Introduction to Networking

Cisco | Networking Academy®
Mind Wide Open™

Objectives

- Describe how networks impact our daily lives.
- Describe the role of data networking in the human network.
- Identify the key components of any data network.
- Identify the opportunities and challenges posed by converged networks.
- Describe the characteristics of network architectures: fault tolerance, scalability, quality of service and security.
- Install and use IRC clients and a Wiki server.

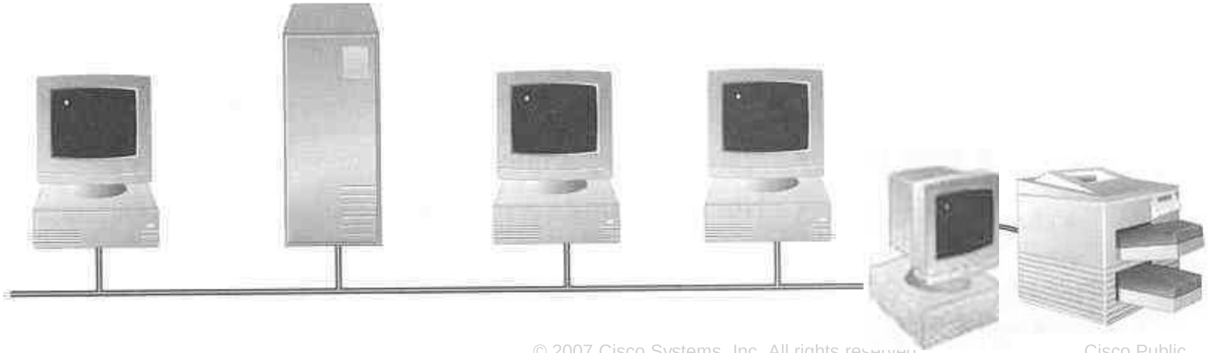
Network Definition

- **A network** can be defined as two or more computers connected together in such a way that they can share resources.
- The purpose of a network is to share resources:

  A file A folder A printer A disk drive

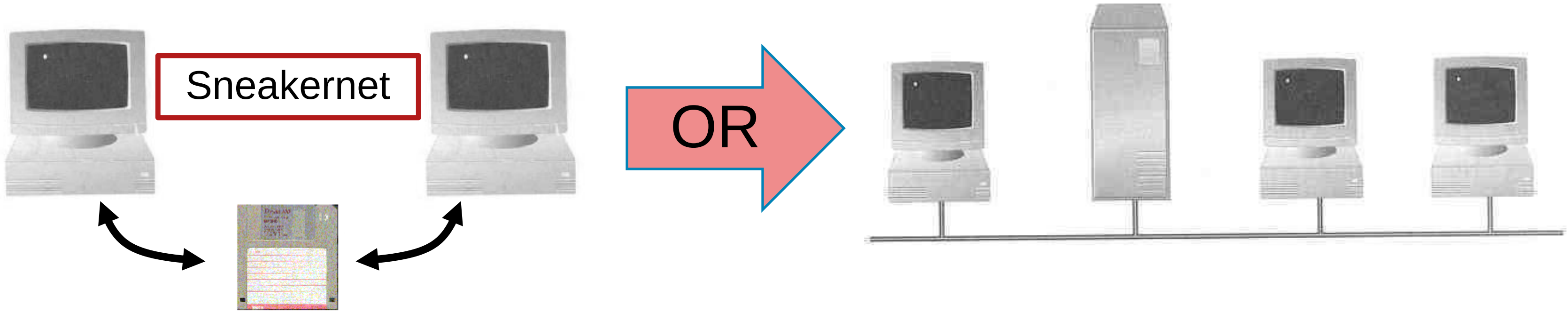
  Or just about anything else that exists on a computer.

- **A network** is simply a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate.
- **Networking** is the term that describes the processes involved in designing, implementing, upgrading, managing and otherwise working with networks and network technologies.



Why Networking?

- **Do you prefer these?**



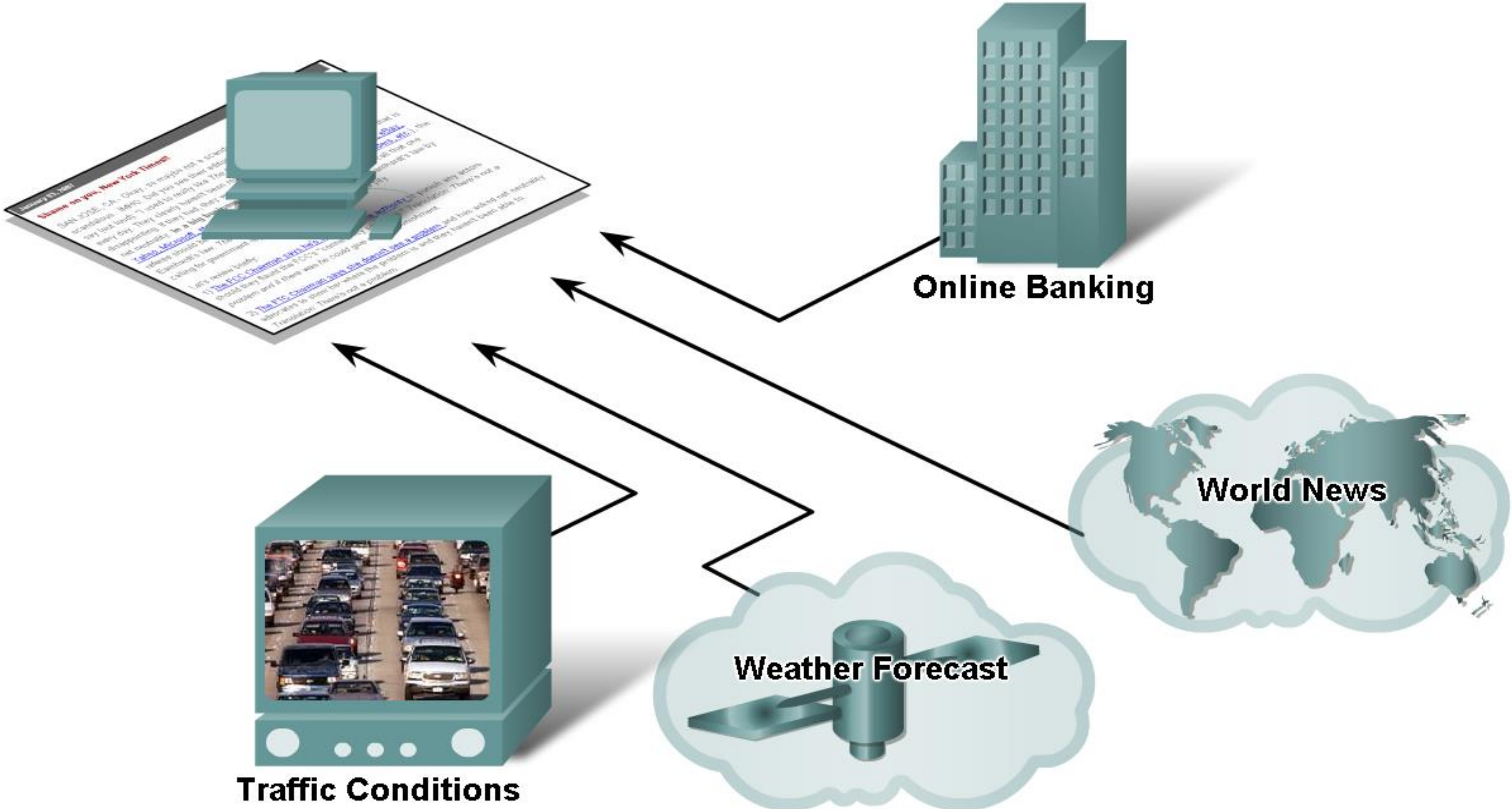
❑ Sharing data through the use of ***storage media*** is not an efficient or cost-effective manner in which to operate businesses.

❑ Businesses needed a solution that would successfully address the following three problems:

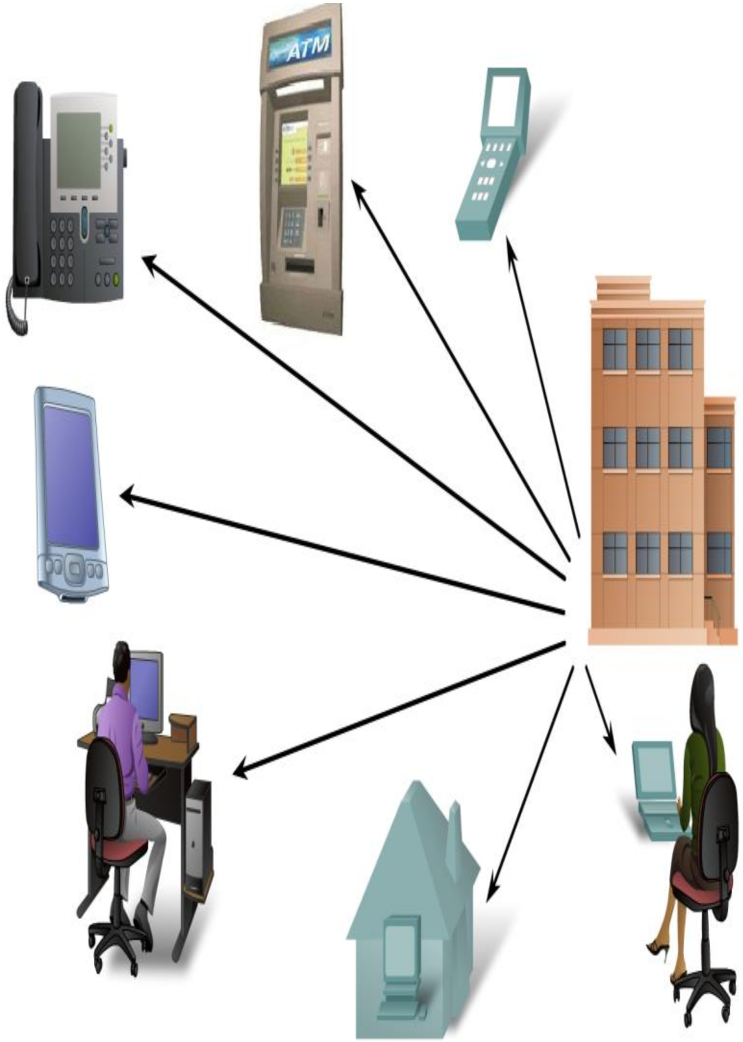
- How to avoid duplication of equipment and resources
- How to communicate efficiently
- How to set up and manage a network

❑ Businesses realized that networking technology could increase productivity while saving money.

How Networks Impact Daily Life



How Networks Impact Daily Life



- Post and share your photographs, home videos, and experiences with friends or with the world.
- Access and submit school work.
- Communicate with friends, family, and peers using email, instant messaging, or Internet phone calls.
- Watch videos, movies, or television episodes on demand.
- Play online games with friends.
- Decide what to wear using online current weather conditions.
- Find the least congested route to your destination, displaying weather and traffic video from webcams.
- Check your bank balance and pay bills electronically.

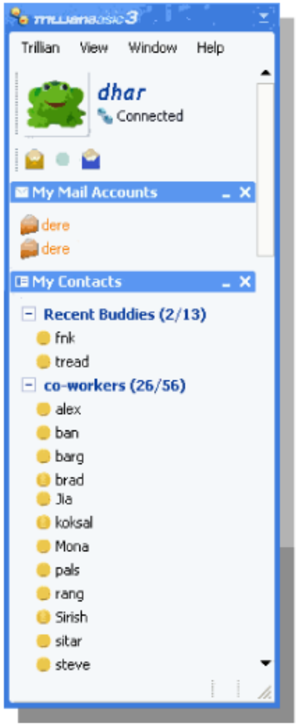
Global communities

- Advancements in networking technologies are perhaps the most significant change agents in the world today.
- They are helping to create a world in which national borders, geographic distances, and physical limitations become less relevant, and present ever-diminishing obstacles.
- The Internet has changed the manner in which social, commercial, political, and personal interactions occur.
- The immediate nature of communications over the Internet encourages the creation of global communities.
- Global communities allow for social interaction that is independent of location or time zone.
- The creation of online communities for the exchange of ideas and information has the potential to increase productivity opportunities across the globe.
- Cisco refers to this as the human network. The human network centers on the impact of the Internet and networks on people and businesses.

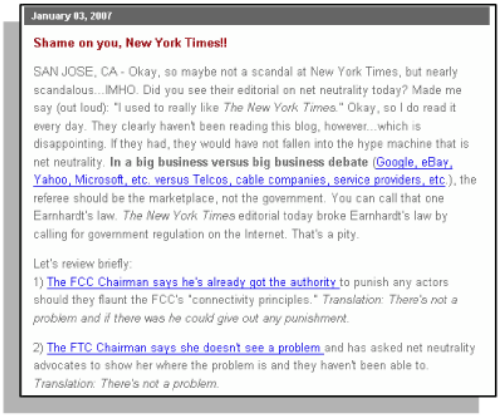
How Networks Impact Our Communications

- IM - Instant Messaging: Internet Relay Cha (IRC)
- Blogs (Weblogs): Personal opinions on any conceivable subject.
- Podcasting: Sharing recordings with a wide audience (Apple iPods)
- Wikis: A collaboration tool. Gives people the opportunity to work together on shared documents.
- Social Media – Social media consists of interactive websites where people and communities create and share user-generated content with friends, family, peers, and the world.
- Peer-to-Peer (P2P) File Sharing

Instant Messaging



Weblog



January 03, 2007

Shame on you, New York Times!!

SAN JOSE, CA - Okay, so maybe not a scandal at New York Times, but nearly scandalous....IMHO. Did you see their editorial on net neutrality today? Made me say (out loud): "I used to really like *The New York Times*." Okay, so I do read it every day. They clearly haven't been reading this blog, however....which is disappointing. If they had, they would have not fallen into the hype machine that is net neutrality. **In a big business versus big business debate** (Google, eBay, Yahoo, Microsoft, etc. versus Telcos, cable companies, service providers, etc.), the referee should be the marketplace, not the government. You can call that one Earnhardt's law. *The New York Times* editorial today broke Earnhardt's law by calling for government regulation on the Internet. That's a pity.

Let's review briefly:

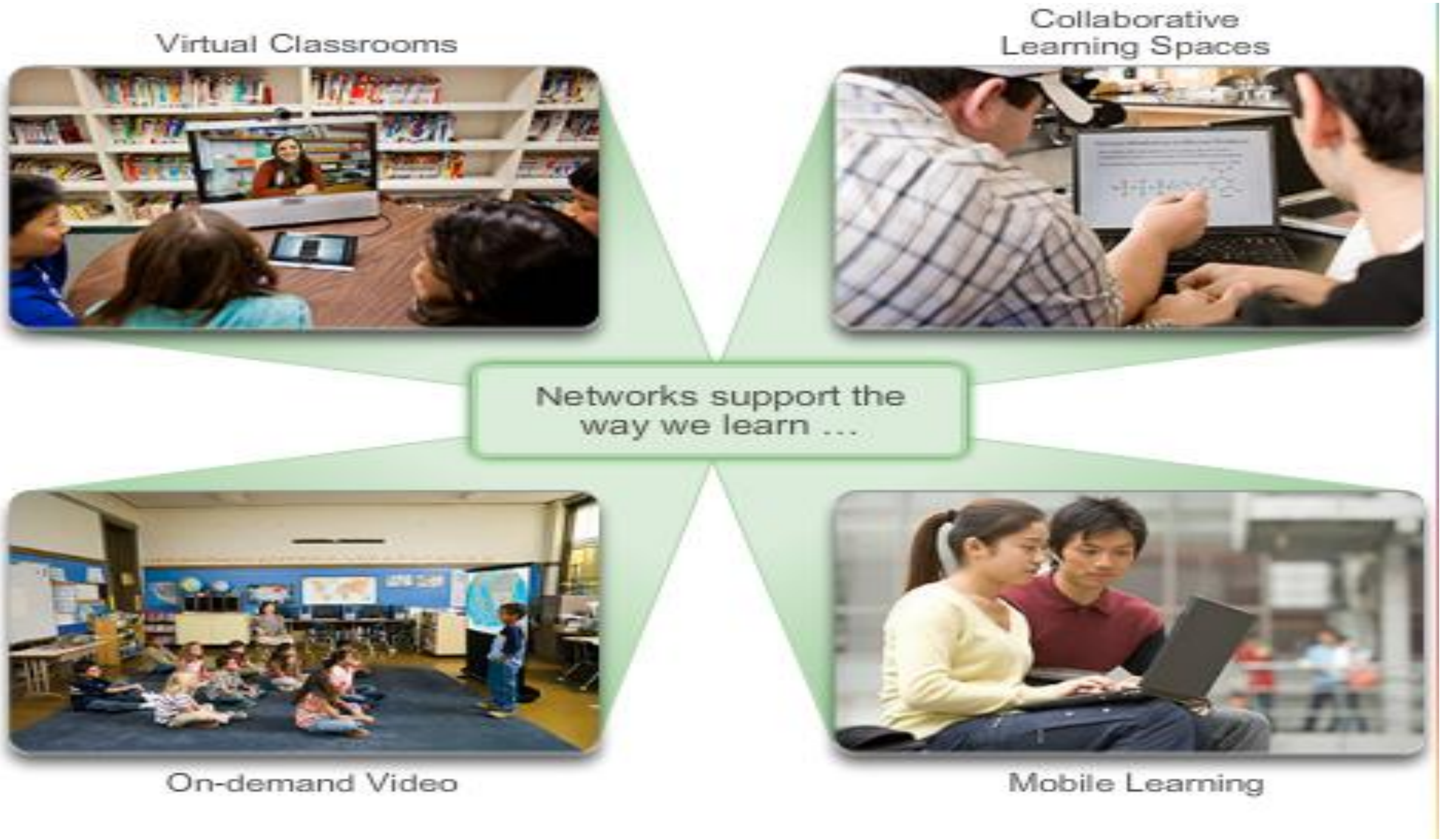
1) The FCC Chairman says he's already got the authority to punish any actors should they flaunt the FCC's "connectivity principles." *Translation: There's not a problem and if there was he could give out any punishment.*

2) The FTC Chairman says she doesn't see a problem and has asked net neutrality advocates to show her where the problem is and they haven't been able to. *Translation: There's not a problem.*

Podcasting

How Networks Impact Daily Life

- teaching and learning

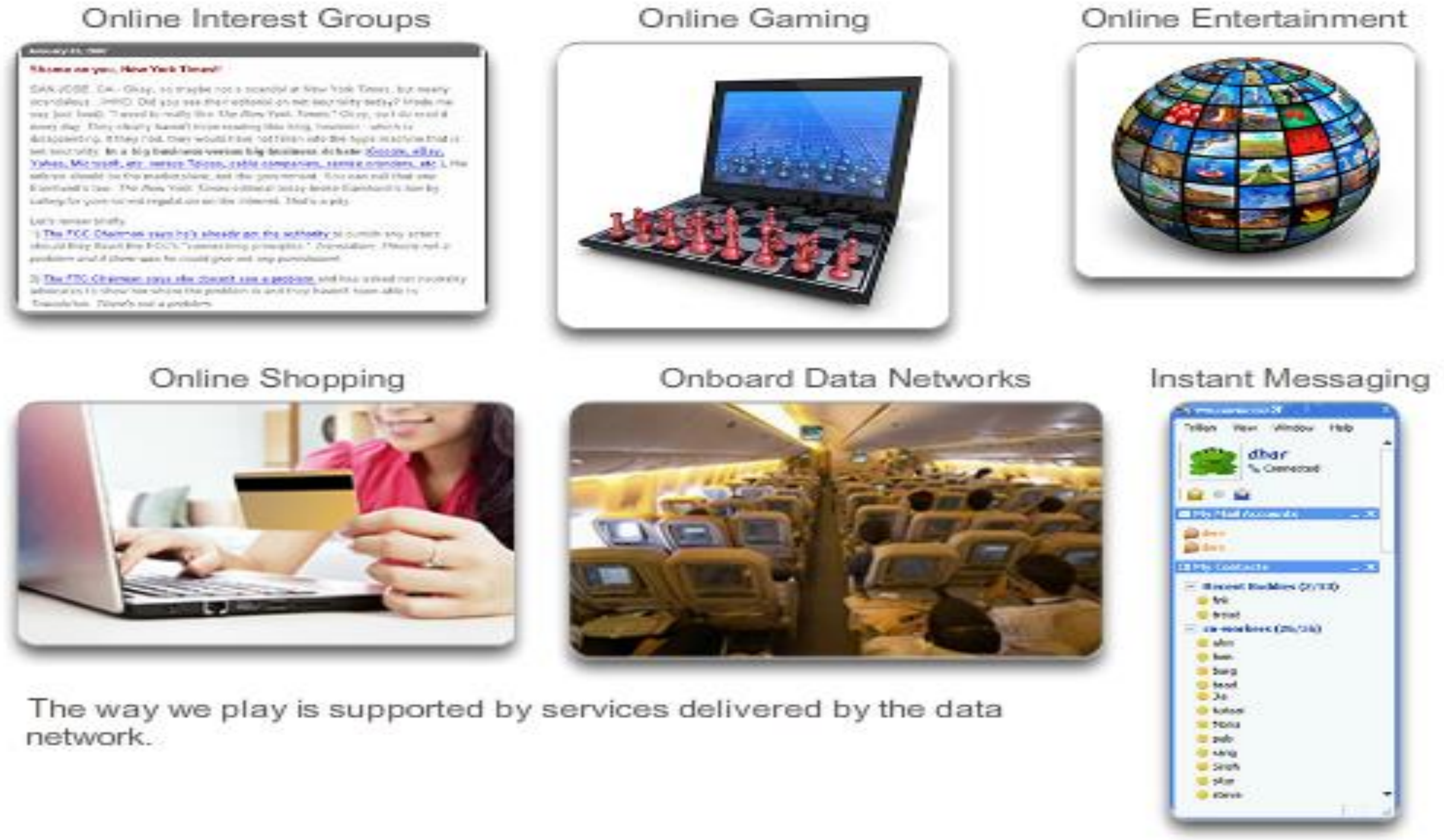

Virtual Classrooms
Collaborative Learning Spaces
Networks support the way we learn …
On-demand Video
Mobile Learning

How Networks Impact Daily Life

- Work

How Networks Impact Daily Life

- Play



Online Interest Groups

Online Gaming

Online Entertainment

Online Shopping

Onboard Data Networks

Instant Messaging

The way we play is supported by services delivered by the data network.

Communications – What is it?

- Communications can take many forms and occurs in many different environments.

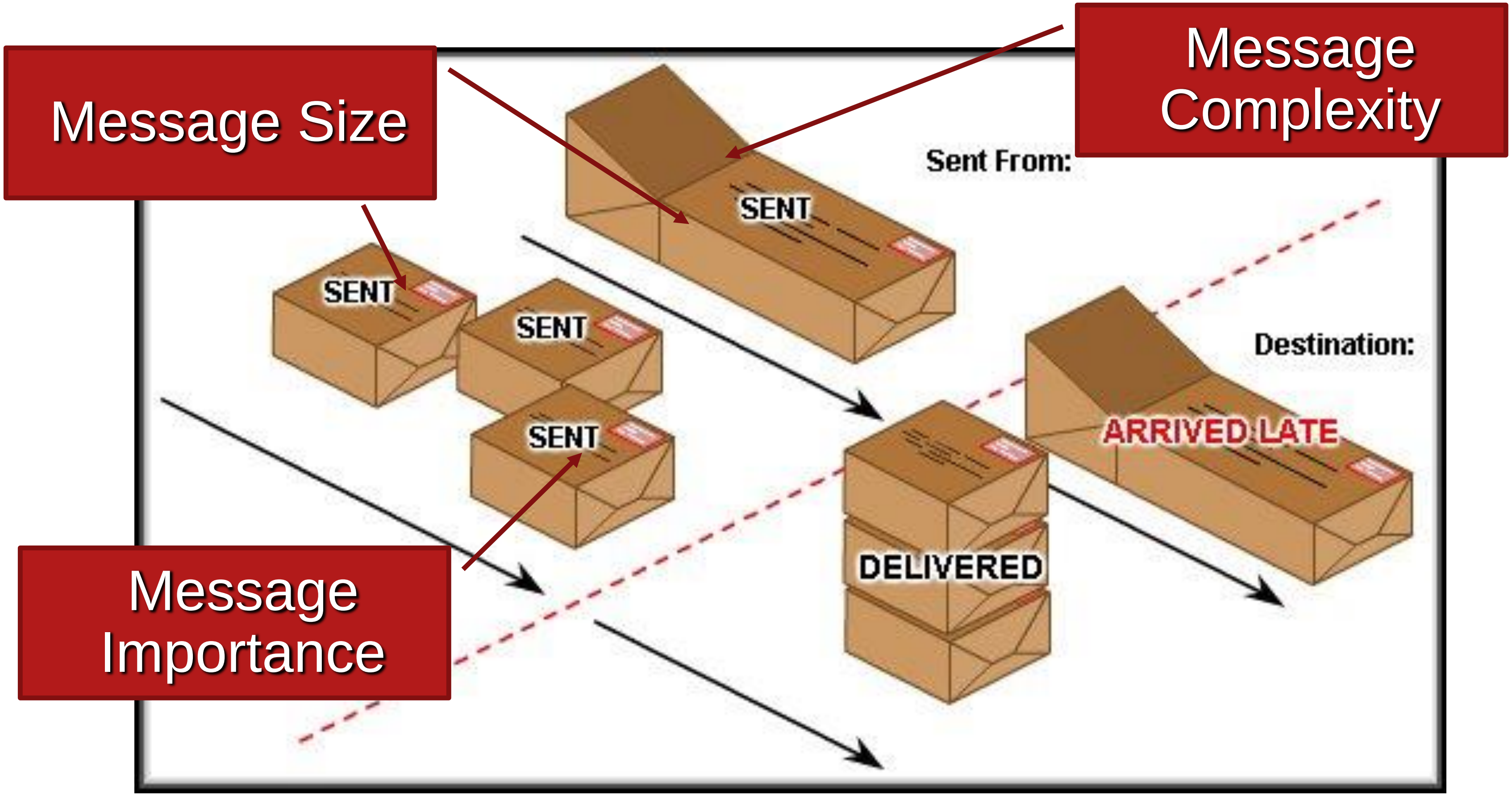
- We establish rules, or protocols, for communicating with each other:
  - Identify the sender and receiver.
  - Agree on the method.
  - Common language.
  - Speed and delivery of the message.
  - Confirmation that the message was received.

- Communications between individuals is successful if the meaning of the received message is the same as the meaning of the message that was sent.

Communications - Quality

- For data networks, we use the same basic criteria to judge successful communication.
- However, there are external factors that can affect the message.
    - The quality of the pathway between the sender and the recipient.
    - The number of times the message has to change form or be redirected or re-addressed.
    - The number of other messages being transmitted simultaneously on the communication network.
    - The amount of time allotted for successful communication.

- There are also internal factors that can affect successful communication.


Message Size

Message Complexity

Message Importance

❑ It is also more difficult to deliver a large, bulky package successfully and without damage than it is to deliver several smaller packages.

Classification of Networks

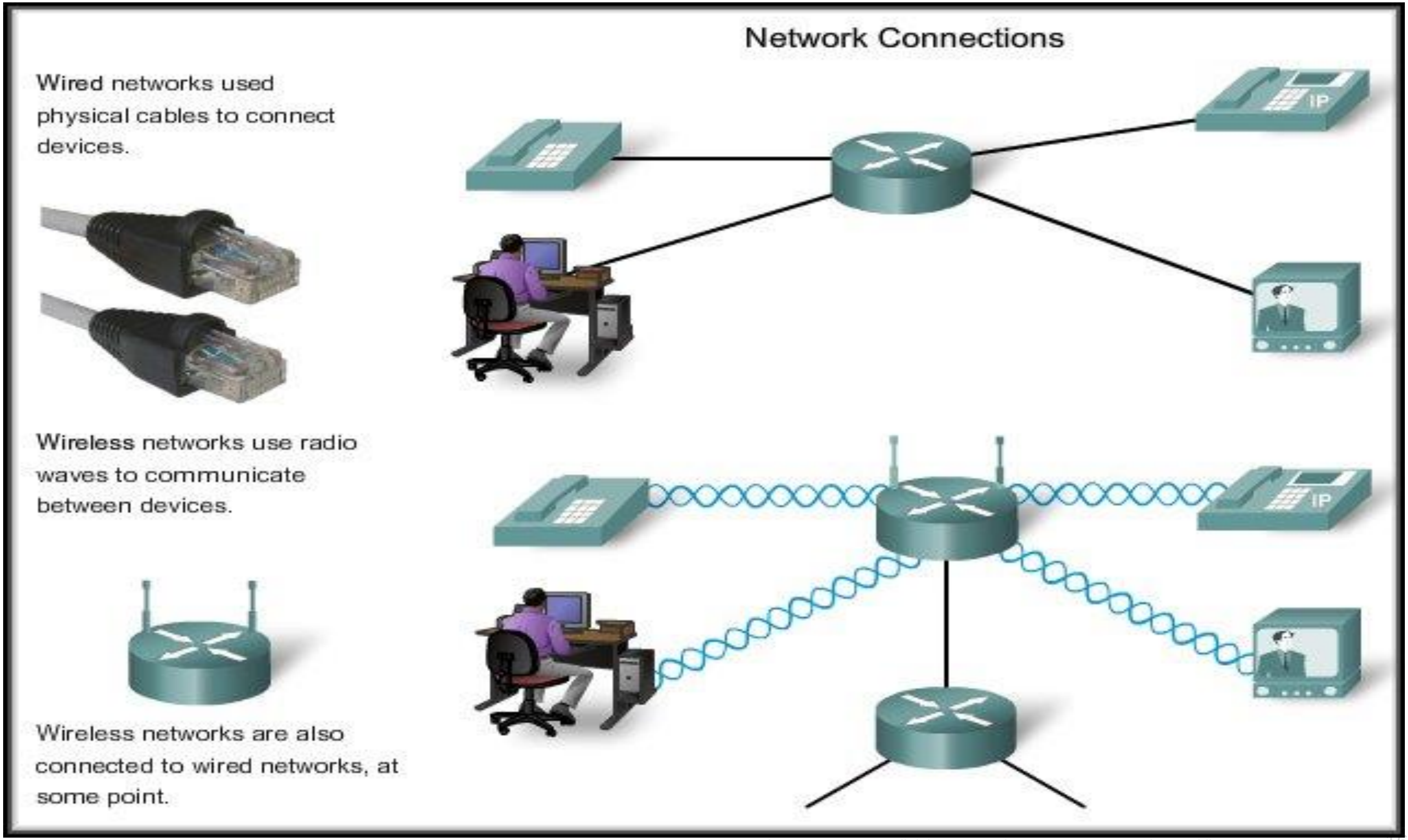
❑ Depending on one’s perspective, we can classify networks in different ways

- Based on transmission media: Wired (UTP, coaxial cables, fiber-optic cables) and Wireless.
- Based on network size: LAN and WAN (and MAN).
- Based on management method: Peer-to-peer and Client/Server.
- Based on topology (connectivity): Bus, Star, Ring …

  :

  :

Classification based on Media



Network Connections

Wired networks used physical cables to connect devices.

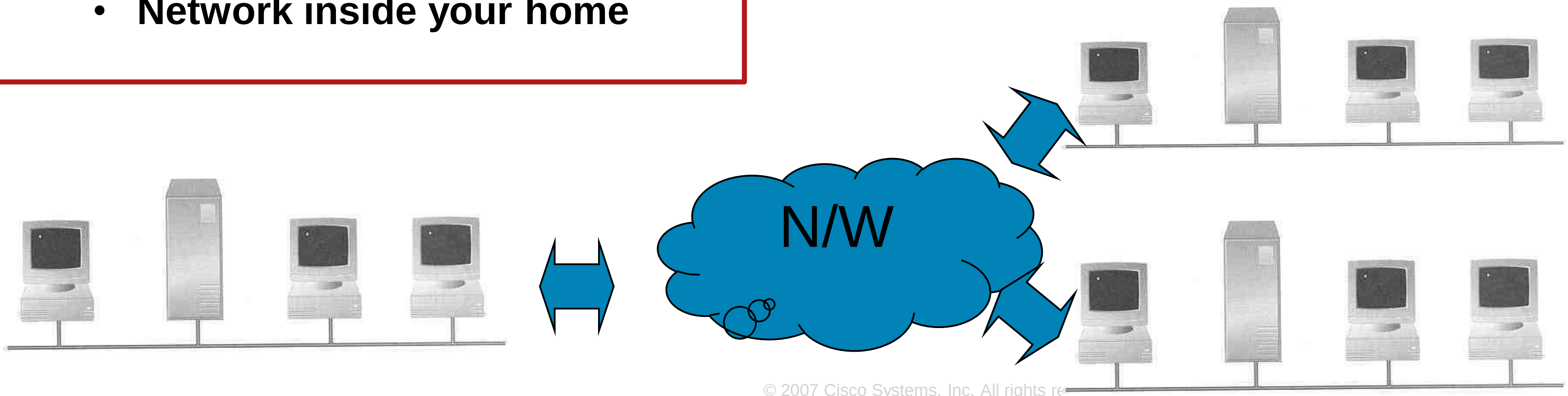
Wireless networks use radio waves to communicate between devices.

Wireless networks are also connected to wired networks, at some point.

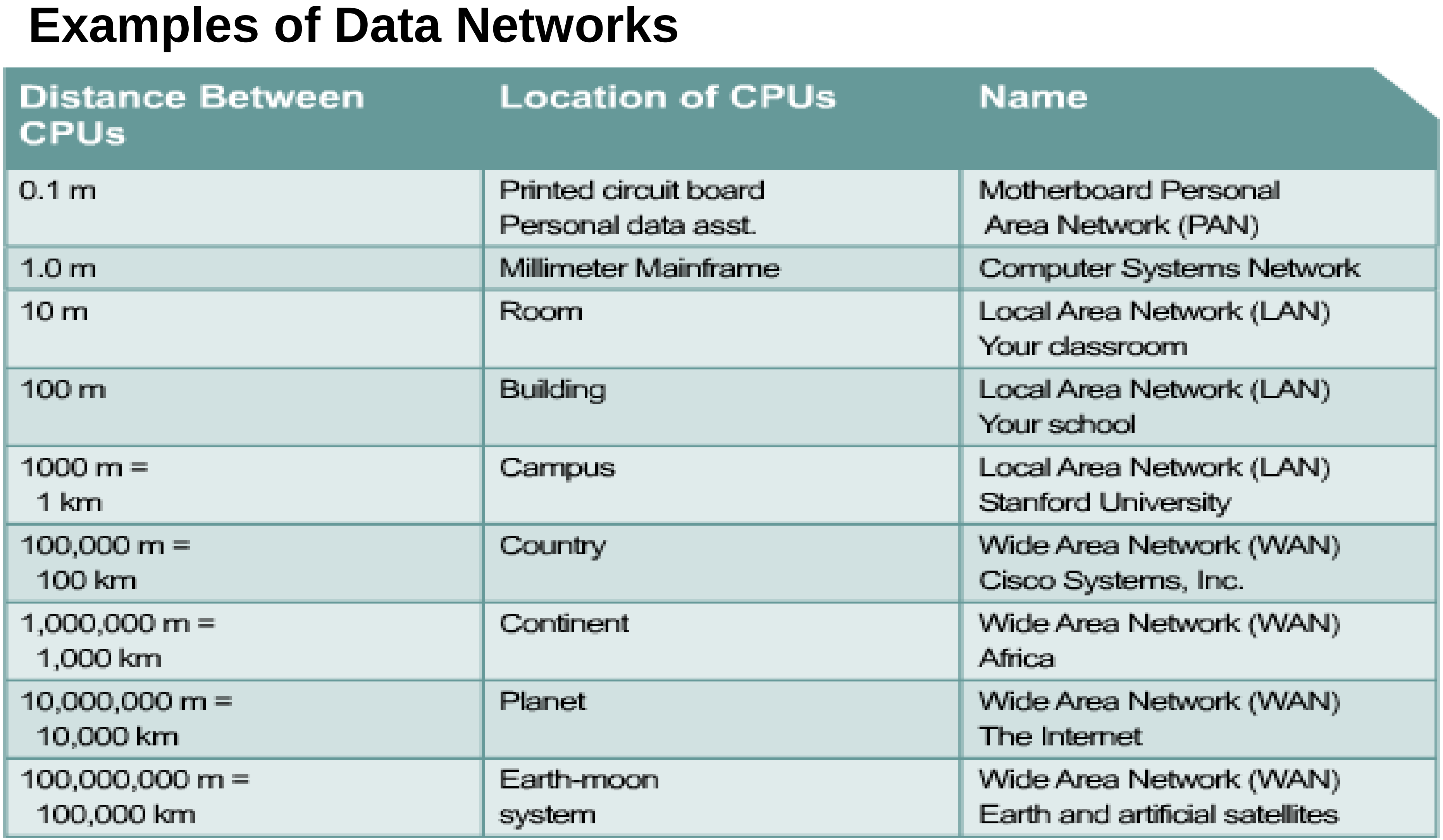
• Classification based on Network Size (I)

- Local Area Network (LAN)
  - Small network, short distance
    - A room, a floor, a building
    - Limited by no. of computers and distance covered
    - Usually one kind of technology throughout the LAN
    - Serve a department within an organization
  - Examples:
    - Network inside the Student Computer Room
    - Network inside CF502
    - Network inside your home

- Wide Area Network (WAN)
  - A network that uses long-range telecommunication links to connect 2 or more LANs/computers housed in different places far apart.
    - Towns, states, countries
  - Examples:
    - Network of our Campus
    - Internet



- **Classification based on Network Size** (II)

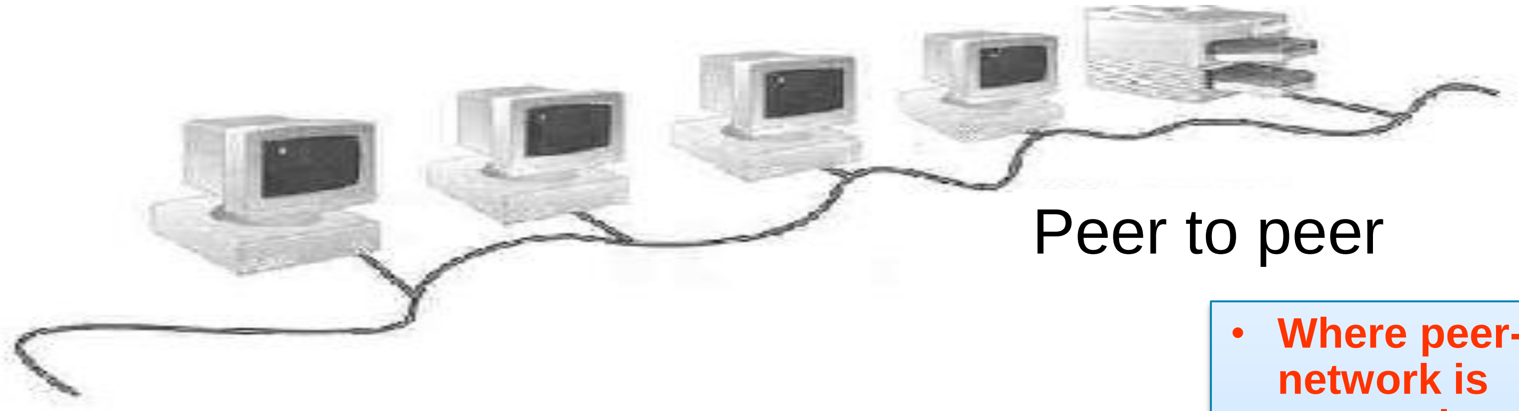


Examples of Data Networks

Distance Between CPUs	Location of CPUs	Name
0.1 m	Printed circuit board Personal data asst.	Motherboard Personal Area Network (PAN)
1.0 m	Millimeter Mainframe	Computer Systems Network
10 m	Room	Local Area Network (LAN) Your classroom
100 m	Building	Local Area Network (LAN) Your school
1000 m = 1 km	Campus	Local Area Network (LAN) Stanford University
100,000 m = 100 km	Country	Wide Area Network (WAN) Cisco Systems, Inc.
1,000,000 m = 1,000 km	Continent	Wide Area Network (WAN) Africa
10,000,000 m = 10,000 km	Planet	Wide Area Network (WAN) The Internet
100,000,000 m = 100,000 km	Earth-moon system	Wide Area Network (WAN) Earth and artificial satellites

Classification based on Management Method

Peer to Peer Networks and Client/Server Networks



- Peer-to-peer network is also called workgroup
- No hierarchy among computers ⇒ all are equal
- No administrator responsible for the network

- Advantages of peer-to-peer networks:
  - Low cost
  - Simple to configure
  - User has full accessibility of the computer

- Disadvantages of peer-to-peer networks:
  - May have duplication in resources
  - Difficult to uphold security policy
  - Difficult to handle uneven loading

- Where peer-to-peer network is appropriate:
  - 10 or less users
  - No specialized services required
  - Security is not an issue
  - Only limited growth in the foreseeable future

Client/Server Networks

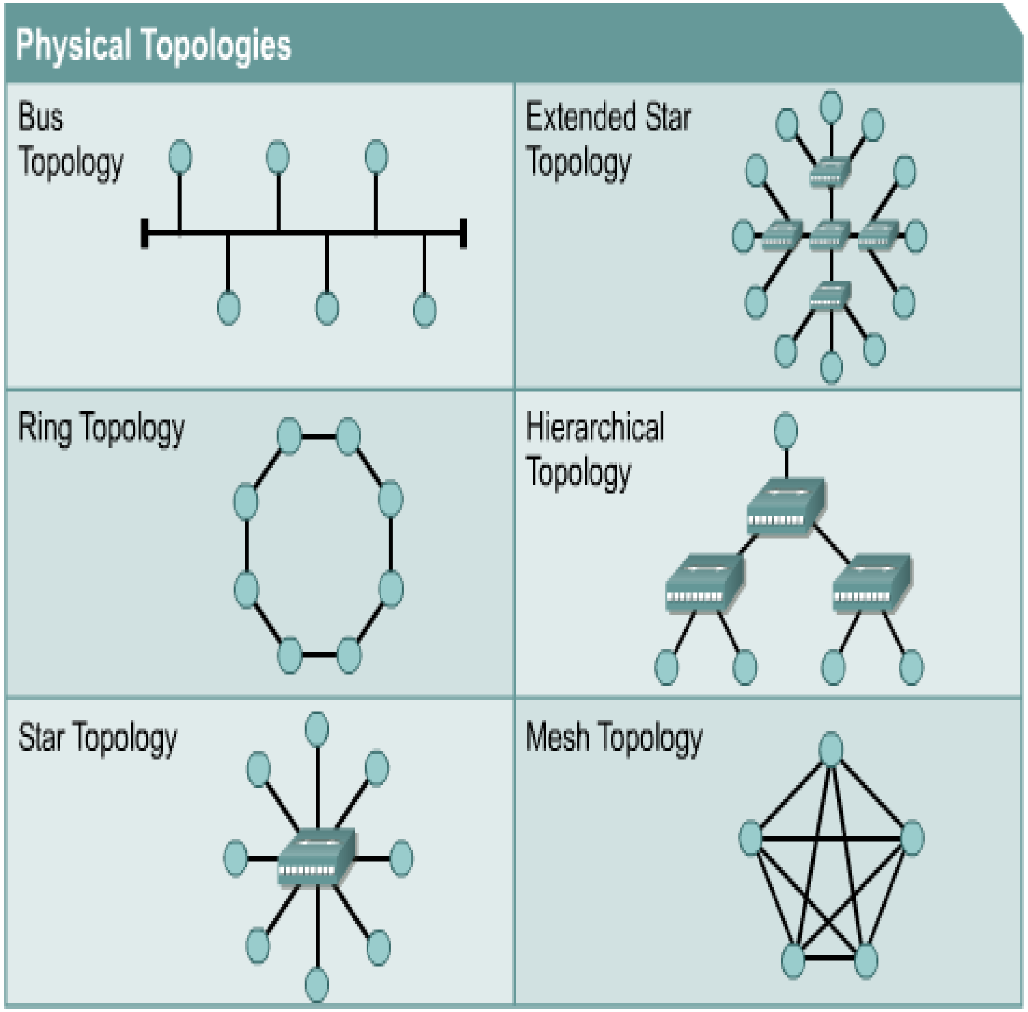
- Network **Clients** (**Workstation**)
  - Computers that request network resources or services
- Network **Servers**
  - Computers that manage and provide network resources and services to clients
    - Usually have more processing power, memory and hard disk space than clients
    - Run Network Operating System that can manage not only data, but also users, groups, security, and applications on the network
    - Servers often have a more stringent requirement on its performance and reliability

- Advantages of client/server networks
  - Facilitate resource sharing – centrally administrate and control
  - Facilitate system backup and improve fault tolerance
  - Enhance security – only administrator can have access to Server
  - Support more users – difficult to achieve with peer-to-peer networks

- Disadvantages of client/server networks
  - High cost for Servers
  - Need expert to configure the network
  - Introduce a single point of failure to the system

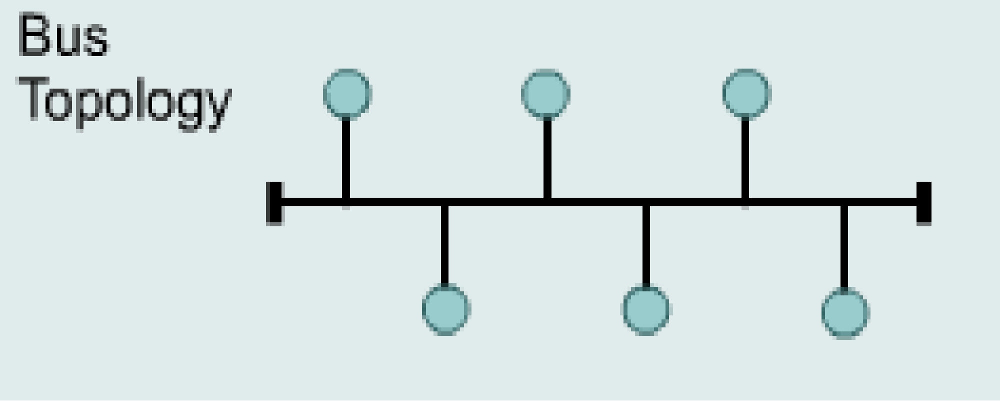
Classification based on Network Topology

- Network topology defines the structure of the network.
- One part of the topology definition is the ***physical topology***, which is the actual layout of the wire or media.
- The other part is the ***logical topology***, which defines how the media is accessed by the hosts for sending data.



Classification based on Network Topology

- Network topology defines the structure of the network.
- One part of the topology definition is the ***physical topology***, which is the actual layout of the wire or media.
- The other part is the ***logical topology***, which defines how the media is accessed by the hosts for sending data.



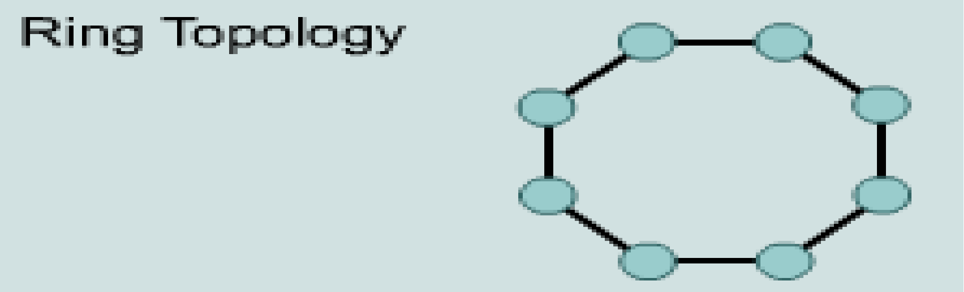
- **Bus Topology**
  - **Simple and low-cost**
  - **A single cable called a trunk (backbone, segment)**
  - **Only one computer can send messages at a time**
  - **Passive topology - computer only listen for, not regenerate data**

Classification based on Network Topology

- Network topology defines the structure of the network.

- One part of the topology definition is the ***physical topology***, which is the actual layout of the wire or media.

- The other part is the ***logical topology***, which defines how the media is accessed by the hosts for sending data.



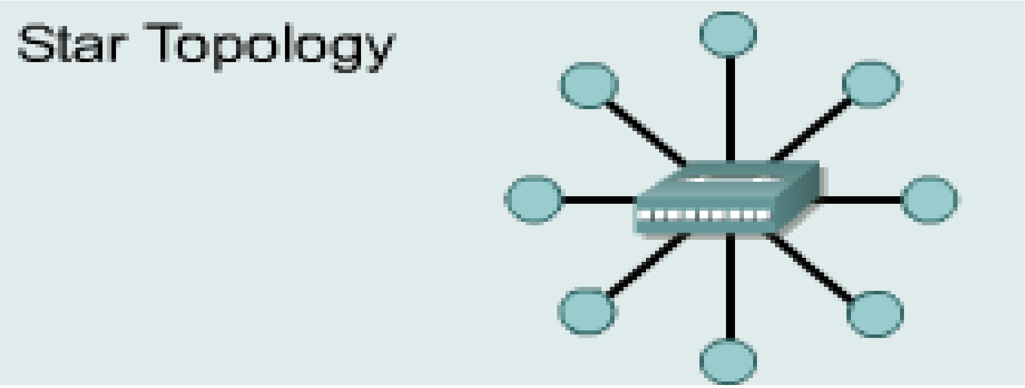
- **Ring Topology**
  - **Every computer serves as a repeater to boost signals**
  - **Typical way to send data:**
    - **Token passing**
      - **only the computer who gets the token can send data**
  - **Disadvantages**
    - **Difficult to add computers**
    - **More expensive**
    - **If one computer fails, whole network fails**

Classification based on Network Topology

- Network topology defines the structure of the network.

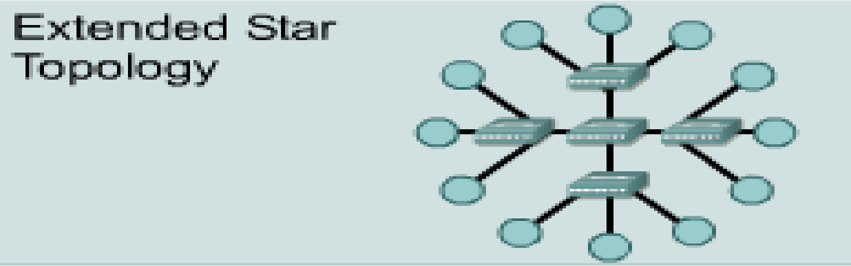
- One part of the topology definition is the ***physical topology***, which is the actual layout of the wire or media.

- The other part is the ***logical topology***, which defines how the media is accessed by the hosts for sending data.



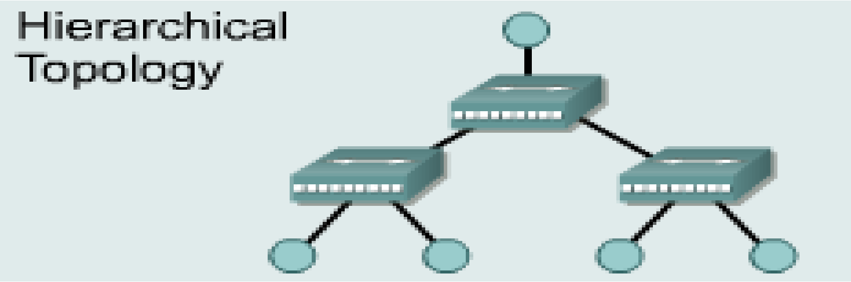
- **Star Topology**
  - **Each computer has a cable connected to a single point**
  - **More cabling, hence higher cost**
  - **All signals transmission through the hub; if down, entire network down**
  - **Depending on the intelligence of hub, two or more computers may send message at the same time**

Classification based on Network Topology



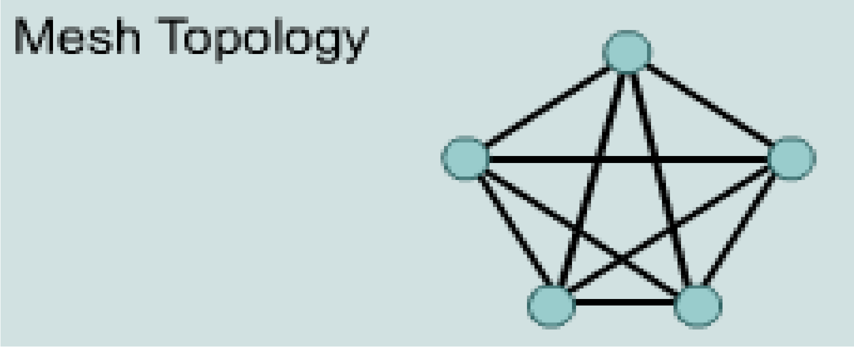
An extended star topology links individual stars together by connecting the hubs and/or switches.

This topology can extend the scope and coverage of the network.



A hierarchical topology is similar to an extended star.

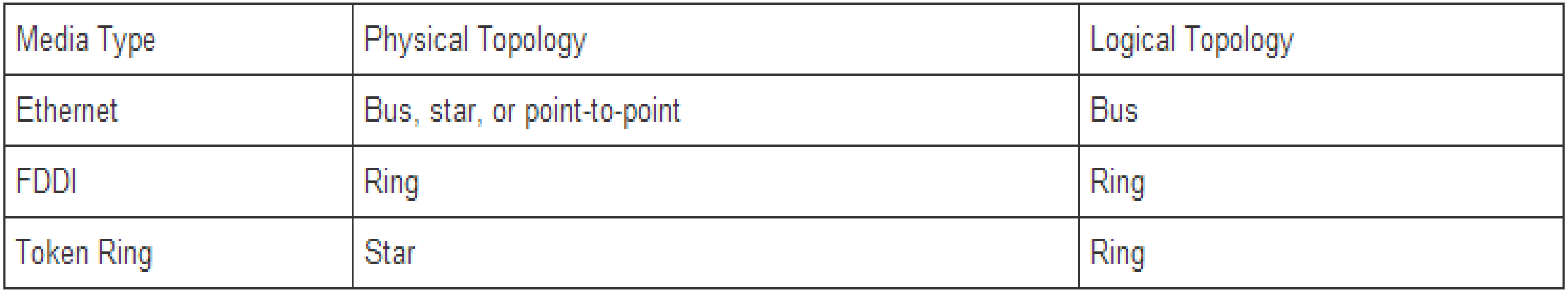
However, instead of linking the hubs and/or switches together, the system is linked to a computer that controls
the traffic on the topology.



A mesh topology is implemented to provide as much protection as possible from interruption of service.
Each host has its own connections to all other hosts. Although the Internet has multiple paths to any one location, it does not adopt the full mesh topology.

Logical Topology

- A logical topology describes how components communicate across the physical topology.
- The physical and logical topologies are independent of each other.



Media Type	Physical Topology	Logical Topology
Ethernet	Bus, star, or point-to-point	Bus
FDDI	Ring	Ring
Token Ring	Star	Ring

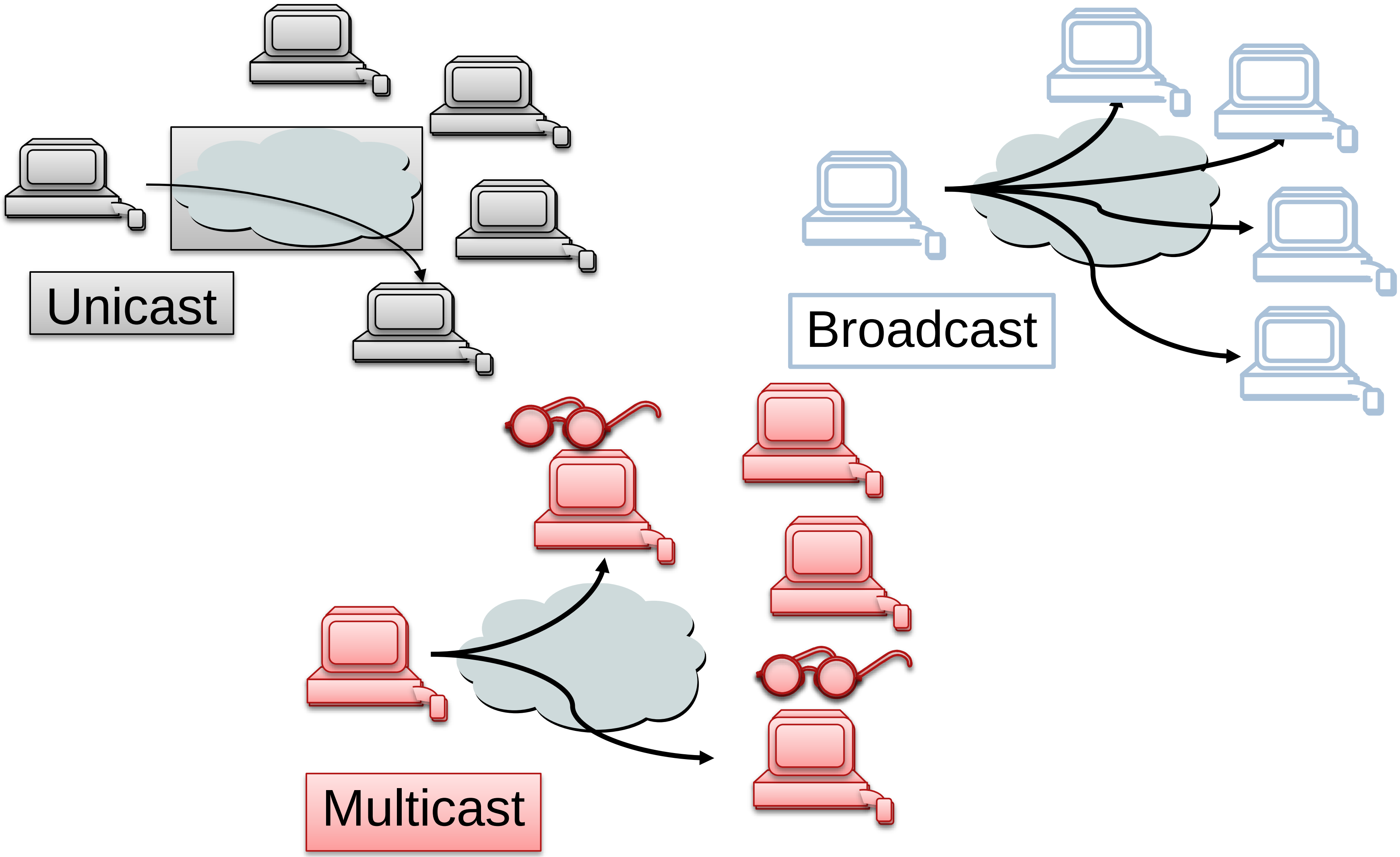
Token Passing Topology

•Token passing controls network access by passing an electronic token sequentially to each host.

•When a host receives the token, that host can send data on the network. If the host has no data to send, it passes the token to the next host and the process repeats itself.

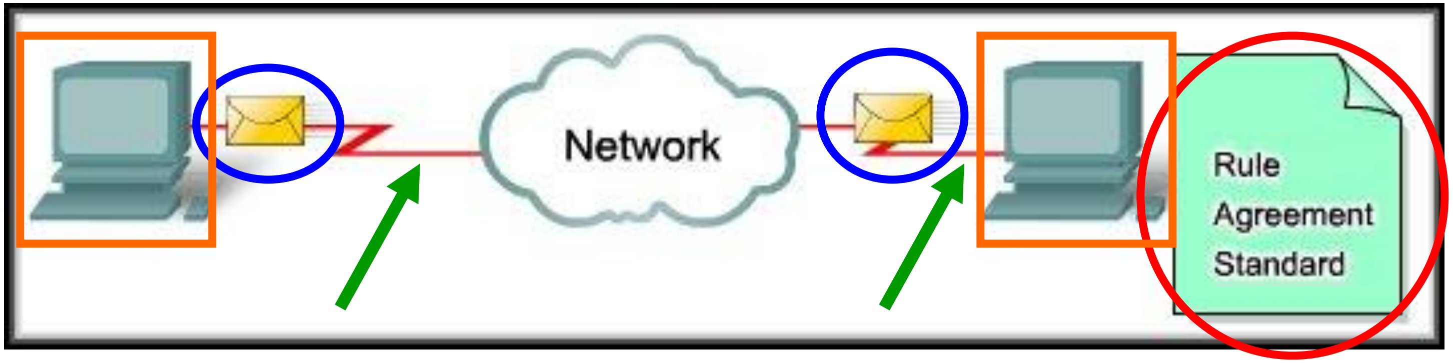
•Two examples of networks that use token passing are ***Token Ring*** and ***Fiber Distributed Data Interface (FDDI).*** .

Network Transmission



Data Networking Role, Components, and Challenges

❑ All networks have **4** basic elements in common:



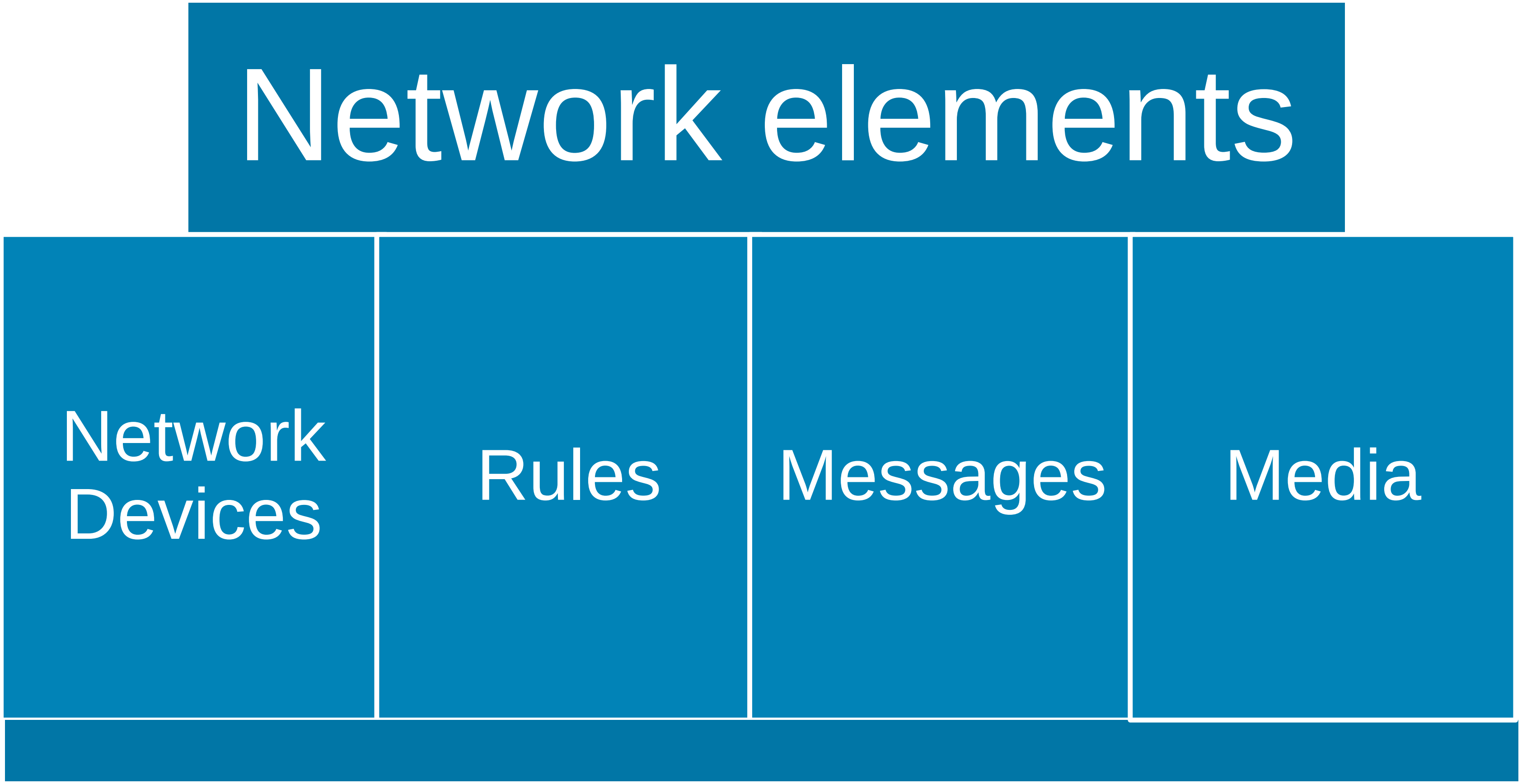
Rules (protocols) to govern the handling of the message.

Messages that travel from one device to another.

Medium that is used to interconnect devices and can transport the messages from one device to another.

Devices on the network that exchange messages.

Network Components (Elements)



Network elements

Network Devices

Rules

Messages

Media

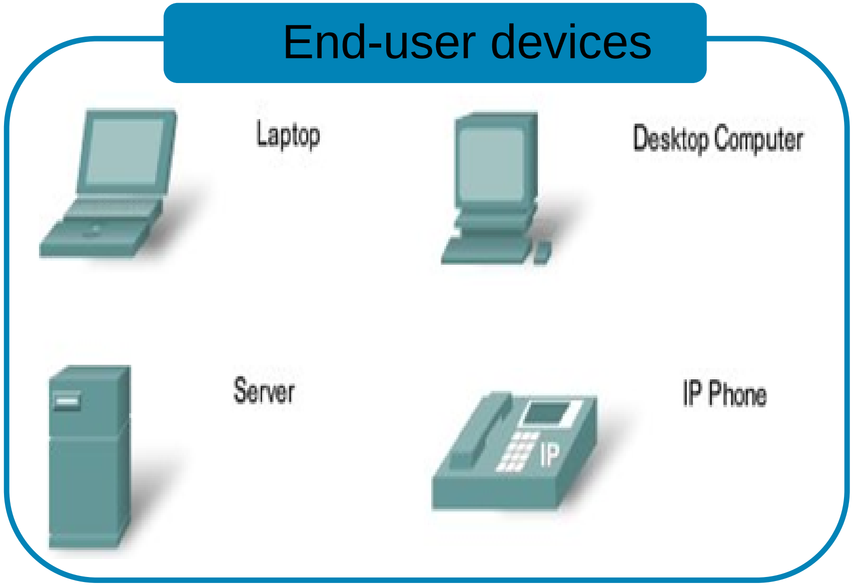
Network Devices

❑ Equipment that connects directly to a network segment is referred to as a device.

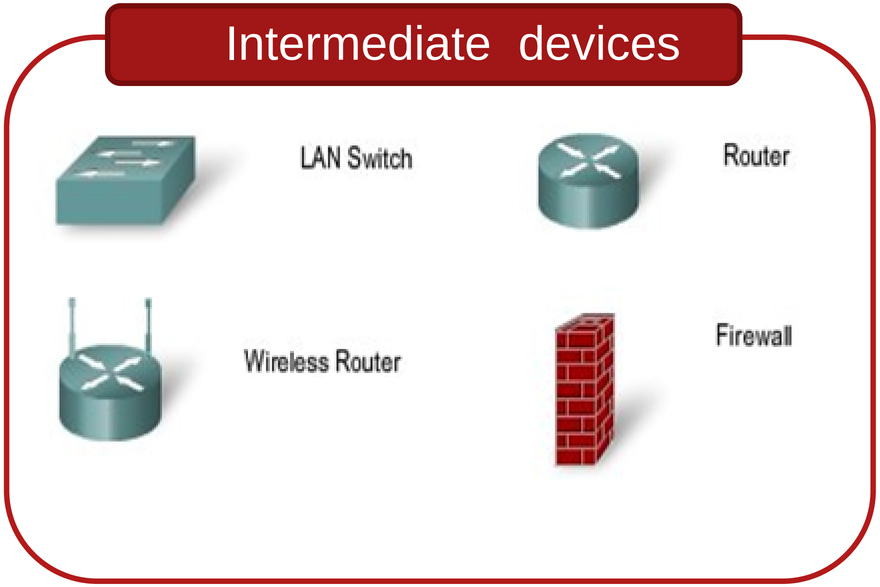
❑ These devices are broken up into two classifications:

  ❑ end-user devices

  ❑ Intermediate network devices

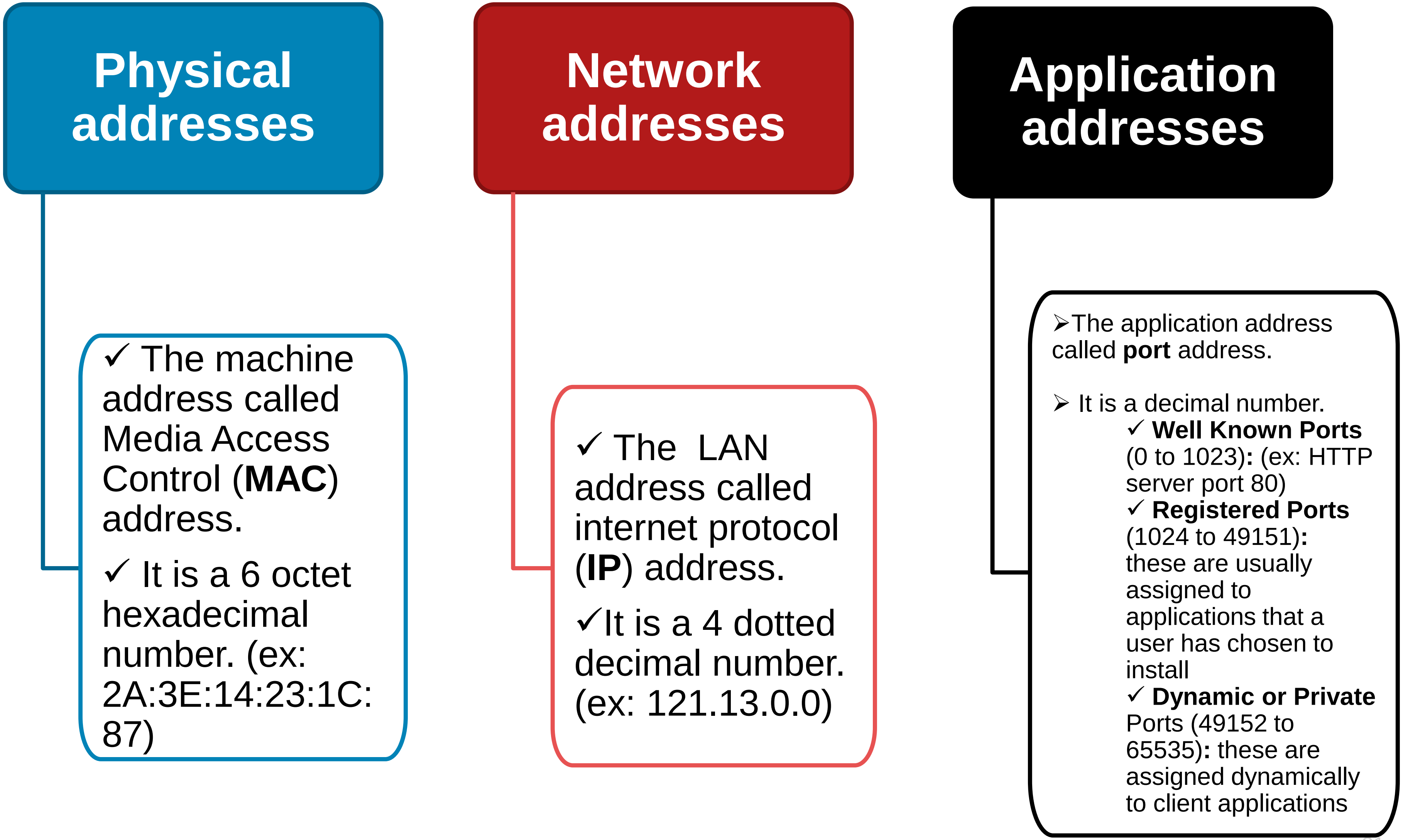


End-user devices



Intermediate devices

Network Devices



Physical addresses

- ✓ The machine address called Media Access Control (**MAC**) address.
- ✓ It is a 6 octet hexadecimal number. (ex: 2A:3E:14:23:1C:87)

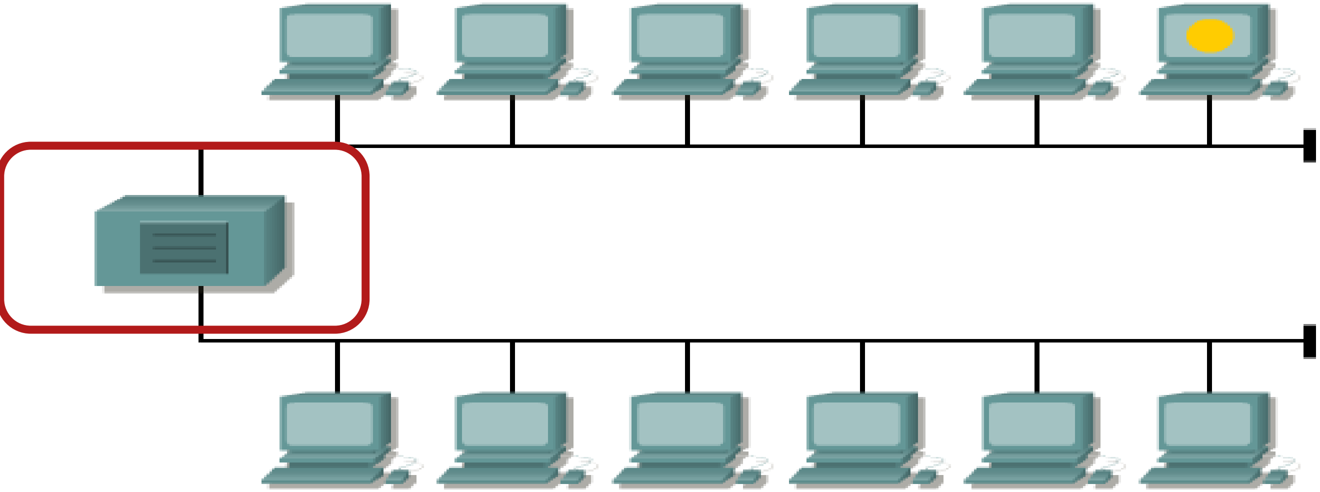
Network addresses

- ✓ The LAN address called internet protocol (**IP**) address.
- ✓It is a 4 dotted decimal number. (ex: 121.13.0.0)

Application addresses

- ➢The application address called **port** address.
- ➢ It is a decimal number.
  - ✓ **Well Known Ports** (0 to 1023)**:** (ex: HTTP server port 80)
  - ✓ **Registered Ports** (1024 to 49151)**:** these are usually assigned to applications that a user has chosen to install
  - ✓ **Dynamic or Private** Ports (49152 to 65535)**:** these are assigned dynamically to client applications

Repeater



•A repeater is a network device used to regenerate a signal.

•Repeaters regenerate analog or digital signals distorted by transmission loss due to attenuation.

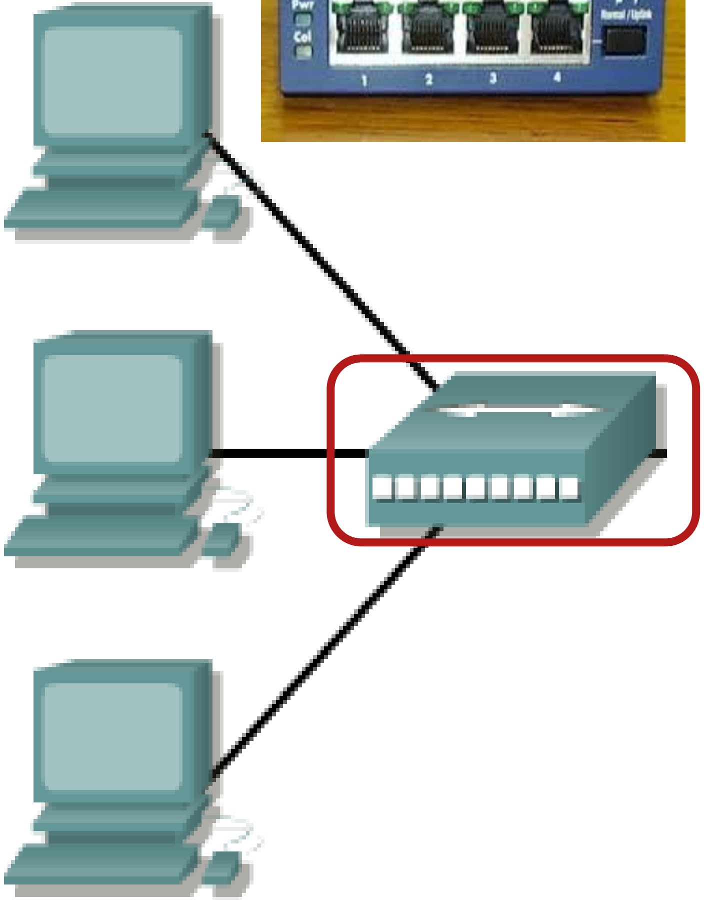
•A repeater does not perform intelligent routing like a bridge or router.

Hub

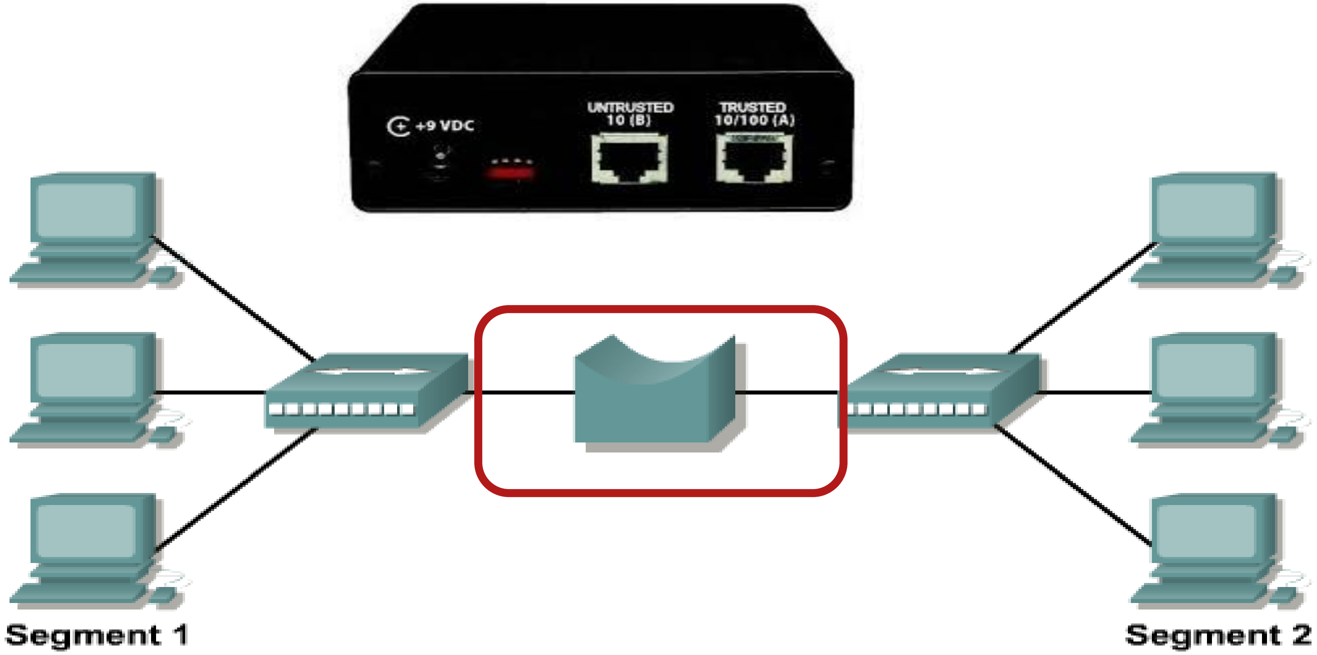
- Hubs concentrate connections. In other words, they take a group of hosts and allow the network to see them as a single unit.

- This is done passively, without any other effect on the data transmission.

- Active hubs not only concentrate hosts, but they also regenerate signals.



Bridge



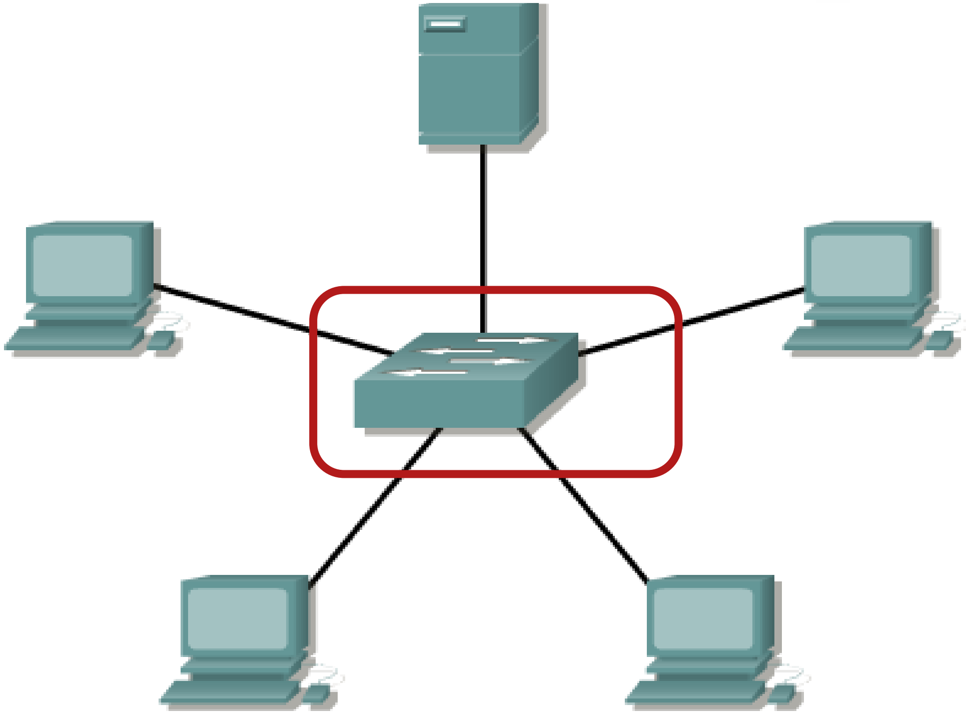
•Bridges convert network transmission data formats as well as perform basic data transmission management.
•Bridges, as the name implies, provide connections between LANs.
• Not only do bridges connect LANs, but they also perform a check on the data to determine whether it should cross the bridge or not.
•This makes each part of the network more efficient.

Switch

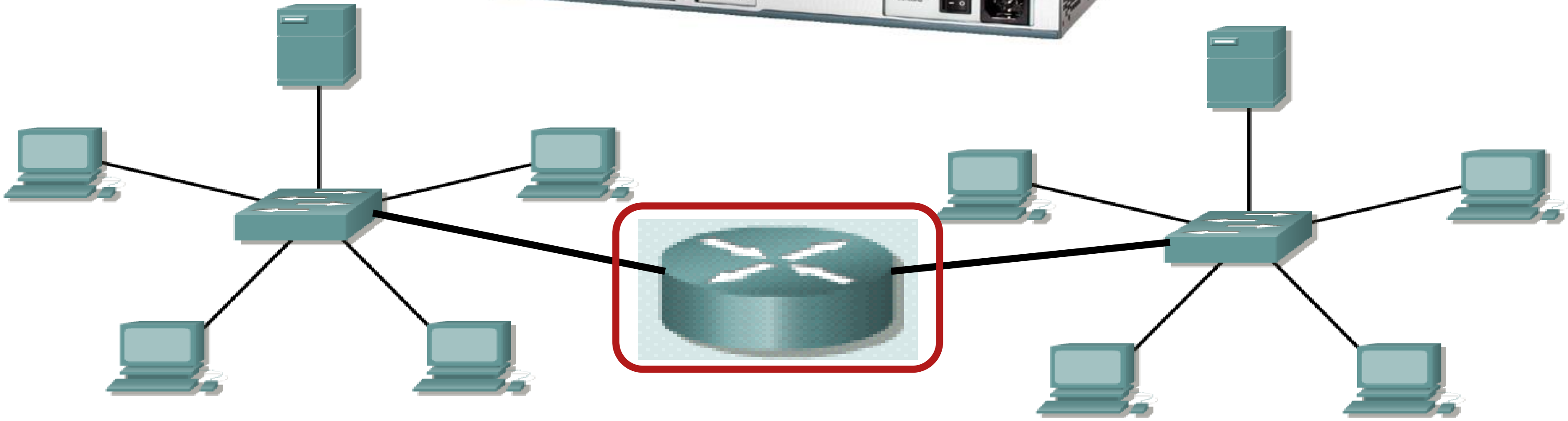
•Workgroup switches add more intelligence to data transfer management.

•Not only can they determine whether data should remain on a LAN or not, but they can transfer the data only to the connection that needs that data.

•Another difference between a bridge and switch is that a switch does not convert data transmission formats.



Router

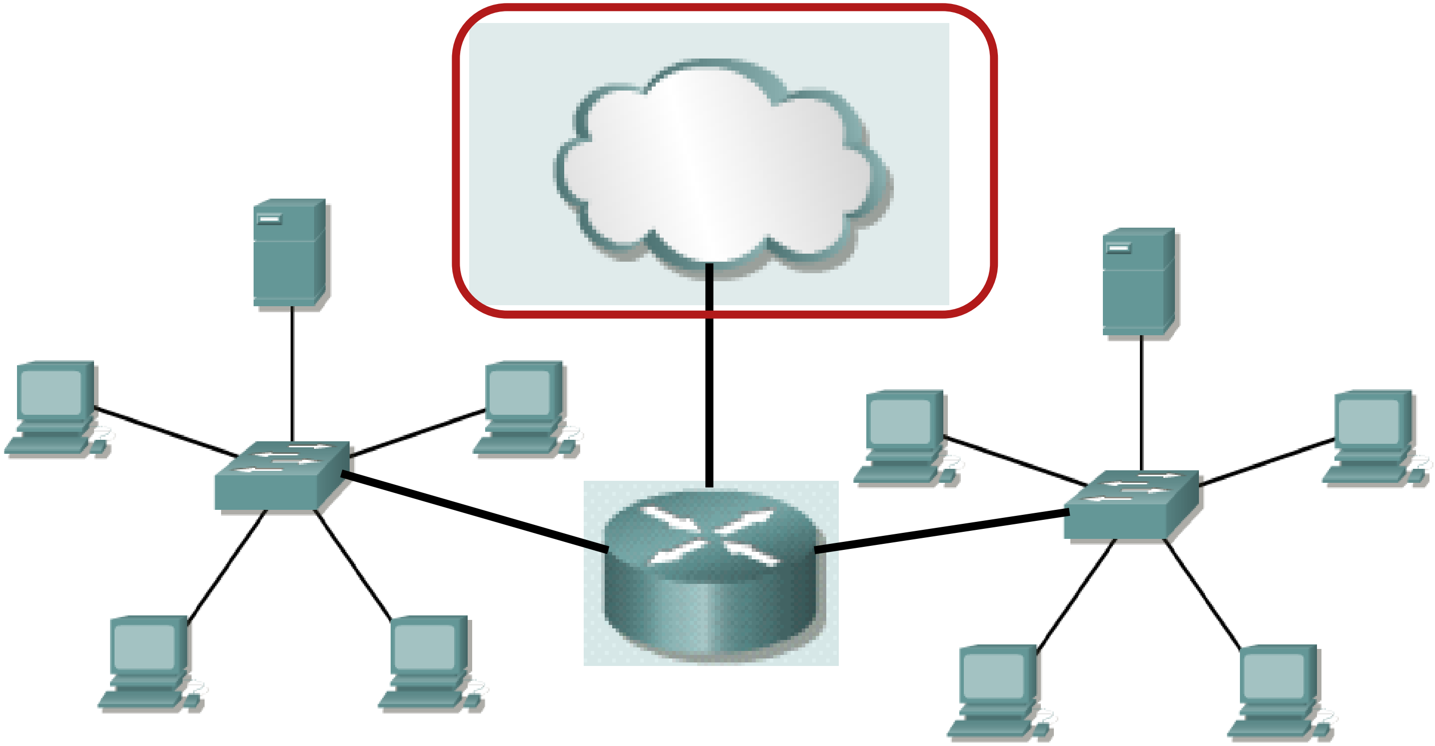


- Routers have all the capabilities of the previous devices. Routers can regenerate signals, concentrate multiple connections, convert data transmission formats, and manage data transfers.
- They can also connect to a WAN, which allows them to connect LANs that are separated by great distances.
- None of the other devices can provide this type of connection.

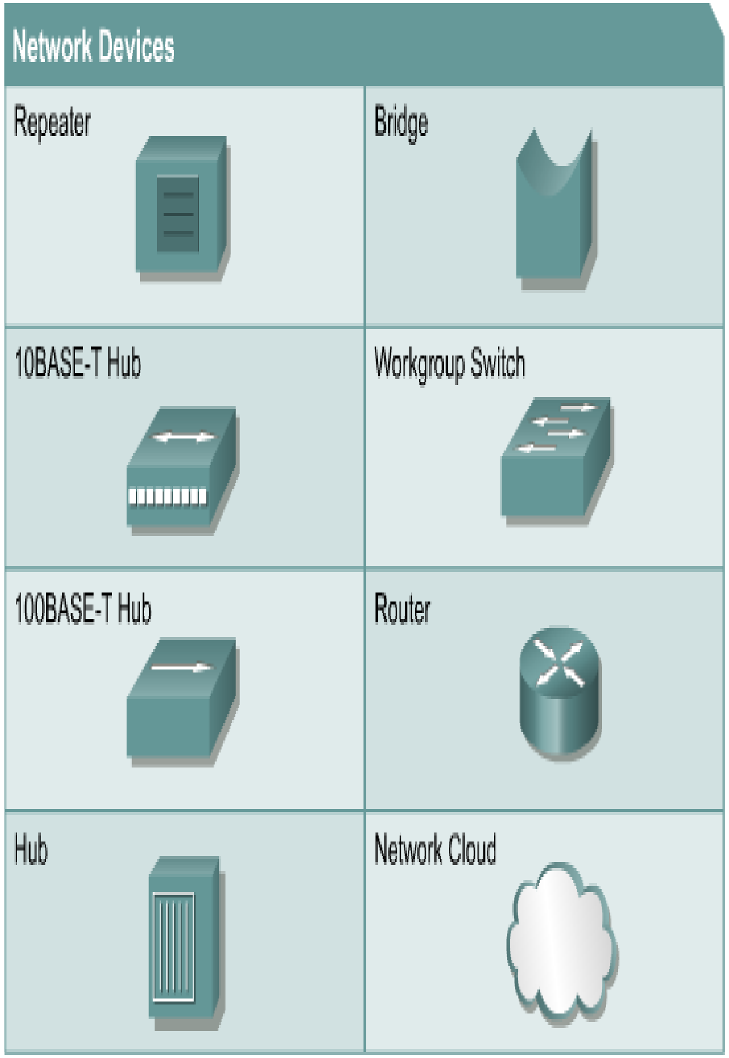
The Cloud

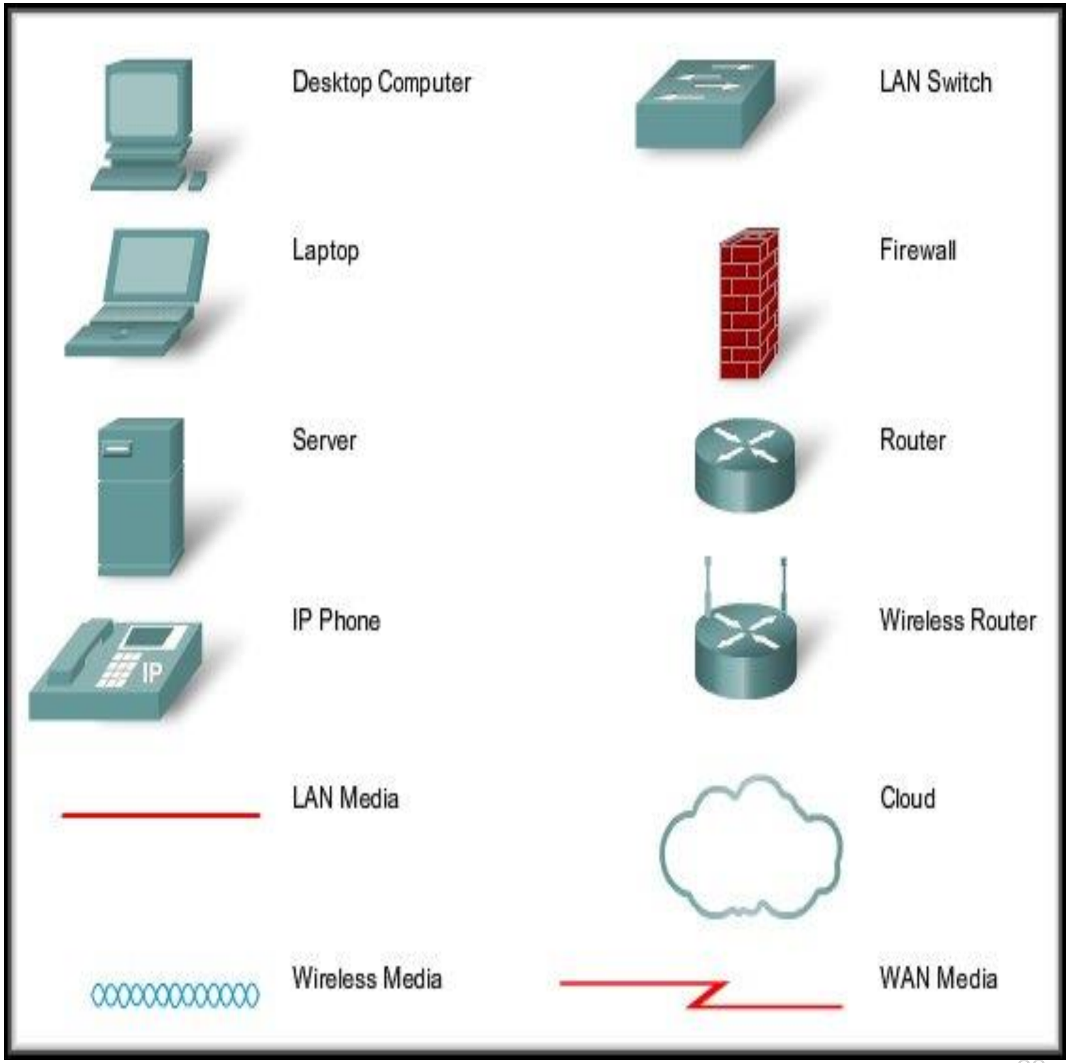
- The cloud is used in diagrams to represent where the connection to the internet is.

- It also represents all of the devices on the internet.

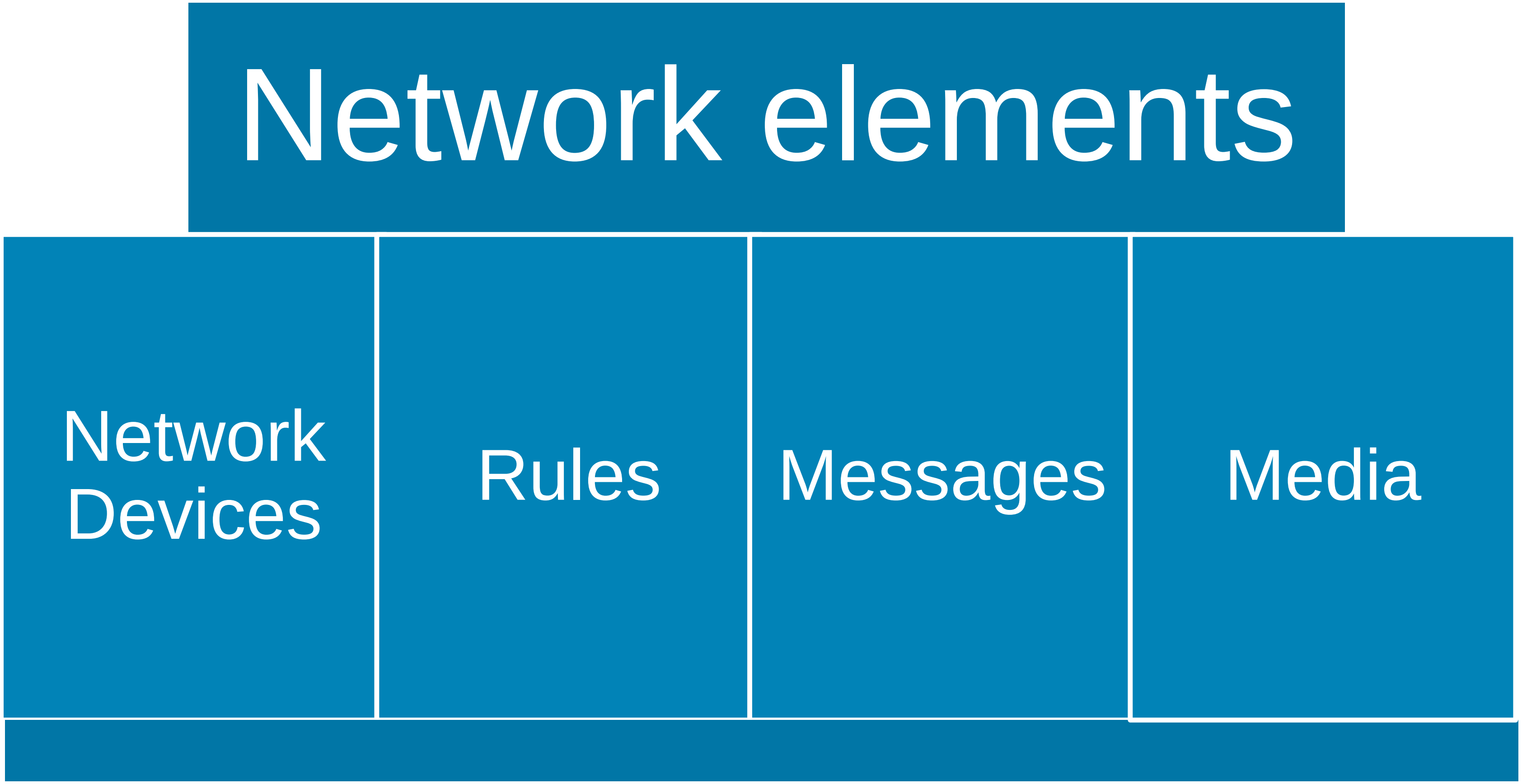


Network Devices





Network Components (Elements)



Network elements

Network Devices

Rules

Messages

Media

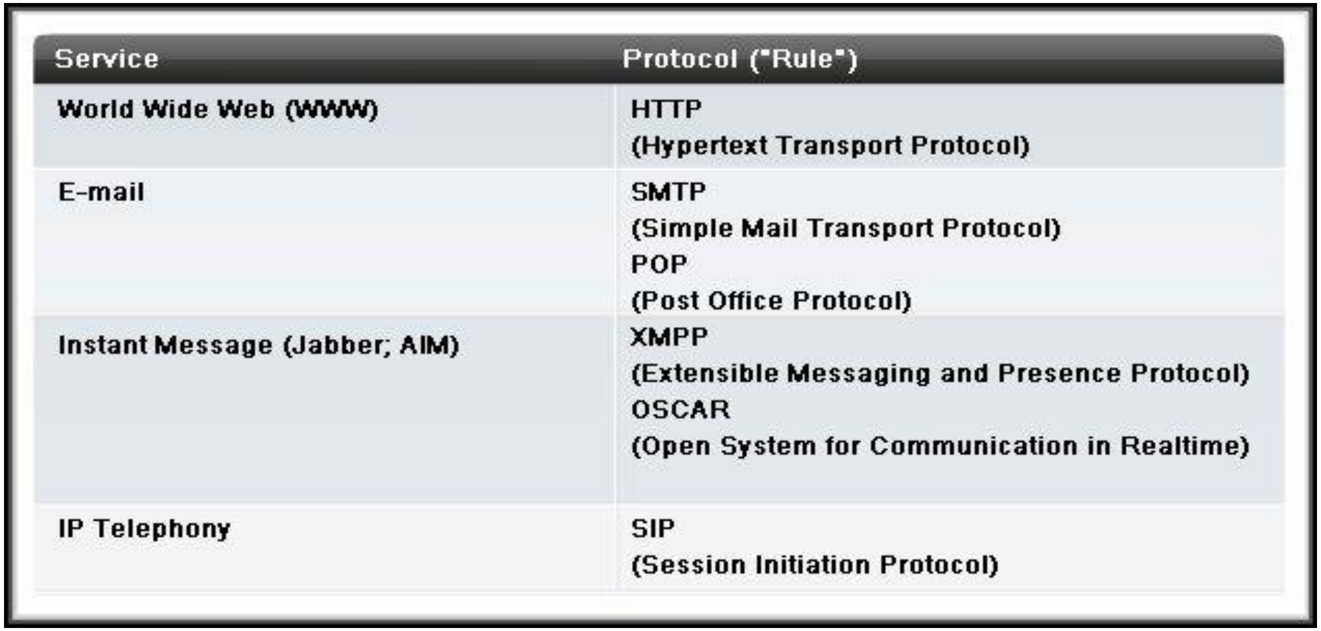
Rules(Protocols)

❑ Protocols are the rules that the networked devices use to communicate with each other.

❑ The industry standard in networking today is a set of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol).

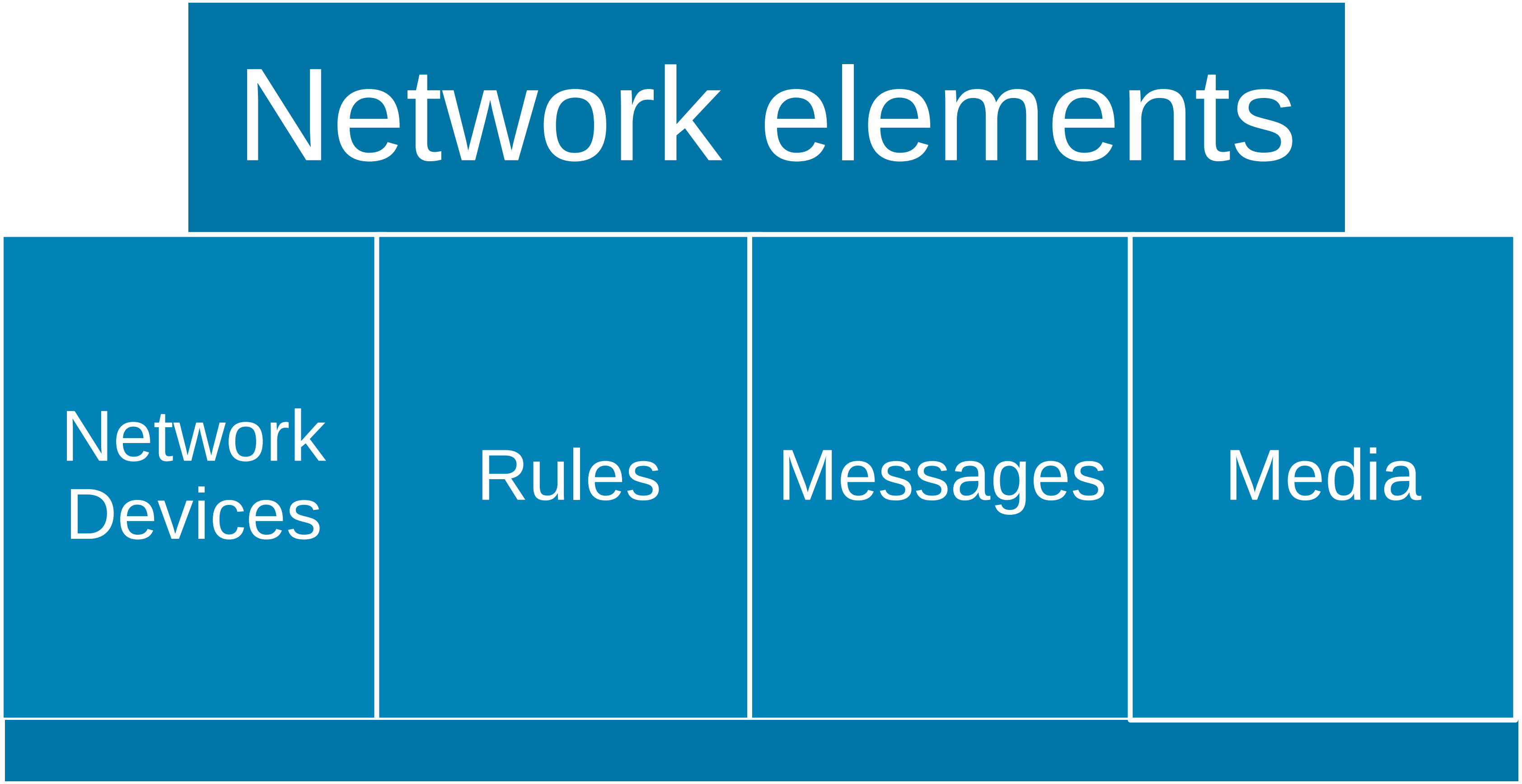
❑ TCP/IP is used in home and business networks, as well as being the primary protocol of the Internet.

❑ It is TCP/IP protocols that specify the formatting, addressing and routing mechanisms that ensure our messages are delivered to the correct recipient.

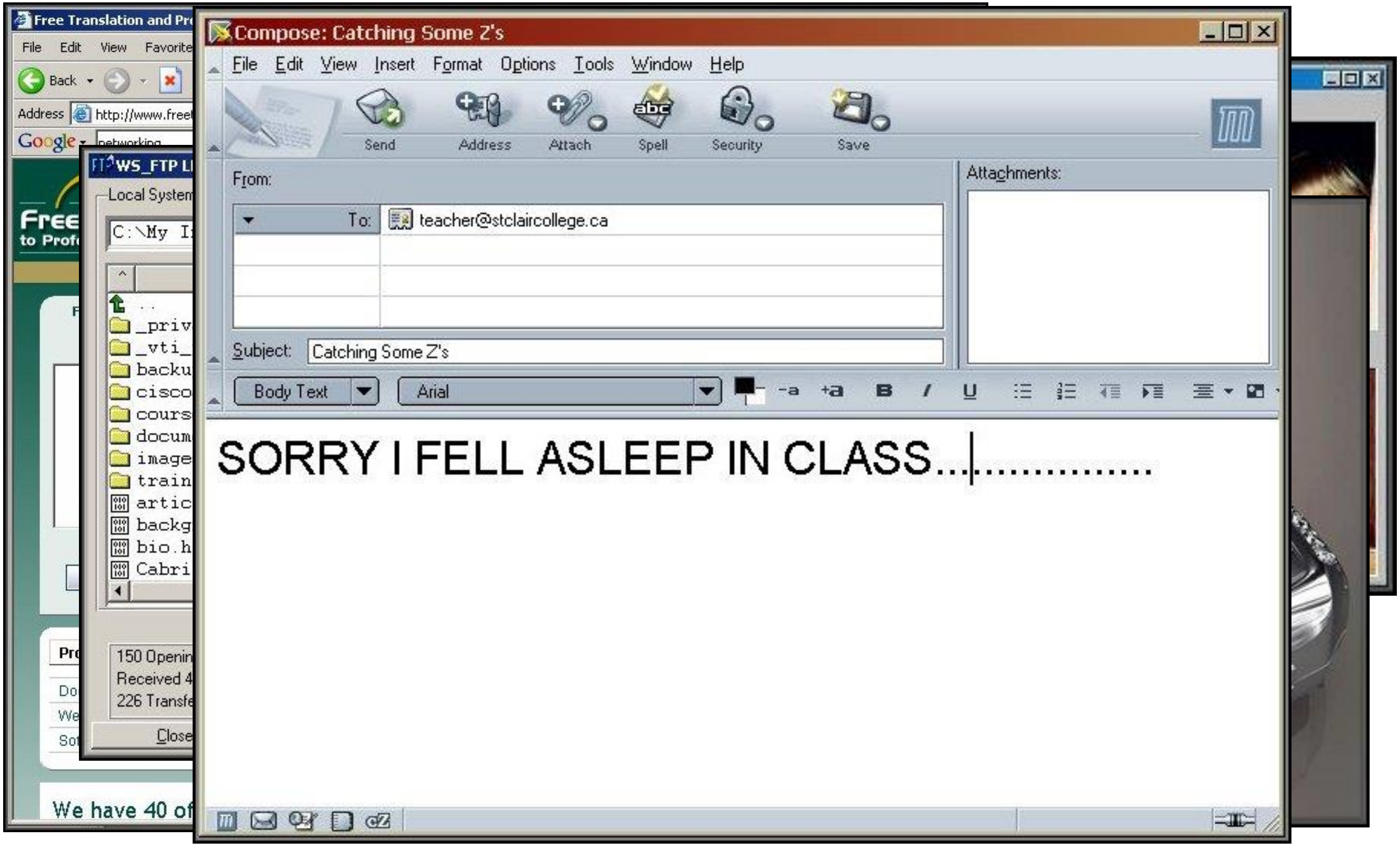


Service	Protocol ("Rule")
World Wide Web (WWW)	HTTP (Hypertext Transport Protocol)
E-mail	SMTP (Simple Mail Transport Protocol) POP (Post Office Protocol)
Instant Message (Jabber; AIM)	XMPP (Extensible Messaging and Presence Protocol) OSCAR (Open System for Communication in Realtime)
IP Telephony	SIP (Session Initiation Protocol)

Network Components (Elements)



Messages



Compose: Catching Some Z's

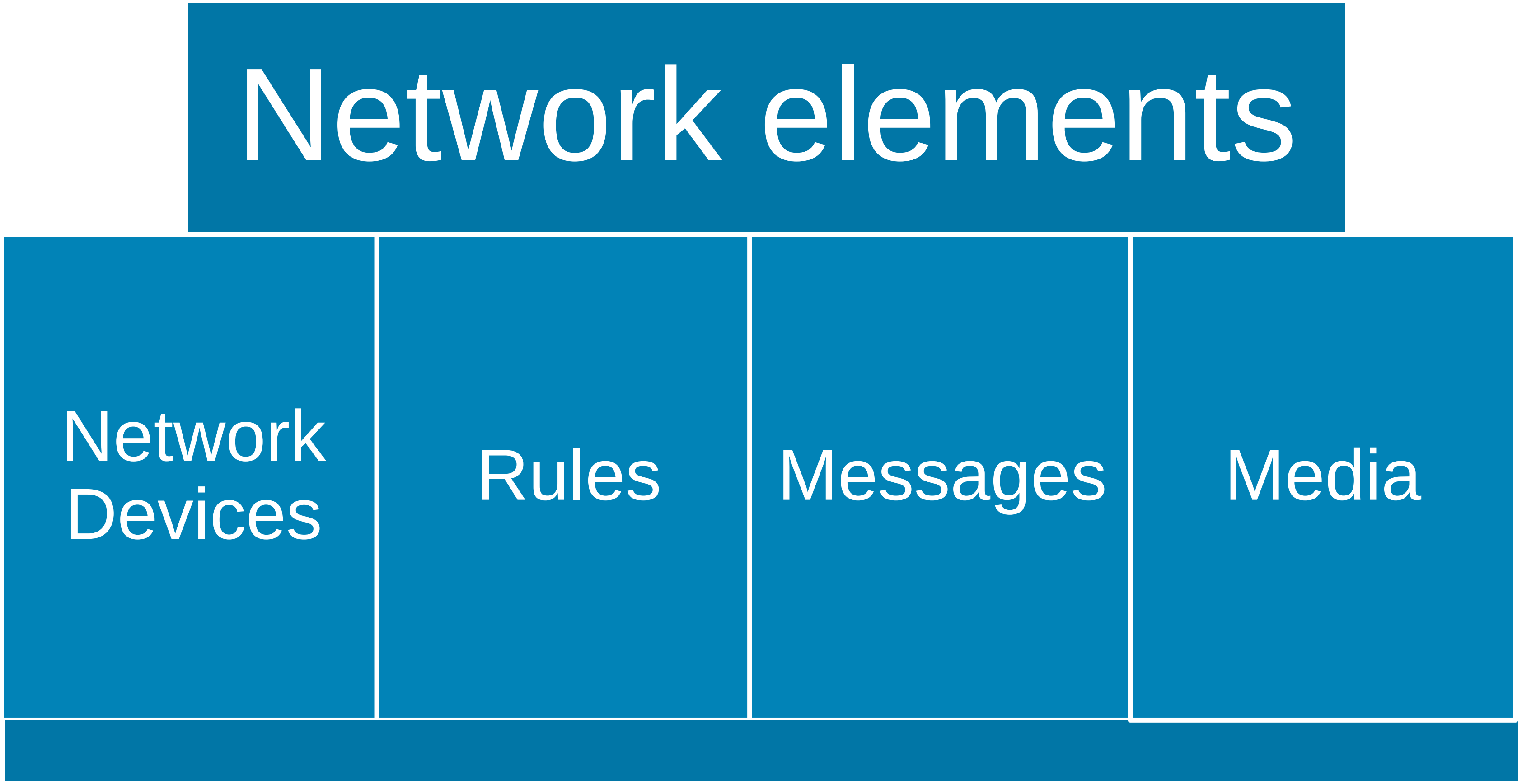
From:

To: teacher@stclaircollege.ca

Subject: Catching Some Z's

SORRY I FELL ASLEEP IN CLASS.................

Network Components (Elements)



Network elements

Network Devices

Rules

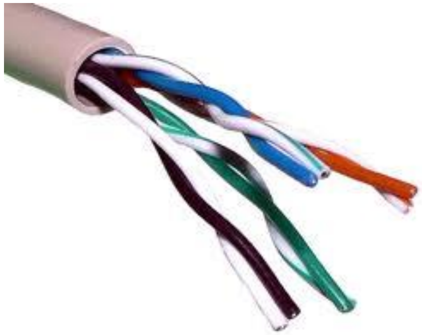
Messages

Media

Media (Network Connections)

- Network connections can be wired or wireless.
- In wired connections, the medium is either copper, which carries electrical signals, or optical fiber, which carries light signals.
- In wireless connections, the medium is the Earth's atmosphere, or space, and the signals are microwaves.

Coaxial cable



Twisted pair cable

Optical fiber cable

CONNECTED
CONNECTED
CONNECTED

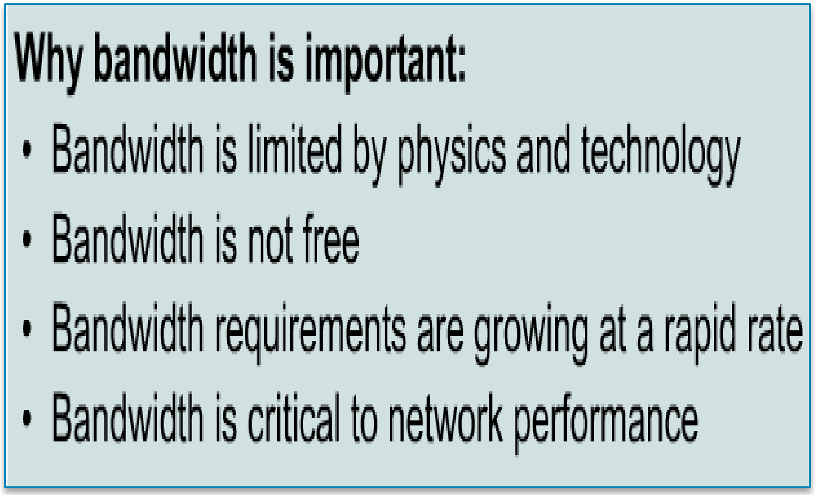
The criteria for choosing network media are:

✓The distance the media can successfully carry a signal
✓The environment in which the media is to be installed
✓The amount of data and the speed at which it must be transmitted
✓The cost of the media and installation

Media Bandwidth

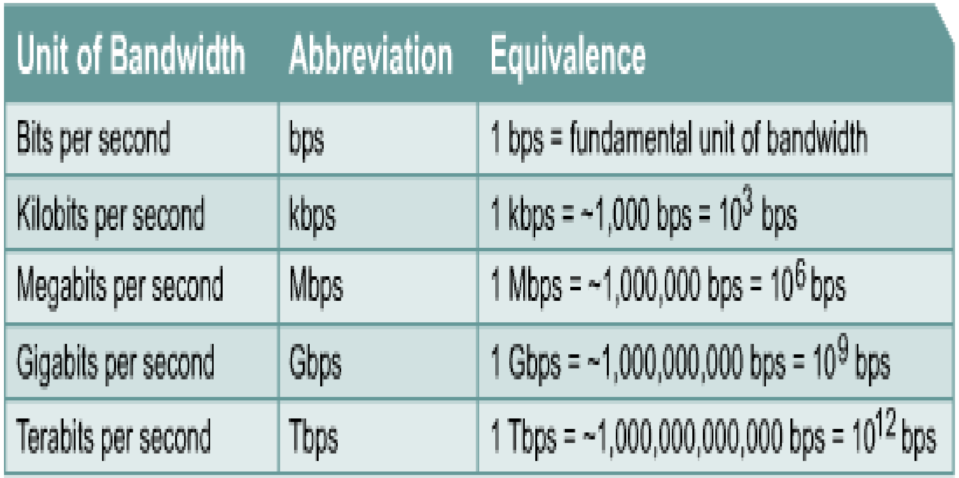
- Bandwidth describes the maximum data transfer rate of a network or Internet connection.
- It measures how much data can be sent over a specific connection in a given amount of time.

Bandwidth is like the number of lanes on a highway.



Why bandwidth is important:

- Bandwidth is limited by physics and technology
- Bandwidth is not free
- Bandwidth requirements are growing at a rapid rate
- Bandwidth is critical to network performance



Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	kbps	1 kbps = ~1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = ~1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps = ~1,000,000,000 bps = 10^9 bps
Terabits per second	Tbps	1 Tbps = ~1,000,000,000,000 bps = 10^{12} bps

Media Throughput

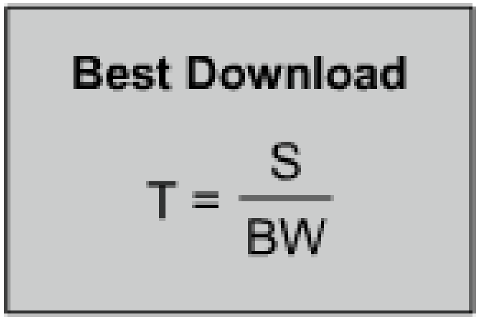
- **Throughput** refers to actual measured bandwidth, at a specific time of day, using specific Internet routes, and while a specific set of data is transmitted on the network.

- Unfortunately throughput is often far less than the maximum possible digital bandwidth of the medium that is being used.

- The following are some of the factors that determine throughput:

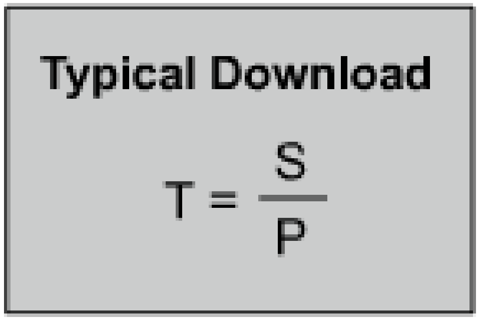
- Internetworking devices
- Type of data being transferred
- Network topology
- Number of users on the network
- User computer
- Server computer
- Power conditions

Media Throughput



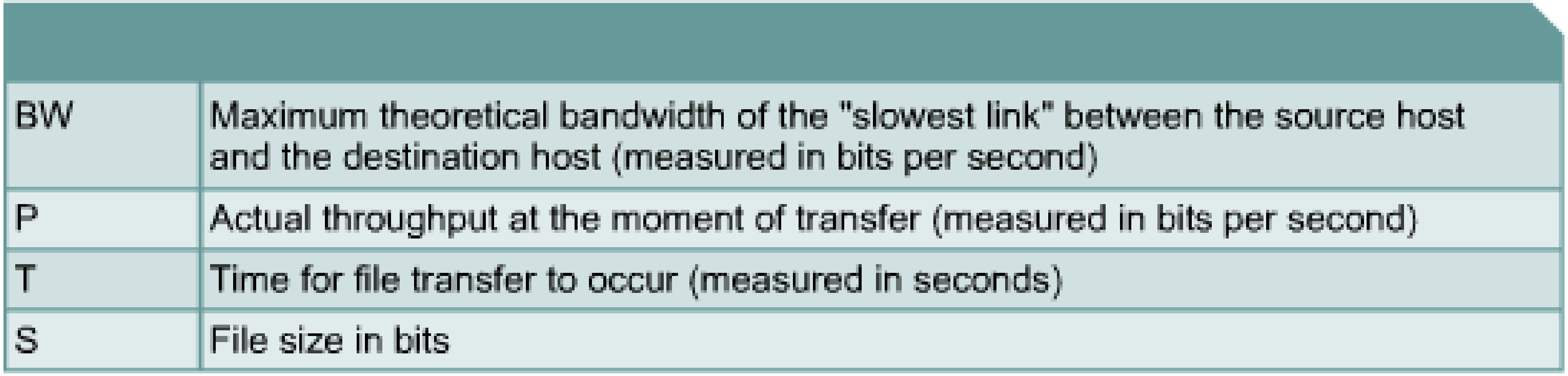
Best Download

$$T = \frac{S}{BW}$$



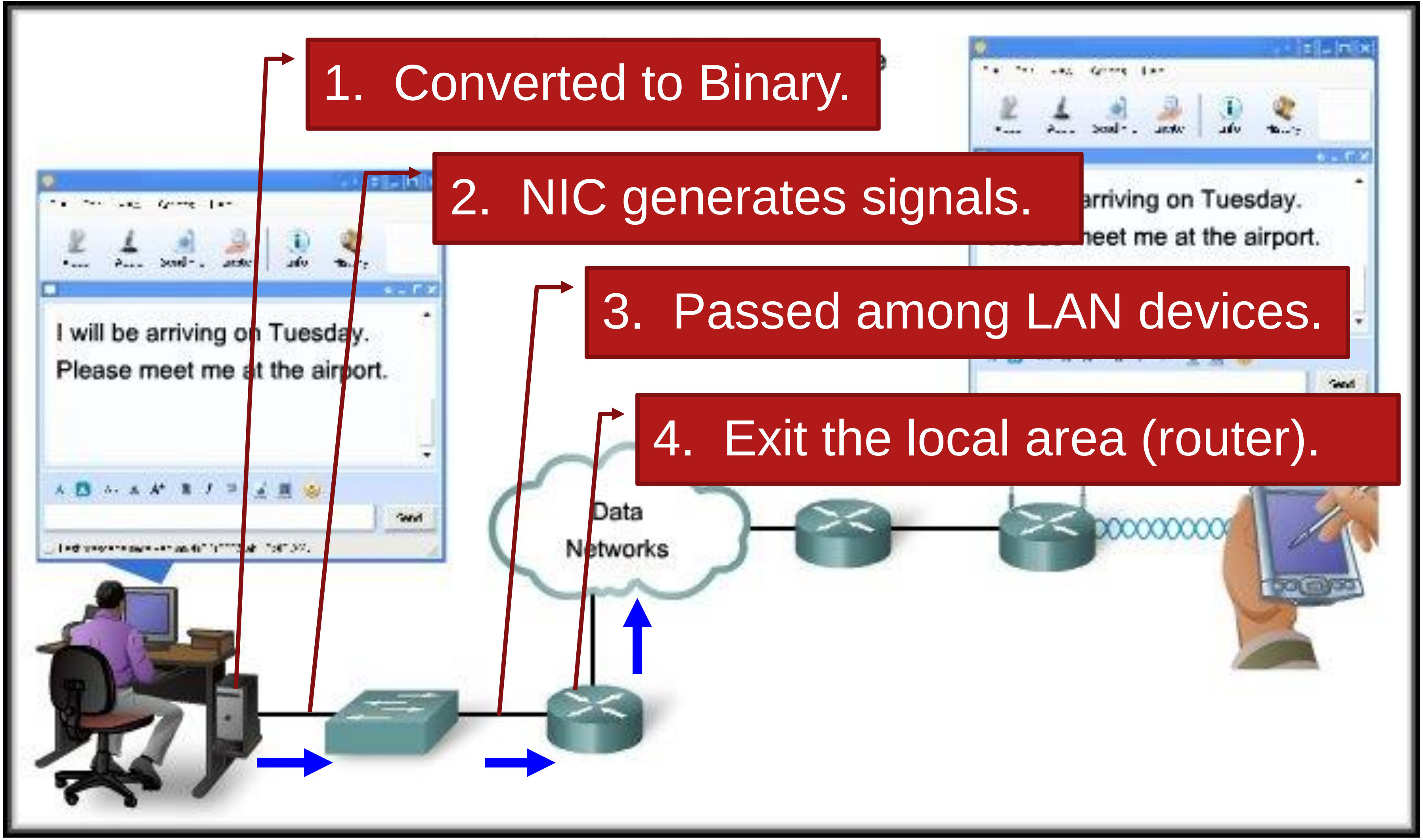
Typical Download

$$T = \frac{S}{P}$$



BW	Maximum theoretical bandwidth of the "slowest link" between the source host and the destination host (measured in bits per second)
P	Actual throughput at the moment of transfer (measured in bits per second)
T	Time for file transfer to occur (measured in seconds)
S	File size in bits

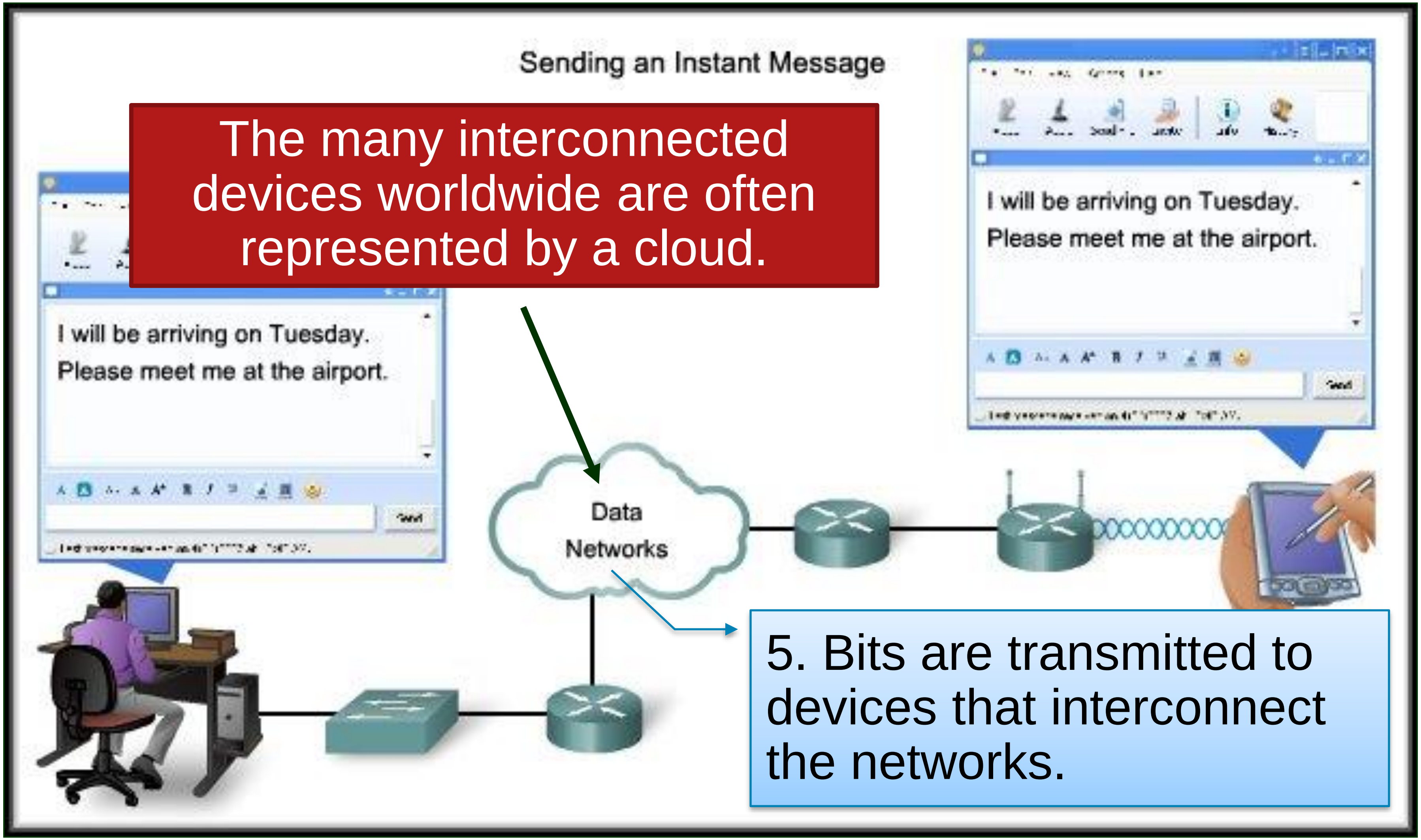
Putting It all Together



1. Converted to Binary.
2. NIC generates signals.
3. Passed among LAN devices.
4. Exit the local area (router).

I will be arriving on Tuesday.
Please meet me at the airport.

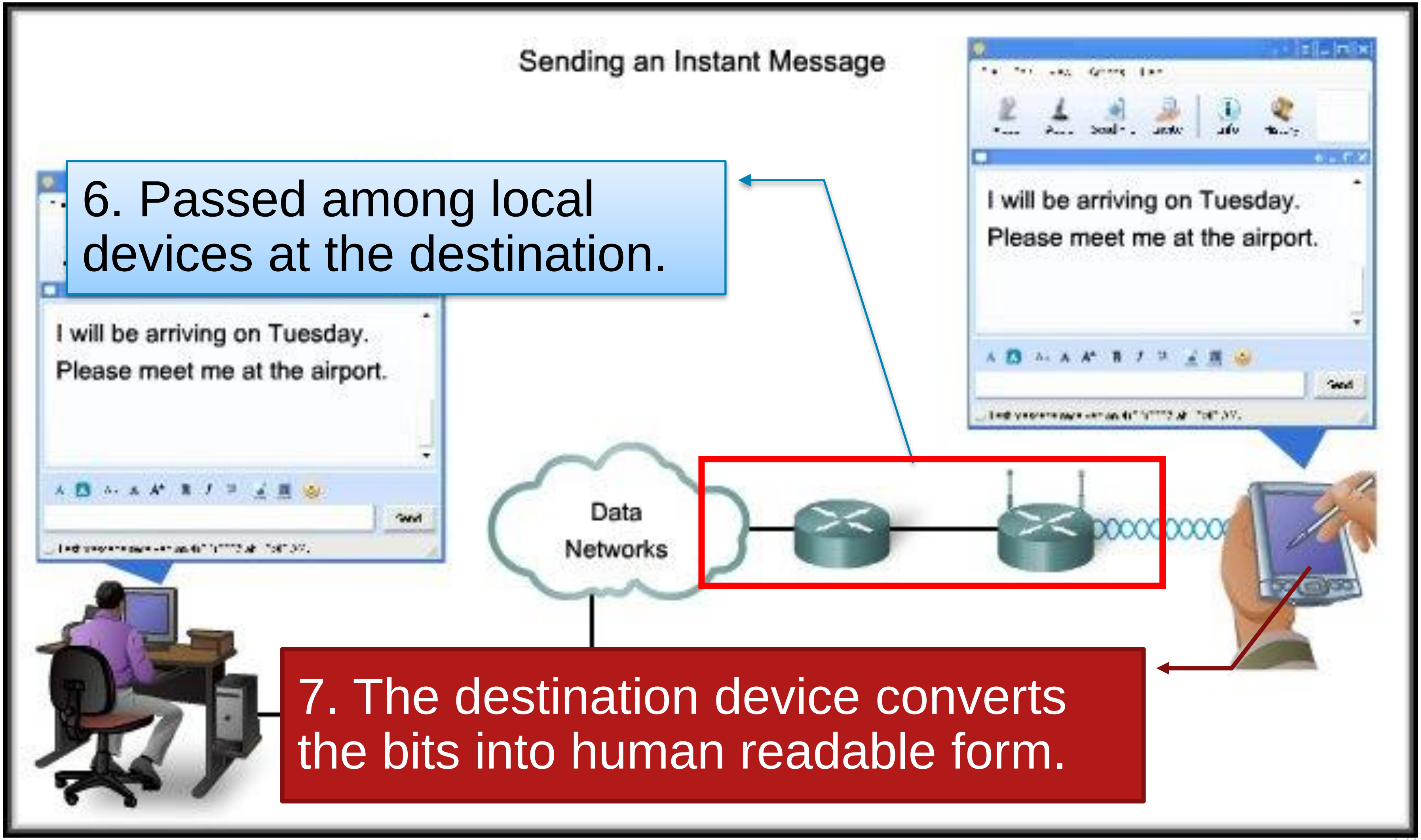
Putting It all Together


Sending an Instant Message
I will be arriving on Tuesday.
Please meet me at the airport.
I will be arriving on Tuesday.
Please meet me at the airport.
Data
Networks

The many interconnected devices worldwide are often represented by a cloud.

5. Bits are transmitted to devices that interconnect the networks.

Putting It all Together



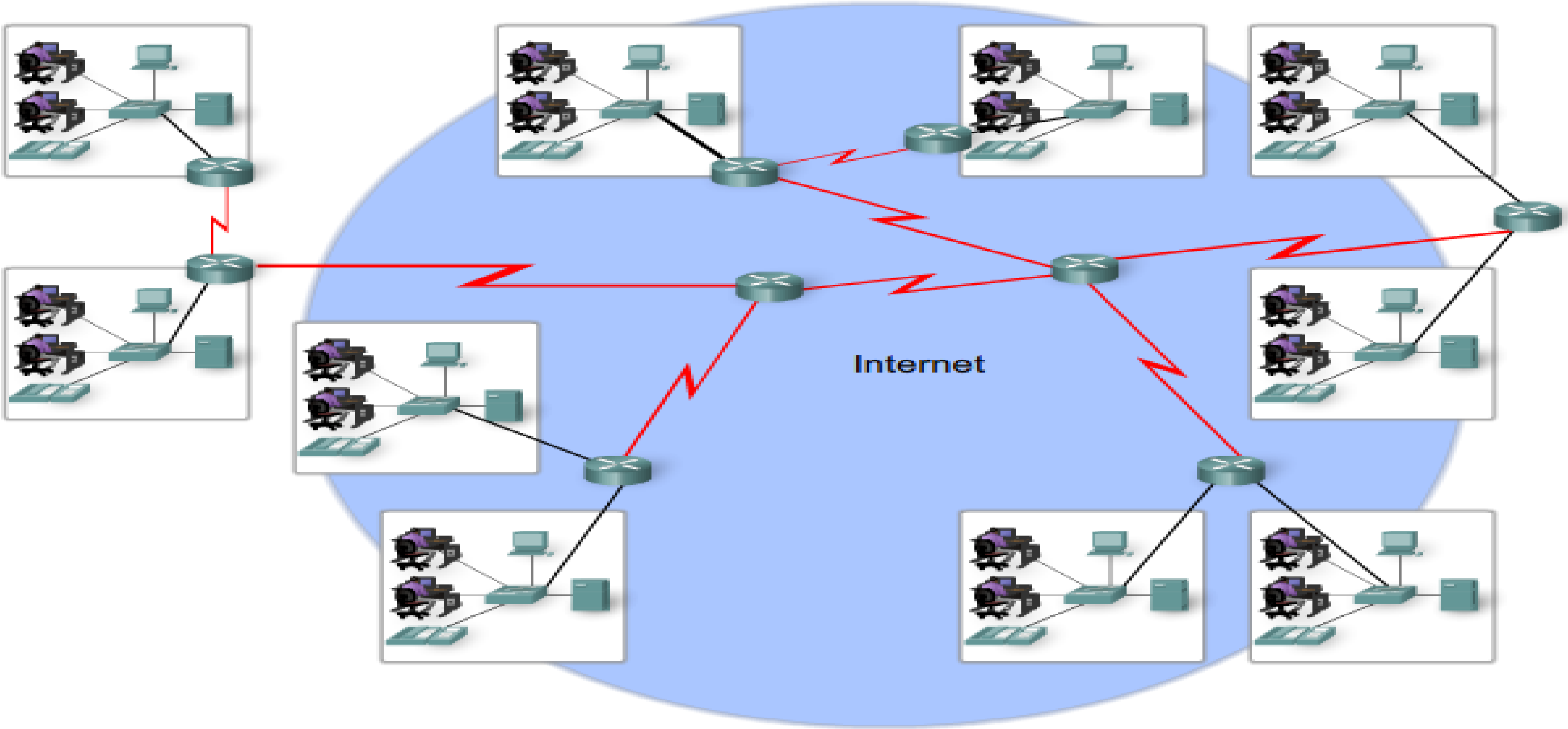
I will be arriving on Tuesday.
Please meet me at the airport.

6. Passed among local devices at the destination.

7. The destination device converts the bits into human readable form.

The Internet

LANs and WANs may be connected into internetworks.



The Internet is a conglomerate of networks and is not actually owned by any individual or group.

The Internet

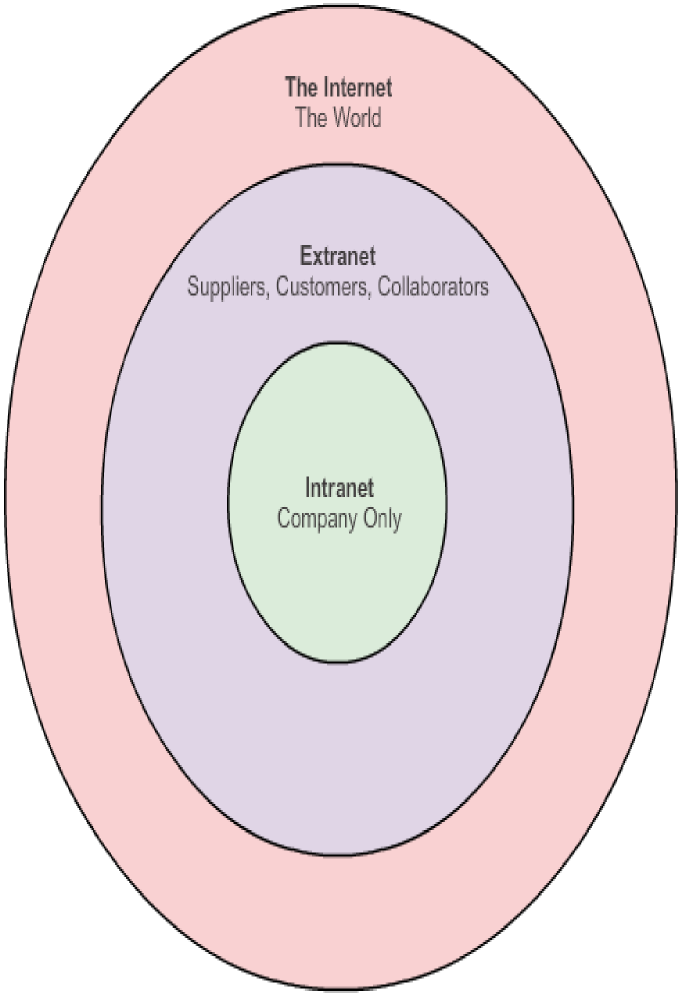
- Ensuring effective communication across this diverse infrastructure requires the application of consistent and commonly recognized technologies and standards as well as the cooperation of many network administration agencies.

- There are organizations that have been developed for the purpose of helping to maintain structure and standardization of Internet protocols and processes. These organizations include the Internet Engineering Task Force (**IETF**), Internet Corporation for Assigned Names and Numbers (**ICANN**), and the Internet Architecture Board (**IAB**), plus many others.

The term internet (with a lower case “i") is used to describe multiple networks interconnected. When referring to the global system of interconnected computer networks or the World Wide Web, the term Internet (with a capital “I”) is used.

The Internet

- Intranet is a term often used to refer to a private connection of LANs and WANs that belongs to an organization, and is designed to be accessible only by the organization's members, employees, or others with authorization.
- Intranets are basically an internet which is usually only accessible from within the organization.
- For example, schools may have intranets that include information on class schedules, online curriculum, and discussion forums.
- Intranets usually help eliminate paperwork and speed up workflows. The intranet may be accessible to staff working outside of the organization by using secure connections to the internal network.



- An organization may use an extranet to provide secure and safe access to individuals who work for a different organizations, but require company data.
- Examples of extranets include:

I. A company providing access to outside suppliers/contractors.
II. A hospital providing a booking system to doctors so they can make appointments for their patients.
III. A local office of education providing budget and personnel information to the schools in its district.

Connecting to the Internet

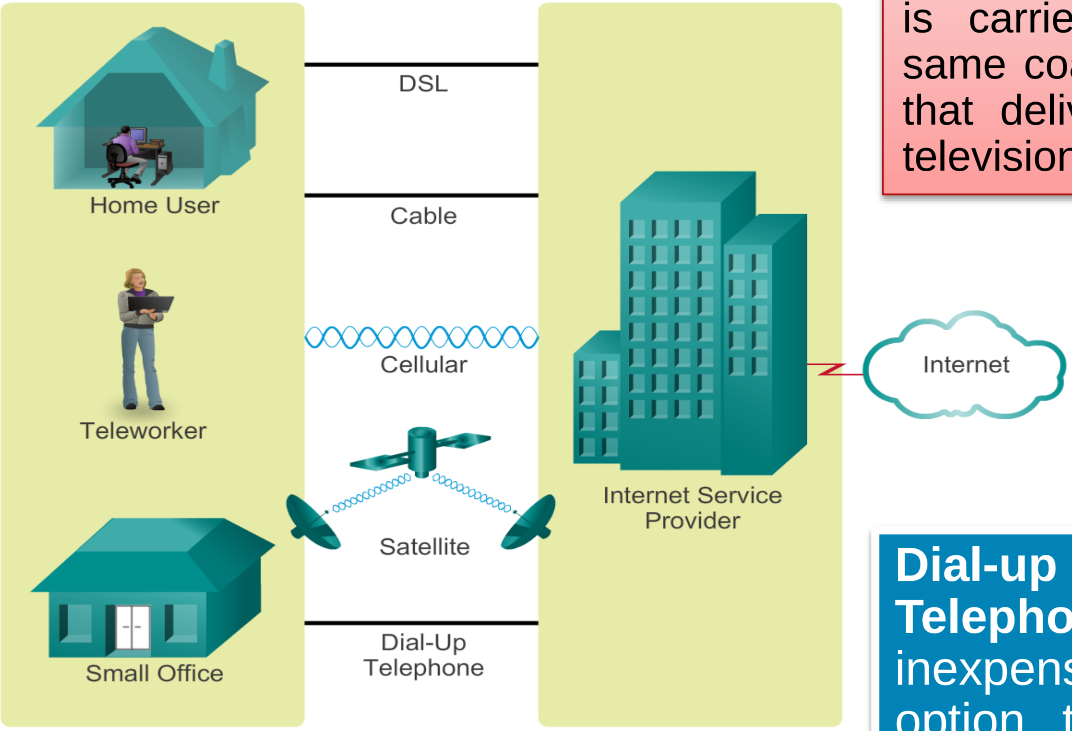
- There are many different ways to connect users and organizations to the Internet.
- Home users, teleworkers (remote workers), and small offices typically require a connection to an Internet Service Provider (ISP) to
- Fast connections are required to support business services including IP phones, video conferencing, and data center storage. access the Internet.
- Popular business-class services include business DSL, leased lines, and Metro Ethernet.

Connecting to the Internet

- ❑ **DSL** - Provides a high bandwidth, always on, connection to the Internet.
- ❑ It requires a special high-speed modem that separates the DSL signal from the telephone signal and provides an Ethernet connection to a host computer or LAN.
- ❑ DSL runs over a telephone line, with the line split into three channels.

Cellular - Cellular Internet access uses a cell phone network to connect.

Connection Options



Satellite - Satellite service is a good option for homes or offices that do not have access to DSL or cable.

CABLE: Typically offered by cable television service providers, the Internet data signal is carried on the same coaxial cable that delivers cable television.

Dial-up Telephone - An inexpensive option that uses any phone line and a modem.

Connecting business to the Internet

Connection Options

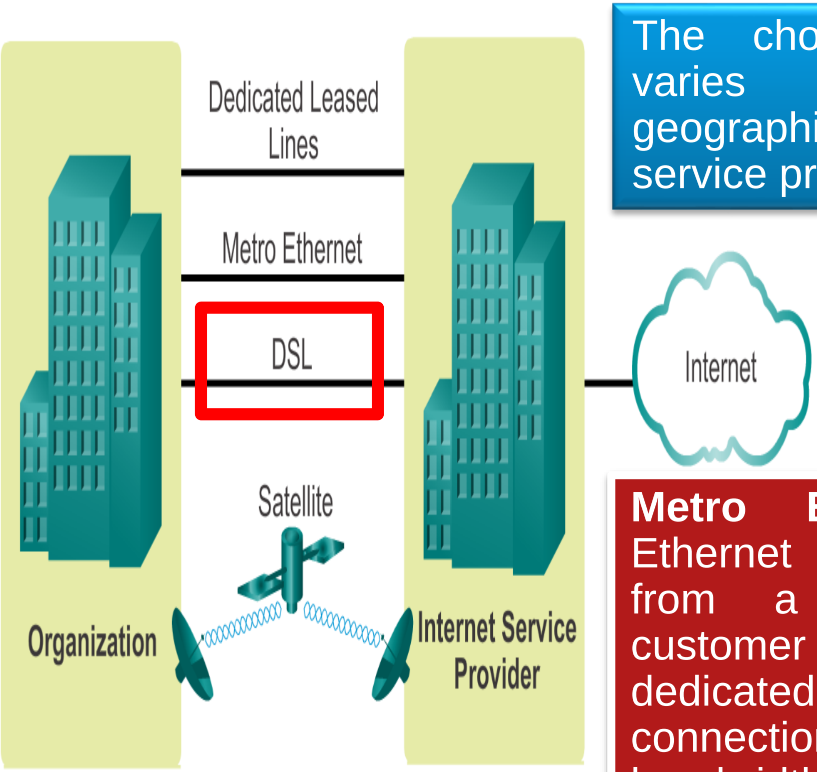
- ➢Corporate connection options differ from home user options.
- ➢Businesses may require higher bandwidth, dedicated bandwidth, and managed services.
- ➢ Connection options available differ depending on the number of service providers located nearby.

▪**Dedicated Leased Line** - This is a dedicated connection from the service provider to the customer premise.

▪ Leased lines are actually reserved circuits that connect geographically separated offices for private voice and/or data networking.

▪The circuits are typically rented at a monthly or yearly rate which tends to make it expensive.

▪In North America, common leased line circuits include T1 (1.54 Mb/s) and T3 (44.7 Mb/s) while in other parts of the world they are available in E1 (2 Mb/s) and E3 (34 Mb/s).

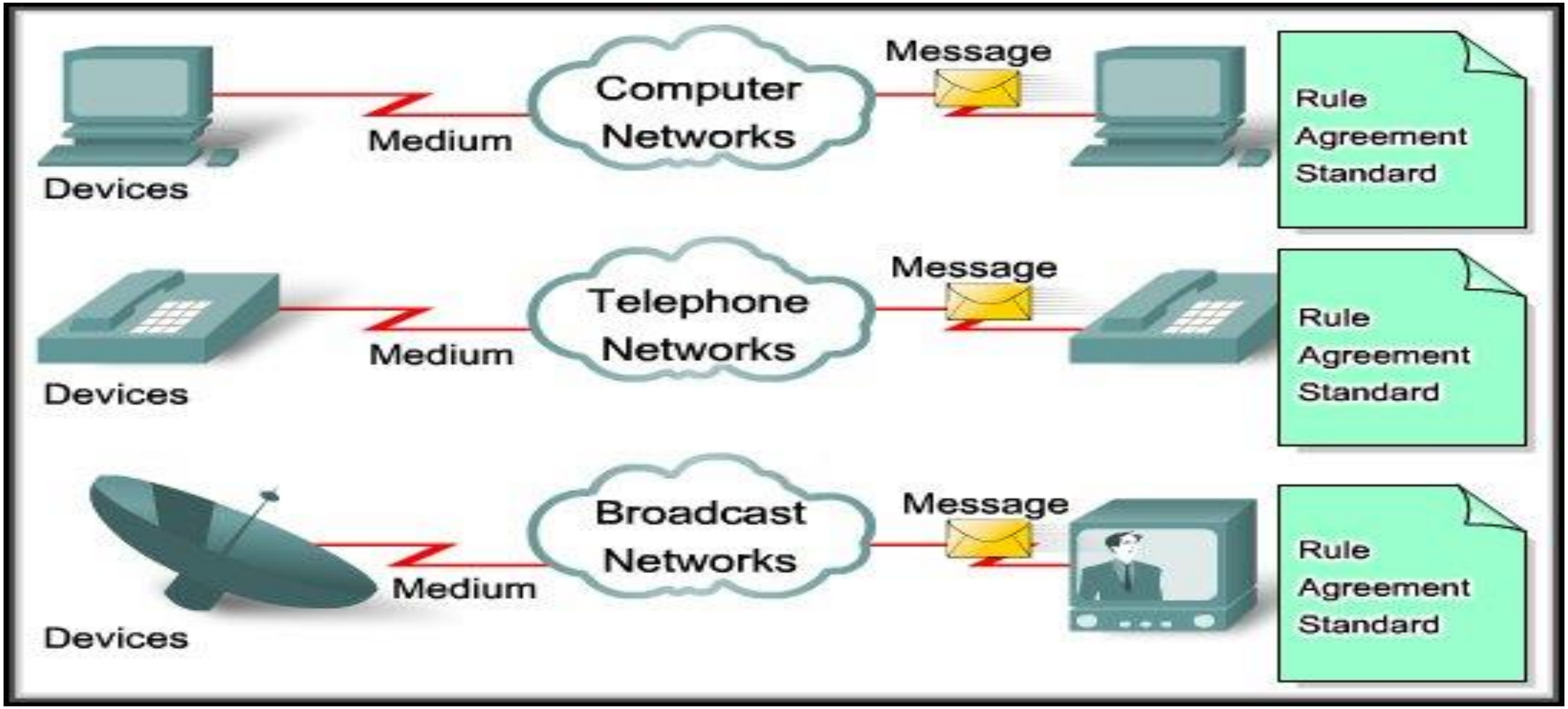


The choice of connection varies depending on geographical location and service provider availability.

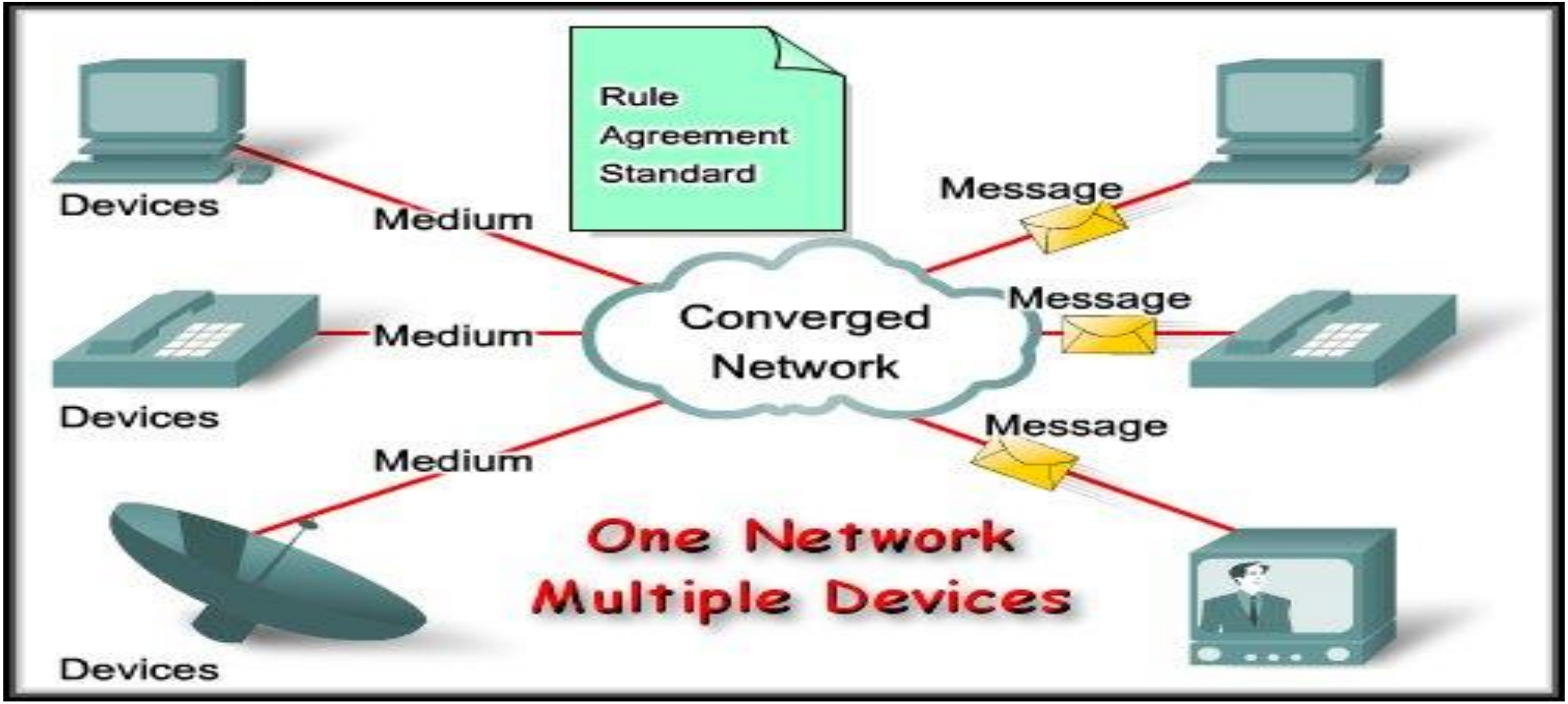
Metro Ethernet - Metro Ethernet is typically available from a provider to the customer premise over a dedicated copper or fiber connection providing bandwidth speeds of 10 Mb/s to 10 Gb/s.

Converged Networks

- ➢ Traditional telephone, radio, television, and computer data networks each have their own individual versions of the four basic network elements.
- ➢In the past, every one of these services required a different technology to carry its particular communication signal.
- ➢Additionally, each service had its own set of rules and standards to ensure successful communication of its signal across a specific medium.



Converged Networks

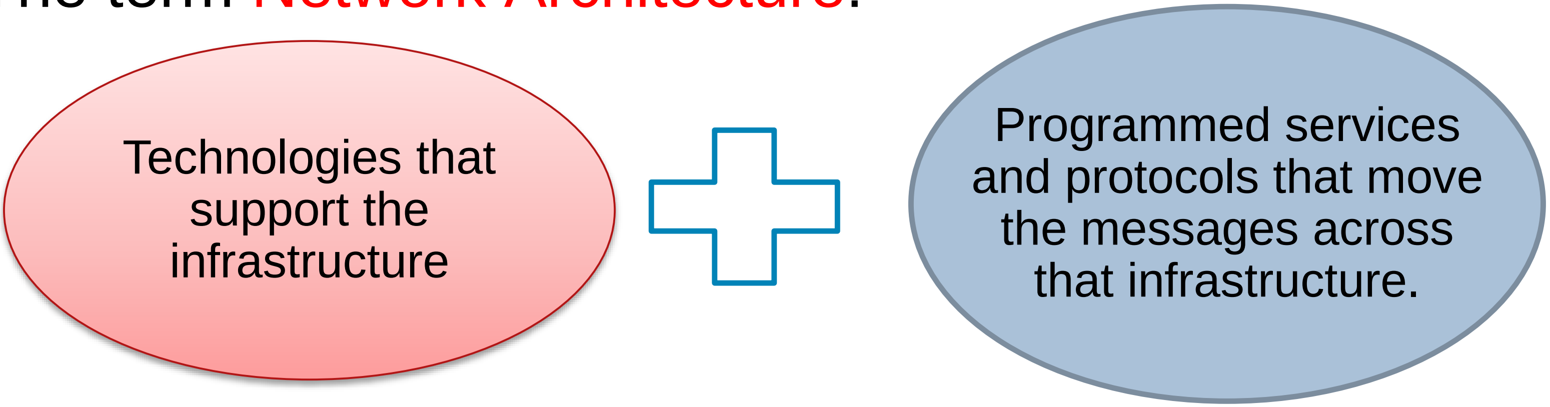


- Currently, the convergence of the different types of communications networks onto one platform represents the first phase in building the intelligent information network.

- In the future, the goal is to consolidate (merge) the applications that generate, transmit, and secure the messages onto integrated network devices.

Network Architecture

- The term Network Architecture:



Technologies that support the infrastructure

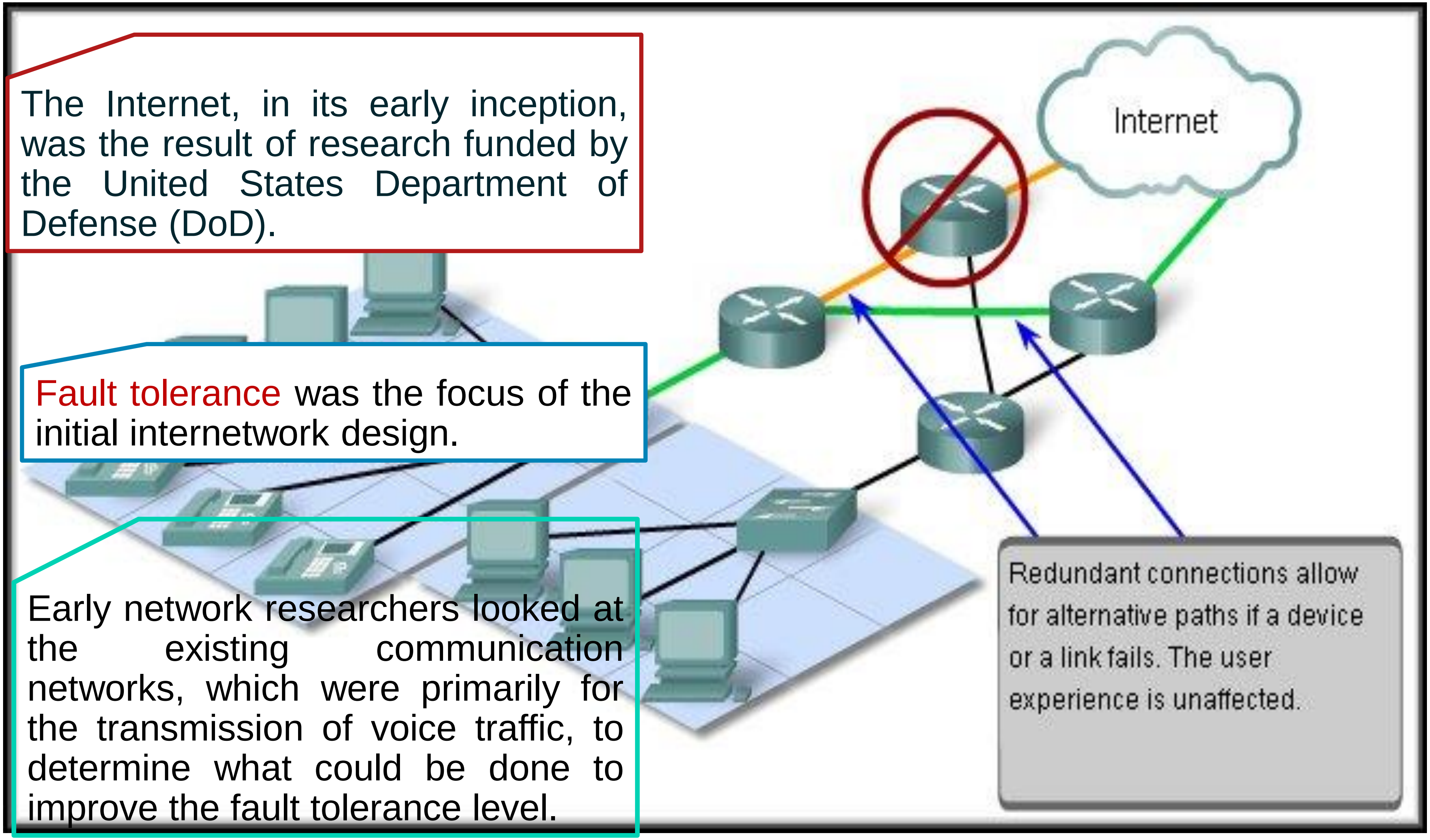
Programmed services and protocols that move the messages across that infrastructure.

- There are 4 basic characteristics for networks in general to meet user expectations:

1. Fault tolerance
2. Scalability
3. Quality of Service (QoS)
4. Security

New applications available to users over internetworks create higher expectations for the quality of the delivered services. Voice and live video transmissions require a level of consistent quality and uninterrupted delivery that was not necessary for traditional computer applications.

Network Architecture → Fault Tolerance



The Internet, in its early inception, was the result of research funded by the United States Department of Defense (DoD).

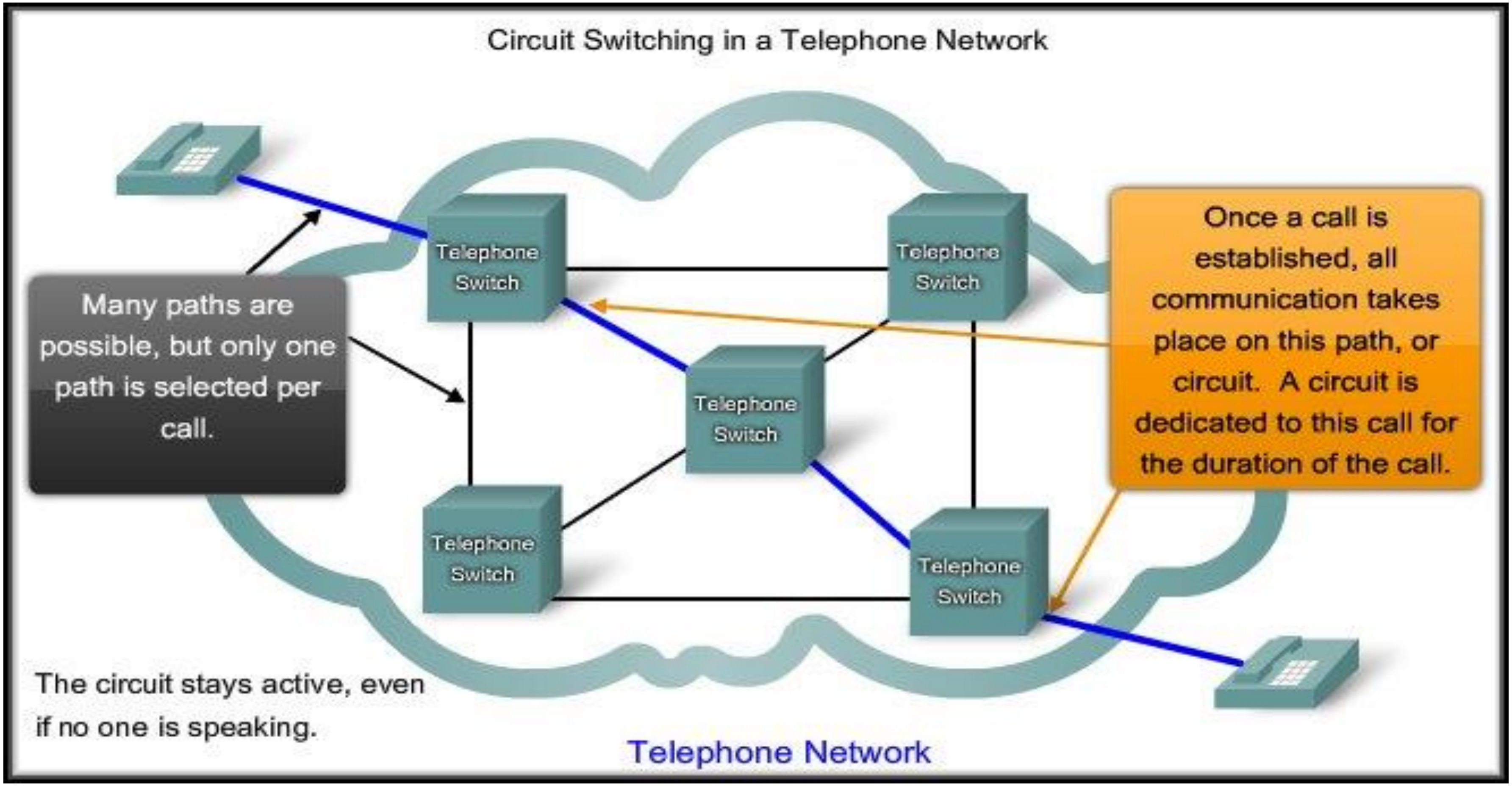
Fault tolerance was the focus of the initial internetwork design.

Early network researchers looked at the existing communication networks, which were primarily for the transmission of voice traffic, to determine what could be done to improve the fault tolerance level.

Redundant connections allow for alternative paths if a device or a link fails. The user experience is unaffected.

Network Architecture → Fault Tolerance

- **Circuit Switching**



Circuit Switching in a Telephone Network

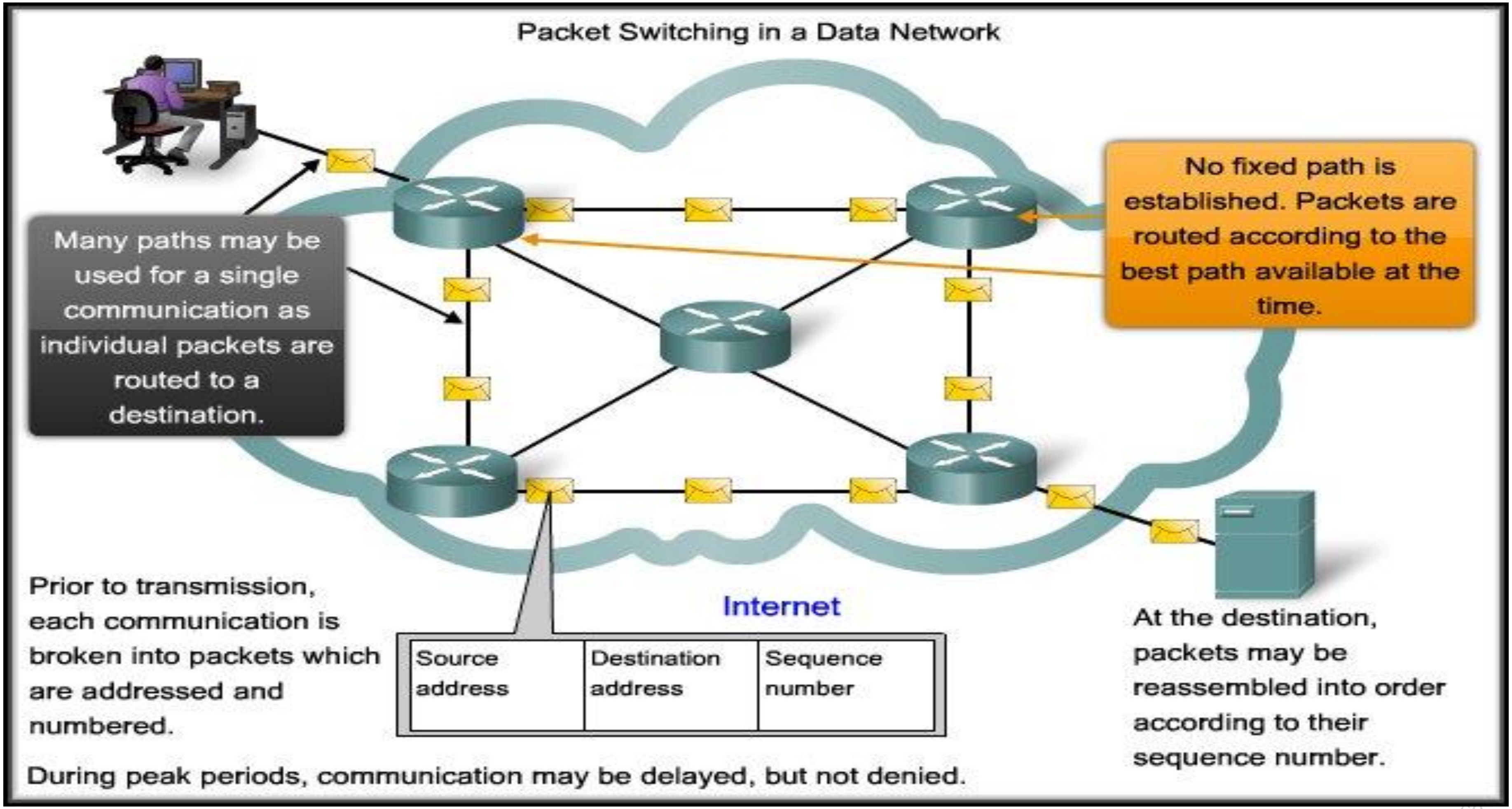
Many paths are possible, but only one path is selected per call.

Once a call is established, all communication takes place on this path, or circuit. A circuit is dedicated to this call for the duration of the call.

The circuit stays active, even if no one is speaking.

Network Architecture → Fault Tolerance

- **Packet Switching**



Packet Switching in a Data Network

Many paths may be used for a single communication as individual packets are routed to a destination.

No fixed path is established. Packets are routed according to the best path available at the time.

Prior to transmission, each communication is broken into packets which are addressed and numbered.

At the destination, packets may be reassembled into order according to their sequence number.

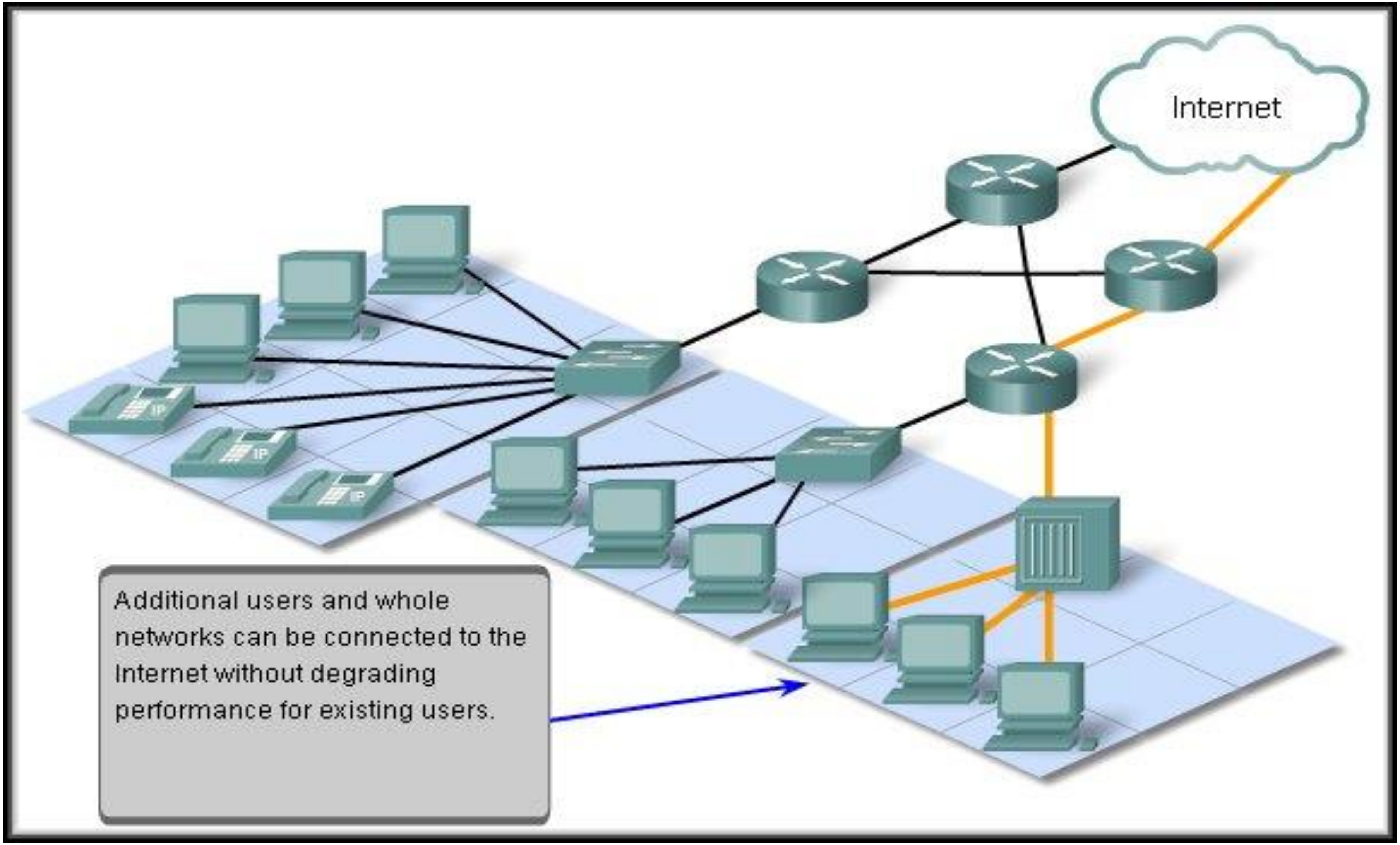
During peak periods, communication may be delayed, but not denied.

Network Architecture → Fault Tolerance

- **Circuit Switching vs. Packet Switching**

Circuit Switched	Packet Switched
Connection-oriented	Connectionless
Dedicated Circuit	Shared Circuit
Guaranteed level of service (Bandwidth, QoS)	Messages divided into packets
Inefficient use of Medium	Efficient use of Medium
Single path, no redundancy	Fault Tolerant, multiple possible paths

Network Architecture ➔ Scalability

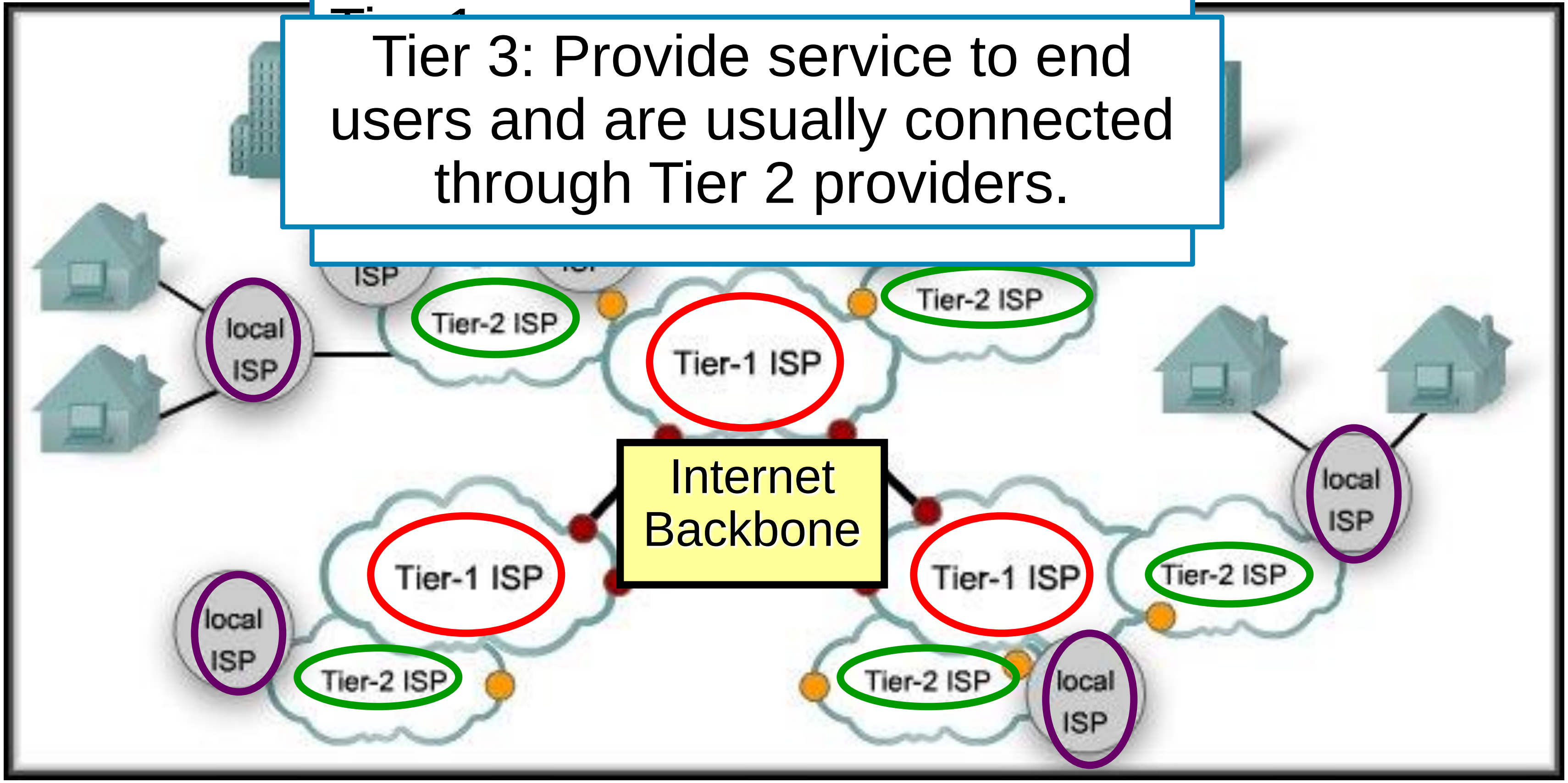


Additional users and whole networks can be connected to the Internet without degrading performance for existing users.

Network Architecture ➔ Scalability

- A good example of scalability is the Tier architecture of the Internet.

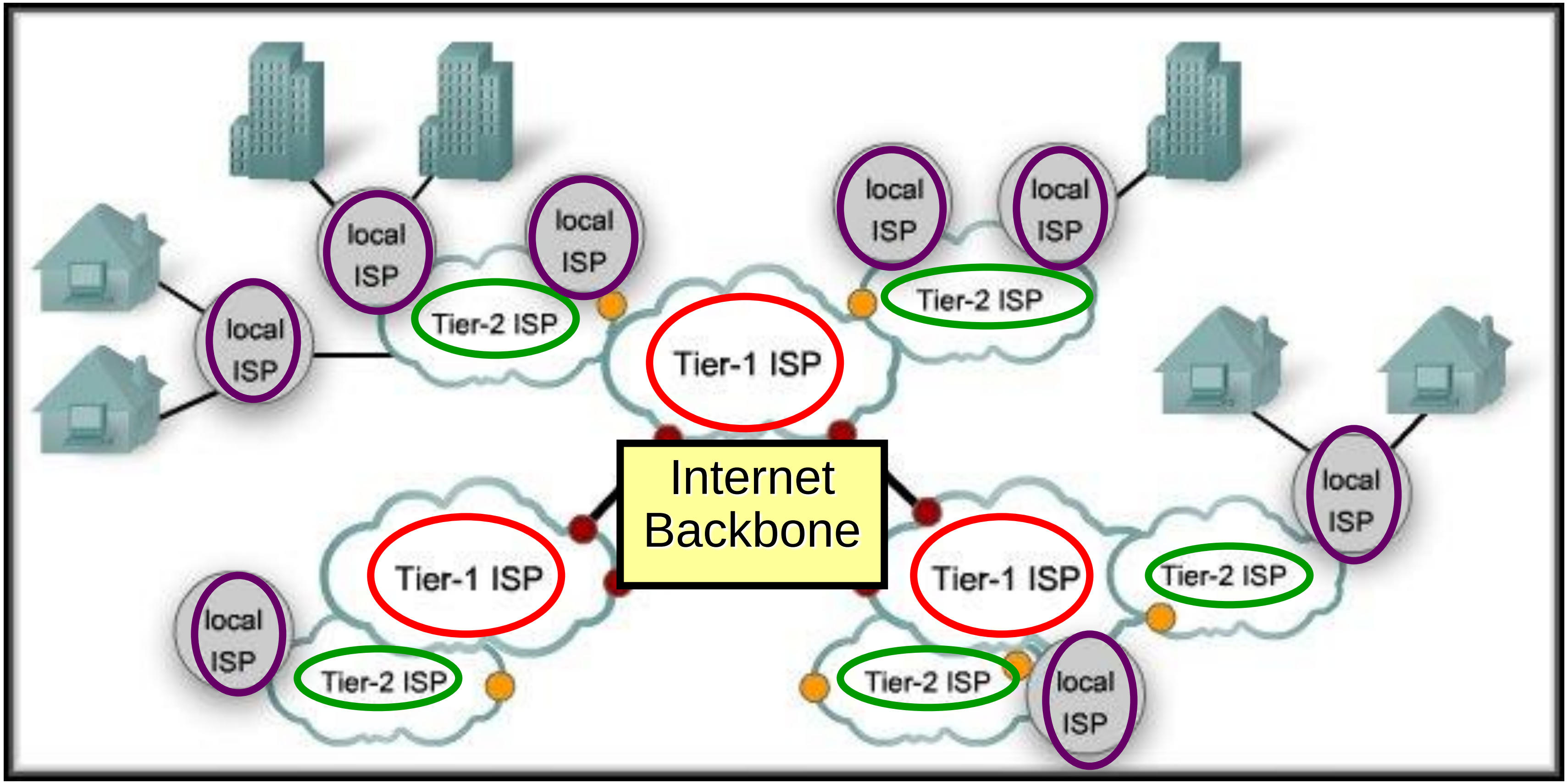
Tier 2: Pay Tier 1 providers for



Tier 3: Provide service to end users and are usually connected through Tier 2 providers.

Network Architecture ➔ Scalability

- Additional providers can be added relatively easily with no disruption of current services. *THAT is scalability!*



Network Architecture → QoS

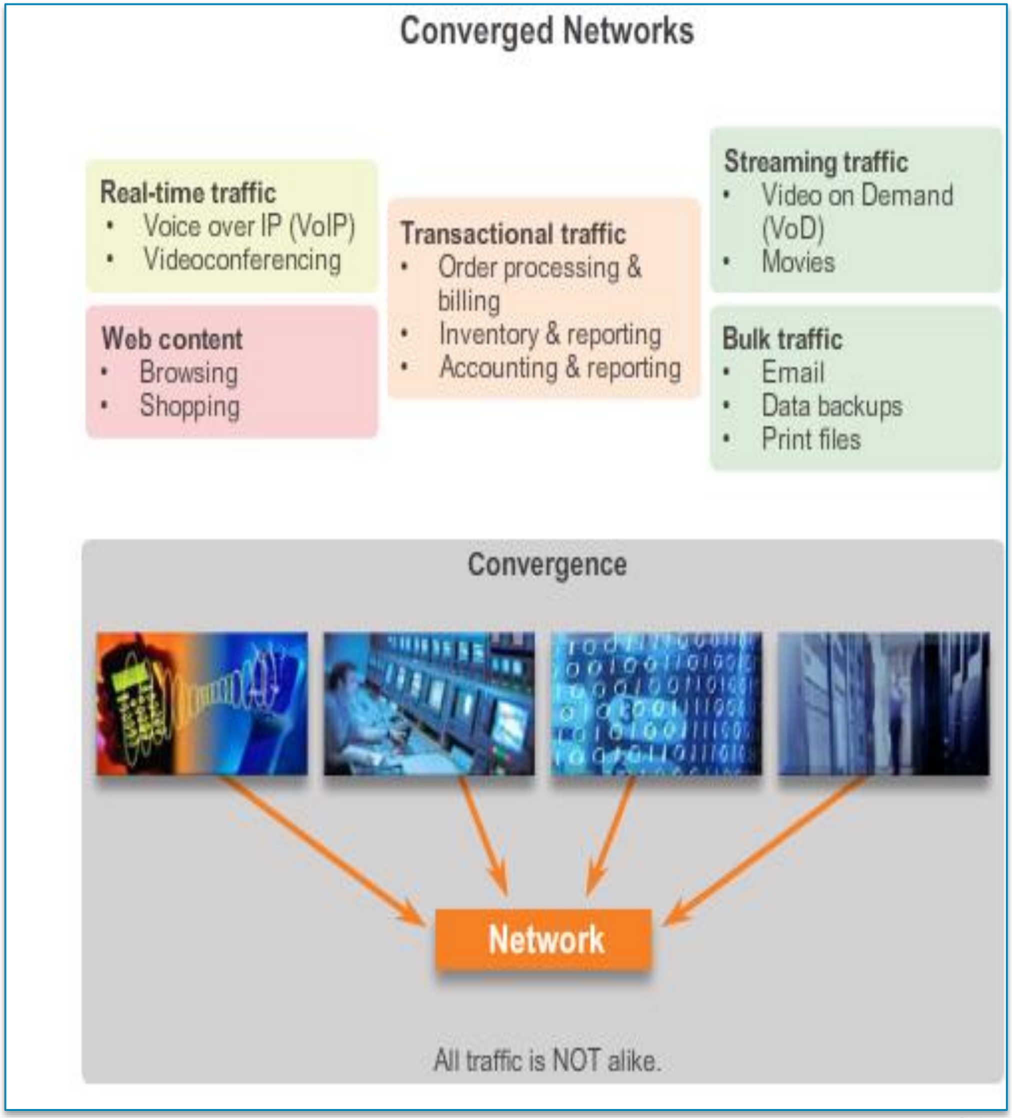
- Networks must provide secure, predictable, measurable, and, at times, guaranteed services.

- Networks also need mechanisms to manage congested network traffic.

- Congestion is caused when the demand on the network resources exceeds the available capacity.

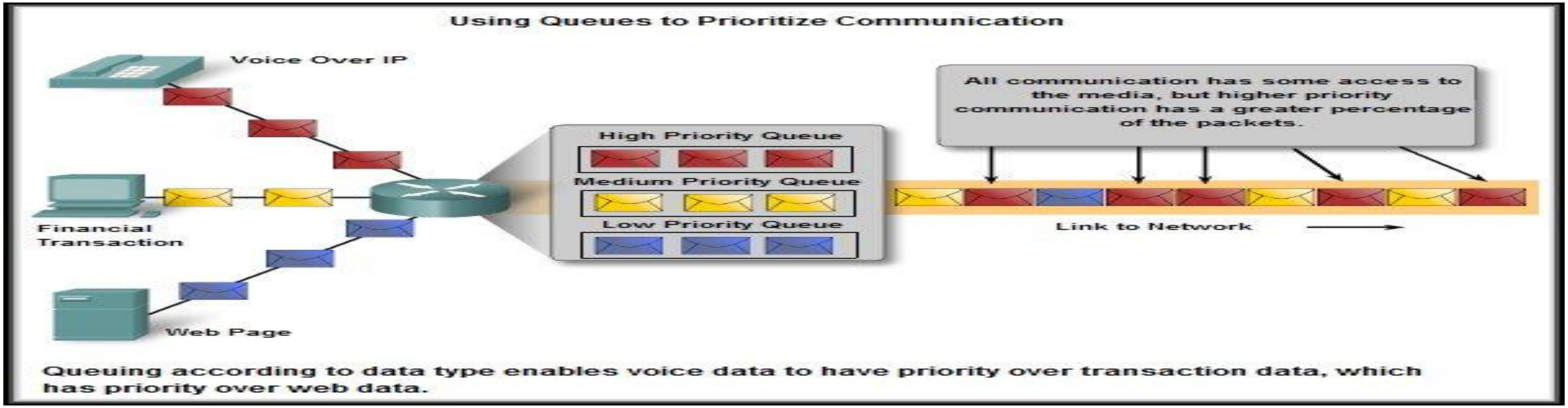
- In most cases, when the volume of packets is greater than what can be transported across the network, devices queue the packets in memory until resources become available to transmit them.

- Queuing packets causes delay. If the number of packets to be queued continues to increase, the memory queues fill up and packets are dropped.



Network Architecture ➔ QoS

- Ensuring QoS requires a set of techniques to manage the utilization of network resources.
- In order to maintain a high quality of service for applications that require it, it is necessary to prioritize which types of data packets must be delivered at the expense of other types of packets that can be delayed or dropped.



Using Queues to Prioritize Communication

All communication has some access to the media, but higher priority communication has a greater percentage of the packets.

Queuing according to data type enables voice data to have priority over transaction data, which has priority over web data.

• Examples of priority decisions for an organization might include:

❑**Time-sensitive communication** - increase priority for services like telephony or video distribution.

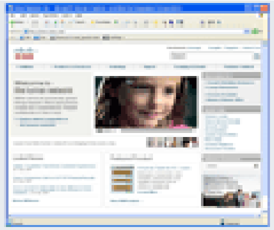
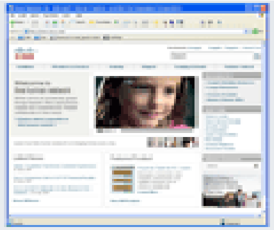
❑**Non time-sensitive communication** - decrease priority for web page retrieval or email.

❑**High importance to organization -** increase priority for production control or business transaction data.

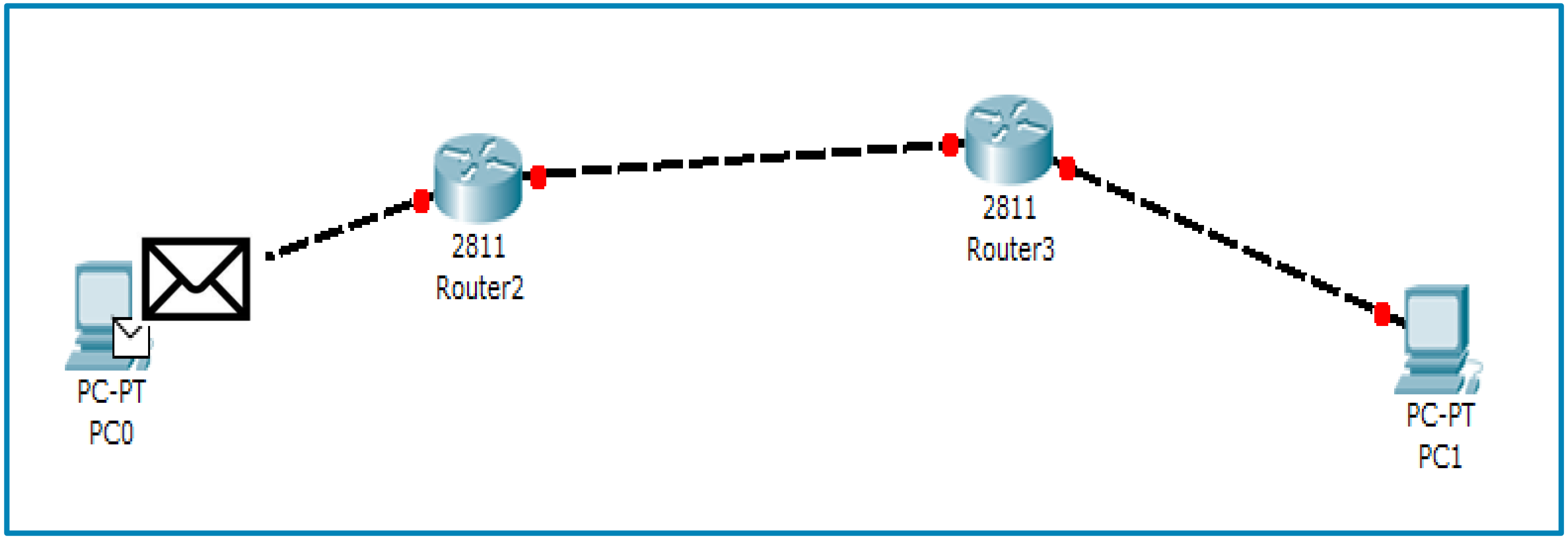
❑**Undesirable communication** - decrease priority or block unwanted activity, like peer-to-peer file sharing or live entertainment.

Network Architecture → QoS

Quality of Service Matters

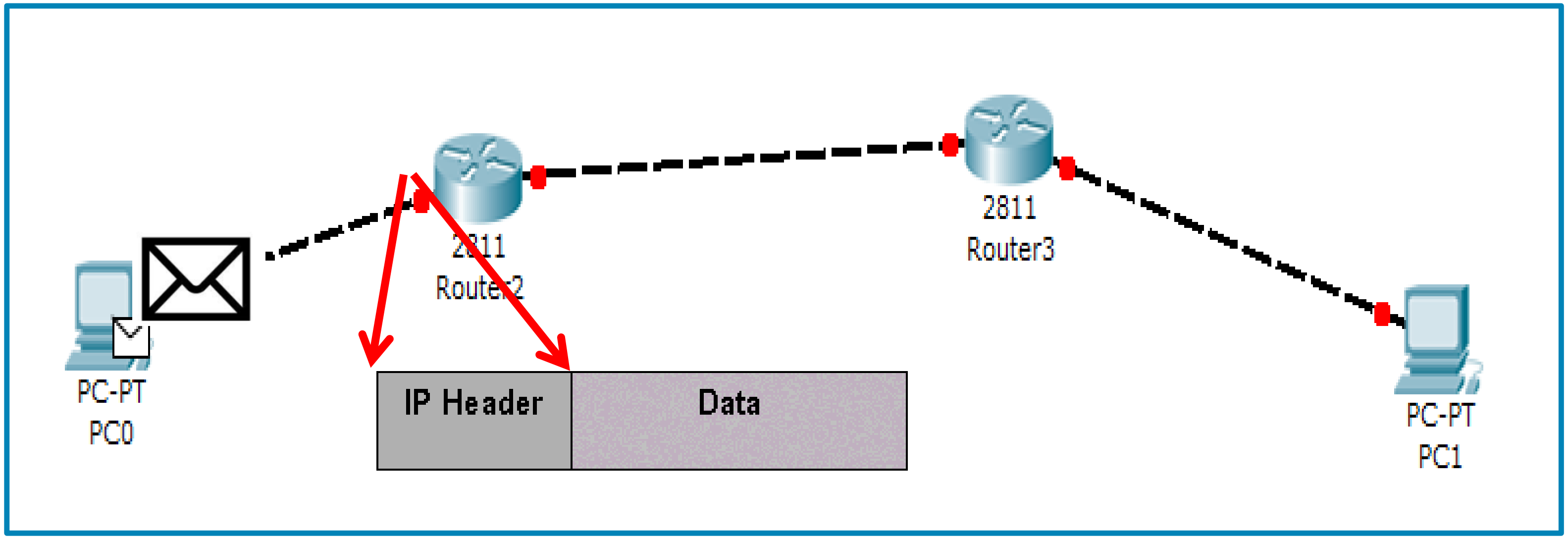
Communication Type	Without QoS	With QoS
Streaming video or audio	 Choppy picture starts and stops.	 Clear, continuous service.
Vital Transactions	Time : Price 02:14:05 $1.54 Just one second earlier...	Time : Price 02:14:04 $1.52 The price may be better.
Downloading web pages (often lower priority)	 Web pages arrive a bit later...	 But the end result is identical.

Delay, loss, and throughput in Packet switched networks



As a packet travels from one node (host or router) to the subsequent node (host or router) along this path, the packet suffers from several different types of delays at *each node along the path.*

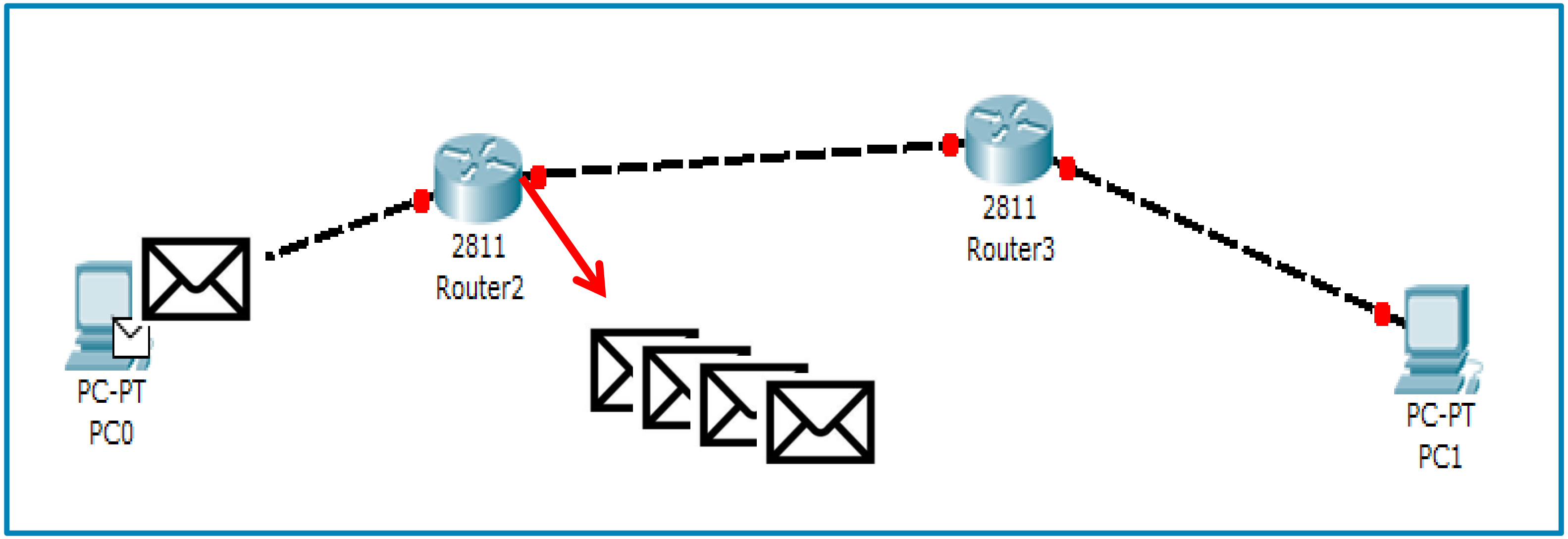
Delay, loss, and throughput in Packet switched networks



Processing Delay

- is the time required to examine the packet's header and determine where to direct the packet.
- The processing delay can also include other factors, such as the time needed to check for bit-level errors in the packet that occurred in transmitting the packet.

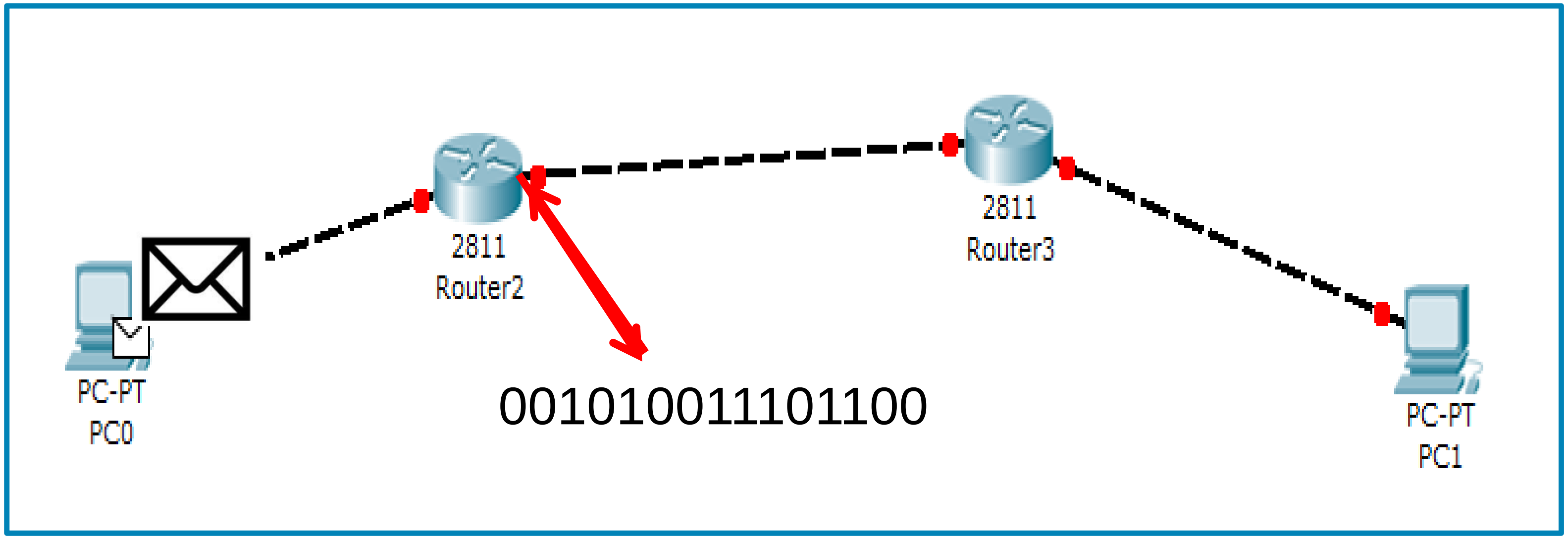
Delay, loss, and throughput in Packet switched networks



Queuing Delay

- After the nodal processing, the router directs the packet to the queue that precedes the link to second router.
- At the queue, the packet experiences a **queuing delay as it waits to be transmitted onto the link.**
- **The queuing delay of a specific** packet will depend on the number of other, earlier-arriving packets that are queued and waiting for transmission across the link;

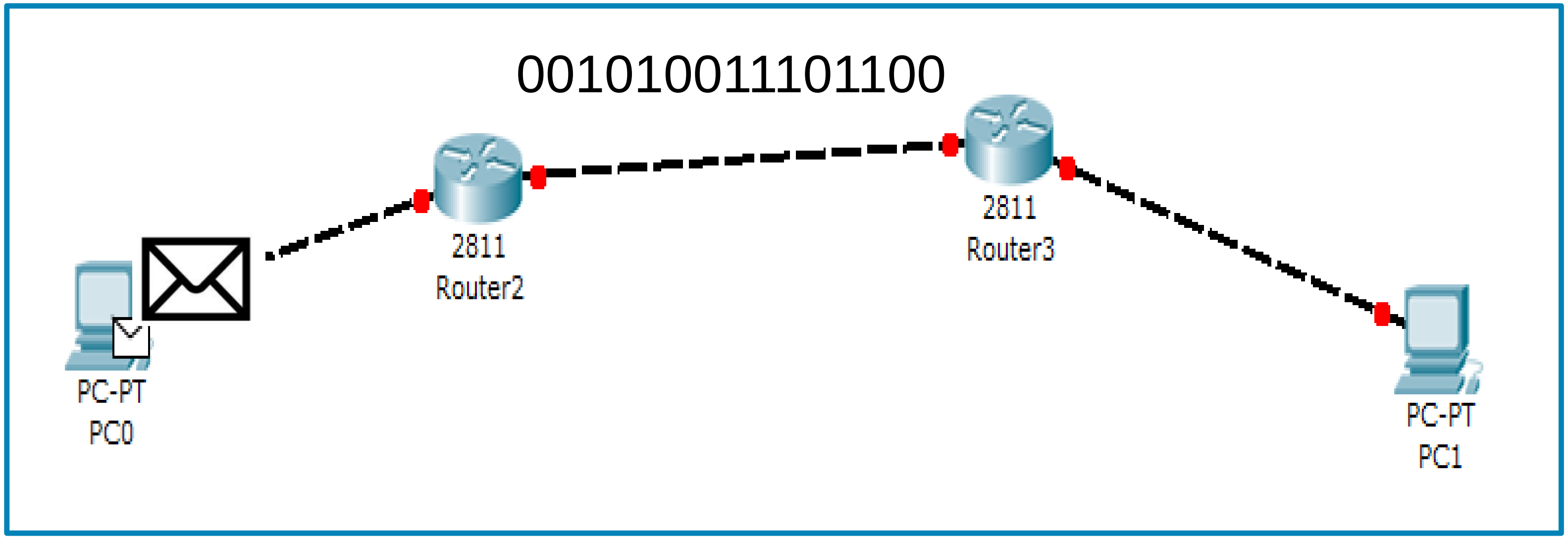
Delay, loss, and throughput in Packet switched networks



Transmission Delay

- Assuming that packets are transmitted in a first-come-first-served manner, as is common in packet-switched networks, our packet can be transmitted only after all the packets that have arrived before it have been transmitted.
- Denote the length of the packet by *L bits and denote the transmission rate of the link (from router A to router B)* by *R bits/sec.*
- *The rate R is determined by transmission rate of the link to router B (For example, for a 10* Mbps Ethernet link).
- *The* **transmission delay (also called the store-and-forward delay, as discussed in Section 1.4) is L/R.**
- **This is** the amount of time required to transmit all of the packet's bits into the link.

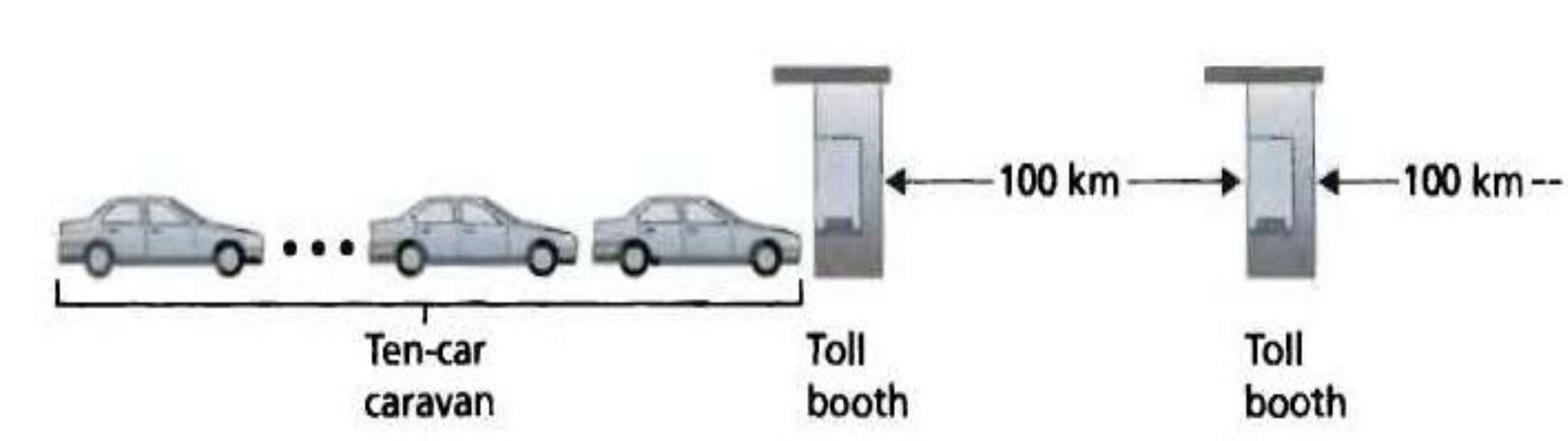
Delay, loss, and throughput in Packet switched networks



Propagation Delay

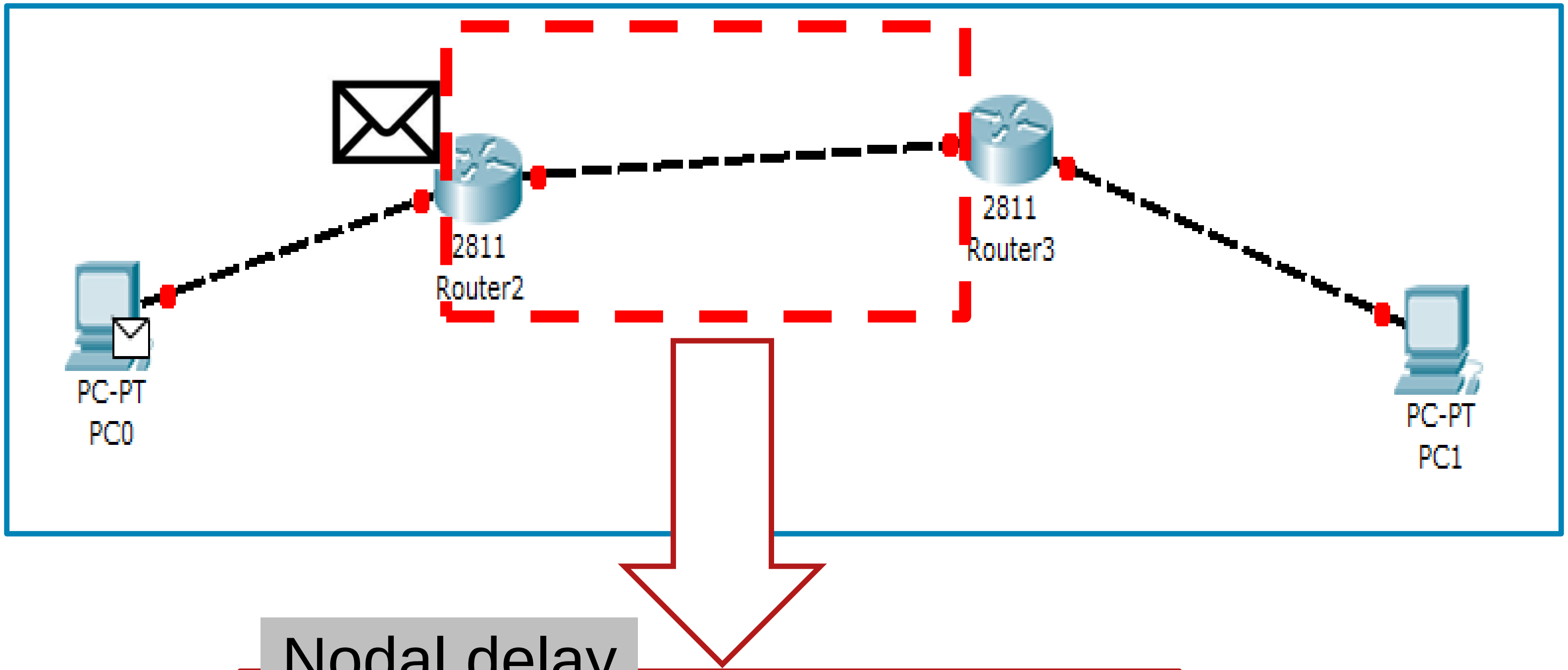
- is the time required to propagate from the beginning of the link to destination at the end of the link.
- The bit propagates at the propagation speed of the link.
- The propagation delay is the distance between two nodes divided by the propagation speed.
- That is, the propagation delay is *d/s, where d is the distance* between node A and node B and *s is the propagation speed of the link.*

Comparing Transmission and propagation Delay



- The time required for the tollbooth to push the entire caravan onto the highway is (10 cars)/(5 cars/minute) = 2 minutes.
- This time is analogous to the transmission delay in a router.
- The time required for a car to travel from the exit of one tollbooth to the next tollbooth is 100 km/(100 km/hour) = 1 hour.
- This time is analogous to propagation delay.
- Therefore, the time from when the caravan is stored in front of a tollbooth until the caravan is stored in front of the next tollbooth is the sum of transmission delay and propagation delay—in this example, 62 minutes.

Delay, loss, and throughput in Packet switched networks



Nodal delay

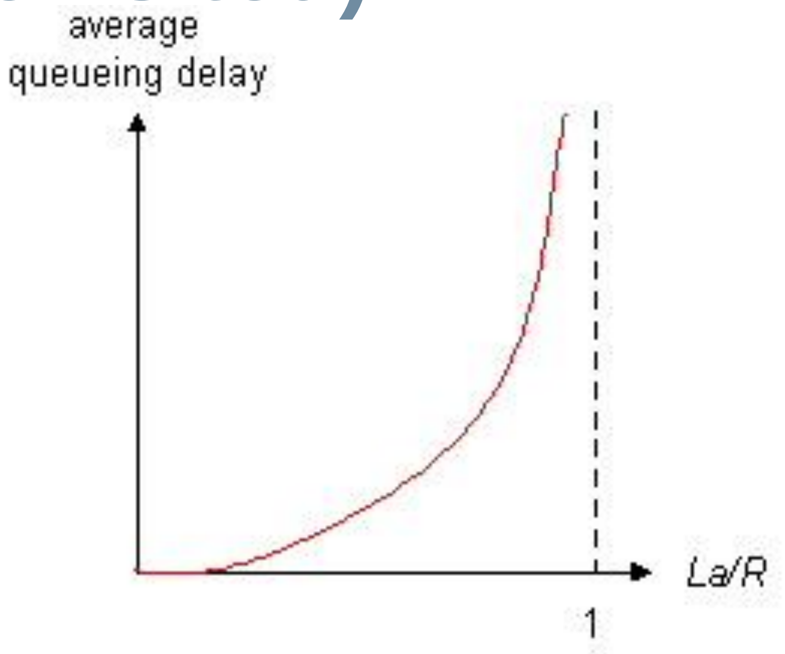
$$d_{\text{nodal}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}$$

d_{prop} = propagation delay
a few microsecs to hundreds of msecs

Queueing delay (revisited)

- R=link bandwidth (bps)
- L=packet length (bits)
- a=average packet arrival rate

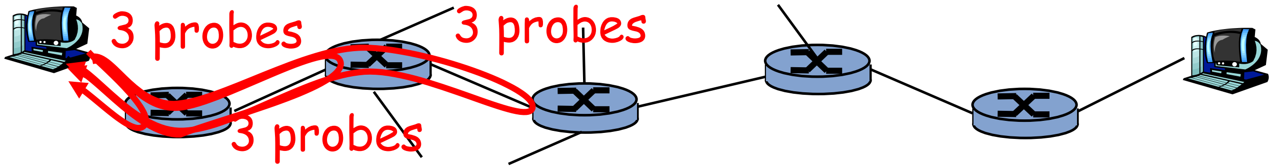
traffic intensity = La/R



- ❑ La/R ~ 0: average queueing delay small
- ❑ La/R -> 1: delays become large
- ❑ La/R > 1: more "work" arriving than can be serviced, average delay infinite!

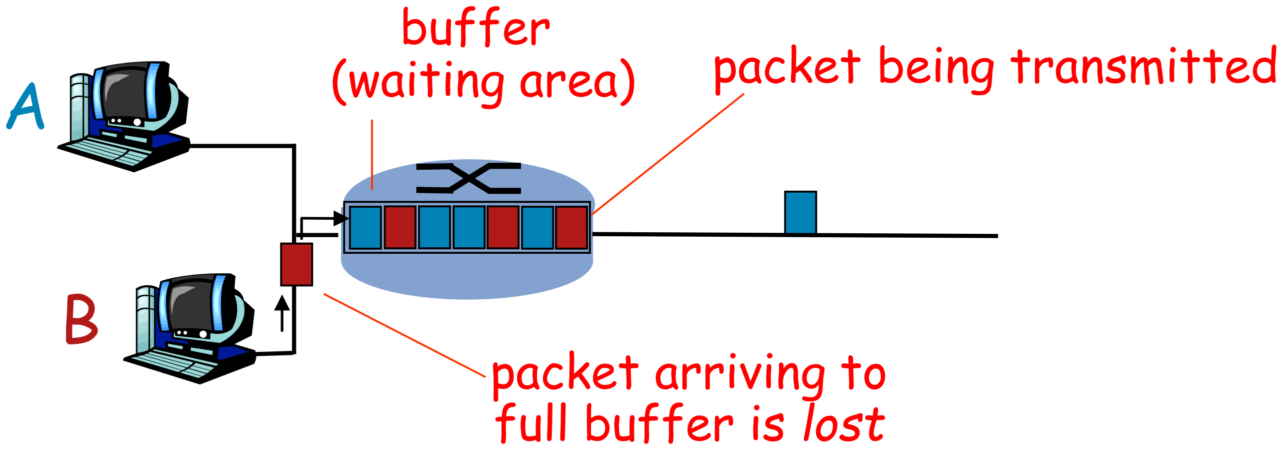
“Real” Internet delays and routes

- What do “real” Internet delay & loss look like?
- `Traceroute` program: provides delay measurement from source to router along end-end Internet path towards destination. For all *i:*
  - ✓sends three packets that will reach router *i* on path towards destination
  - ✓router *i* will return packets to sender
  - ✓sender times interval between transmission and reply.



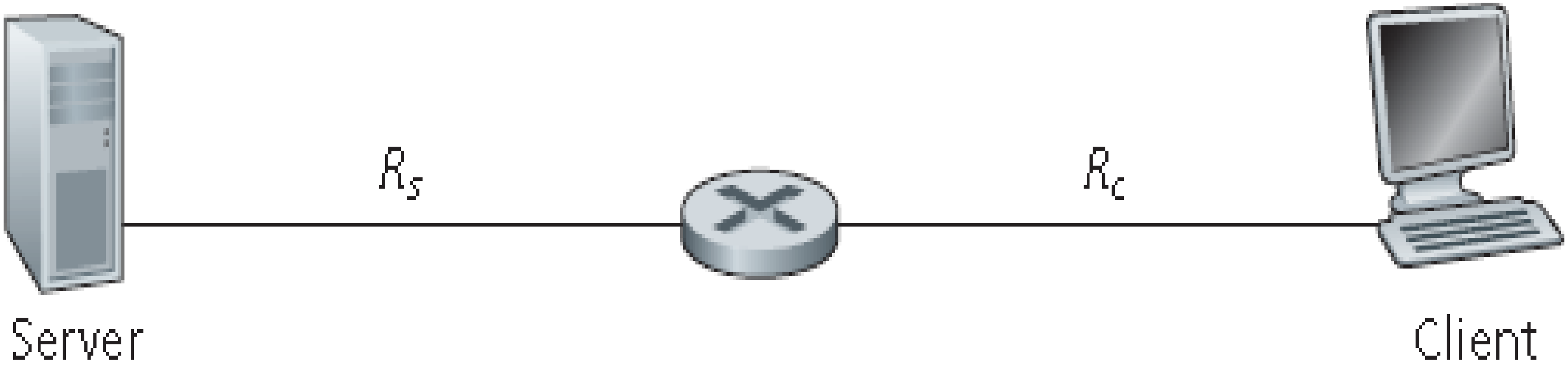
Packet loss

- queue (aka buffer) preceding link in buffer has finite capacity
- packet arriving to full queue dropped (aka lost)
- lost packet may be retransmitted by previous node, by source end system, or not at all



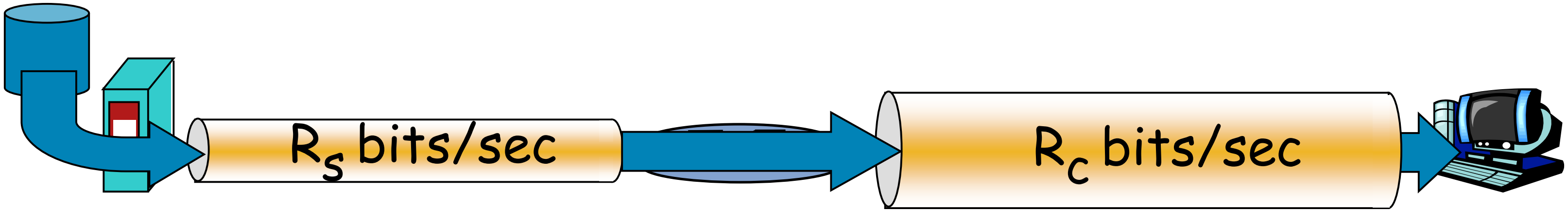
Throughput

- *throughput:* rate (bits/time unit) at which bits transferred between sender/receiver
  - *instantaneous:* rate at given point in time
  - *average:* rate over longer period of time



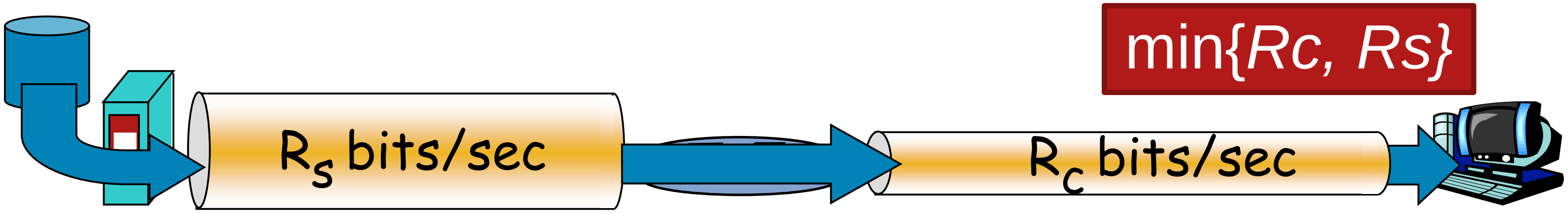
Throughput (more)

- $R_s < R_c$ What is average end-end throughput?



- □ $R_s > R_c$ What is average end-end throughput?

min{*Rc, Rs*}



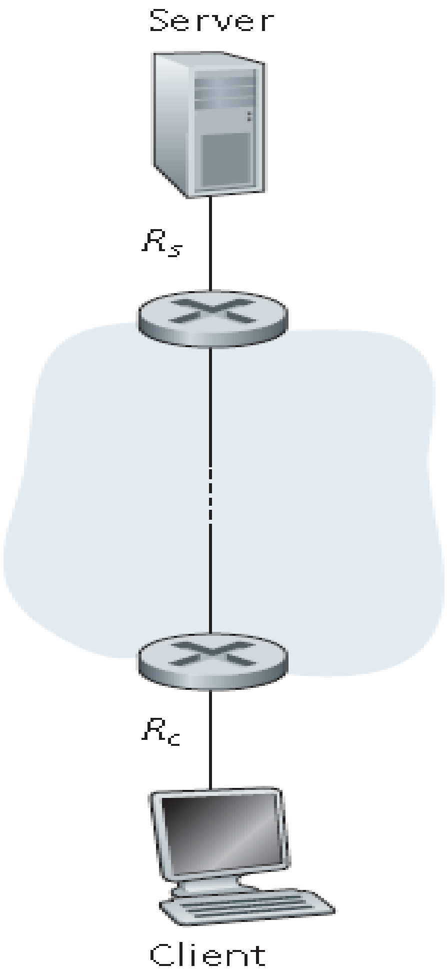
bottleneck link

link on end-end path that constrains end-end throughput

Throughput (more)

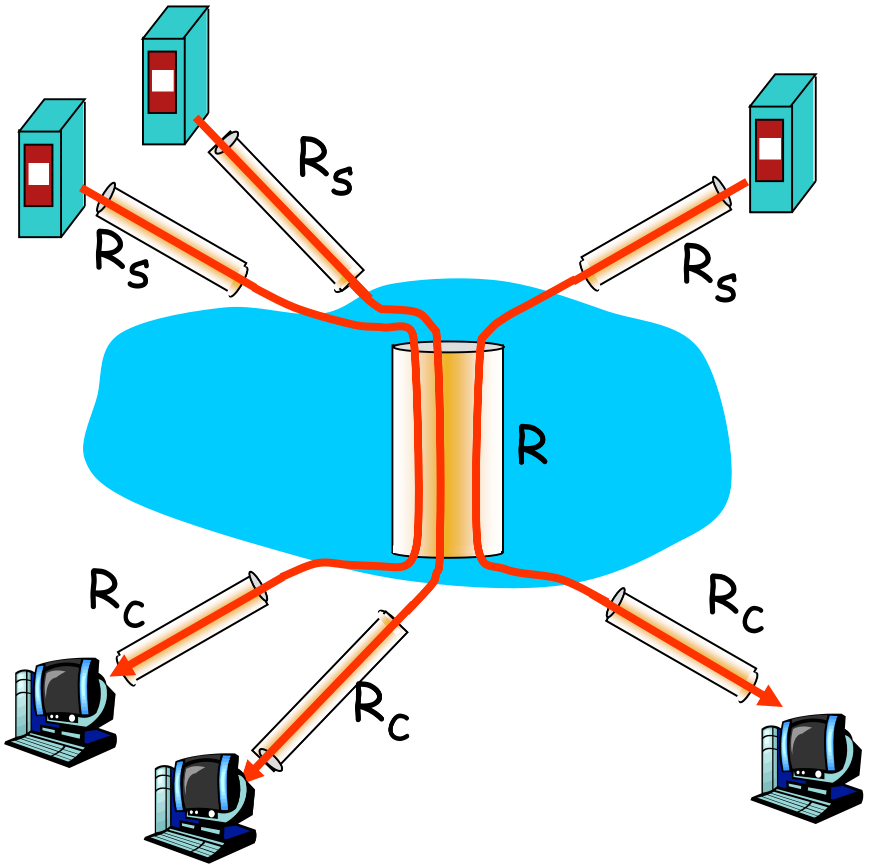
- Suppose you are downloading an MP3 file of *L= 32 million bits,*
- *the server has a transmission rate of Rs = 2 Mbps,*
- you have an access link of *Rc = 1 Mbps.*
- *What is the time needed to download the file?*

- *The time needed to transfer the file is* then 32 seconds.
- These expressions for throughput and transfer time are only approximations, as they do not account for store-and-forward and processing delays as well as protocol issues.



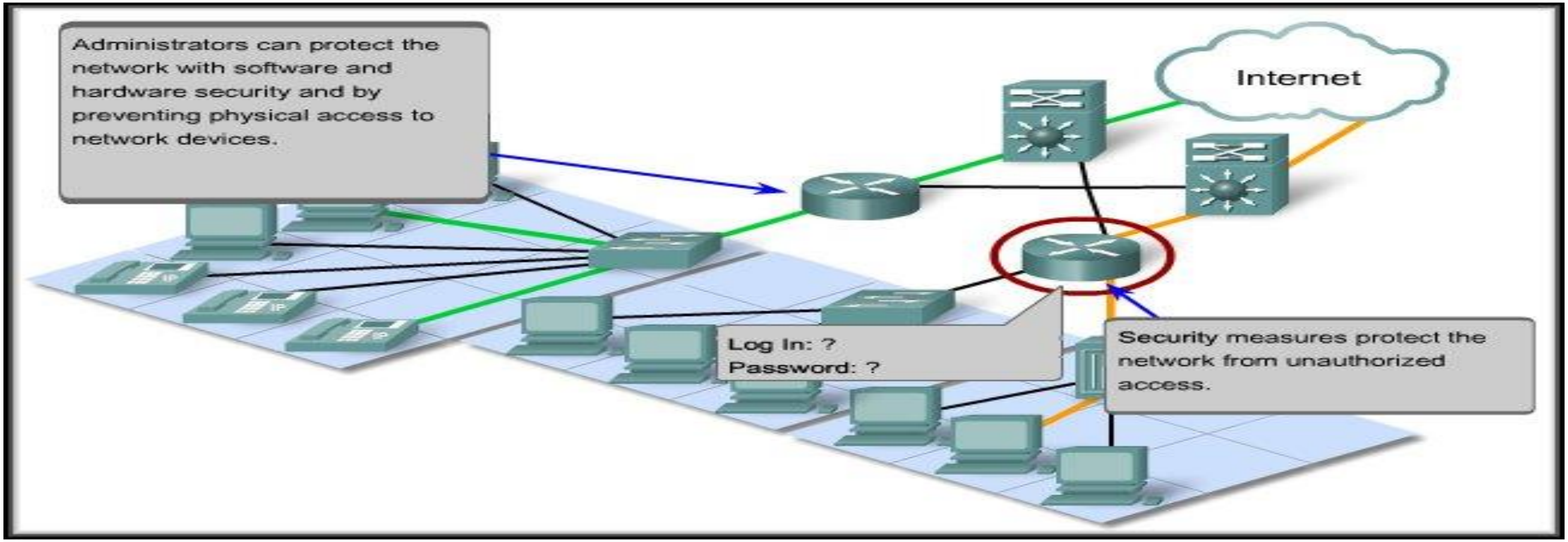
Throughput: Internet scenario

- per-connection end-end throughput: min(R_c,R_s,R/10)
- in practice: R_c or R_s is often bottleneck



10 connections (fairly) share backbone bottleneck link R bits/sec

Network Architecture ➔ Security

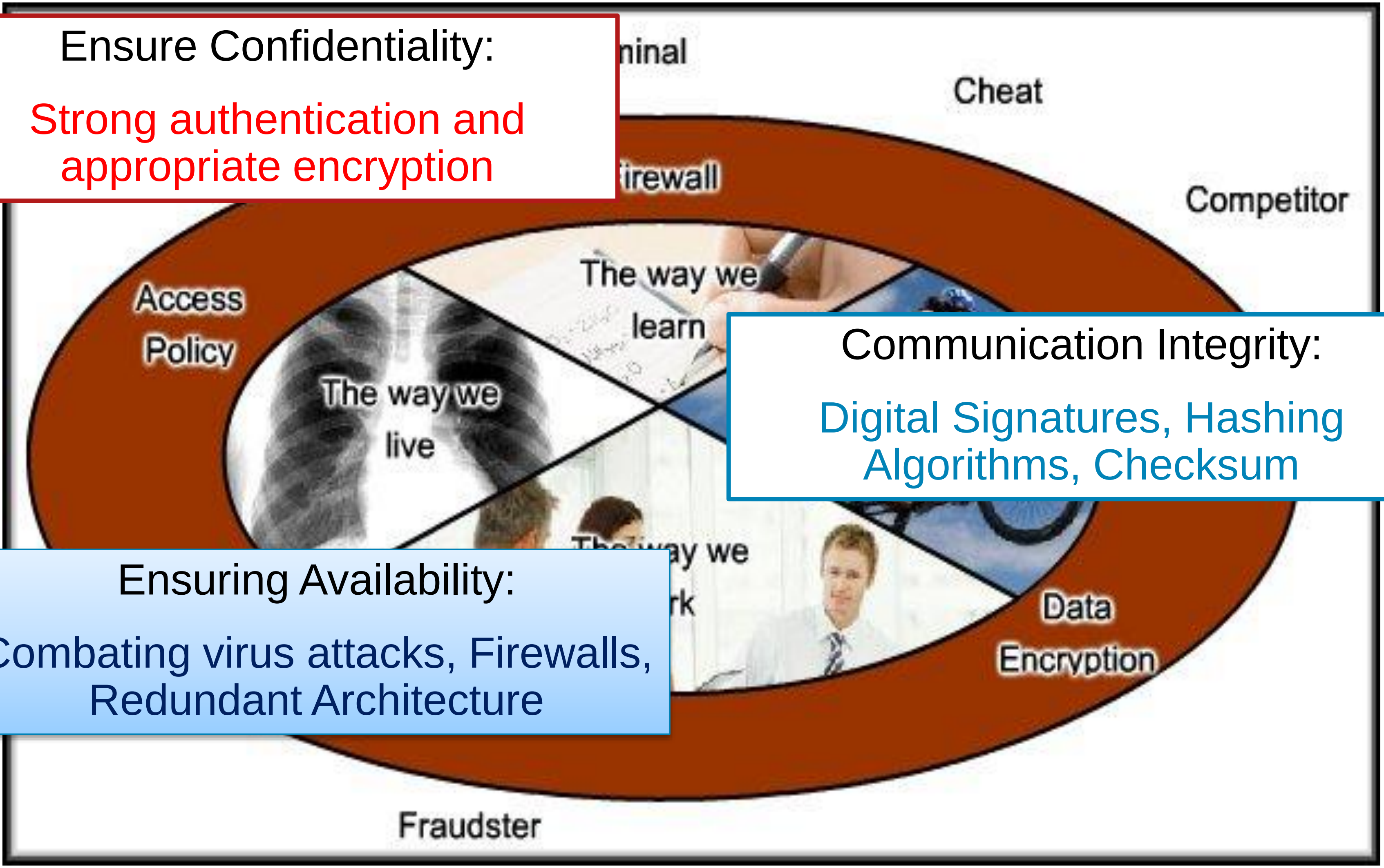

Administrators can protect the network with software and hardware security and by preventing physical access to network devices.
Internet
Log In: ?
Password: ?
Security measures protect the network from unauthorized access.

- There are two types of network security concerns that must be addressed to prevent serious consequences: network infrastructure security and content security.

Securing a network infrastructure includes the physical securing of devices that provide network connectivity and preventing unauthorized access to the management software that resides on them.

Content security refers to protecting the information contained within the packets being transmitted over the network and the information stored on network attached devices.

Network Architecture → Security



Ensure Confidentiality:

Strong authentication and appropriate encryption

Communication Integrity:

Digital Signatures, Hashing Algorithms, Checksum

Ensuring Availability:

Combating virus attacks, Firewalls, Redundant Architecture

Using Layered Models

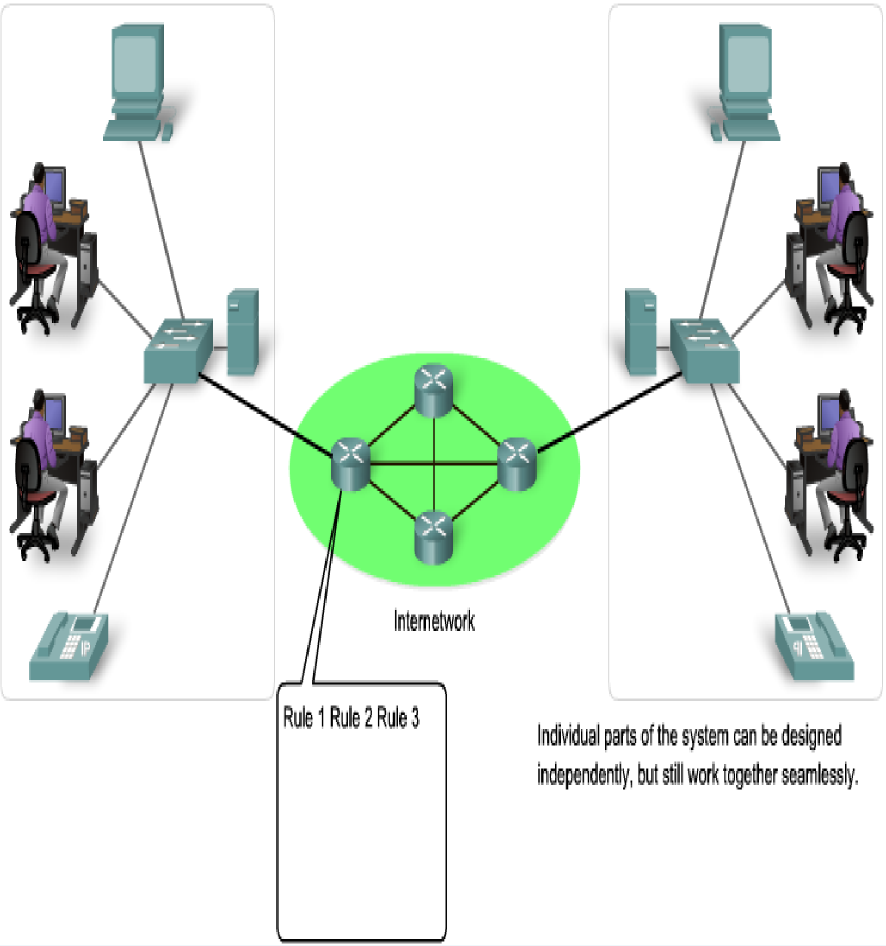
Objective

- To visualize the interaction between various protocols, it is common to use a layered model.
- A layered model depicts the operation of the protocols occurring within each layer, as well as the interaction with the layers above and below it.

Benefits

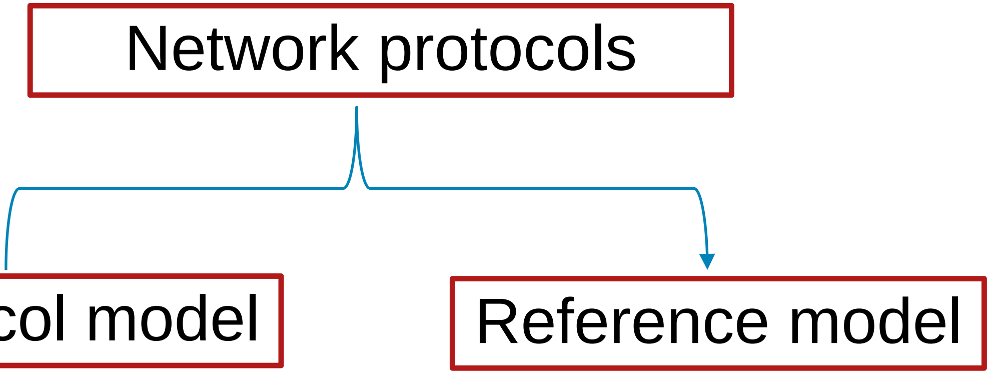
- Assists in protocol design, because protocols that operate at a specific layer have defined information that they act upon and a defined interface to the layers above and below.
- Fosters competition because products from different vendors can work together.
- Prevents technology or capability changes in one layer from affecting other layers above and below.
- Provides a common language to describe networking functions and capabilities.

Using a layered model helps in the design of complex, multi-use, multi-vendor networks.



Individual parts of the system can be designed independently, but still work together seamlessly.

Using Layered Models



- Matches the structure of a particular protocol suite.

- The hierarchical set of related protocols in a suite typically represents all the functionality required to interface the human network with the data network.
- Ex: TCP/IP

- A reference model is **<u>not</u>** intended to be an implementation specification or to provide a sufficient level of detail to define precisely the services of the network architecture.

- The primary purpose of a reference model is to aid in clearer understanding of the functions and process involved.

- Ex: OSI model

OSI Model

- To address the problem of networks increasing in size and in number, the International Organization for Standardization (ISO) researched many network schemes and recognized that there was a need to create a network model that would help network builders implement networks that could communicate and work together and therefore, released the OSI reference model in 1984.

Don’t Get Confused.

ISO - International Organization for Standardization

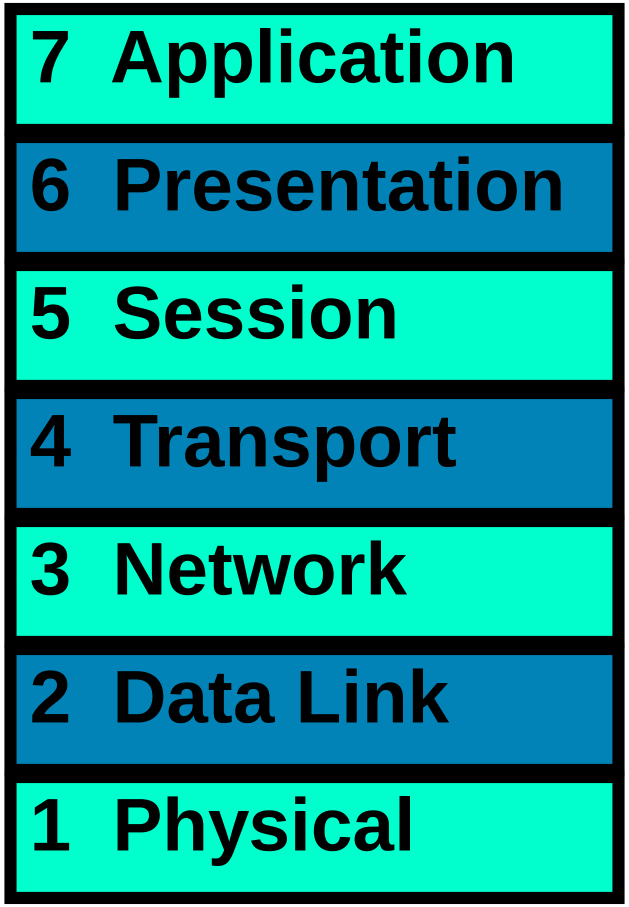
OSI - Open System Interconnection

IOS - Internetwork Operating System

The ISO created the OSI to make the IOS more efficient. The “ISO” acronym is correct as shown.

To avoid confusion, some people say “International Standard Organization.”

The OSI Reference Model



7 Application

6 Presentation

5 Session

4 Transport

3 Network

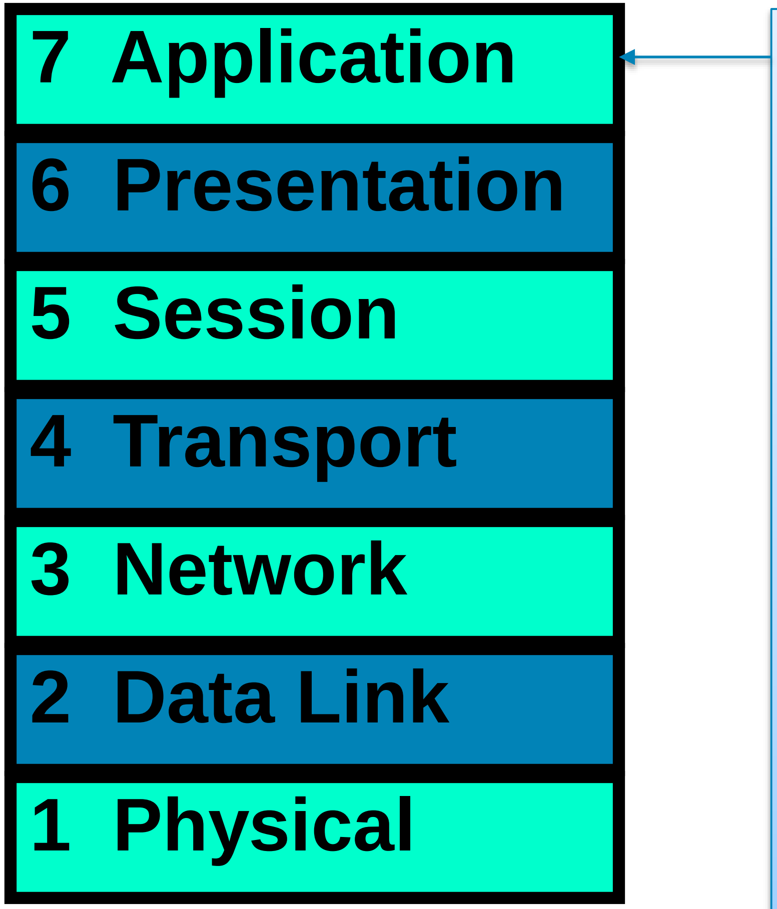
2 Data Link

1 Physical

The OSI Model will be used throughout your entire networking career!

Memorize it!

Layer 7 - The Application Layer



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

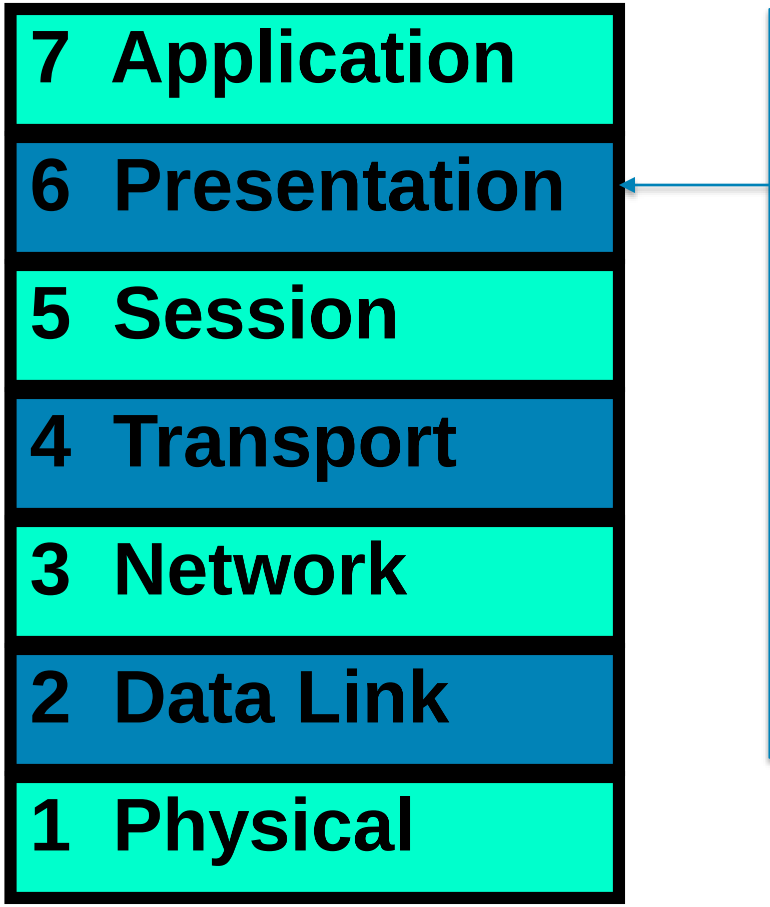
This layer deal with networking applications.

Examples:

- Email
- Web browsers

PDU – Protocol Data Unit
(Application Data)

Layer 6 - The Presentation Layer



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

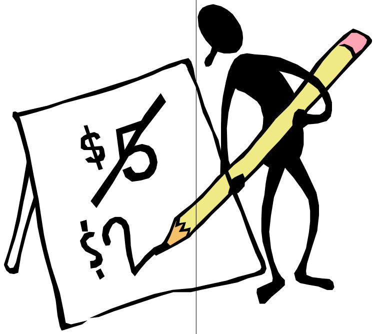
This layer is responsible for presenting the data in the required format which may include:

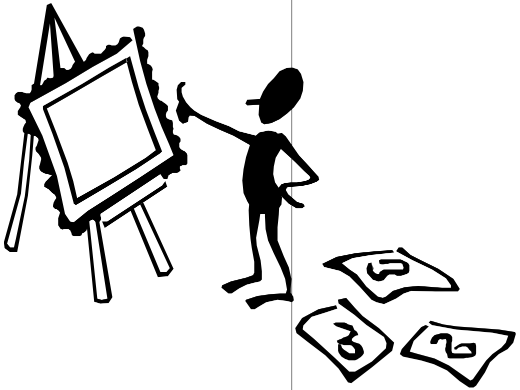
- Encryption
- Compression

PDU - Formatted Data

This image cannot currently be displayed.

Presentation Layer





- Text
- Data

  ASCII
  EBCDIC
  Encrypted

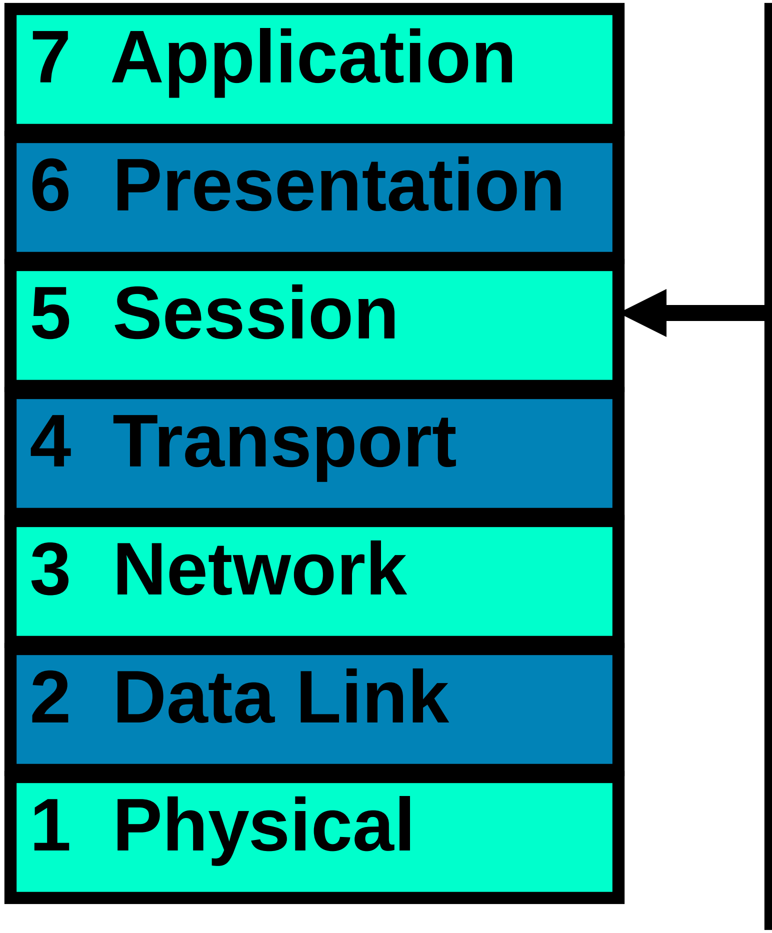
- Sound
- Video

  MIDI
  MPEG
  QuickTime

- Graphics
- Visual Images

  TIFF
  JPEG
  GIF

Layer 5 - The Session Layer



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

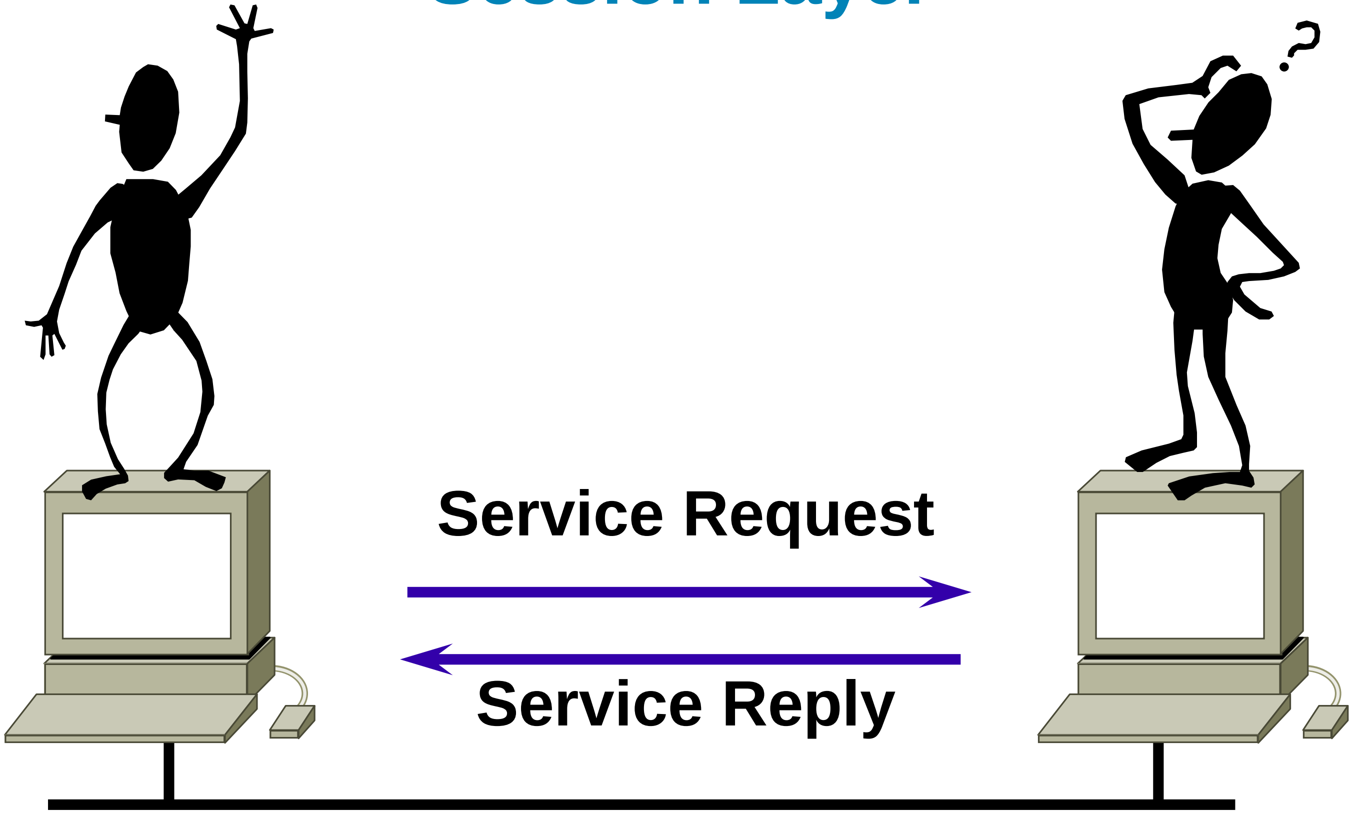
This layer establishes, manages, and terminates sessions between two communicating hosts.

Example:

- Client Software (Used for logging in)

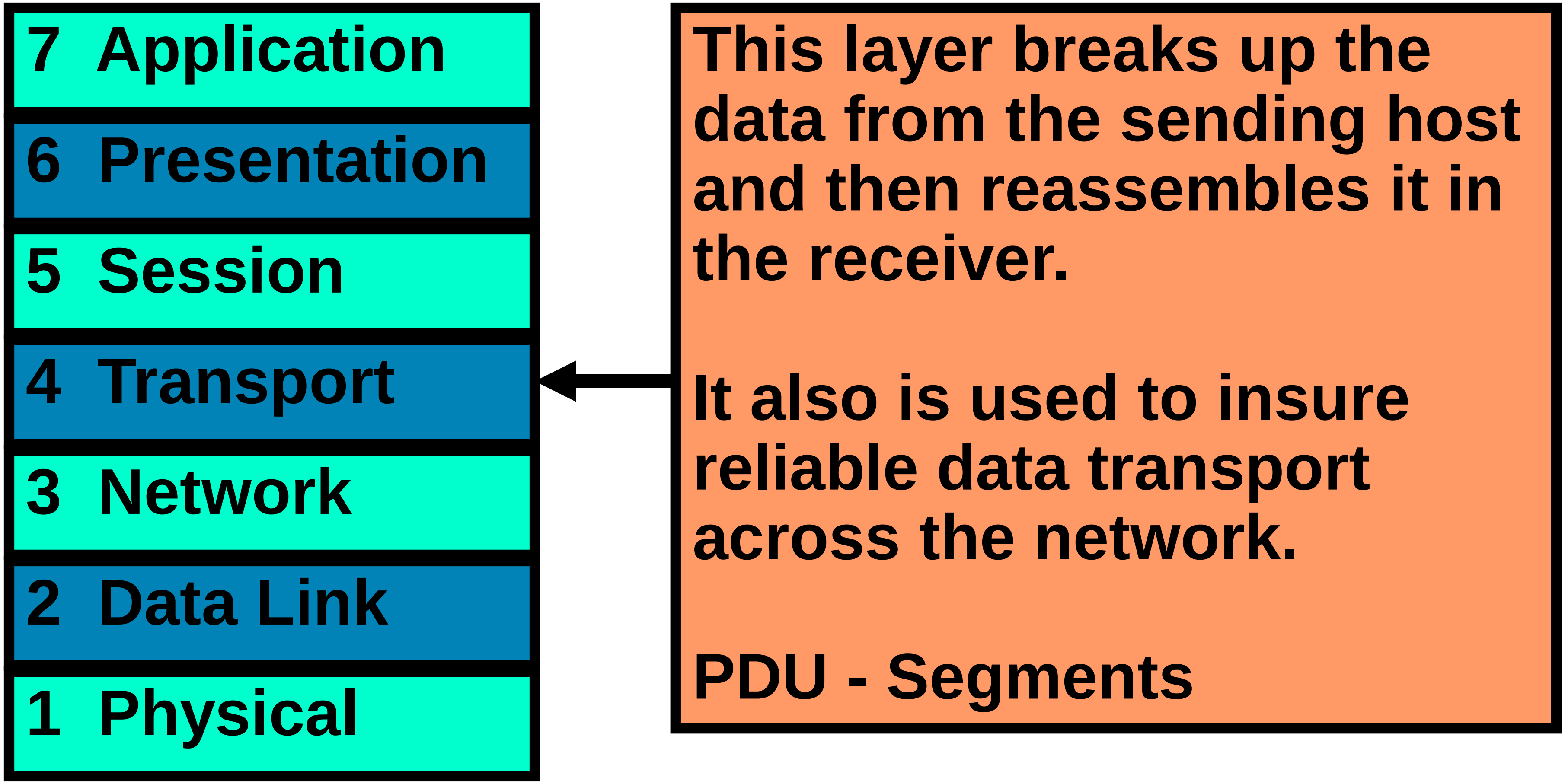
PDU - Formatted Data

Session Layer



Vocabulary of two processes

Layer 4 - The Transport Layer



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

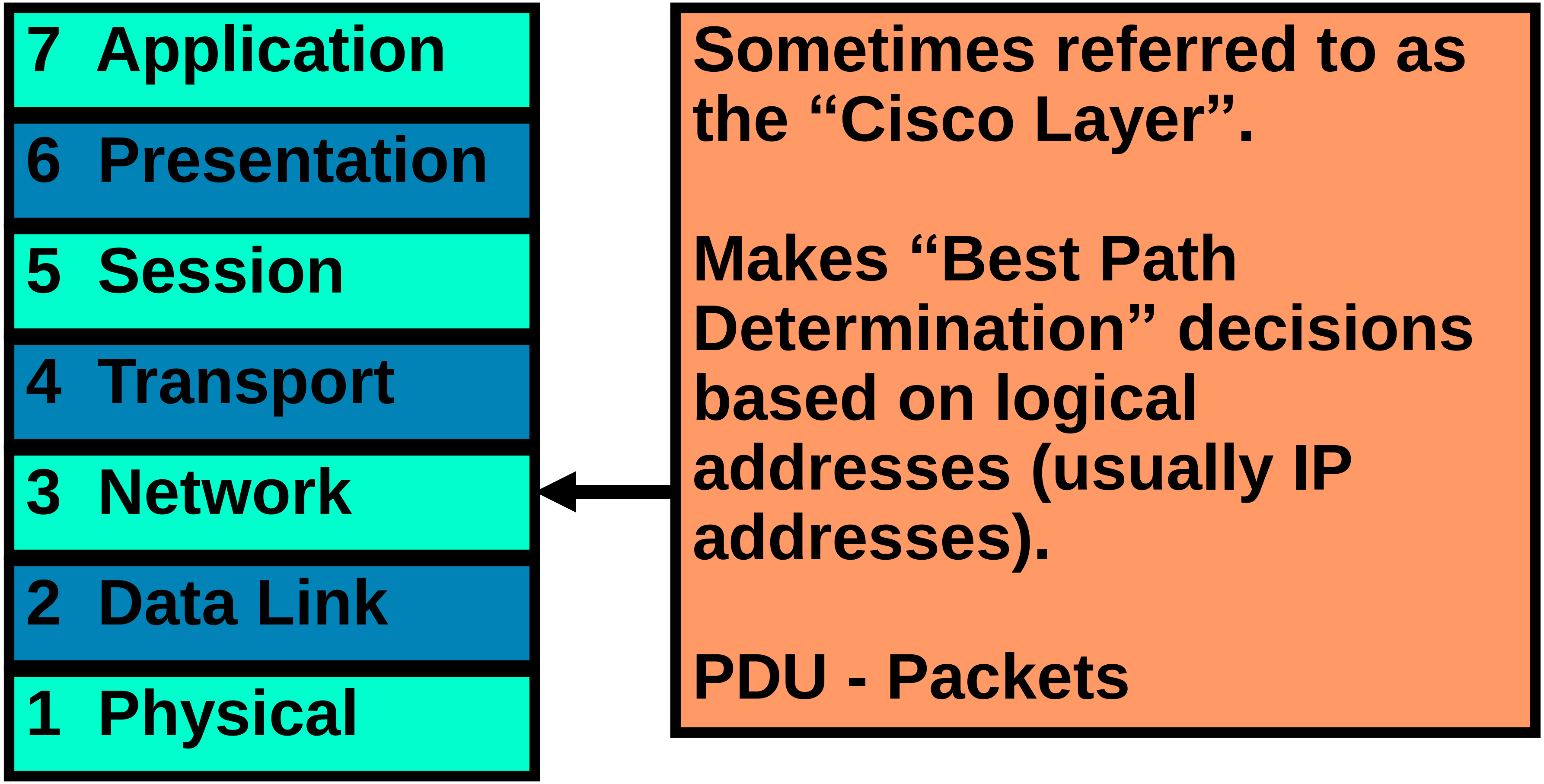
1 Physical

This layer breaks up the data from the sending host and then reassembles it in the receiver.

It also is used to insure reliable data transport across the network.

PDU - Segments

Layer 3 - The Network Layer



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

Sometimes referred to as the “Cisco Layer”.

Makes “Best Path Determination” decisions based on logical addresses (usually IP addresses).

PDU - Packets

3

Network Layer

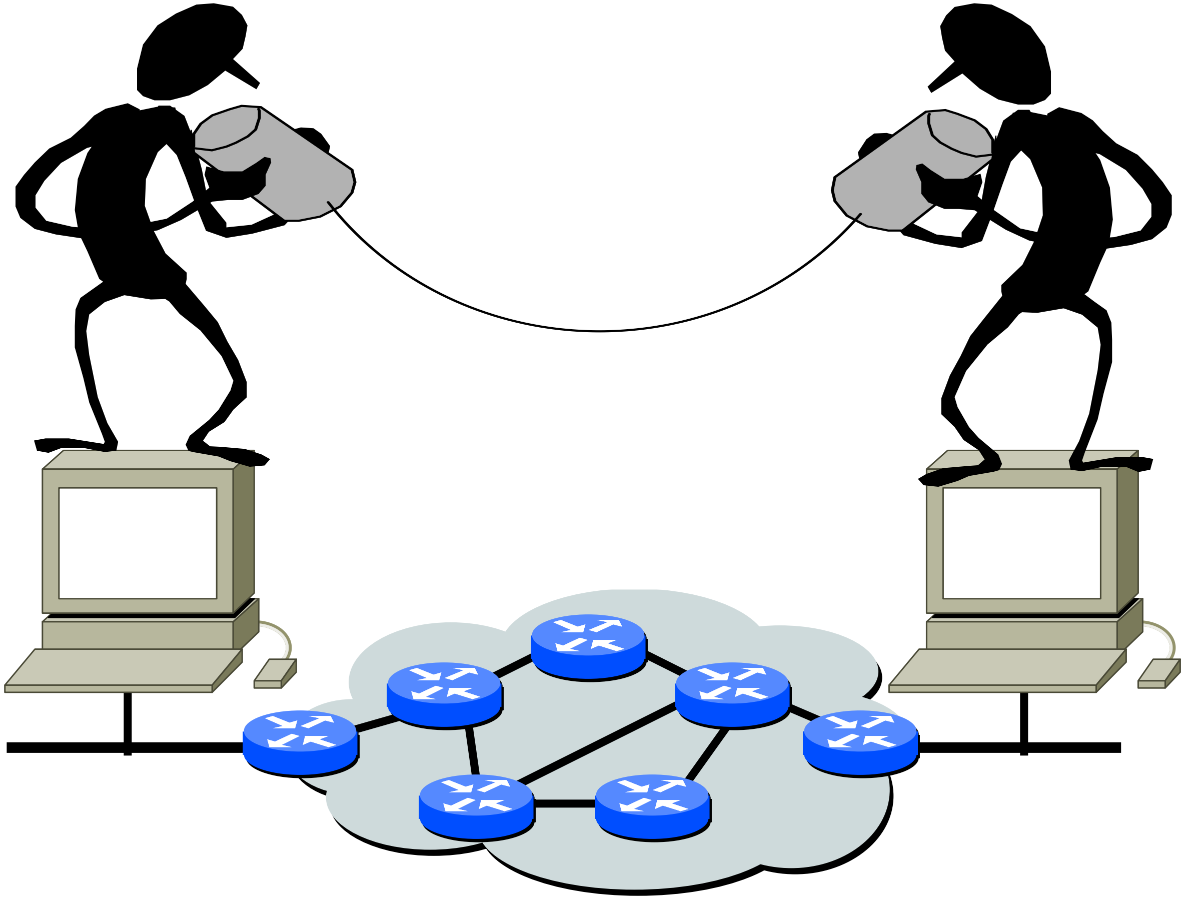
Path selection based on network addresses (e.g. IP addresses)

Segmentation and reassembly (block formation)

Error detection and possibly correction

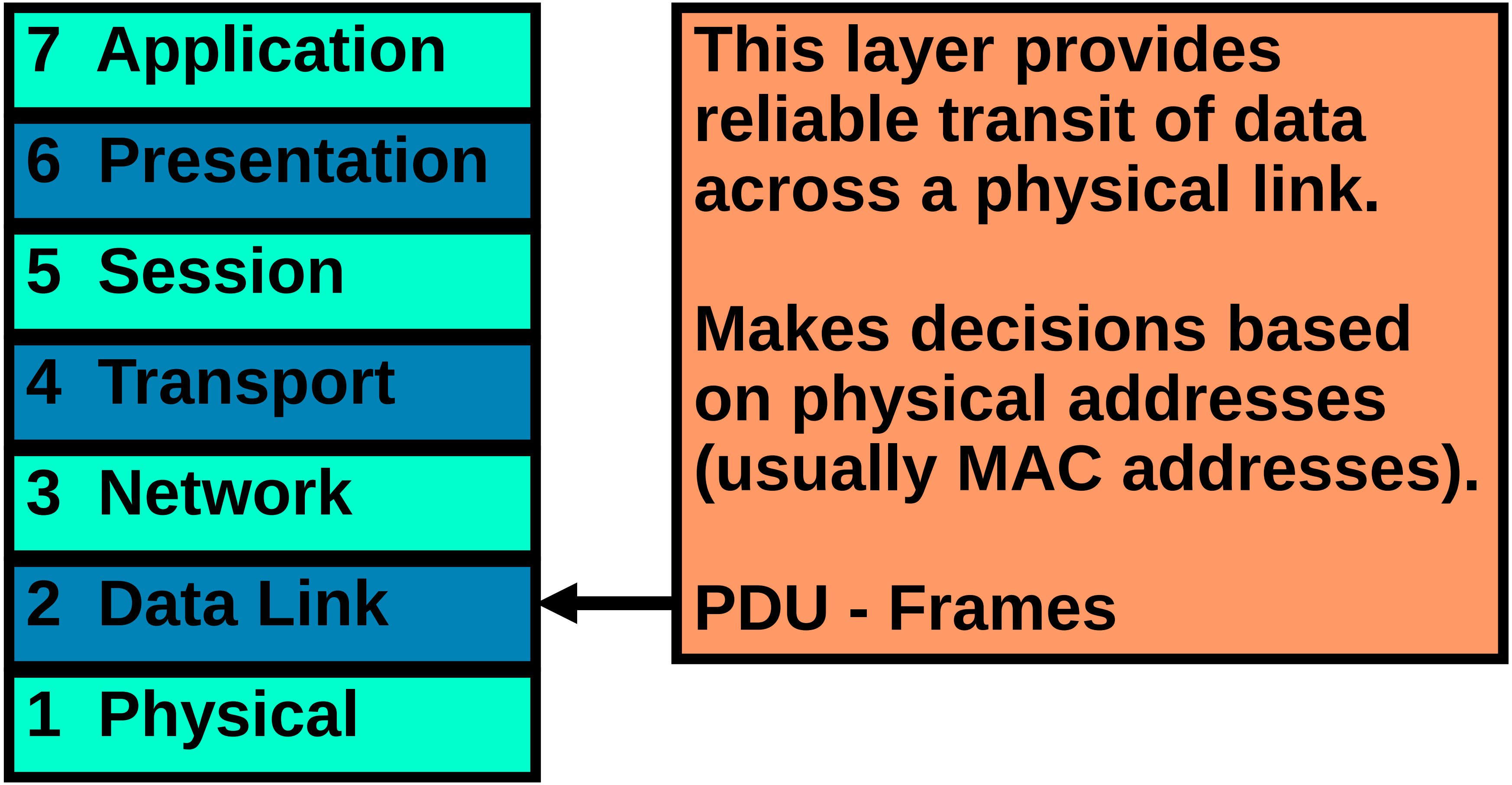
Possibly flow control at network level

Network Layer



Provision of the “best“ route

Layer 2 - The Data Link Layer



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

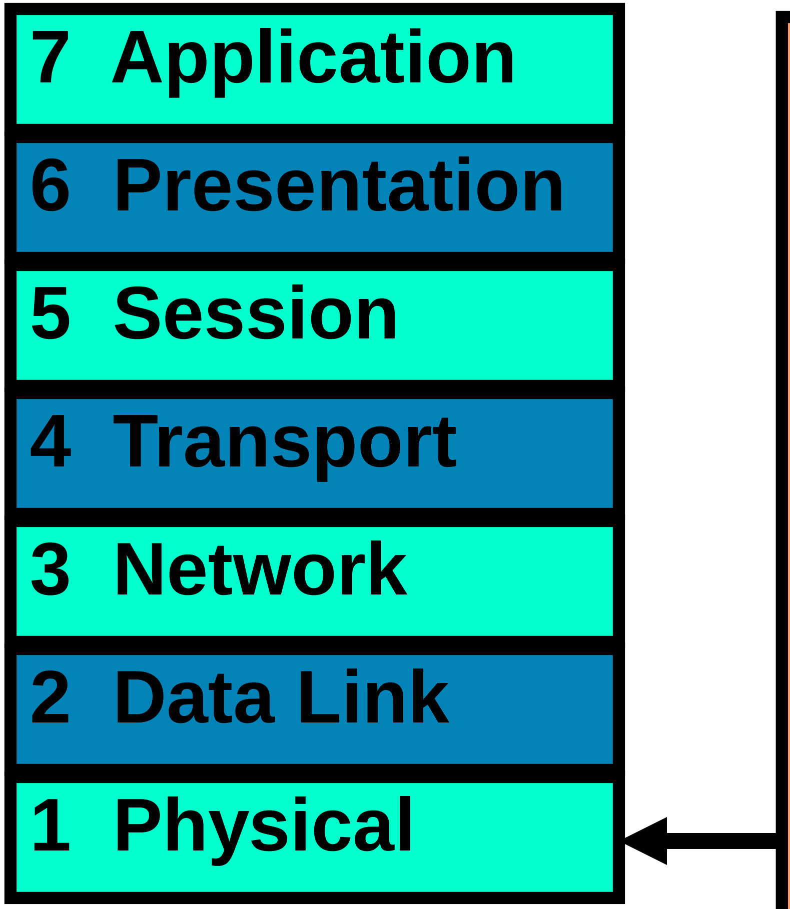
1 Physical

This layer provides reliable transit of data across a physical link.

Makes decisions based on physical addresses (usually MAC addresses).

PDU - Frames

Layer 1 - The Physical Layer



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

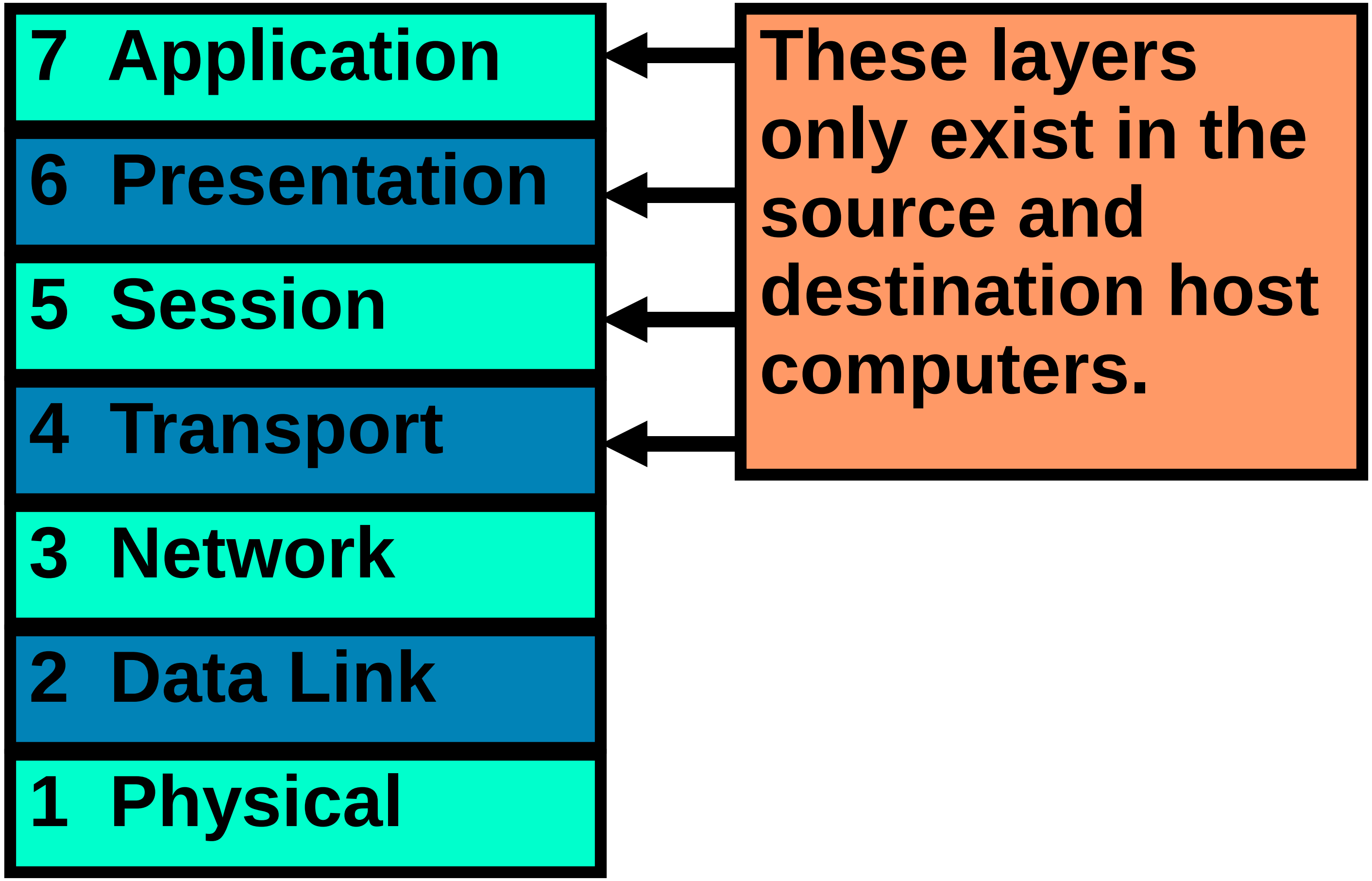
This is the physical media through which the data, represented as electronic signals, is sent from the source host to the destination host.

Examples:

- CAT5 (what we have)
- Coaxial (like cable TV)
- Fiber optic

PDU - Bits

Host Layers



7 Application

6 Presentation

5 Session

4 Transport

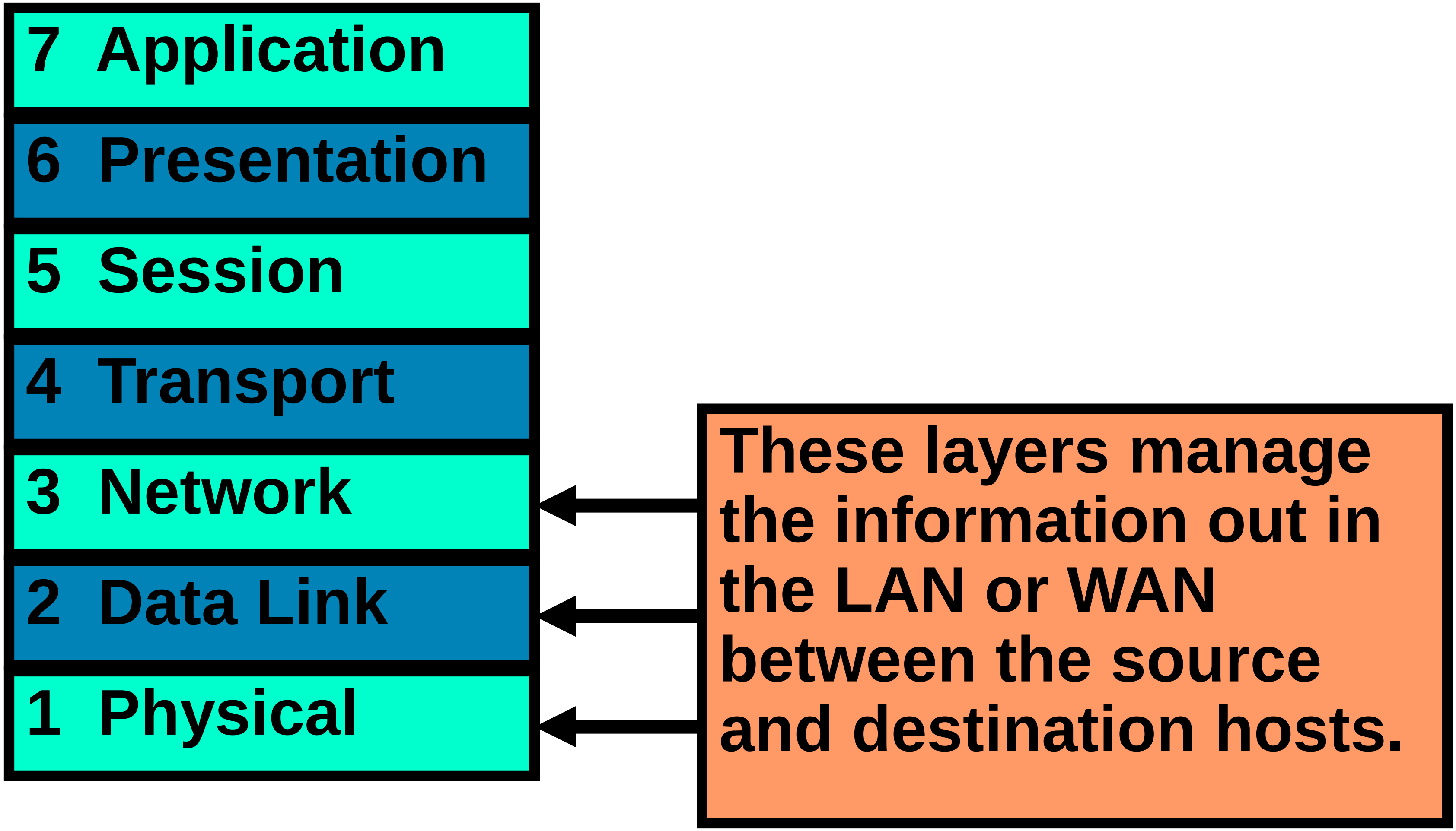
3 Network

2 Data Link

1 Physical

These layers only exist in the source and destination host computers.

Media Layers



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

These layers manage the information out in the LAN or WAN between the source and destination hosts.

TCP/IP Model

Although the OSI reference model is universally recognized, the historical and technical open standard of the Internet is Transmission Control Protocol / Internet Protocol (TCP/IP).

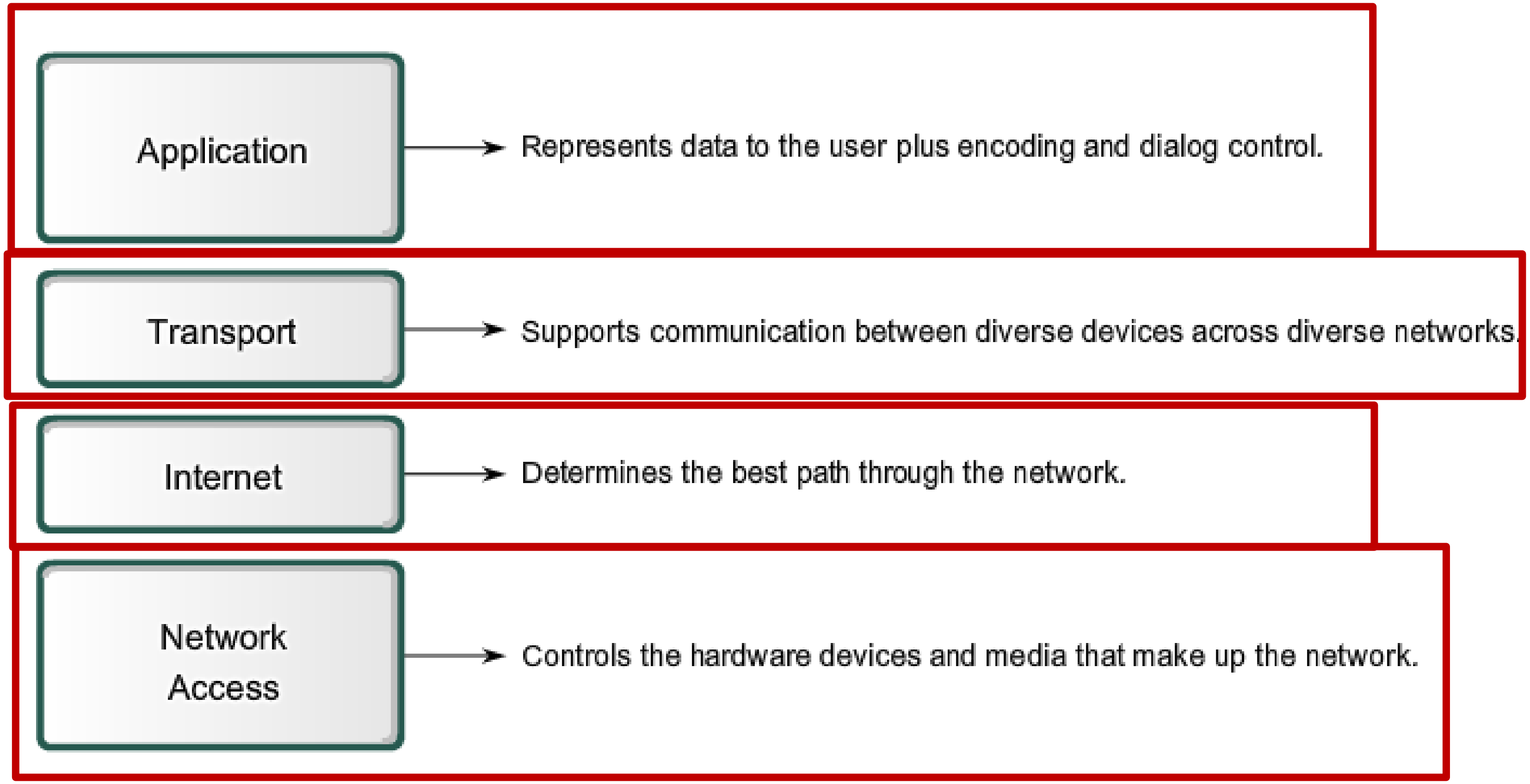
- The TCP/IP model describes the functionality of the protocols that make up the TCP/IP protocol suite.

The TCP/IP reference model and the TCP/IP protocol stack make data communication possible between any two computers, anywhere in the world, at nearly the speed of light.

The U.S. Department of Defense (DoD) created the TCP/IP reference model because it wanted a network that could survive any conditions, even a nuclear war.

TCP/IP Model

TCP/IP model



TCP/IP Model

Application → Represents data to the user plus encoding and dialog control.

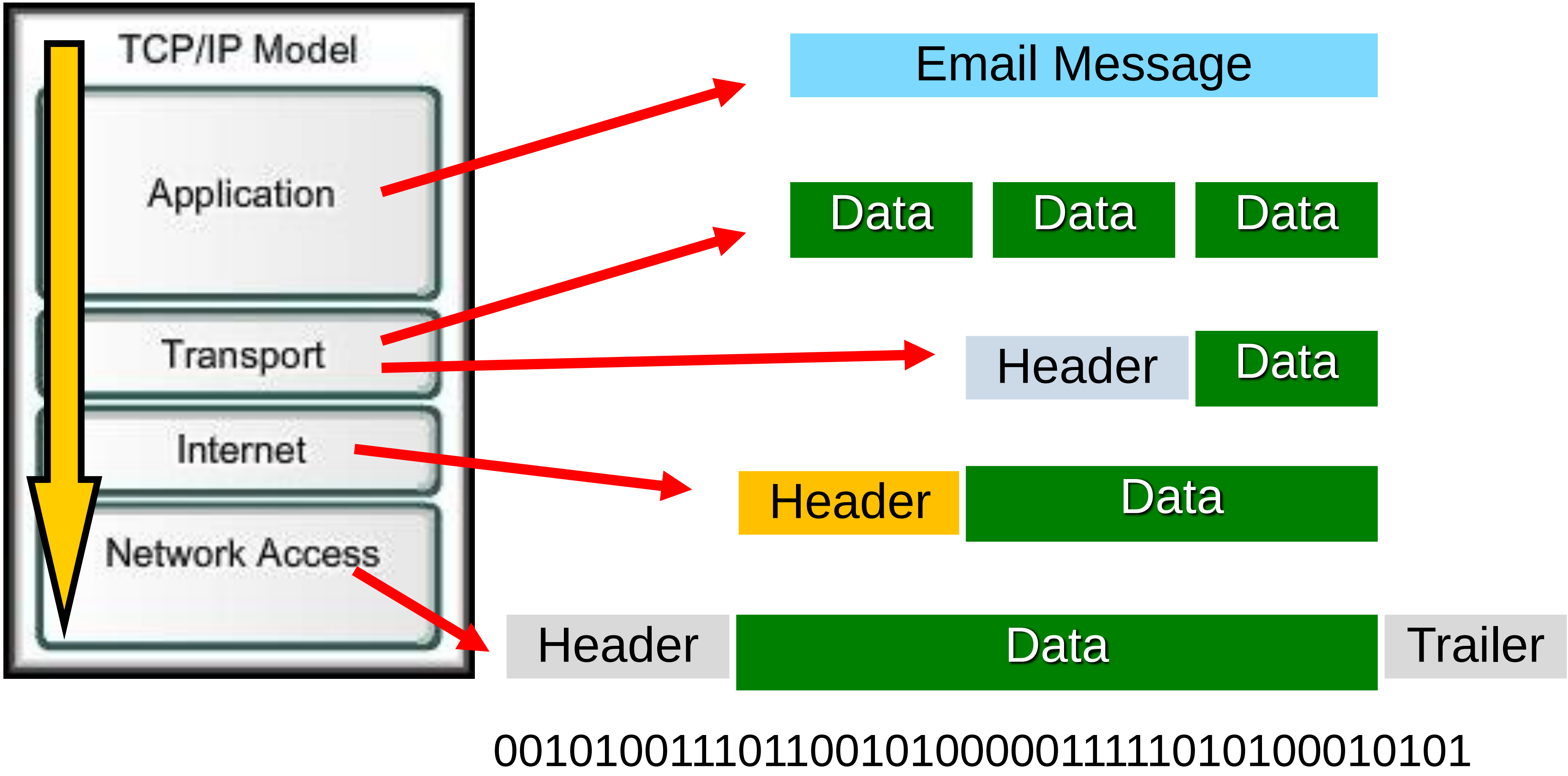
Transport → Supports communication between diverse devices across diverse networks.

Internet → Determines the best path through the network.

Network Access → Controls the hardware devices and media that make up the network.

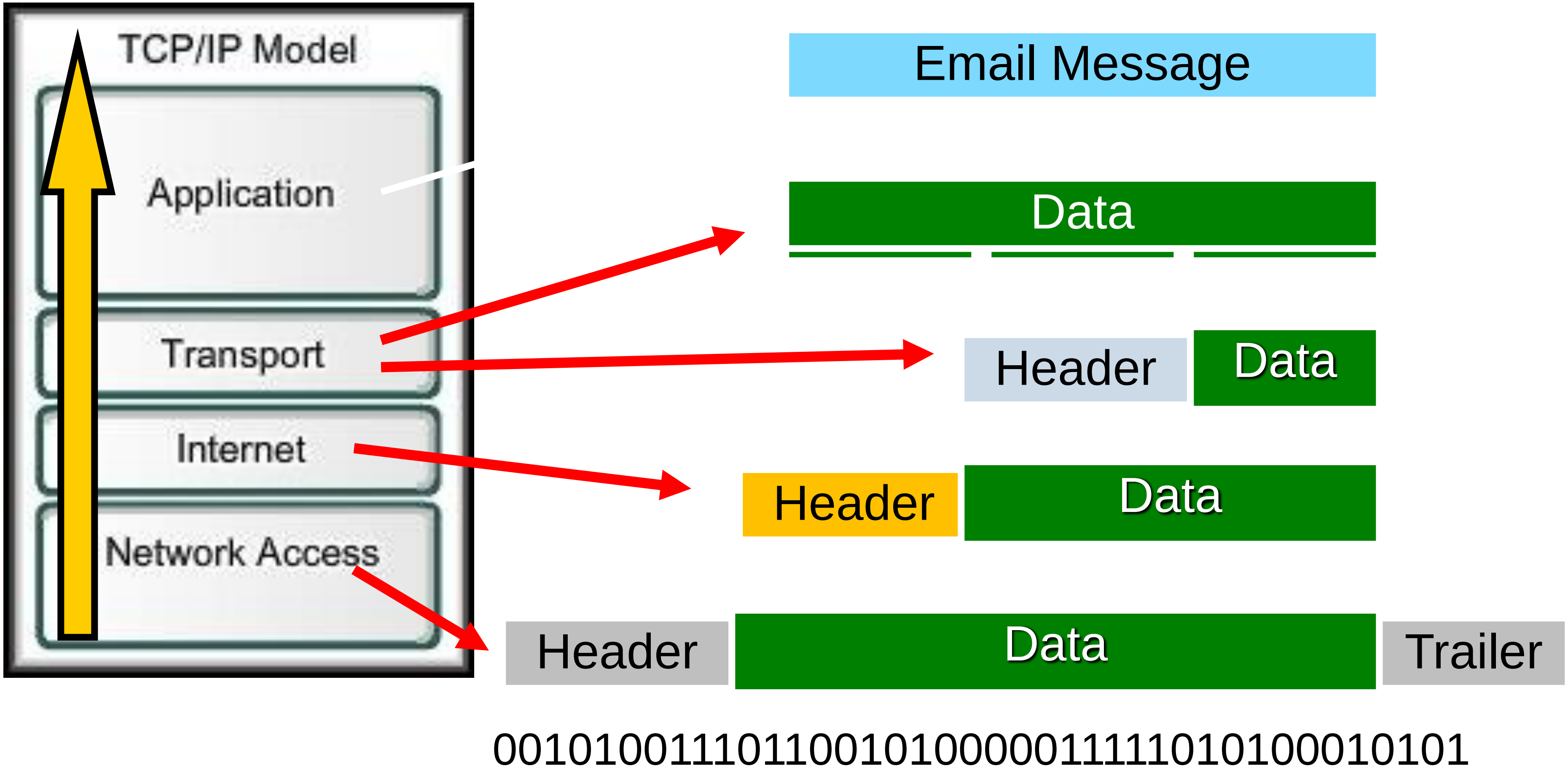
TCP/IP Model

Segmentation and Encapsulation

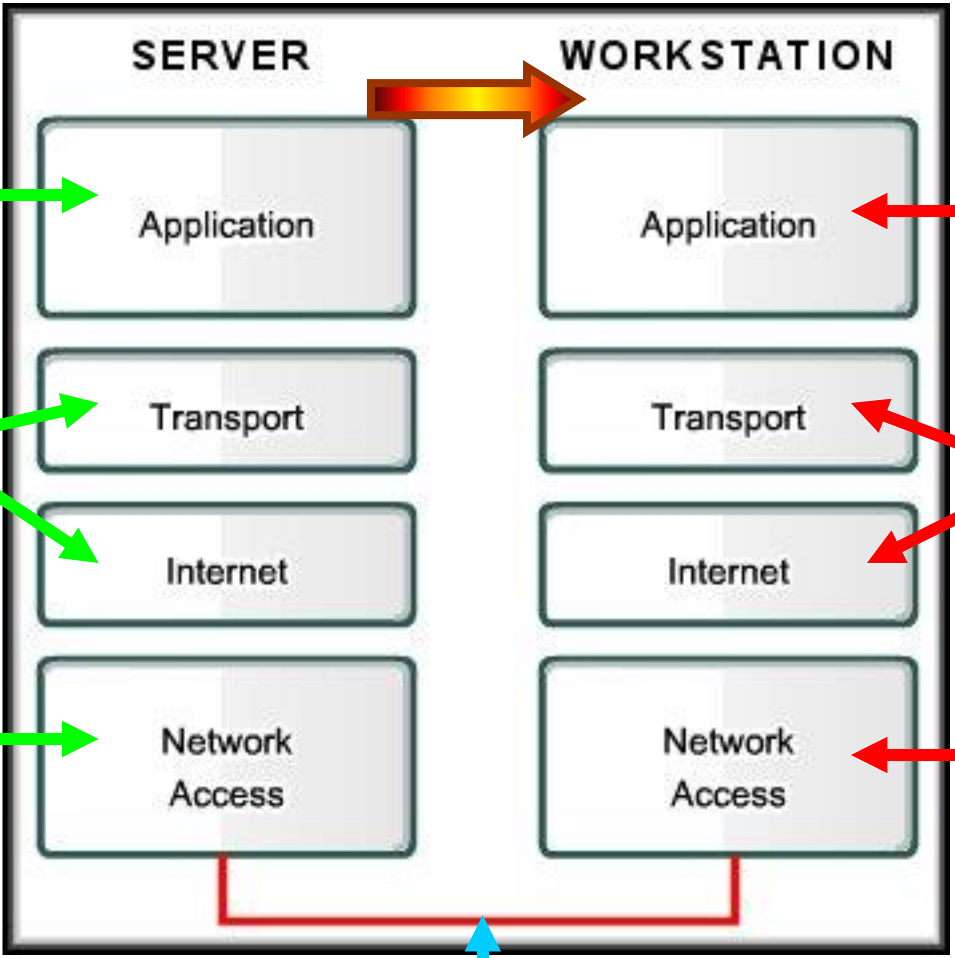


TCP/IP Model

Decapsulation and Reassembly



TCP/IP Model: Communication Process



Create Data

Segment and Encapsulate

Generate on to the media

Pass data to application

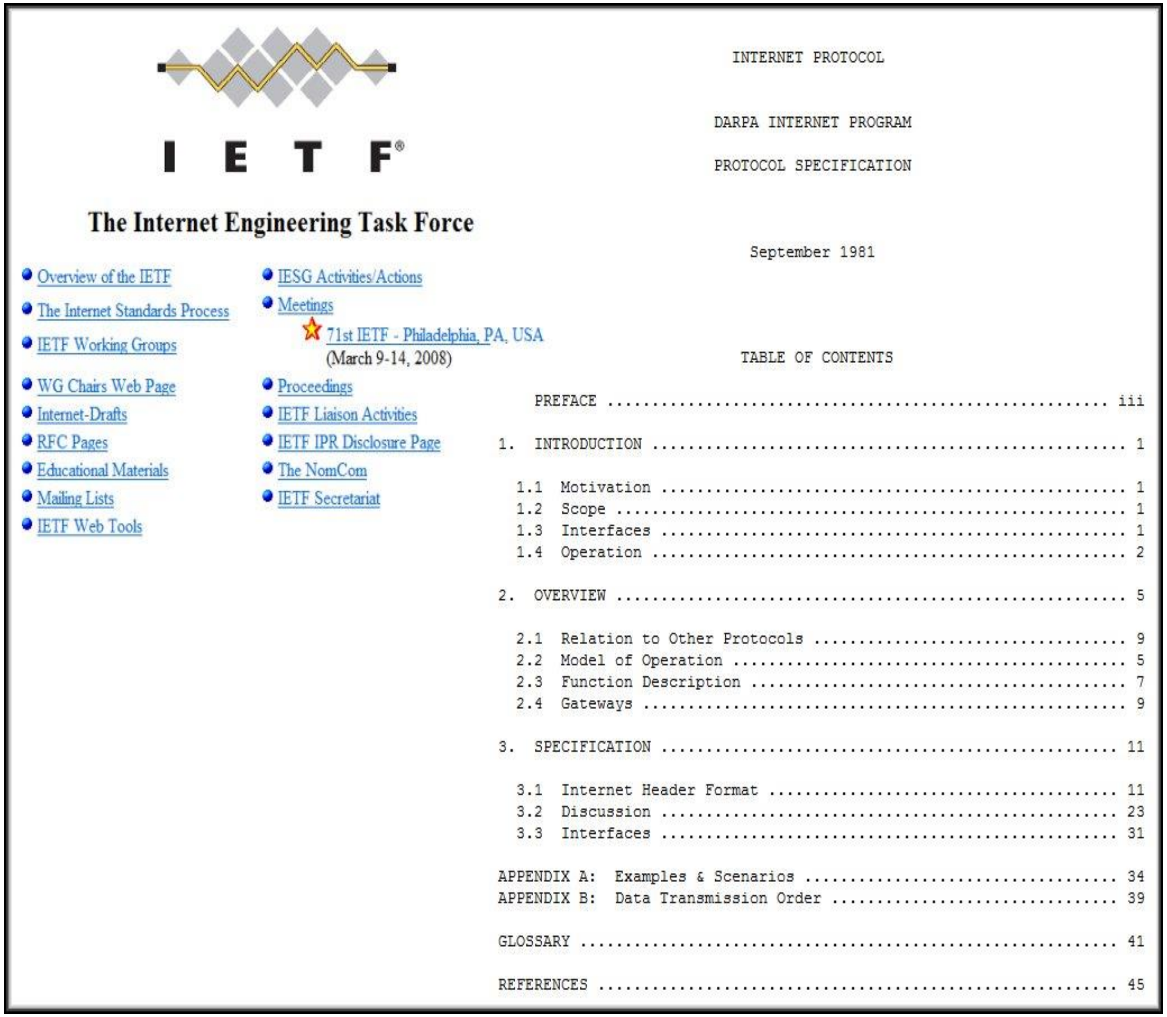
Decapsulate and Reassemble

Receive from the media

Transport through the segment

TCP/IP Model

- Open Standard
- No one company controls it.
- *Governed by IETF* Working Groups
- Standards proposed using *Request for Comments (RFCs)*.



IETF®

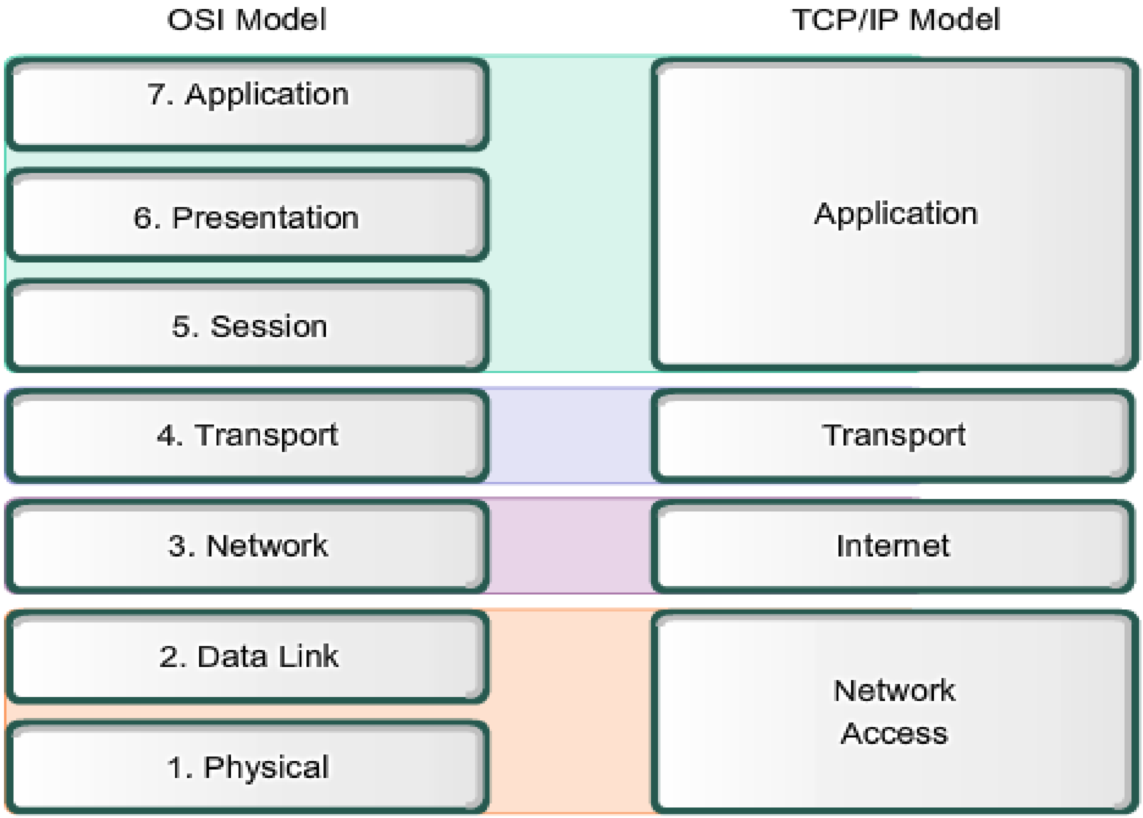
The Internet Engineering Task Force

- Overview of the IETF
- The Internet Standards Process
- IETF Working Groups
- WG Chairs Web Page
- Internet-Drafts
- RFC Pages
- Educational Materials
- Mailing Lists
- IETF Web Tools
- IESG Activities/Actions
- Meetings
  - ☆ 71st IETF - Philadelphia, PA, USA (March 9-14, 2008)
- Proceedings
- IETF Liaison Activities
- IETF IPR Disclosure Page
- The NomCom
- IETF Secretariat

```
                       INTERNET PROTOCOL


                    DARPA INTERNET PROGRAM

                    PROTOCOL SPECIFICATION



                        September 1981




                      TABLE OF CONTENTS

    PREFACE ........................................................ iii

1.  INTRODUCTION ..................................................... 1

  1.1  Motivation .................................................... 1
  1.2  Scope ......................................................... 1
  1.3  Interfaces .................................................... 1
  1.4  Operation ..................................................... 2

2.  OVERVIEW ......................................................... 5

  2.1  Relation to Other Protocols ................................... 9
  2.2  Model of Operation ............................................ 5
  2.3  Function Description .......................................... 7
  2.4  Gateways ...................................................... 9

3.  SPECIFICATION ................................................... 11

  3.1  Internet Header Format ....................................... 11
  3.2  Discussion ................................................... 23
  3.3  Interfaces ................................................... 31

APPENDIX A:  Examples & Scenarios ................................... 34
APPENDIX B:  Data Transmission Order ................................ 39

GLOSSARY ............................................................ 41

REFERENCES .......................................................... 45
```

TCP/IP Model

Comparing the OSI and TCP/IP models



OSI Model	TCP/IP Model
7. Application	Application
6. Presentation	
5. Session	
4. Transport	Transport
3. Network	Internet
2. Data Link	Network Access
1. Physical	