4. Network Traffic

CHAPTER 4

Dr. Mahmud Mansour

Network Traffic Factors

- Traffic flow
- Location of traffic sources and data stores
- Traffic load
- Traffic behavior

To understand network traffic flow, First we identify user communities and data stores for existing and new application

User community

A user community is a set of workers who use a particular application or set of applications. A user community can be a corporate department or set of departments.

- Application usage crosses departmental boundaries.
- It becomes increasingly necessary to characterize user communities by application and protocol usage rather than by departmental boundary.
- To document user communities, ask your customer to help you fill out the User Communities chart shown in the next Slide

User community

User Community Name	Size of Community (Number of Users)	Location of Community	Applications Used by Community
PC users in Computing Center	30, will grow to 60	Basement of library	Homework, email, web research, library card catalog
Mac users in the Computing Center	15, will grow to 30	Basement of library	Homework, email, web research, library card catalog
Library patrons	15, will grow to 30	Floors 1–3 of library	Email, web research, library card catalog
Business/Social Sciences PC users	15, will grow to 30	Business and Social Sciences building	Homework, email, web research, library card catalog
Arts/ Humanities Mac users	15, will grow to 25	Arts and Humanities building	Homework, email, web research, library card catalog, graphics upload

Data Stores

- Characterizing traffic flow also requires that you document major data stores.
- A data store (called a data sink) is an area in a network where application layer data resides.
- A data store can be a server, a server farm, a storage-area network (SAN), a mainframe, a tape backup unit, a digital video library, or any device or component of an internetwork where large quantities of data are stored.
- Document major data stores, By asking your customer to help you to fill out Table

Data Stores

Data Store	Location	Application	Used by User Community (or Communities)
Library card catalog Windows server	Computing Center server farm	Library card catalog	All
Apple Filing Protocol (AFP) file server	Computing Center server farm	Homework	Mac users in the Computing Center and in Arts and Humanities building
Windows file/print server	Computing Center server farm	Homework	PC users in all buildings
Windows web server	Computing Center server farm	Hosts the WVCC website	All
Windows email server	Computing Center server farm	Email	All users except visitors (who use their own servers)

Network Traffic Flow

- Network flow can be characterized by its direction and symmetry
- Identifying sources and destinations of network traffic.
- Analyzing the direction and symmetry of data traveling between sources and destinations.
- In some applications, the flow is bidirectional and symmetric. (Both ends of the flow send traffic at about the same rate.) In other applications, the flow is bidirectional and asymmetric. (Clients send small queries and servers send large streams of data.)
- In a broadcast application, the flow is unidirectional and asymmetric

Types of Traffic Flow

- Classify network traffic flow to the following well-known types:
  - Terminal/host
  - Client/server
  - Thin client
  - Peer-to-peer
  - Server/server
  - Distributed computing

Types of Traffic Flow

Terminal/host traffic flow

Terminal/host traffic is usually asymmetric. The terminal sends a few characters and the host sends many characters. Telnet is an example of Terminal/host.

Client/server traffic flow

- Clients rely on servers for access to resources, such as storage, application software, and processing power.
- The flow is usually bidirectional and asymmetric.

Types of Traffic Flow

- *Thin client traffic flow*

  Software or hardware that is designed to be particularly simple and to work in an environment where the bulk of data processing occurs on a server.

- *Peer-to-peer traffic flow*

With peer-to-peer traffic, the flow is usually bidirectional and symmetric.

- *Server/Server*

Server/server traffic includes transmissions between servers and transmissions between servers and management applications.

Types of Traffic Flow

- *Distributed computer traffic flow*

  applications that require multiple computing nodes working together to complete a job.

Sizes of Objects

- Terminal screen: 4 Kbytes
- Simple e-mail: 10 Kbytes
- Simple web page: 50 Kbytes
- High-quality image: 50,000 Kbytes
- Database backup: 1,000,000 Kbytes or more

Traffic Flow

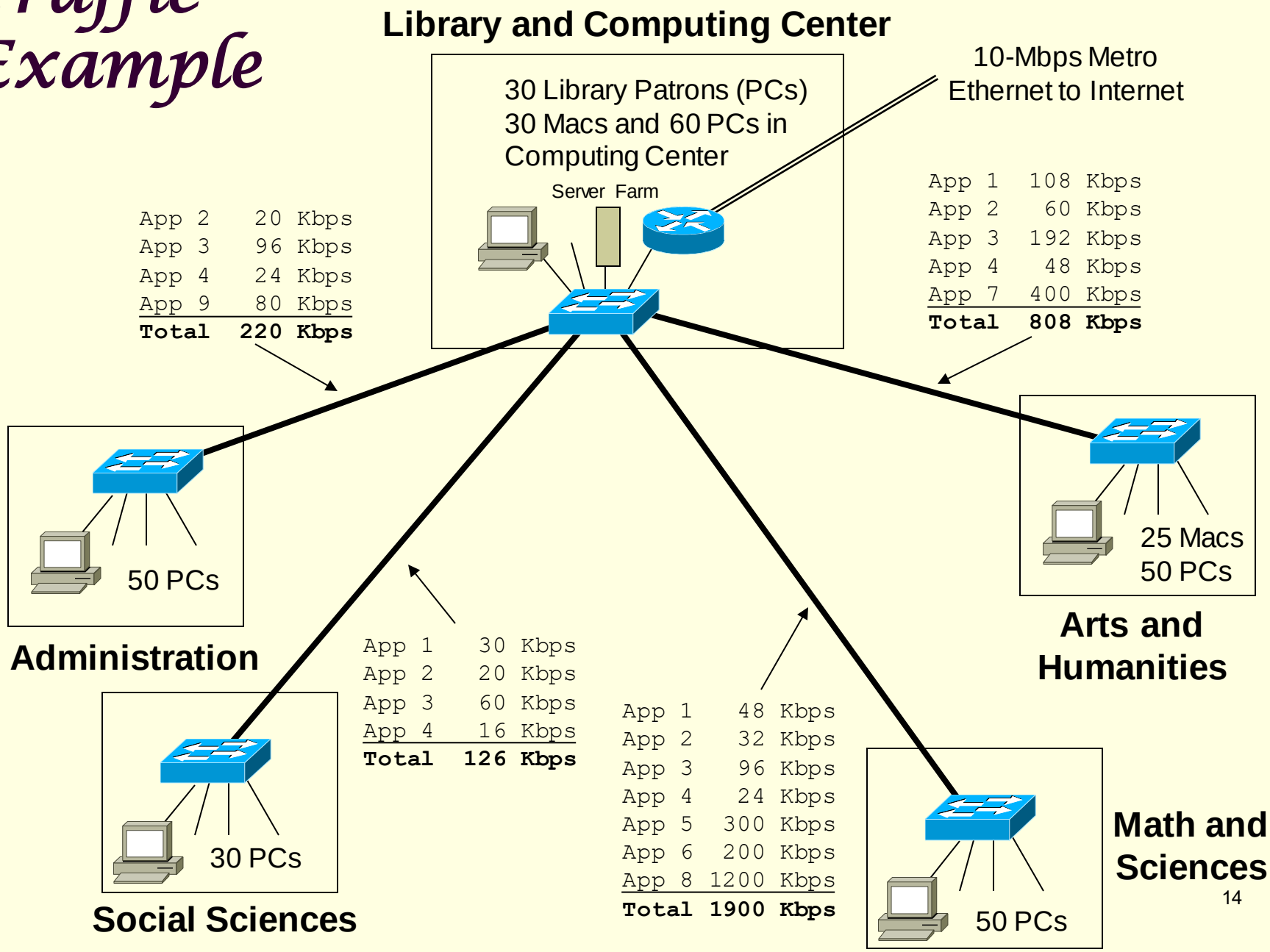
- To characterize the size of a flow, use a protocol analyzer or network management system to record load between important sources and destinations.

- You can also use Cisco NetFlow, which collects and measures data as it enters router and switch interfaces, including source and destination IP addresses, source and destination TCP or UDP port numbers, packet and byte counts, and so on.

Traffic Flow

	Destination 1 MB/sec	Destination 2 MB/sec	Destination 3 MB/sec	Destination *n* MB/sec
Source 1				
Source 2				
Source 3				
Source *n*				

Traffic Example



Traffic Flow for VOIP

- The most important concept to understand when considering traffic flow in VoIP networks is that there are two flows: The flow associated with transmitting the audio voice is separate from the flows associated with call setup and teardown.
  - The flow for transmitting the digital voice is essentially peer-to-peer. Cisco IP and Skype.
  - Call setup and teardown is a client/server flow
    - A phone needs to talk to a server or phone switch that understands phone numbers, IP addresses, capabilities negotiation, and so on.

Applications Traffic Characteristics

Name of Application	Type of Traffic Flow	Protocol(s) Used by Application	User Communities That Use the Application	Data Stores (Servers, Hosts, and so on)	Approximate Bandwidth Requirements	QoS Requirements

Traffic Load

- Characterizing traffic load can help you design networks with sufficient capacity for local usage and internetwork flows.
- The goal is simply to avoid a design that has any critical bottlenecks.
- To avoid bottlenecks, you can research application-usage patterns, idle times between packets and sessions, frame sizes, and other traffic behavioral patterns for application and system protocols.

Calculating Traffic Load

- If bandwidth is not a constraint in your network designs, you can skip this section.
- To calculate whether capacity is sufficient, you should know:
  - The number of stations
  - The average time that a station is idle between sending frames
  - The time required to transmit a message once medium access is gained
- That level of detailed information can be hard to gather, however

Traffic Behavior

- Measuring traffic flow behavior can help a network designer determine which routers should be peers in routing protocols that use a peering system, such as the Border Gateway Protocol (BGP). Measuring traffic flow behavior can also help network designers do the following:
- Characterize the behavior of existing networks.
- Plan for network development and expansion.
- Quantify network performance.
- Verify the quality of network service.
- Ascribe network usage to users and applications

An individual network traffic flow can be defined as protocol and application information transmitted between communicating entities during a single session.

Traffic Behavior

- Broadcasts
  - All ones data-link layer destination address
  - Doesn't necessarily use huge amounts of bandwidth
  - But does disturb every CPU in the broadcast domain
- Multicasts
  - First bit sent is a one
  - Should just disturb NICs that have registered to receive it
  - Requires multicast routing protocol on internetworks

Network Efficiency

- Efficiency refers to whether applications and protocols use bandwidth effectively. Efficiency is affected by:
  - Frame size
  - Protocol interaction
  - Windowing and flow control
  - Error-recovery mechanisms

Topology Design Themes

- Hierarchy
- Redundancy
- Modularity
- Well-defined entries and exits
- Protected perimeters

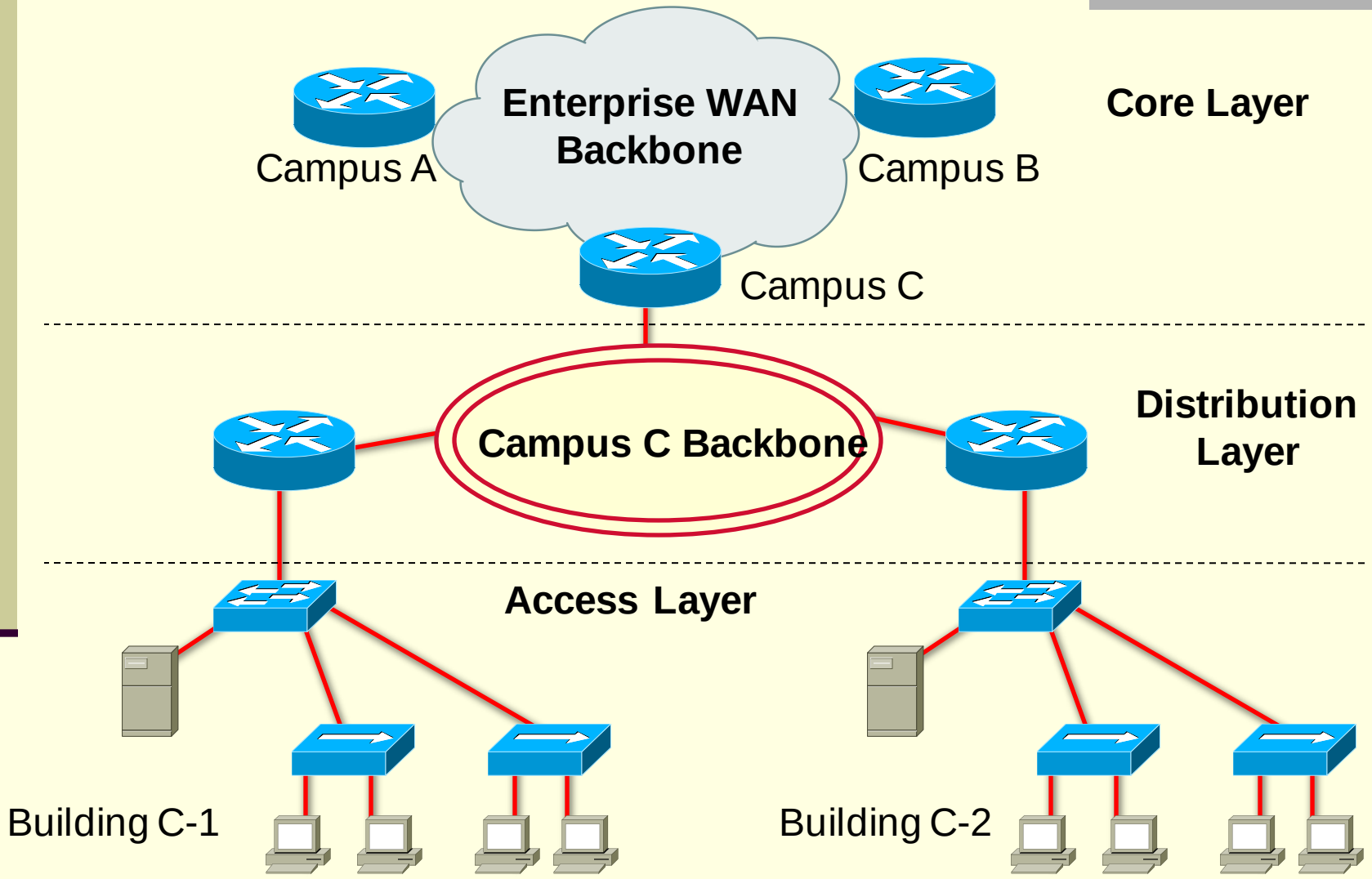
Hierarchical Model

- Network design experts have developed the hierarchical network design model to help you develop a topology in discrete layers. Each layer can be focused on specific functions, allowing you to choose the right systems and features for the layer.

Hierarchical Model

- Reduces workload on network devices
  - Avoids devices having to communicate with too many other devices (reduces "CPU adjacencies")
- Constrains broadcast domains
- Enhances simplicity and understanding
- Facilitates changes
- Facilitates scaling to a larger size

Hierarchical Design



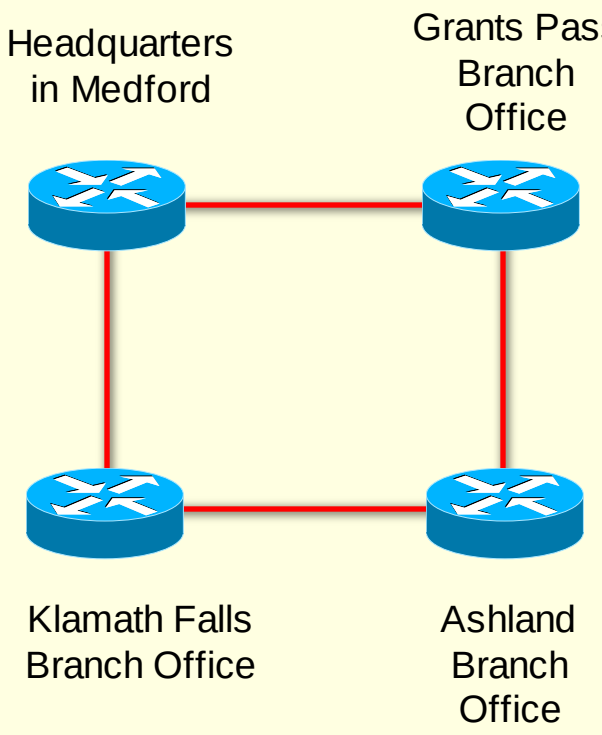
Hierarchical Model

- You can purchase the appropriate internetworking devices for each layer of the hierarchy.
- Using a hierarchical model can help you minimize costs or (avoiding spending money).
- Hierarchical design model enables accurate capacity planning within each layer of the hierarchy, thus reducing wasted bandwidth.
- Modularity enables you to keep each design element simple and easy to understand.

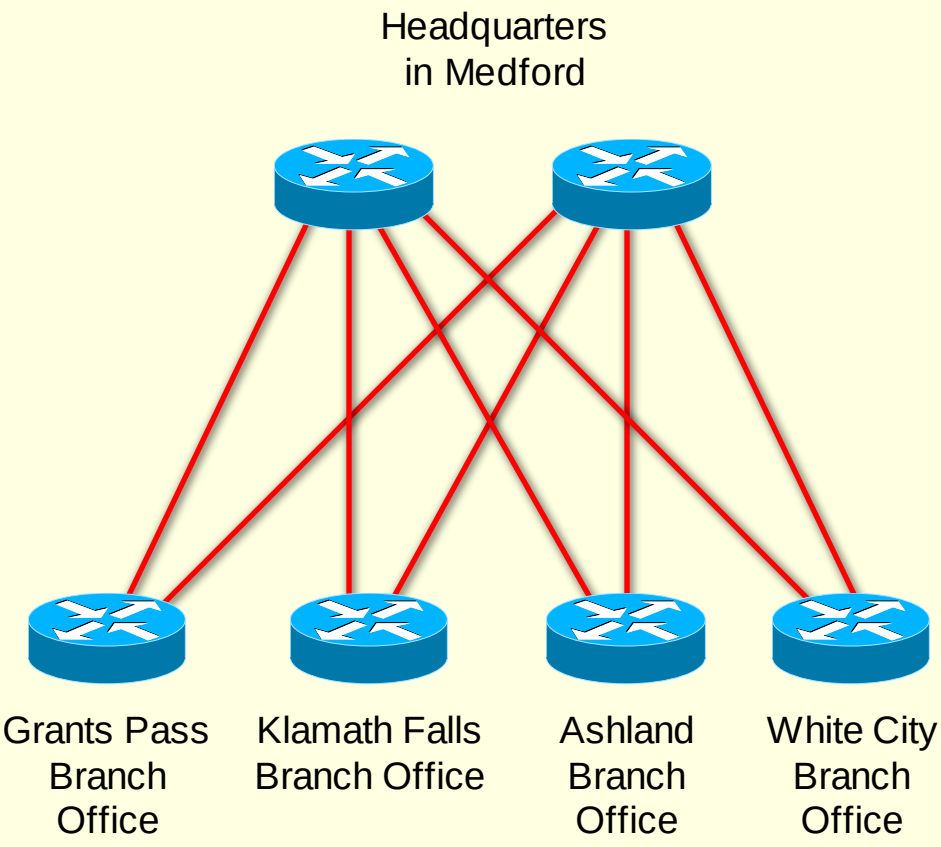
Cisco's Design Model

- A core layer of high-end routers and switches that are optimized for availability and speed.
- A distribution layer of routers and switches that implement policies and segment traffic, In small and medium-sized organizations, the core and distribution layers can be combined.
- An access layer that connects users via lower-end switches and other devices

Flat Versus Hierarchy



Flat Loop Topology

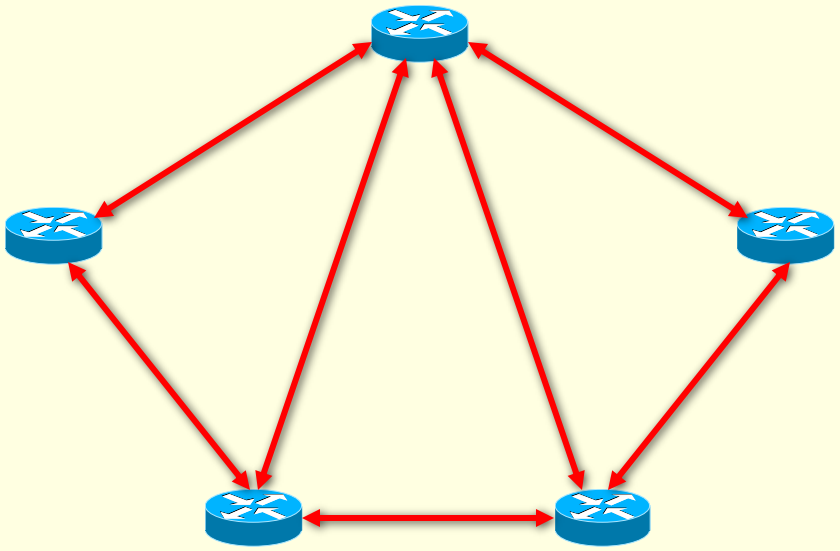


Hierarchical Redundant Topology

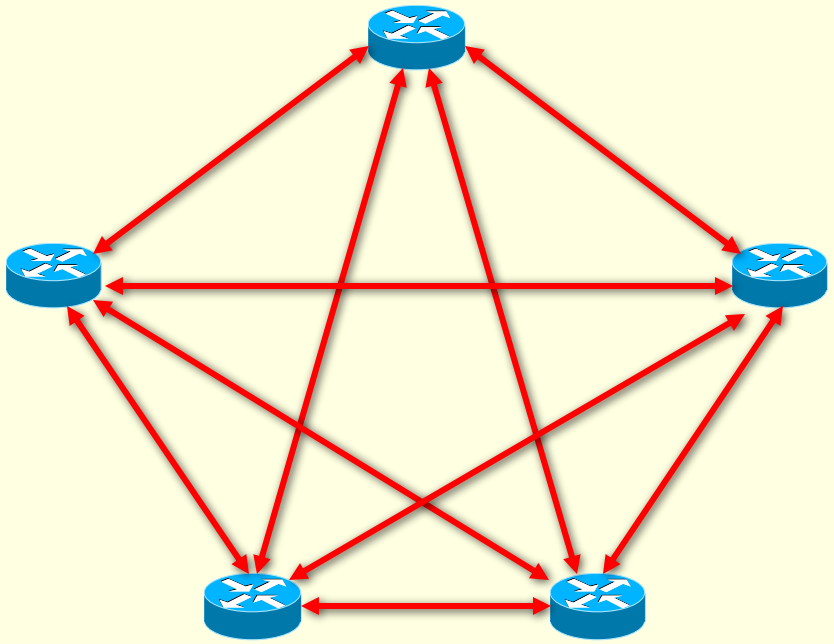
Flat Versus Hierarchy

- A flat network topology is adequate for small networks.
- In a large flat (switched) network, broadcast packets are burdensome. A broadcast packet interrupts the CPU on each device within the broadcast domain.
- The CPU workload required for routers to communicate with many other routers and process numerous route advertisements.

Mesh Designs

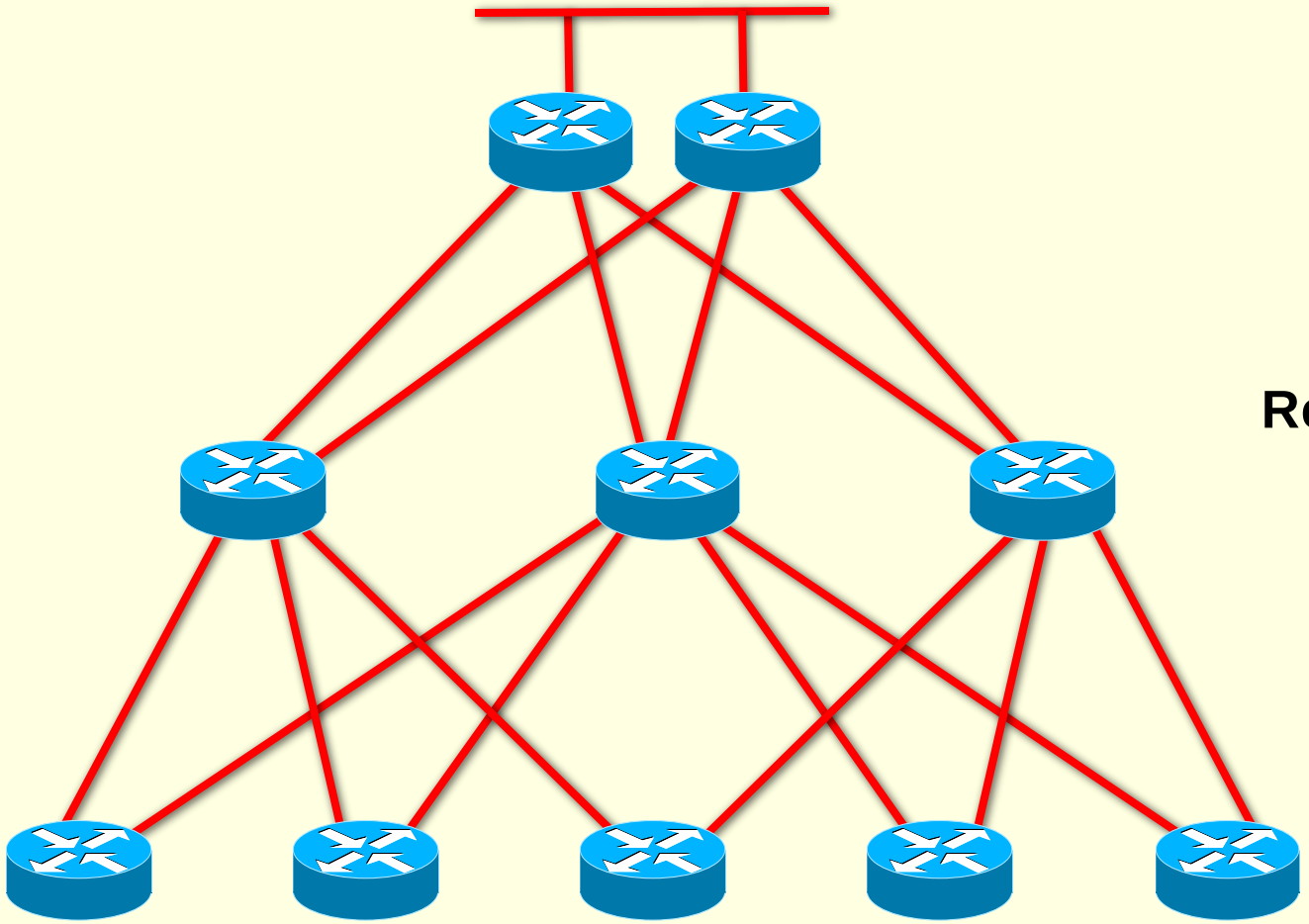


Partial-Mesh Topology



Full-Mesh Topology

A Partial-Mesh Design

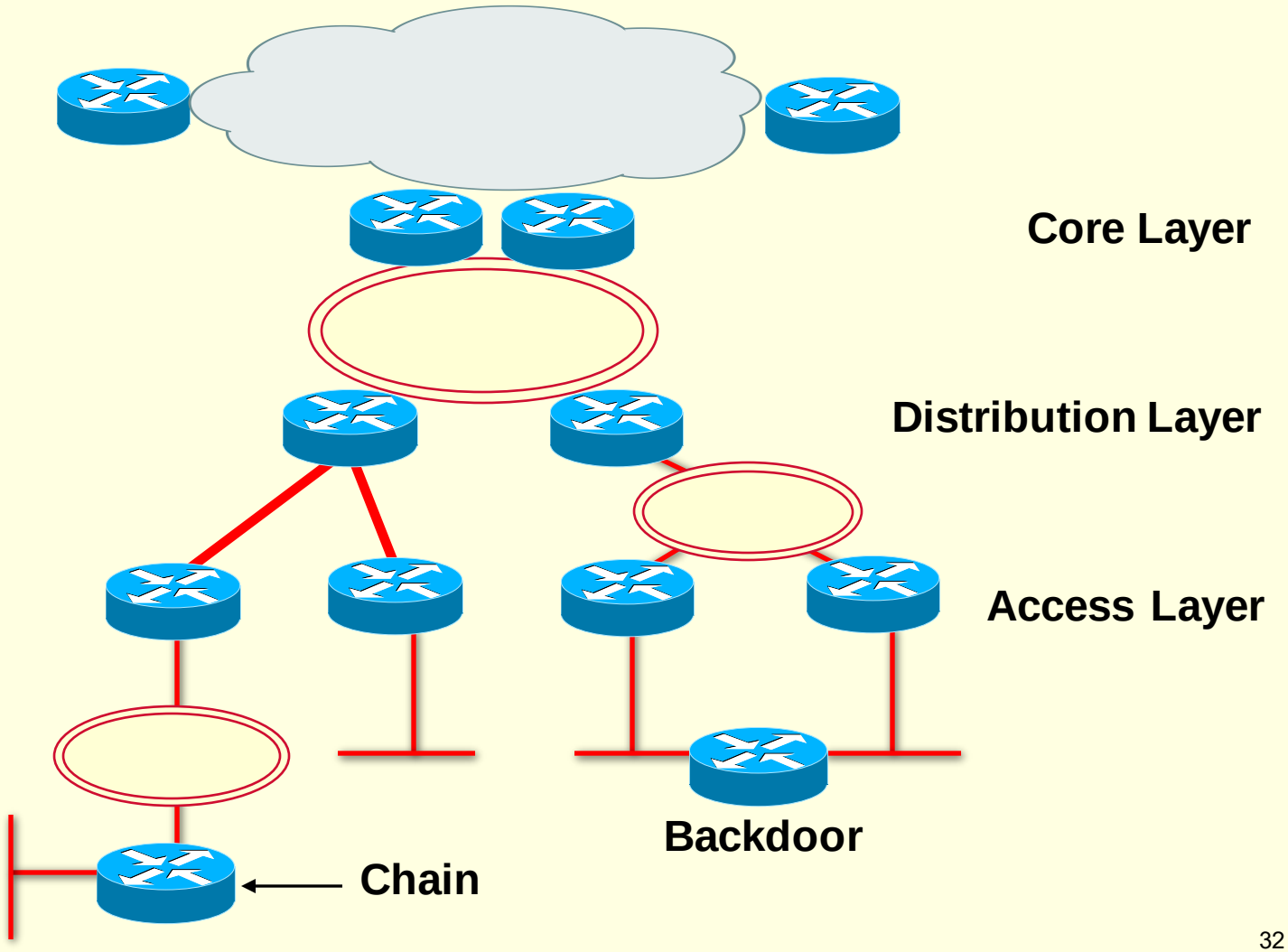


Headquarters (Core Layer)

Regional Offices (Distribution Layer)

Branch Offices (Access Layer)

Avoid Chains and Backdoors



Redundant Network Design Topologies

- Enable you to meet requirements for network availability by duplicating elements in a network.
- eliminate any single point of failure on the network.
- enable business survivability after a disaster and offer performance benefits from load sharing, some organizations have completely redundant data centers.

Backup Paths

- Backup path for packets to travel when there are problems on the primary path.
- Two aspects of the backup path considers:
- How much capacity the backup path supports
- How quickly the network will begin to use the backup path.

- It is quite common for a backup path to have less capacity than a primary path. Individual backup links within the backup path often use different technologies. For example, a leased line can be in parallel with a backup dialup line or ISDN circuit.

Load Sharing -1

- Load sharing, sometimes called load balancing, allows two or more interfaces or paths to share traffic load.
- In WAN environments, you can facilitate load sharing by configuring channel aggregation. Channel aggregation means that a router can automatically bring up multiple channels as bandwidth requirements increase.
- The Multilink Point-to-Point Protocol (MPPP) is an Internet Engineering Task Force (IETF) standard for channel aggregation. MPPP ensures that packets arrive in sequence at the receiving router.
- To accomplish this, data is encapsulated within the Point-to-Point Protocol (PPP), and datagrams are given a sequence number. At the receiving router, PPP uses the sequence number to re-create the original data stream. Multiple channels appear as one logical link to upper-layer protocols.

Load Sharing -2

- Most vendors' implementations of IP routing protocols support load sharing across parallel links that have equal cost. (Cost values are used by routing protocols to determine the most favorable path to a destination.
- Depending on the routing protocol, cost can be based on hop count, bandwidth, delay, or other factors.) With EIGRP, Cisco supports load sharing even when the paths do not have the same cost.
- Using a feature called variance, EIGRP can load share across paths that do not have the same cost. Cisco supports load sharing across six parallel paths.