applications they want to use
- QoS helps to manage these issues for traffic flows within the network infrastructure and for the applications that use the network.
- Some Cisco devices, such as routers, have built-in QoS mechanisms.

What is Quality of Service and why is it needed?



Play flash from Chapter 4.3.1 (1)

What is Quality of Service and why is it needed?

- Some applications are extremely sensitive to bandwidth requirements, packet delays, network jitter, and possible packet loss. These applications include real-time IP telephony and streaming video.
- IP Telephony Requirements
- The requirements of IP telephony illustrate many of the problems of real-time applications in a converged network. Voice traffic requires more than a simple connection between users. The quality of the transmissions is extremely important. When delays occur, voices break up and words become distorted.

What is Quality of Service and why is it needed?

- To avoid substandard transmission quality, IP telephony requires that QoS mechanisms be in place. Voice packets must not have a one-way delay greater than 150 ms. It is critical in the deployment of IP telephony solutions that voice packets have low latency and low jitter at each hop along a given path.

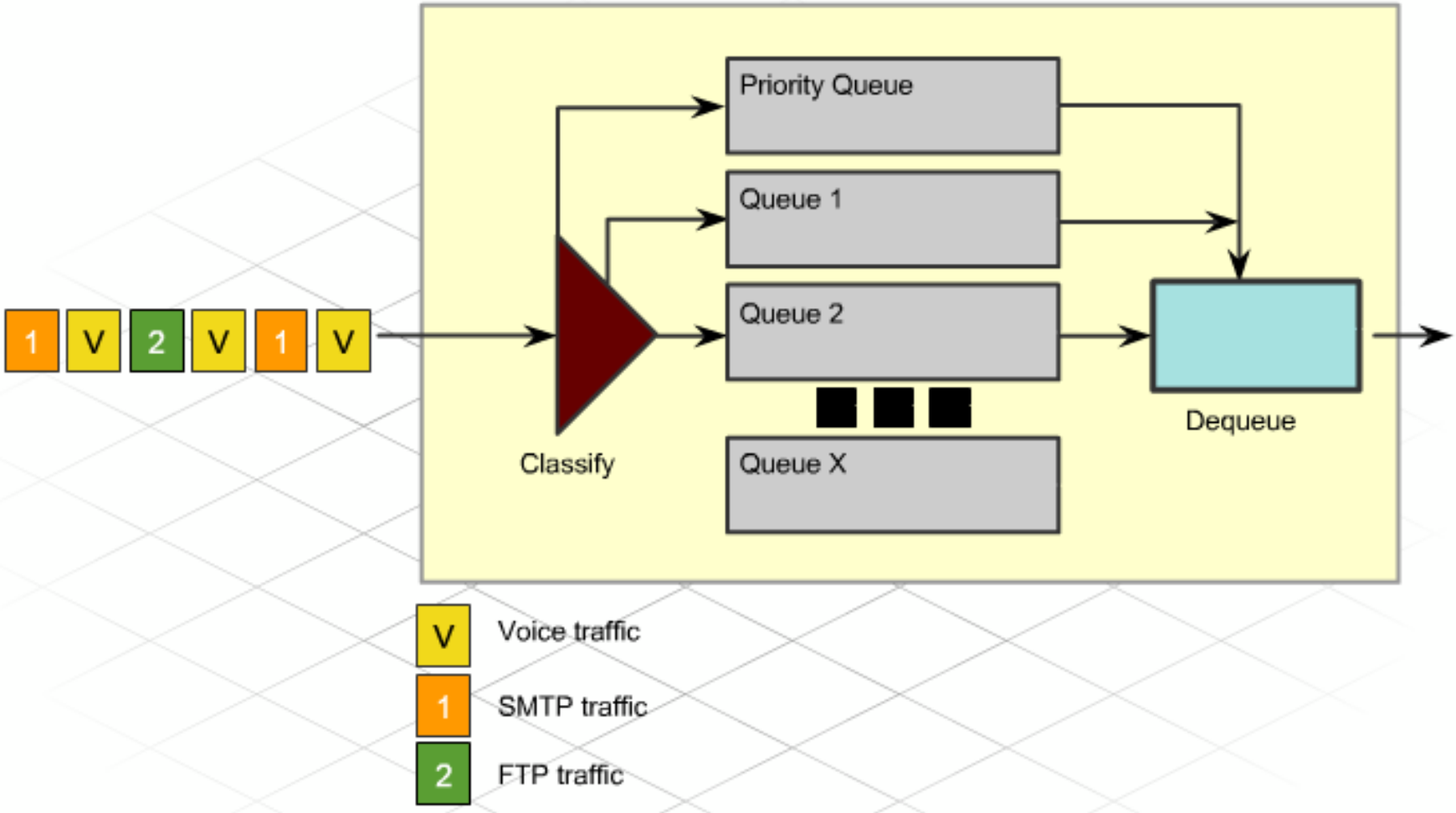
What is Quality of Service and why is it needed?

- Streaming Video Requirements
- Streaming video is a video feed that is usually sent from prerecorded files. It can be distributed in a live broadcast converting the video into a compressed digital signal and then transmitted by a special web server. This media stream is sent as a multicast so multiple users can view the stream at the same time.

What is Quality of Service and why is it needed?

- In a network without QoS, all packets receive the same treatment, and real-time applications suffer
- QoS does not actually create more bandwidth. Instead, it prioritizes bandwidth use to support the applications, such as IP telephony, that need it most. To do this, QoS uses traffic queues to help manage priority traffic on converged networks.

What is Quality of Service and why is it needed?



Play flash from chapter 4.3.1 (2)

Traffic Queuing

- Voice and Data Traffic
- In a converged network, constant, small-packet voice traffic competes with larger, irregular data flows from server updates and file transfers. Although typically the packets carrying voice traffic on a converged network are small, delays that occur while they traverse the network will cause poor voice quality.
- Data from real-time applications, such as IP telephony, must be processed at the same rate as it is sent, and there is no time to retransmit packets with errors. Therefore, VoIP uses UDP as a best-effort transport protocol.

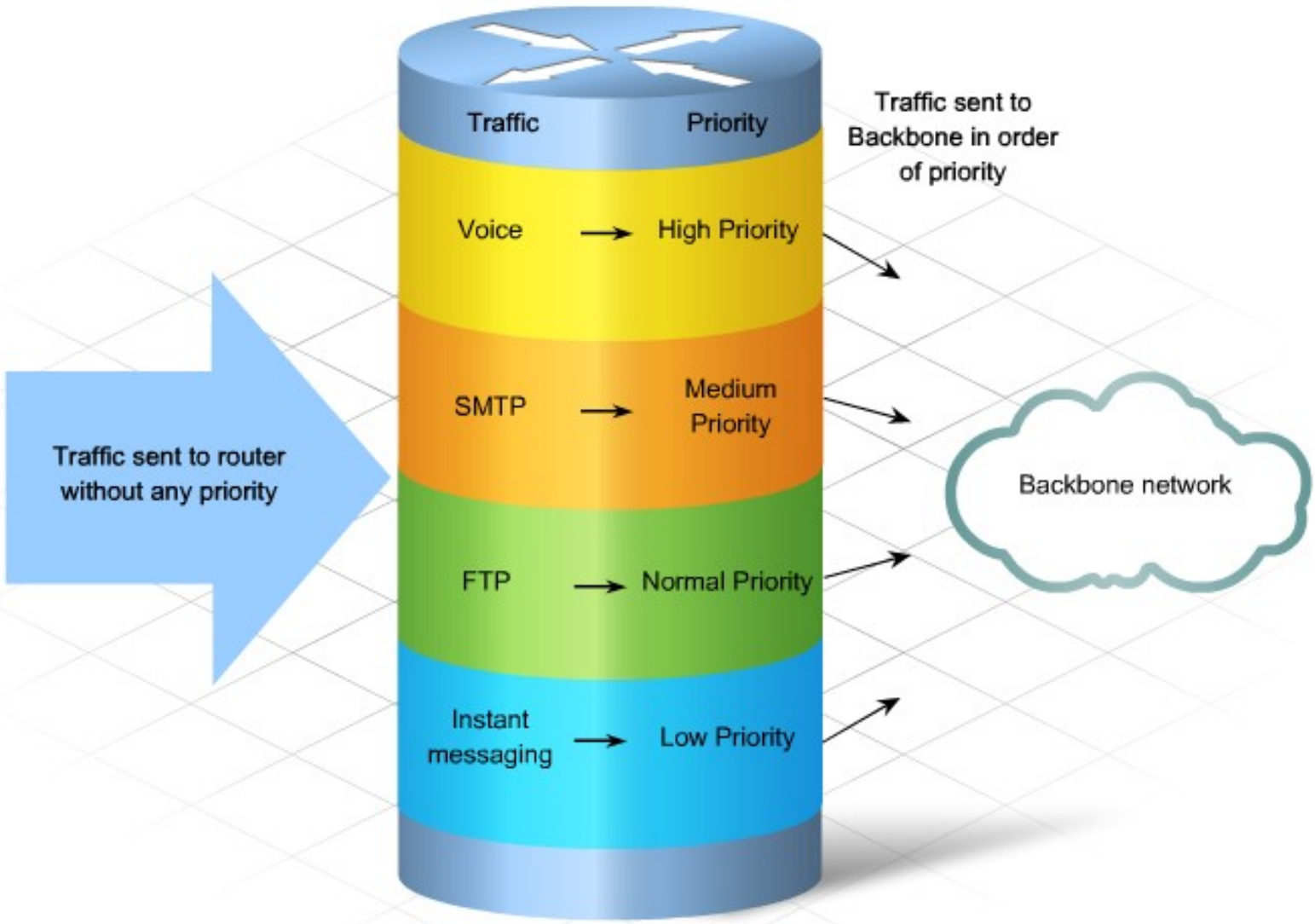
Traffic Queuing

- Conversely, packets carrying file transfer data typically are large. These packets use the error-checking and retransmission features of TCP to survive delays and packet drops.
- It is possible to retransmit part of a dropped data file, but it is not feasible to retransmit part of a voice conversation. For this reason, critical, time-sensitive, voice and video traffic must have priority over data traffic.

Traffic Queuing

- QoS Mechanisms
- Mechanisms must be in place to provide QoS priority. The priorities for traffic can be high, medium, normal, and low. Traffic queues are only one of the QoS mechanisms available for prioritizing traffic on the network. Traffic queues assist in providing secure, predictable, and guaranteed services. Even a brief network outage on a converged network can seriously disrupt business operations.

Traffic Queuing



Traffic Queuing

- Hardware and Software Queues
- Queues are used to manage traffic flow with QoS. Hardware queues store traffic as it is received and send packets out in the order received, on a first-come first-served basis. The hardware queue is sometimes referred to as the transmit queue, or TxQ. This is the physical queue where packets wait for forwarding based on their priority.

Traffic Queuing

- Software queues allow the packets to be sent out based on the priority set by the network designer or administrator. The queues are based on the QoS requirements. Priority queuing (PQ) and Custom Queuing (CQ) are examples of software queues.
- Implementing QoS in Traffic Queues
- To implement QoS on a network, the designer follows three basic steps to ensure that traffic is properly prioritized:

Traffic Queuing

- Step 1: Identify Traffic Requirements
- Determine the QoS requirements needed for the different types of traffic such as voice, mission-critical applications, and which low priority traffic can be marked as best-effort.
- Step 2: Define Traffic Classes
- After traffic has been identified, it can be placed in appropriate classes, such as voice traffic, which has the highest priority, followed by mission-critical applications. All other traffic can be prioritized as normal or low depending on the purpose of the data.

Traffic Queuing

- Step 3: Define QoS Policies
- The last step is to define the QoS policies to be applied to each class. These policies include scheduling traffic queues and rules for managing congestion.

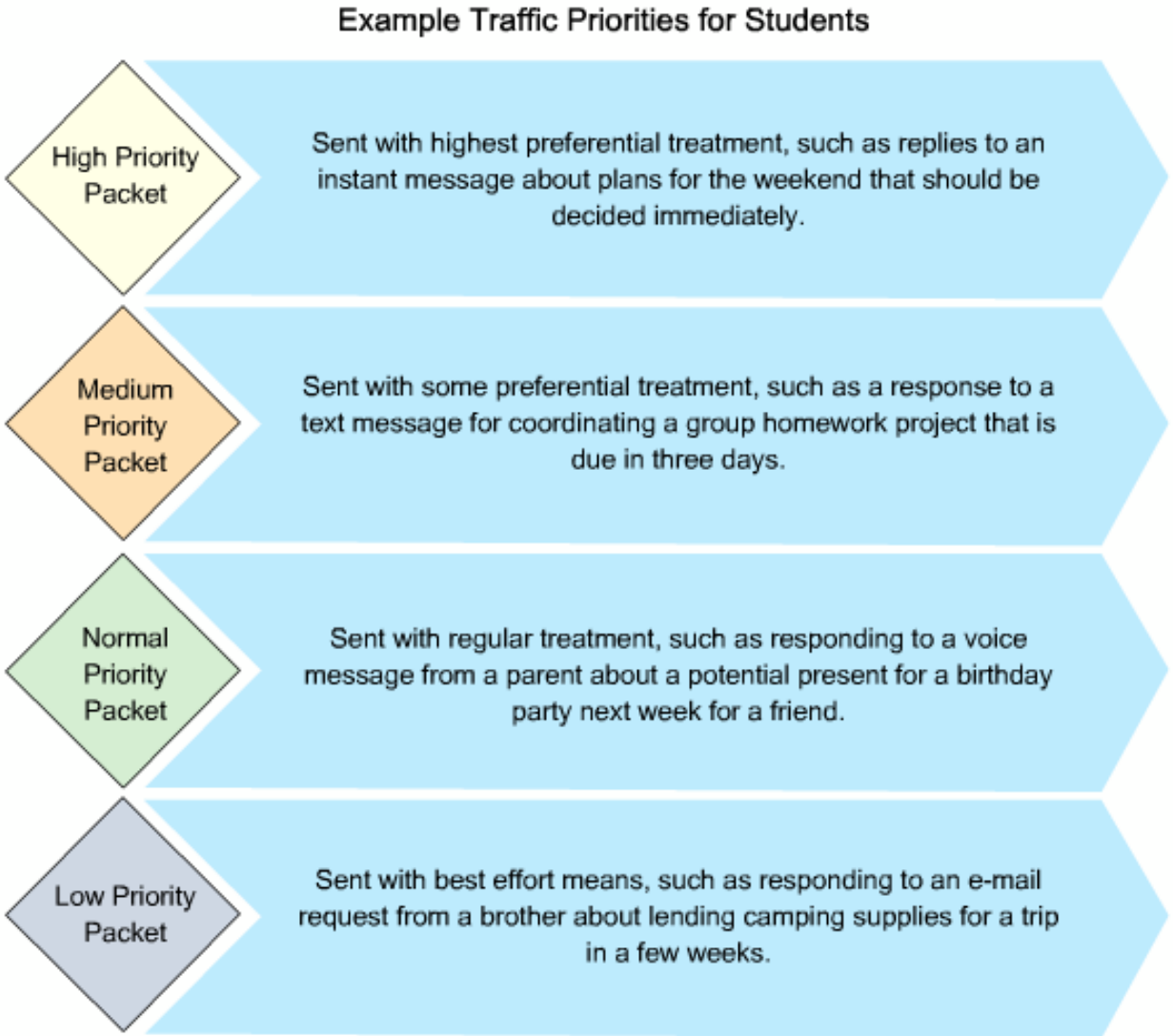
Priorities and traffic management

- Many methods are available for managing traffic on a network. One method is Priority Queuing (PQ). As part of implementing QoS on a network, Priority Queuing classifies traffic as high, medium, normal, or low priority. Priority Queuing can then be applied to these QoS classes.
- Priority Queuing is useful for time-sensitive, mission-critical protocols. PQ works by establishing four output interface queues - high, medium, normal, and low - each serving a different level of priority. These queues are configurable for the following characteristics:
- Queue type
- Traffic assignment
- Size

Priorities and traffic management

- Incoming traffic is classified, marked to indicate its class, and forwarded.
- Traffic is assigned to the various queues based on QoS policies defined in a priority list. These policies can be based on protocol, port number, or other criteria established for the designated traffic type. They represent a set of filters that separate different traffic types into the four class-based queues.

Priorities and traffic management



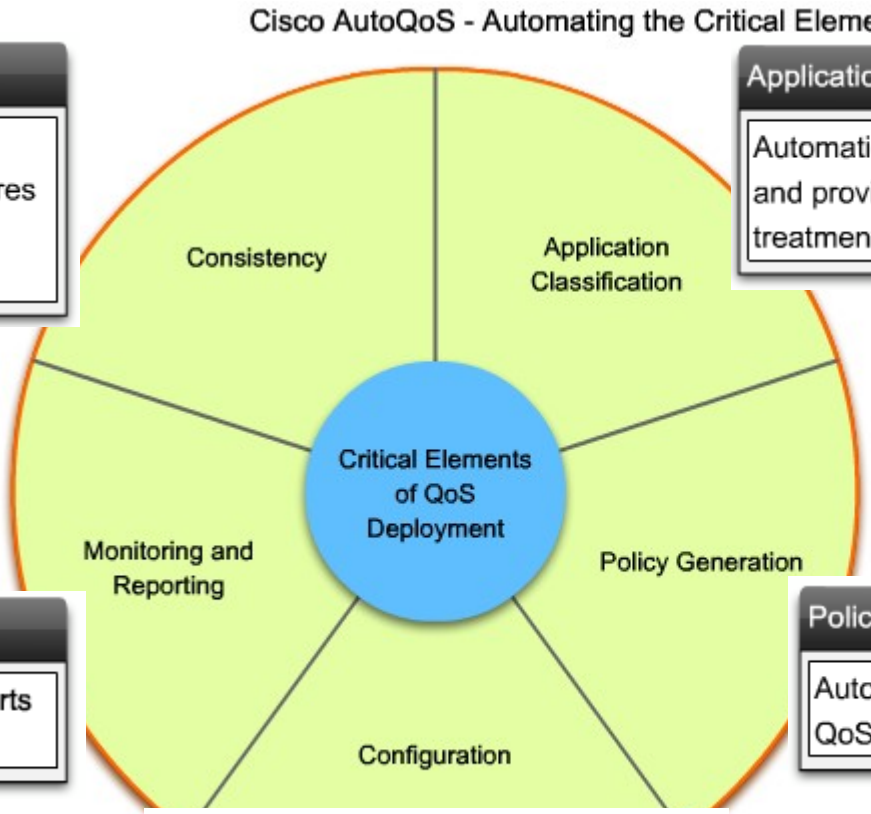
Priorities and traffic management

- Cisco is incorporating tools to assist with the configuration of QoS. One of those tools is AutoQoS, which is available as part of the Cisco IOS software.
- Cisco AutoQoS provides a simple, intelligent Command Line Interface (CLI). This CLI enables LAN and WAN QoS for VoIP on Cisco switches and routers.

Priorities and traffic management

- Auto QoS incorporates the Cisco best practices for implementing quality of service and makes it easy for customers to configure their networks to support high priority traffic, such as voice or video.
- Cisco AutoQoS can reduce the deployment cost and time frame by as much as two-thirds, when compared to a manual approach.

Priorities and traffic management



Consistency

Enabling automatic, seamless interoperability among all QoS features and parameters across a network topology LAN, MAN, and WAN

Application Classification

Automatically discovering applications and providing appropriate QoS treatment

Monitoring and Reporting

Generating intelligent, automatic alerts and summary reports

Policy Generation

Auto-generation of initial and ongoing QoS policies

Configuration

Automating complex configurations with simple
easy-to-use commands

Where can QoS be implemented?

- When configuring QoS features, the network administrator can select the specific network traffic, prioritize it according to its relative importance, and use congestion-management techniques to provide preferential treatment. QoS can be implemented at the Access, Distribution, and Core Layers of a network.
- Layer 2 Devices
- Layer 2 switches at the Access Layer can support QoS based on IEEE 802.1p Class of Service (CoS). The Layer 2 switch QoS uses classification and scheduling to prioritize sending frames from the switch into the network.

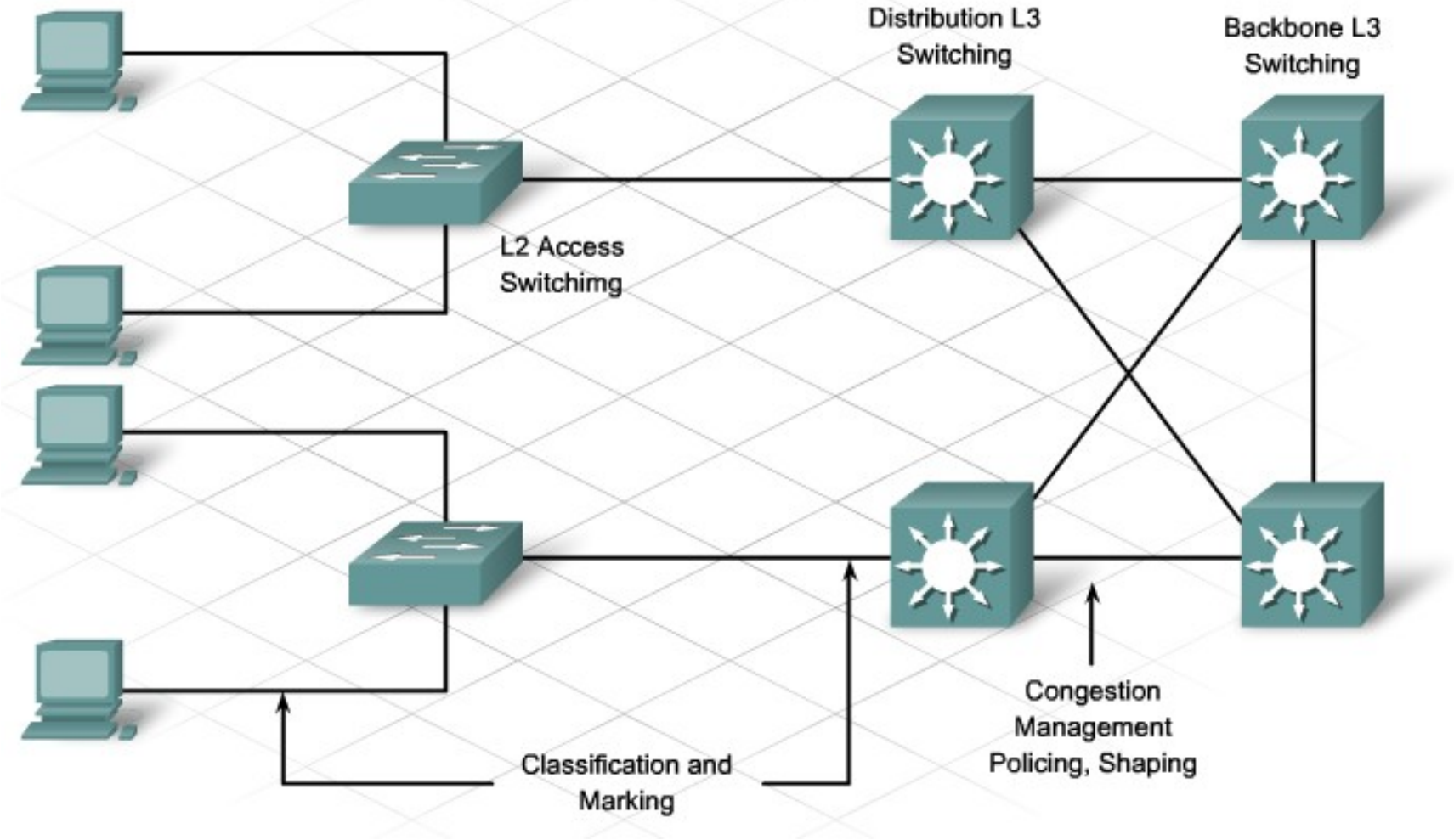
Where can QoS be implemented?

- Layer 3 Devices
- Layer 3 devices can support QoS based on physical interface, IP addresses, logical port numbers, and QoS bits in the IP packet. QoS in Distribution and Core Layer devices must be supported in both directions of traffic flow.
- Classification and Marking
- Classification is the process by which traffic is grouped. Classifications are made based on how traffic is marked or by protocol.

Where can QoS be implemented?

- Traffic can be marked by Layer 2 class of service, an IP precedence, or a Differentiated Services Code Point (DSCP) value:
- Class of service (CoS) is the first 3 bits of an 802.1q VLAN tag.
- IP precedence is the first 3 bits of the Type of Service (ToS) byte in the IP header.
- DSCP can be assigned by the router or switch. It is the first 6 bits in the ToS byte in the header.
- Classification and marking allow the partitioning of traffic into multiple priority levels, or classes of service.

Where can QoS be implemented?



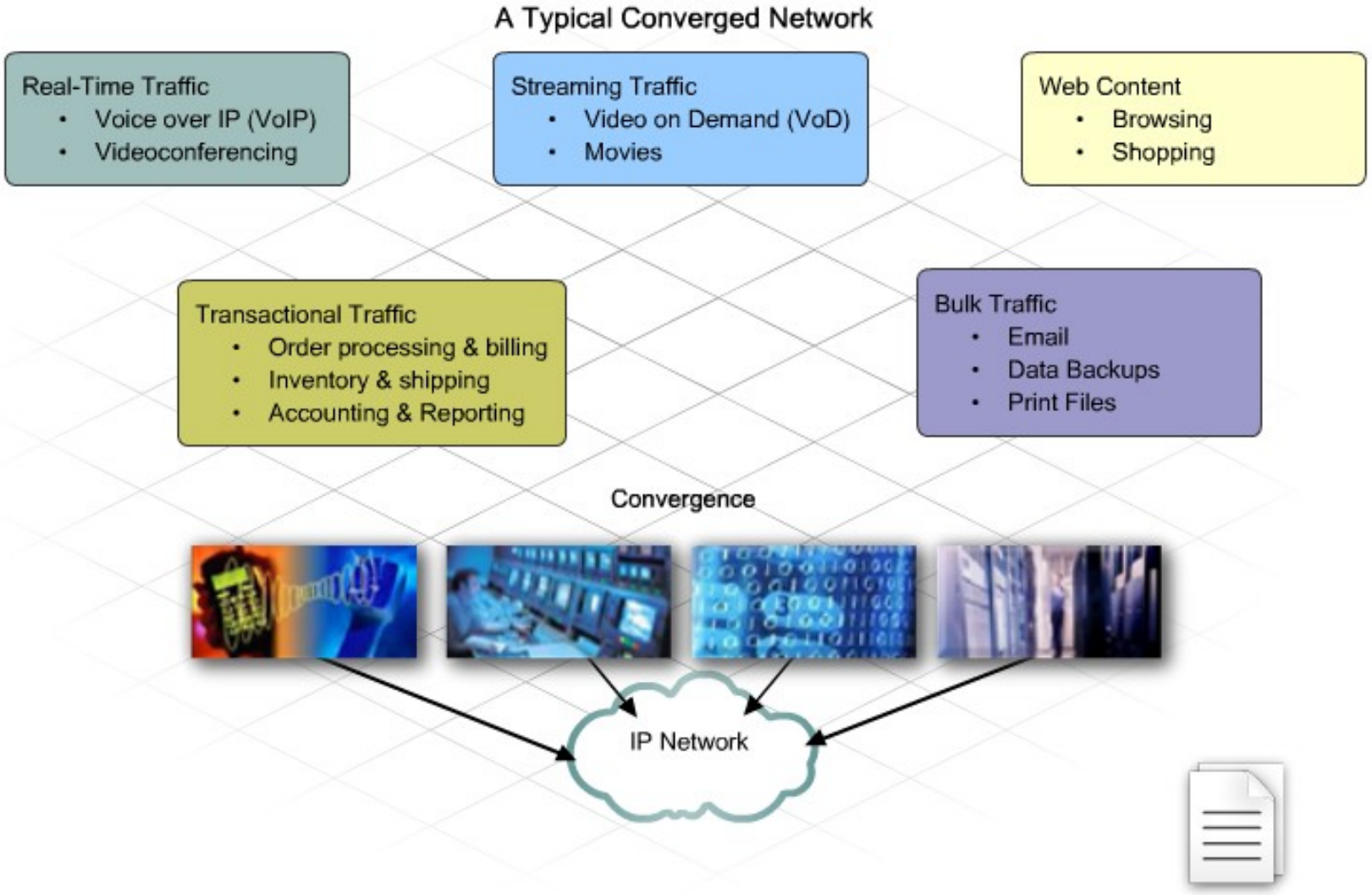
Converged Network Consideration

- Modern networks can support converged services where video and voice traffic are merged with data traffic. The network in the stadium is a typical example.
- Managing Converged Networks
- Control methods for voice and video traffic on converged networks are different from control methods for other traffic, such as web-based (HTTP) traffic.

Converged Network Consideration

- Quality of Service (QoS) on Converged Networks
- All networks perform better when QoS controls:
- Delay and jitter
- Bandwidth provisioning
- Packet loss parameters
- Converged networks require strong performance and security features to manage the conflicting requirements of their traffic. For this reason, QoS mechanisms are mandatory.

Converged Network Consideration



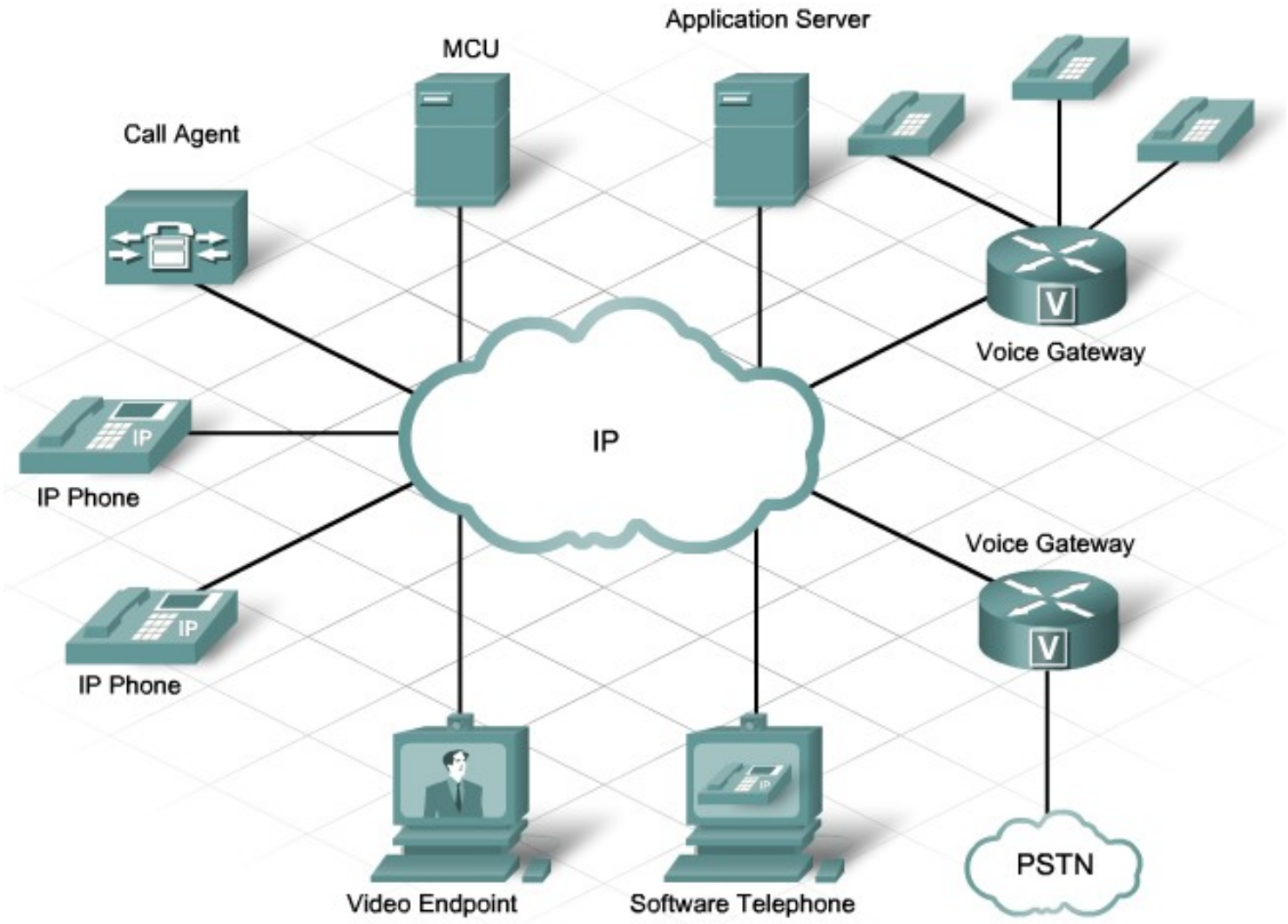
Requirements of an IP telephony solution

- One of the technical requirements of the stadium network is to upgrade to an IP telephony solution.
- IP Telephony Design Considerations
- The proposed network design must include:
- Power and capacity planning
- Identifying contending traffic flows
- Selecting the components for the IP telephony solution

Requirements of an IP telephony solution

- The components of an IP telephony solution can include:
- IP phones
- Gateway
- Multipoint control unit (MCU)
- Call agent
- Application servers
- Video endpoint
- Software telephone
- Other components, such as software voice applications and interactive voice response (IVR) systems, provide additional services to meet the needs of enterprise sites.

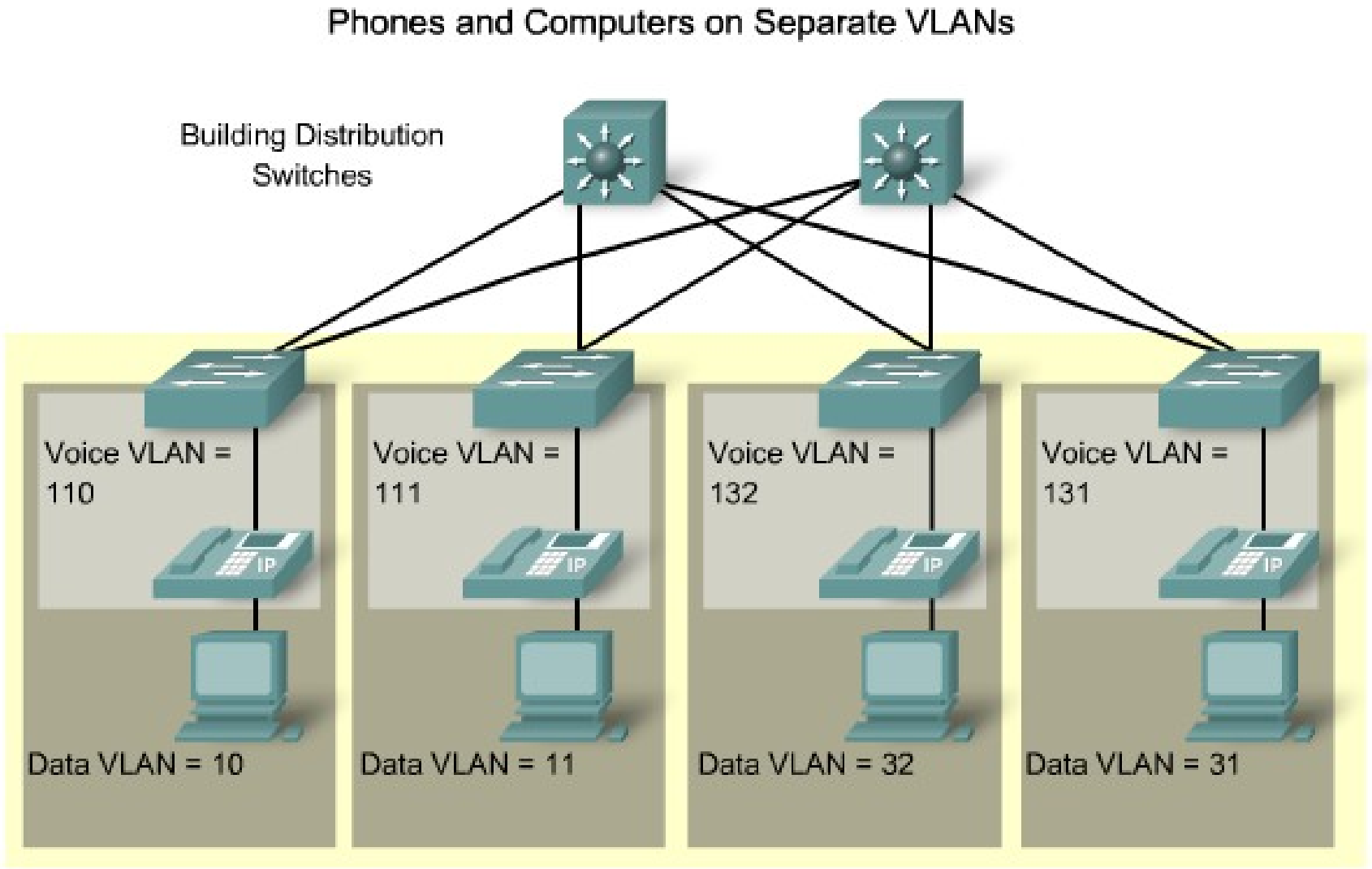
Requirements of an IP telephony solution



Requirements of an IP telephony solution

- Isolating Traffic
- If both the client PC and the IP phone are on the same VLAN, each will try to use the available bandwidth without considering the other device. The simplest method to avoid a conflict is to use separate VLANs for IP telephony traffic and data traffic.
- Benefits of Separate VLANs
- Using separate VLANs provides these benefits:
- QoS can prioritize the IP telephony traffic as it crosses the network.
- Network administrators can identify and troubleshoot network problems more easily when phones are on separate IP subnets and VLANs.

Requirements of an IP telephony solution



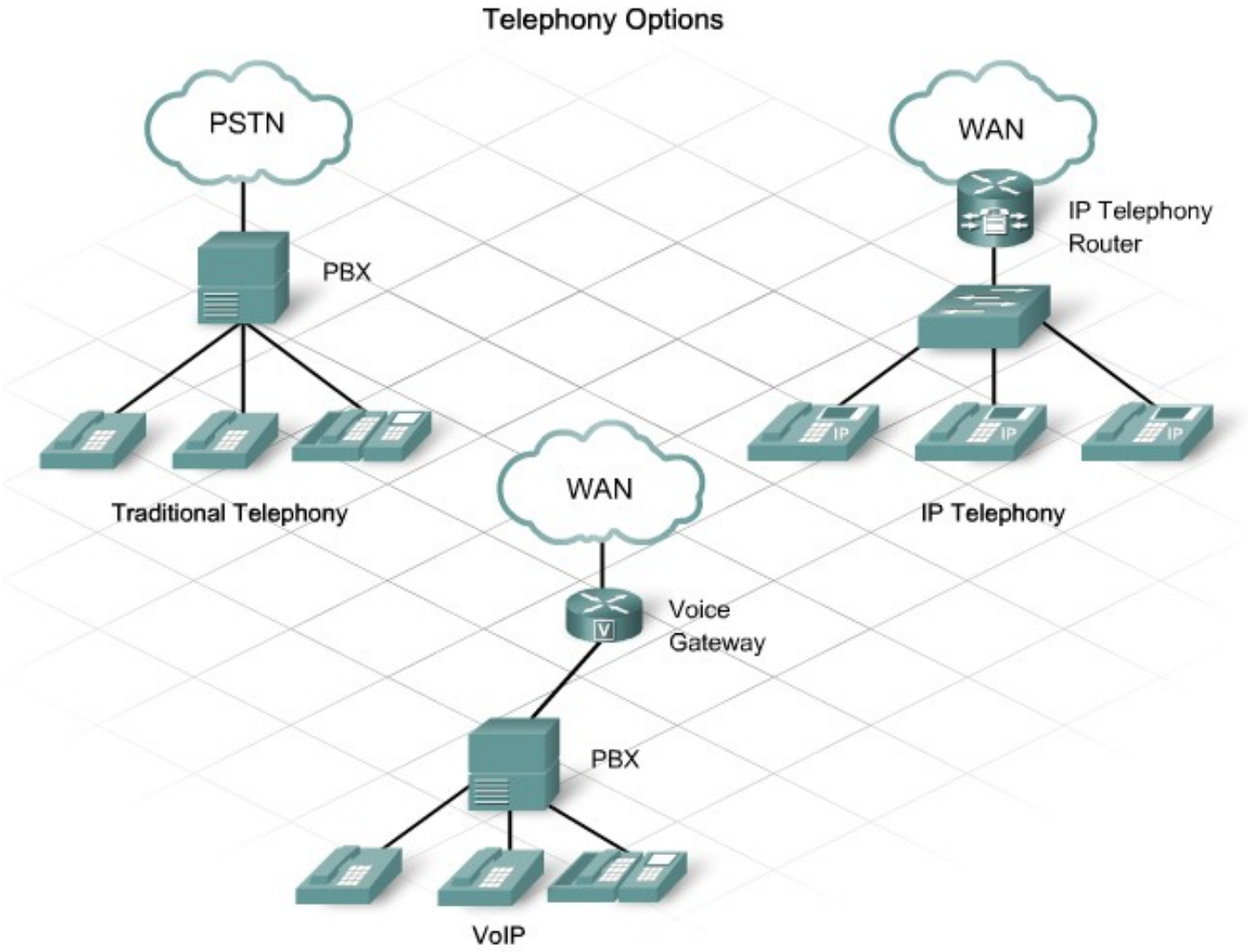
Requirements of an IP telephony solution

- The stadium management wants to replace their digital telephone system with IP telephony.
- Traditional Telephony
- Traditional business telephone systems are typically built around a central control unit, called a Private Branch Exchange (PBX). The PBX routes voice calls via analog or digital lines, depending on the type of device. For example, an analog fax machine or analog phone uses an analog line, and a digital desktop phone uses a digital line.

Requirements of an IP telephony solution

- VoIP
- Cisco uses the term VoIP when using voice-enabled routers to convert analog voice from traditional telephones into IP packets and route those packets between locations. Within the IT industry, VoIP is used interchangeably with IP telephony. With VoIP, the PBX connects to a voice-enabled router. It does not connect to a PSTN or to another PBX. Businesses use VoIP to reduce costs by consolidating WAN links, decreasing long distance calling charges and reducing the number of support staff.

Requirements of an IP telephony solution



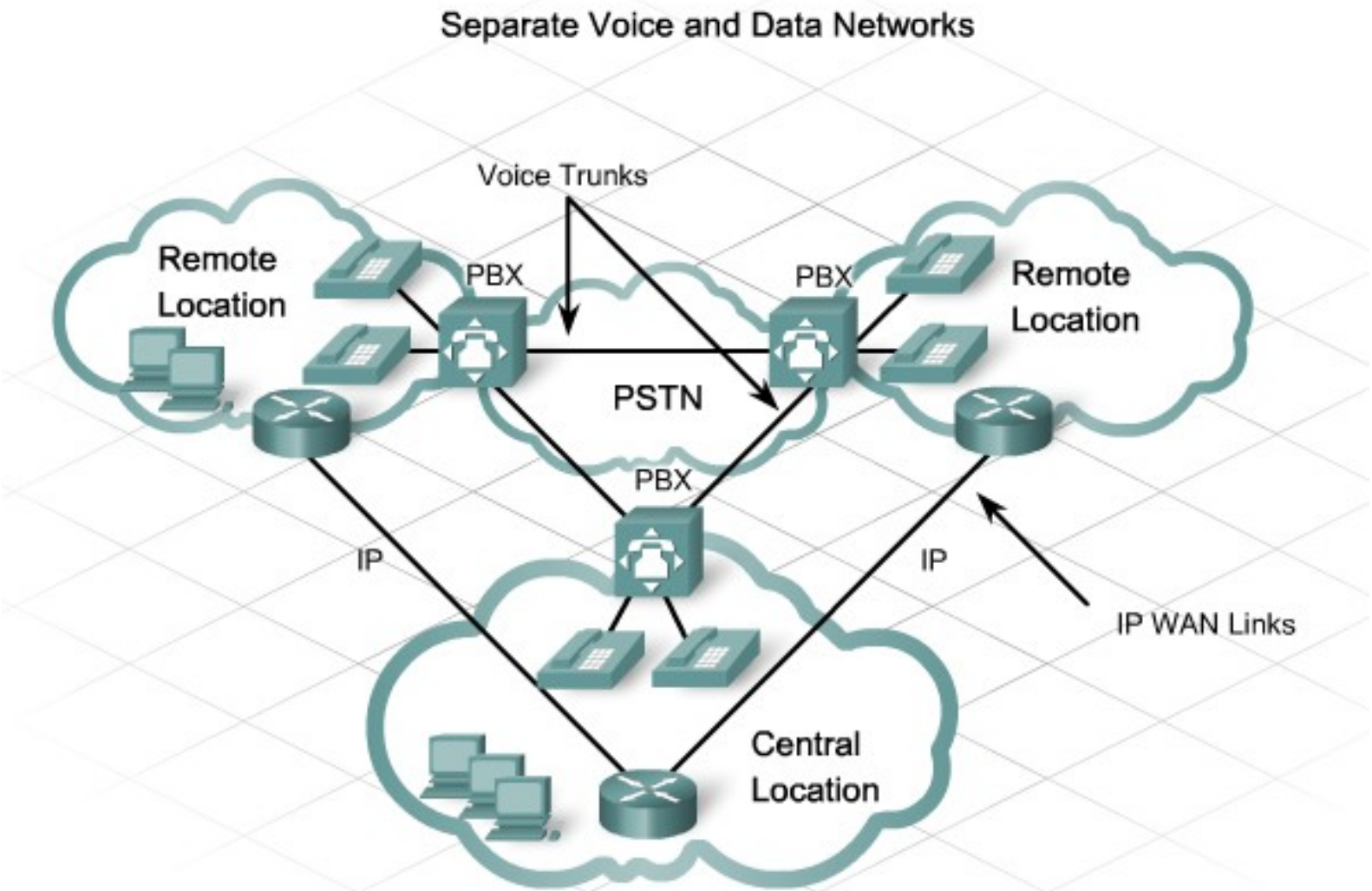
Requirements of an IP telephony solution

- IP Telephony
- IP telephony replaces traditional phones with IP phones and uses Cisco Unified Communications Manager, which is a server for call control and signaling. IP telephony has the following features:
- Integrates voice and voice-messaging applications that connect via the IP network rather than via the analog or digital systems.
- Uses an IP phone to perform voice-to-IP conversion.
- Creates peer-to-peer relationships between the phones involved in a conversation rather than centrally routing calls as a PBX does.

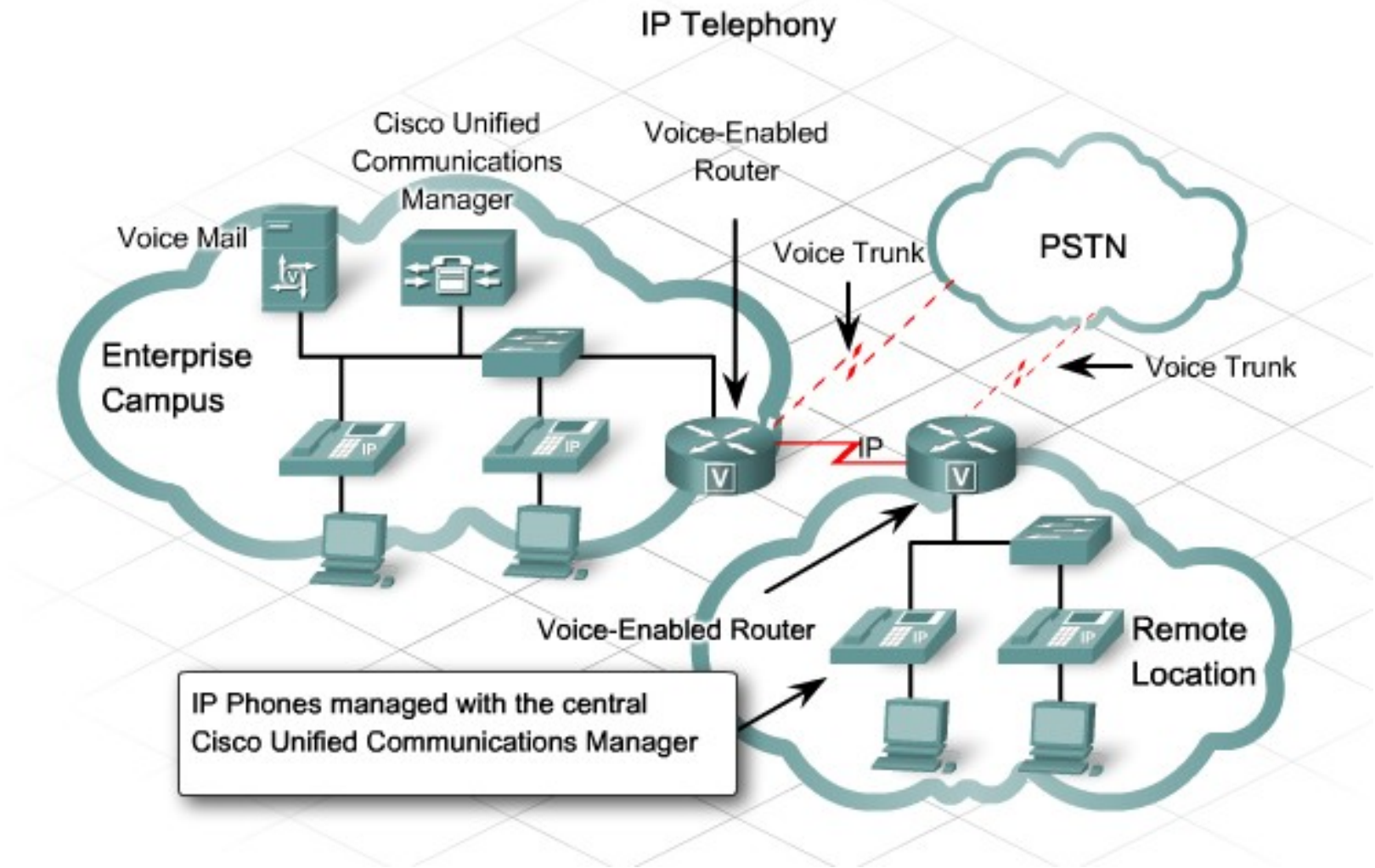
Requirements of an IP telephony solution

- The network designer and customer can incorporate VoIP or IP telephony onto the existing data network, creating a converged network.
- The stadium company expects to gain the following benefits of IP telephony:
- Simplified administration of office moves, additions, and changes
- Additional applications, such as directories and web pages, to the telephony system
- Reduced cost to manage the separate infrastructures

Requirements of an IP telephony solution



Requirements of an IP telephony solution



Requirements of an IP telephony solution

	Traditional Phone System	VoIP System	IP Telephony System
Uses a PBX for call control	✓		
Converts voice signals to IP traffic at voice-enabled routers		✓	
Converts voice signals to IP traffic at the phone			✓
Depends on physical cable infrastructure for phone addressing	✓		
Uses a server such as Cisco Unified Communications Manager for call control and signalling			✓
Voice traffic uses the corporate WAN		✓	
Integrates voice and data over the IP network		✓	
Connects to the PSTN	✓		

Video-live and on-demand

- Live Video
- Live video, or streaming video, enables users to see content before all the media packets are inside their computer system. Streaming media files do not have a waiting period for viewing; they are available immediately as a continuous stream of data packets. Streaming video eliminates the need to store large media files or to allocate storage space for the files before playing them. A live video feed is often sent using multicast packets to many users at the same time.

Video-live and on-demand

- VoD
- With VoD, users can either stream or download all of the content to their computer cache before they view it. Downloading the complete video file before viewing is also called store-and-forward. This method minimizes the load on system resources. Installing a server to direct streaming media into a computer cache allows users to retain the content and view it at a later time. VoD is sent using unicast packets to the specific user requesting the video. .

Video-live and on-demand

Video on Demand

Streaming Video

Video-live and on-demand

	VoD	Streaming
The video data packets are unicast to the user	✓	
The video data packets are multicast to the user		✓
The video can be stored for later viewing by the user	✓	
The video can be viewed as it is delivered to the user		✓
The live stream of video data packets are prioritized by the network		✓

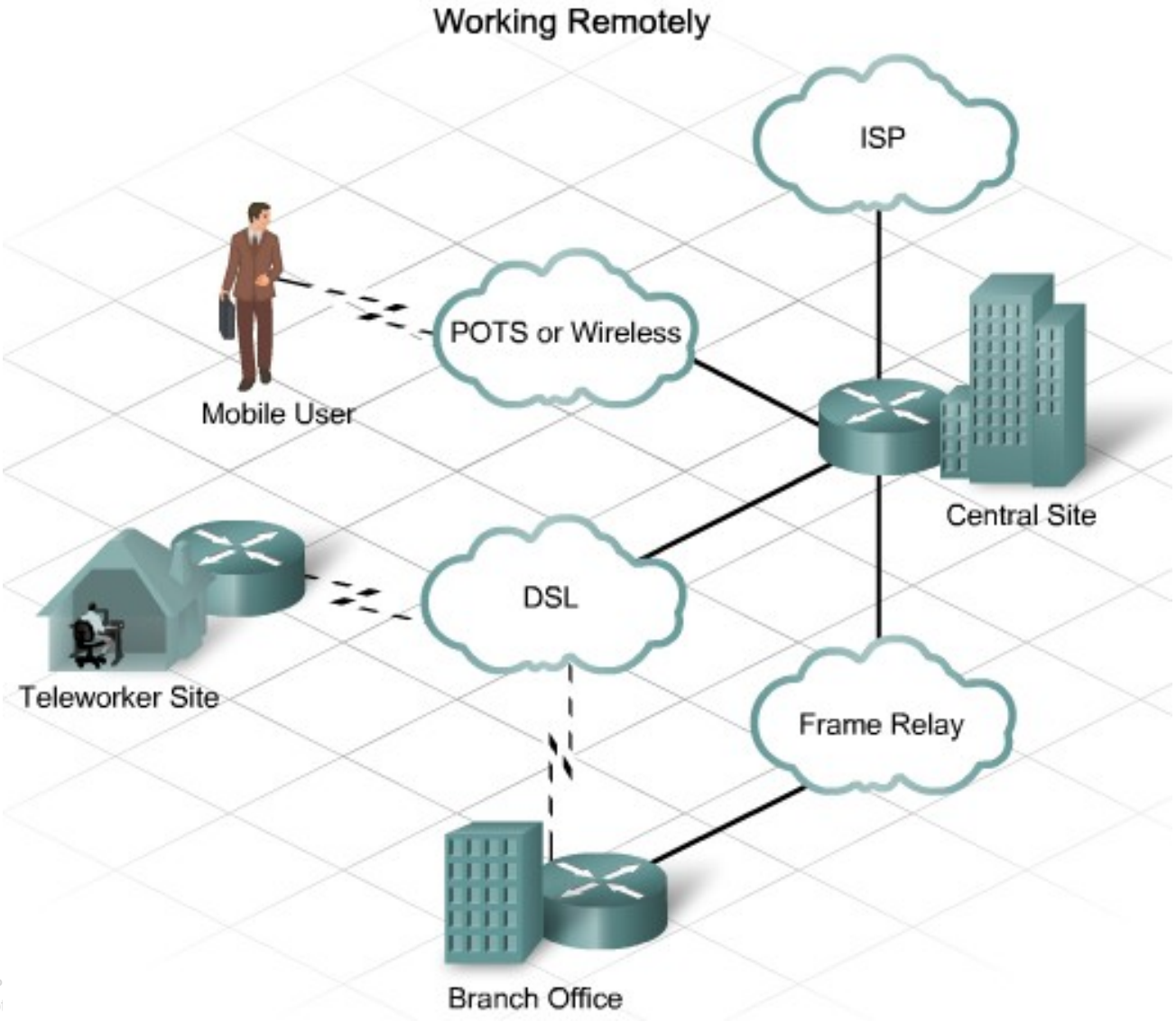
Supporting Remote users with voice and video

- Technology developments allow greater flexibility to workers in terms of how and where to work. At the stadium, for example, workers connect to the central site from several remote sites.
- To take advantage of central site resources and communications, a teleworker, branch office, or mobile user typically has at least one WAN connection to the central site. The bandwidth requirements for the WAN connection depend on the type of network resources that the users need to function in their job. If remote workers are part of the IP telephony network, a call manager system may need to be located remotely.

Supporting Remote users with voice and video

- This access impacts bandwidth. For example, streaming video may be used for a corporate meeting. These design decisions require assessing the bandwidth at the central site WAN connection as well.
- Permanent Link or On Demand?
- The network designer decides whether it is better to use permanent or on-demand links to the central site. The designer works with the customer to consider cost, security, and availability requirements.

Supporting Remote users with voice and video



Supporting Remote users with voice and video

- A high-speed Internet connection is a good solution for teleworkers. It is easy to set up in remote offices and is also available in many hotels. The stadium management plans to provide an Internet connection using wireless APs in the luxury boxes and the stadium restaurant.
- Sometimes, asynchronous dialup connections are the only remote access solution available to travelers. Employees who travel can use a PC with a modem and the existing telephone network to connect to the company.

Supporting Remote users with voice and video

- WAN connections at telecommuter sites can have the following features:
- Asynchronous dialup
- ISDN BRI
- Cable modems
- DSL
- Wireless and satellite
- VPN

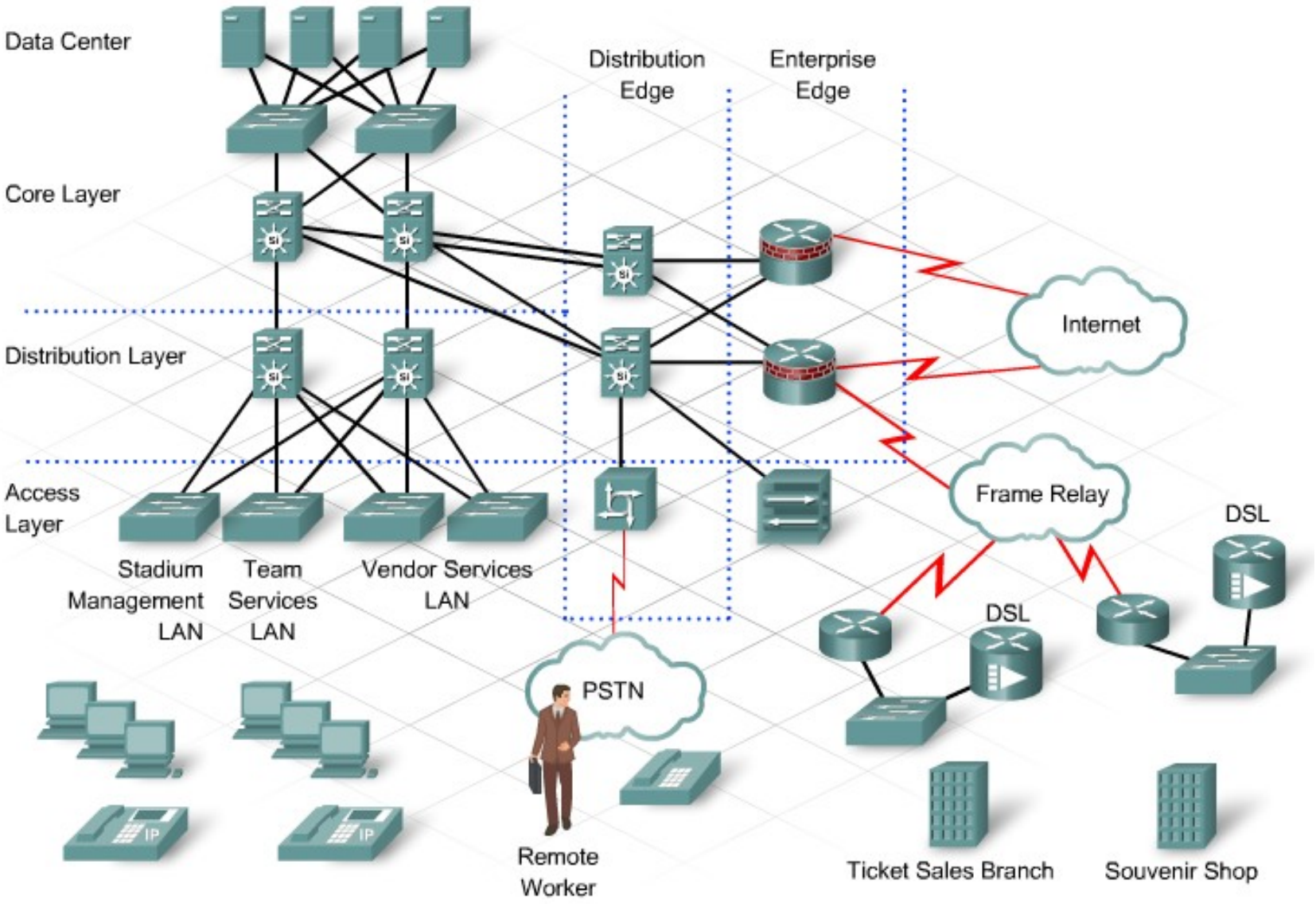
What is a traffic flow

- Traffic Flow
- Traffic flow on a network is similar to the traffic flow on city streets. Just as cars move from one location to another throughout the city, traffic generated from applications moves from one location in the network to another.
- A car on the street travels from a starting point to a destination. Similarly, a traffic flow created by an application travels as a unidirectional stream of packets between a source and a destination.

What is a traffic flow

- The path is typically defined by a Network Layer IP address. Depending on the QoS and policies configured in the network, the path can be influenced by other information such as Transport Layer source and destination port numbers.
- The path is typically defined by a Network Layer IP address. Depending on the QoS and policies configured in the network, the path can be influenced by other information such as Transport Layer source and destination port numbers.

What is a traffic flow



What is a traffic flow

- Application Traffic Flows
- The flow of application traffic in and out of a portion of the network can be minimal at times and significantly higher at others. For instance, in the sports stadium, early morning traffic may include email requests, Internet access, and file uploads to the stadium servers. Afternoon traffic might include VoIP, email, file transfers, and transaction processes from ticket sales.

What is a traffic flow

- If the network designer does not correctly estimate the volume of application traffic during the initial design of the stadium network, all applications could experience network congestion and degraded performance. Customers at concession stands and ticket purchasing kiosks might encounter significant delays or even an inability to access the applications. Customer satisfaction would diminish.

What is a traffic flow

- To aid in visualizing current and future traffic on the network, the designer creates a diagram of traffic flows. The first step is to identify the projected applications on the network. This information is gathered from the following sources:
- Customer input
- Network audit
- Traffic analysis

What is a traffic flow

Application Type	Application	Priority	Comments
Internal email	Outlook	High	
External email	Outlook	Normal	
Voice Networking	IP Telephony	High	The company is introducing IP Phones as a replacement for basic telephony.
Web Browsing	Internet Explorer, Netscape Navigator, Opera	Low	
Video On Demand	IP/TV	High	Wireless video will be available throughout the stadium.
Database		High	Servers are located around the network.
Customer Support Applications	Application list from stadium	High	

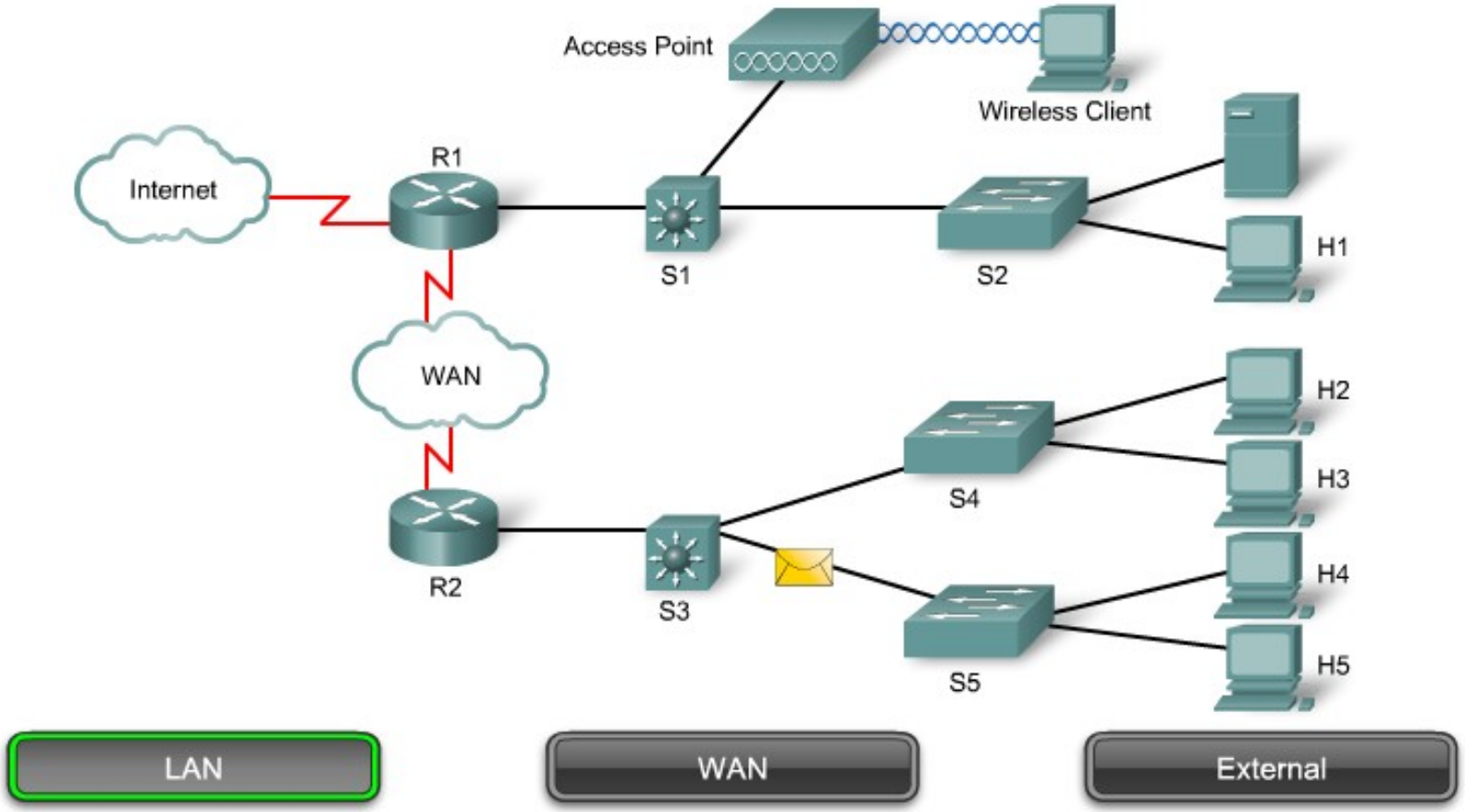
What is a traffic flow

- It is extremely important to identify traffic flows between hosts. The network designer uses the contents of logical or physical diagrams to plan the design to accommodate both existing and new applications traffic.
- The network designer generally uses a design program, such as MS Visio, to create a diagram that shows the identified applications and the logical topology of the network.

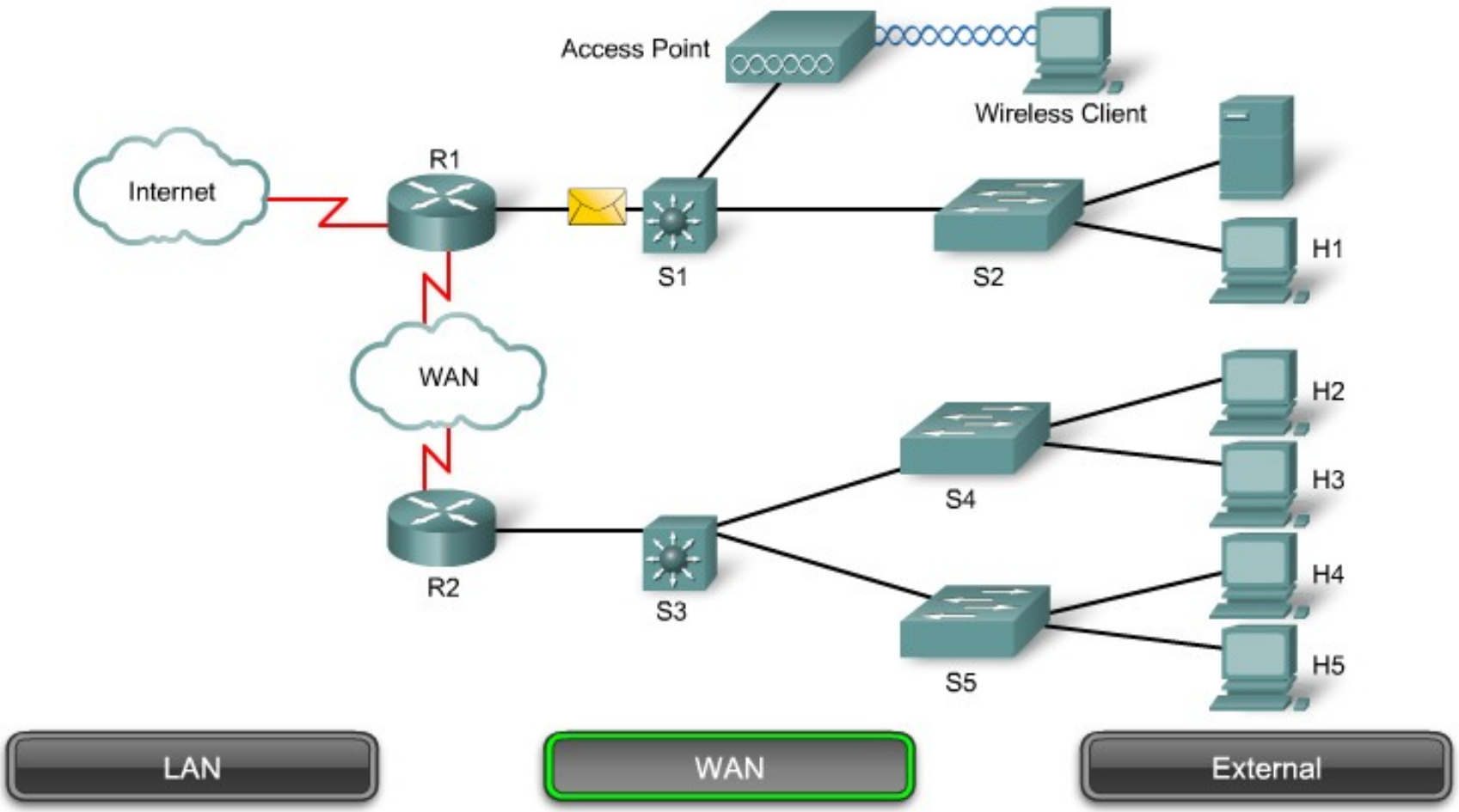
What is a traffic flow

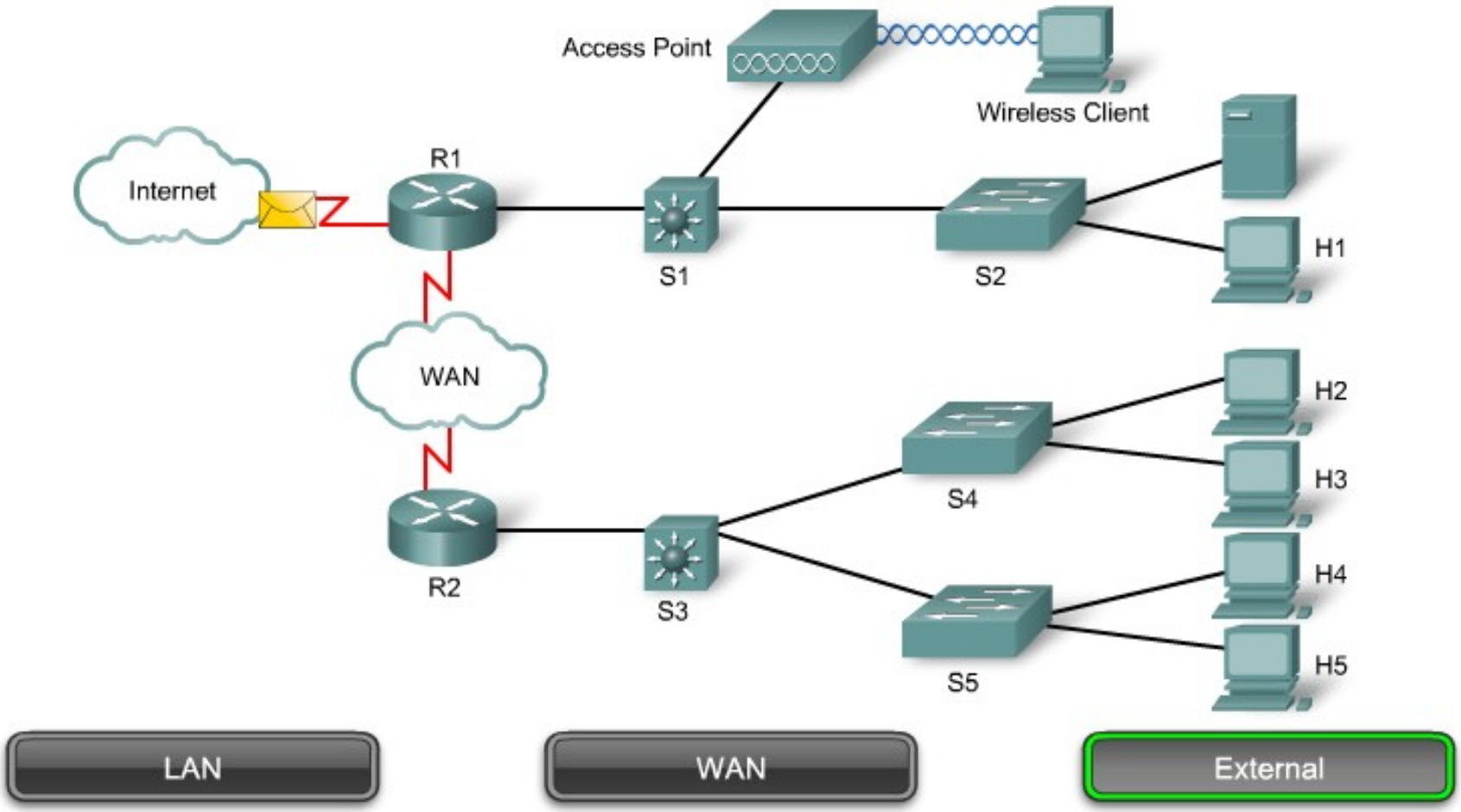
- From the logical diagram, the designer identifies possible areas of congestion. The designer then determines the equipment needed to handle the traffic flowing from host to host and from host to server.
- In the stadium, the logical topology diagram shows the traffic flows from host to host and from host to servers. The connection of the devices also shows the applications that will be used. The traffic generated between the hosts is relatively minor when compared to the traffic generated from the hosts to the servers.

What is a traffic flow



What is a traffic flow





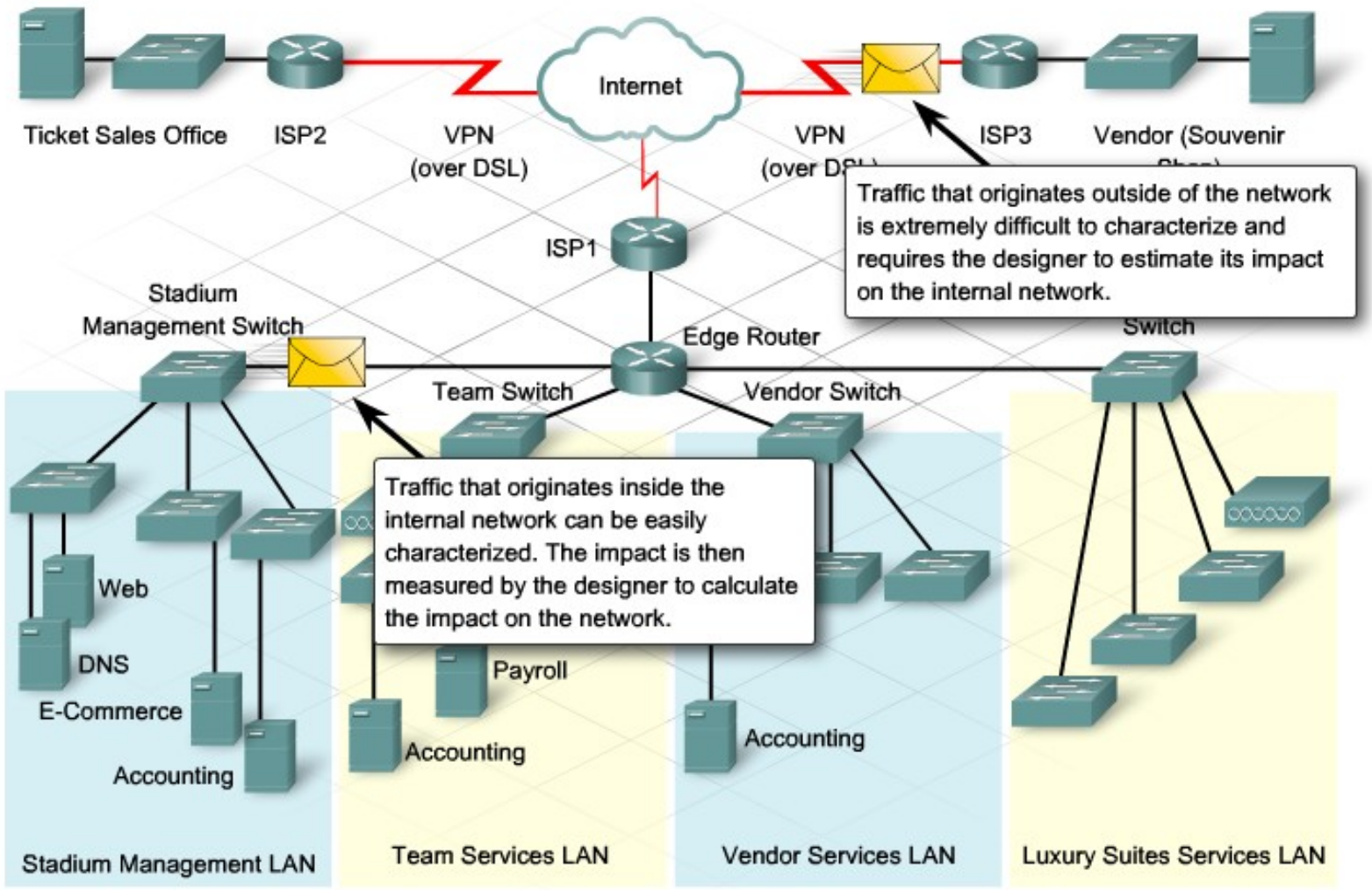
Diagramming Internal (Intranet) traffic flow

- The stadium network serves a complex organization that has many operational areas. The management offices, servers, vendors, and ticket offices are all a part of the larger network.
- Each LAN within the stadium handles traffic being sent from host to host and host to server. General file transfers from host to host and email traffic do not consume large amounts of bandwidth. However, the daily backups to the server consume large amounts of bandwidth and need to be analyzed during the design phase.

Diagramming Internal (Intranet) traffic flow

- All traffic flows, from both the internal and external networks, must be carefully assessed when designing a new network or proposing upgrades for an existing network. This assessment poses unique challenges for the network designer:
- Traffic within the internal network is easy to identify. This traffic can be used to estimate utilization of the network.
- Traffic from external sources is difficult to characterize. The designer needs to estimate the bandwidth requirements for external traffic flows.

Diagramming Internal (Intranet) traffic flow



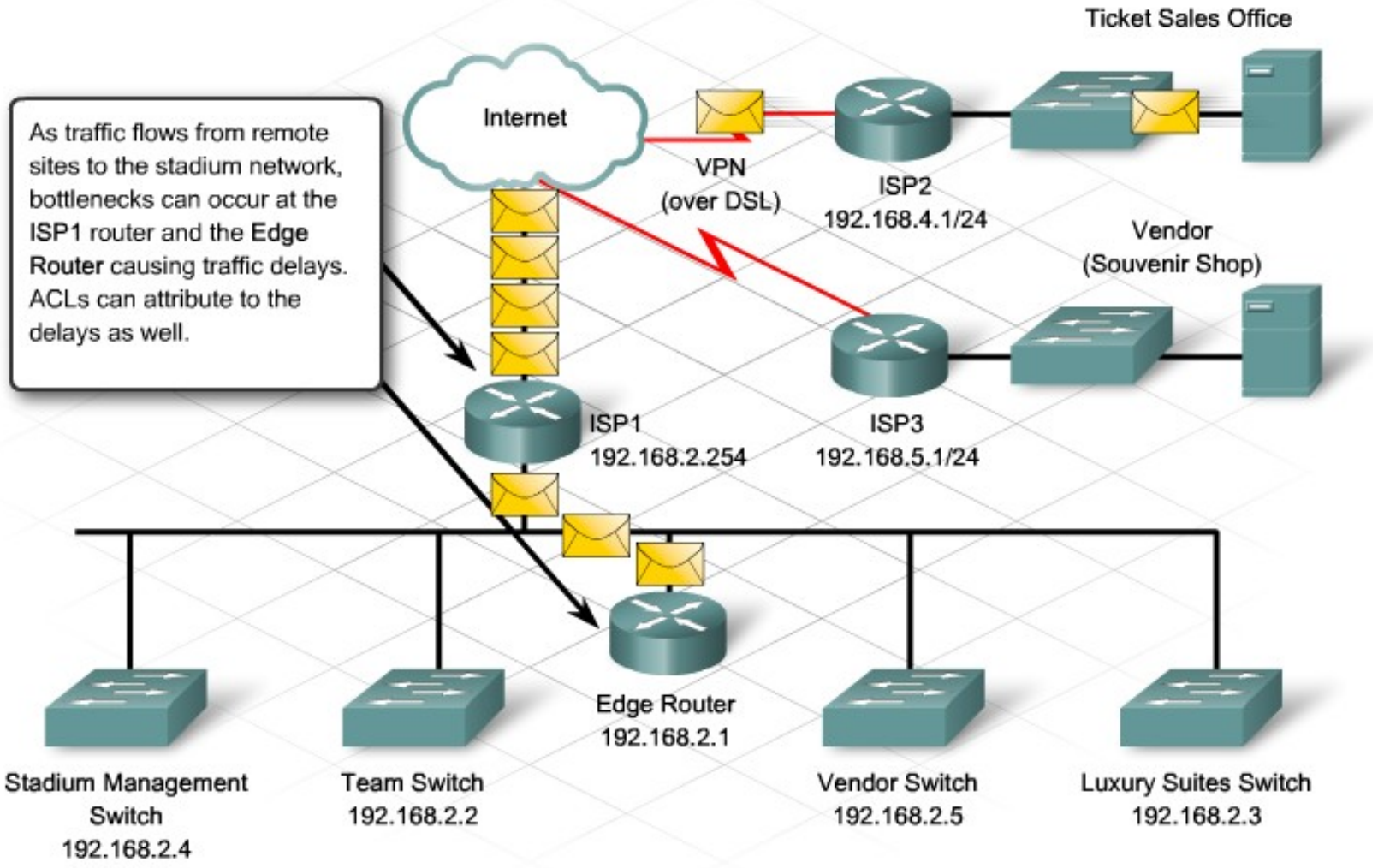
Diagramming traffic flows to and from remote sites

- After all sections of the internal LAN have been characterized and diagrammed, the network designer focuses on the remote sites and VPNs.
- The amount of traffic sent to or received from a remote site can be small. In the stadium network, the traffic flows may be small, but they are primarily transactional processes sent from the ticket office to the servers located at the stadium. Because these applications are mission-critical, it is important to identify the flows for QoS, redundancy, and security purposes.

Diagramming traffic flows to and from remote sites

- As with the LAN topology, the remote devices that generate traffic on the network need to be identified. All switches and routers that are used to connect the remote sites to the stadium are part of the path that the application traffic takes.
- The network designer should calculate the amount of traffic flowing from the remote sites as part of the external traffic flows into the stadium network. The designer should also determine if any ACLs or firewalls will interfere with the flow of appropriate traffic.

Diagramming traffic flows to and from remote sites



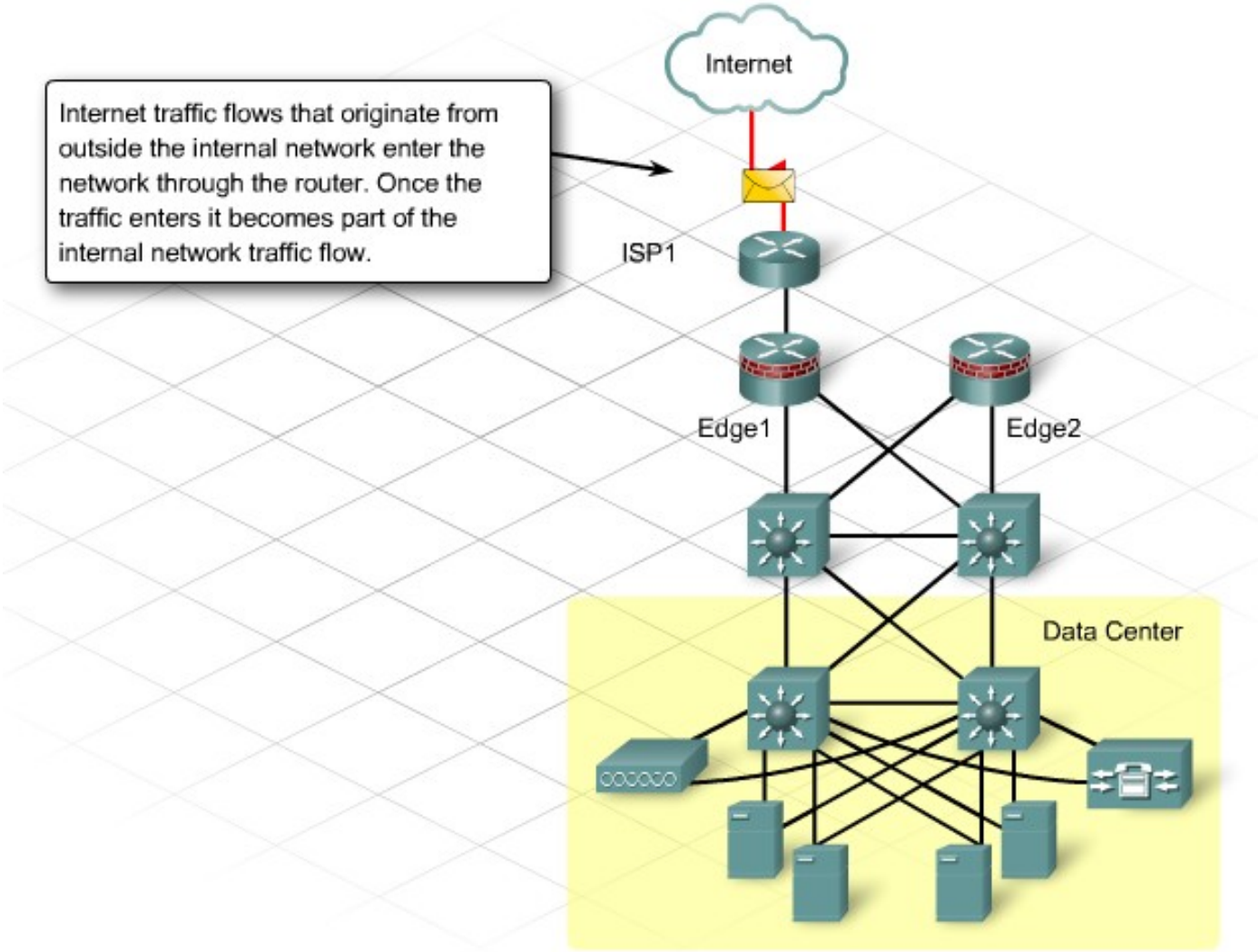
Diagramming External Traffic Flows

- Although most of the traffic in the existing stadium network is internal, the network designer must consider the external traffic that is destined for the Internet.
- Diagramming the Internet is impossible, considering the number of devices that are connected to it. However, it is possible to determine:

Diagramming External Traffic Flows

- The outgoing traffic flows destined for the Internet. An example of outgoing traffic in the stadium network is users in the stadium who require access to external resources, such as online sports news.
- The incoming traffic flows from the Internet to locally-provided services. An example of incoming traffic is customers purchasing tickets online who need access to the internal servers to process the purchases.

Diagramming External Traffic Flows



Diagramming Extranet Traffic Flows

- The stadium has a remote site and a vendor that is allowed to access the internal network through VPNs. These VPNs permit access to the stadium internetwork via secure, encrypted connections. The stadium also has a web-based e-commerce server that allows customers to buy tickets. This server is protected using SSL.
- vendor and customers are using IPSec to secure traffic flows into the stadium network.

Diagramming Extranet Traffic Flows