

Computer Networks- UNIT 1

Prepared by
Jobin T J

UNIT 1

- Basic communications model
- Protocol layers and service definitions
- OSI model
- Internet protocols
- the role of standard organizations
- History of Internet
- Security in the Internet
- concept of Quality of Service (QoS).

What Is a Computer Network?

- A computer network is a system in which multiple computers are connected to each other to share information and resources.



What is a Computer Network?

- A **computer network** or **data network** is a telecommunications **network** which allows **computers** to exchange data.
- In **computer networks**, networked computing devices exchange data with each other using a data link.
- The *connections* between nodes are established using either *cable media* or *wireless media*.

Characteristics of a computer network

- Share Resources from one computer to another
- Create files and store them in one computer, access those files from the other computer(s) connected over the network
- Connect a printer, scanner, or a fax machine to one computer within the network and let other computers of the network use the machines available over network.

Computer Network

- Following is the **list of hardware's** required to setup a computer network.
 - Network Cables
 - Distributors
 - Routers
 - Internal Network Cards
 - External Network Cards

Network Cables

- Network cables are used to connect computers. The most commonly used cable is **Category 5 cable RJ-45**.



Distributors

- A computer can be connected to another one via a serial port but if we need to connect many computers to produce a network, this serial connection will not work.
- The solution is to use a **central body** to which other *computers, printers, scanners* etc. can be connected and then this body will **manage or distribute network traffic**.



Router

- A **router** is a type of device which **acts as the central point among computers and other devices that are part of a network.**
- **A router is equipped with holes called ports and computers and other devices are connected to a router using network cables.** Now-a-days router comes in **wireless** modes using which computers can be connected without any physical cable.



Network Card

- Network card is a necessary component of a computer *without which a computer cannot be connected over a network.*
- It is also known as network adapter or **Network Interface Card (NIC).**
- Most branded computers have network card pre-installed.
- Network cards are of two types : **Internal and External Network Cards.**

Internal Network Cards

- Motherboard has a slot for internal network card where it is to be inserted.
- Internal network cards are of two types in which first type uses Peripheral Component Interconnect (**PCI**) connection while the second type uses Industry Standard Architecture (**ISA**).
- Network cables are required to provide network access.



External Network Cards

- External network cards come in two flavours : Wireless and USB based.
- Wireless network card need to be inserted into the motherboard but no network cable is required to connect to network.



Universal Serial Bus (USB)

- USB card are easy to use and connect via USB port.
- Computers automatically detect USB card and can install the drivers required to support the USB network card automatically.



Basic communications model

- Today's **Internet** is the **largest engineered system** ever created by mankind –
 - with **hundreds of millions of connected computers**, communication links, and switches; with billions of users who connect via laptops, tablets, and smart phones; and with an **array of new Internet-connected devices** such as **sensors**, Web cams, game consoles, picture frames, and even washing machines.
- Internet is so large and has so many diverse components and uses.

what *is the* Internet ?

- First, we can describe the nuts and bolts of the Internet, that is, the **basic hardware and software components that make up the Internet.**
- Second, we can describe the Internet in terms of a **networking infrastructure that provides services to distributed applications**

What is Internet - A Nuts-and-Bolts Description

- The Internet is a *computer network* that interconnects hundreds of millions of computing devices throughout the world.
 - *Nontraditional Internet end systems such as laptops, smart phones, tablets, TVs, gaming consoles, Web cams, automobiles, environmental sensing devices, picture frames, and home electrical and security systems are being connected to the Internet.*
- Many nontraditional devices that are being hooked up to the Internet.

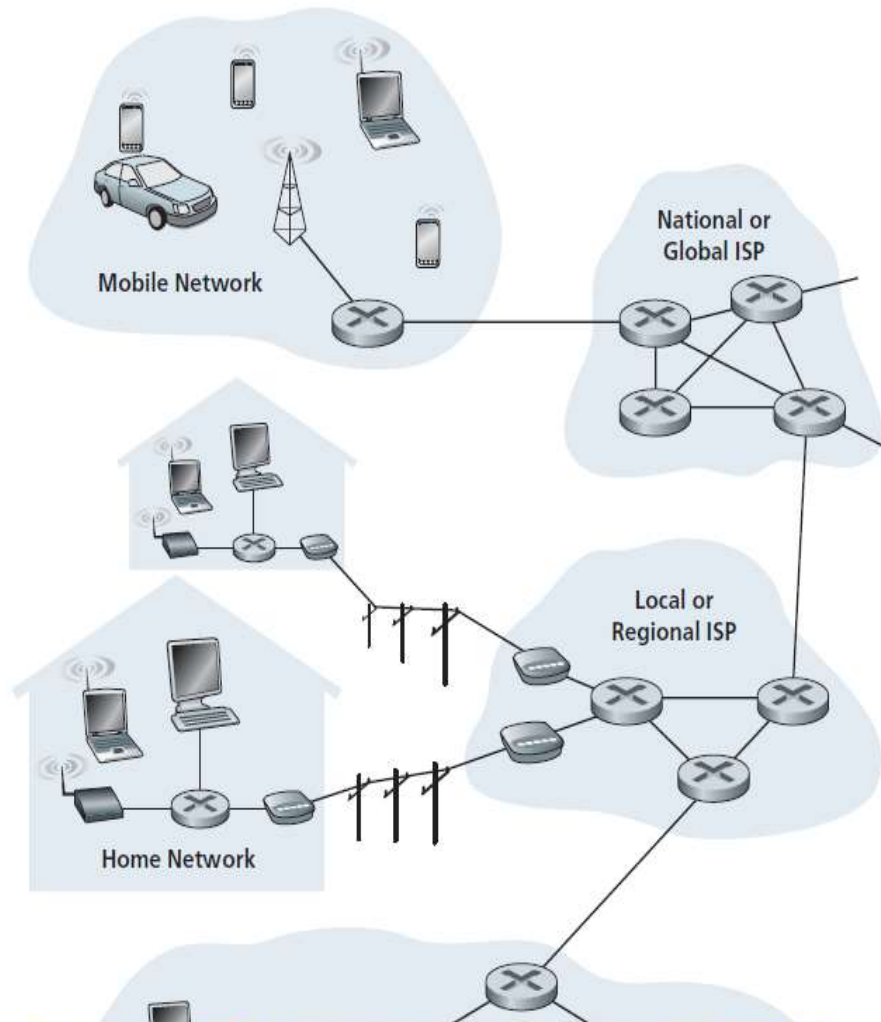
Pieces of Internet

Computer_Networking_A_Top-Down_Approach.pdf - Adobe Reader

File Edit View Window Help

3 (30 of 889) 125%

Tools Sign Comment



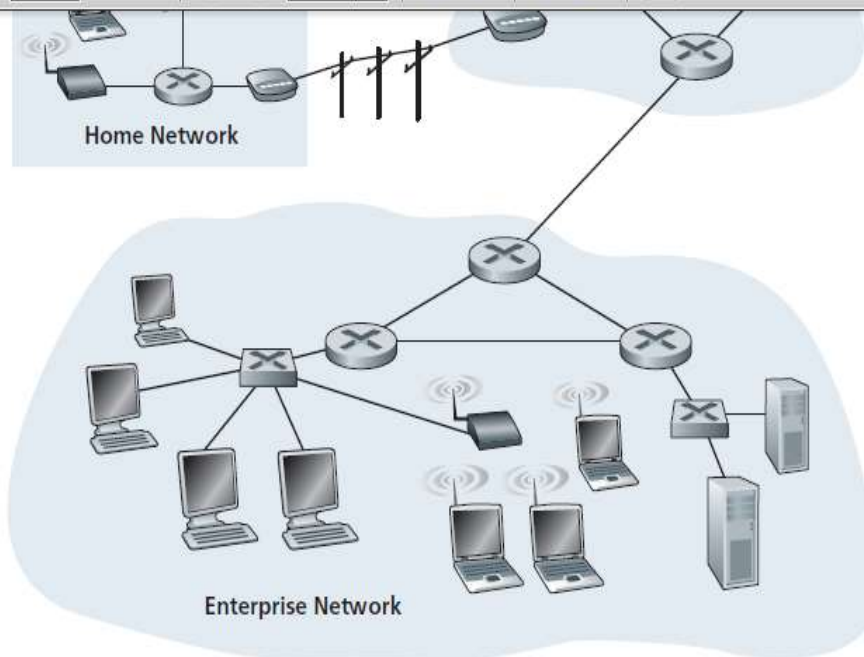
Pieces of Internet

Computer_Networking_A_Top-Down_Approach.pdf - Adobe Reader

File Edit View Window Help

3 (30 of 889) 125%

Tools Sign Comment



Key:



Figure 1.1 ♦ Some pieces of the Internet



Basic communications model

- End systems are connected together by a network of **communication links and packet switches**.
- there are many **types of communication links**, which are made up of **different types of physical media**, including coaxial cable, copper wire, optical fiber, and radio spectrum.

Basic communications model

- Different links can transmit data at different rates, with the **transmission rate of a link measured in bits/second**.
- When one end system has data to send to another end system, the sending end system segments the data and adds header bytes to each segment.
- The resulting packages of information, known as **packets**, are then sent through the network to the destination end system, where they are reassembled into the original data.

Basic communications model

- A packet switch takes a packet arriving on one of its incoming communication links and forwards that packet on one of its outgoing communication links. Packet switches in today's Internet are **routers and link-layer switches**.
- **Both types of switches forward** packets toward their ultimate destinations.
- Link-layer switches are used in access networks, while routers are used in the network core.
- The sequence of communication links and packet switches traversed by a packet from the sending end system to the receiving end system is known as a ***route or path*** through the network.

Basic communications model

- Packet-switched networks (which transport packets) are in many ways similar to transportation networks of highways, roads, and intersections (which transport vehicles).
- For example, a factory that needs to **move a large amount of cargo to some destination** warehouse located thousands of kilometers away.
 - At the factory, the cargo is segmented and loaded into a fleet of trucks. Each of the trucks then independently travels through the network of highways, roads, and intersections to the destination warehouse.
 - At the destination warehouse, the cargo is unloaded and grouped with the rest of the cargo arriving from the same shipment.
- Thus, in many ways, **packets are analogous to trucks, communication links are analogous to highways and roads, packet switches are analogous to intersections, and end systems are analogous to buildings. Just as a truck takes a path through the transportation network, a packet takes a path through a computer network.**

Basic communications model

- End systems access the Internet through **Internet Service Providers (ISPs)**, including residential ISPs such as local cable or telephone companies; corporate ISPs; university ISPs; and ISPs that provide Wi-Fi access in airports, hotels, coffee shops, and other public places.
- Each ISP is in itself a network of packet switches and communication links. ISPs provide a variety of types of network access to the end systems, including residential broadband access such as cable modem or DSL, high-speed local area network access, wireless access.

Basic communications model

- The Internet is all about connecting end systems to each other, so the ISPs that provide access to end systems must also be interconnected.

Basic communications model

- End systems, packet switches, and other pieces of the Internet run **protocols** that control the sending and receiving of information within the Internet.
- The **Transmission Control Protocol (TCP)** and **the Internet Protocol (IP)** are **two of** the most important protocols in the Internet.
- **The IP protocol specifies the format of the packets that are sent and received among routers and end systems.**
- The Internet's principal protocols are collectively known as **TCP/IP.**

Internet- *an infrastructure that provides services to applications*

- These applications include
 - electronic mail,
 - Web surfing,
 - social networks,
 - instant messaging,
 - Voiceover- IP (VoIP),
 - video streaming,
 - distributed games,
 - peer-to-peer (P2P) file sharing,
 - television over the Internet,
 - remote login etc.
- The applications are said to be **distributed applications**, since they involve multiple end systems that exchange data with each other.

Basic communications model

- Internet applications run on end systems—they do not run in the packet switches in the network core.
- Although packet switches facilitate the exchange of data among end systems, they are not concerned with the application that is the source or sink of data.

Basic communications model

- Because **applications run on end systems**, you are going to need to write programs that run on the end systems.
- You might, for example, write your programs in Java, C, or Python. Now, because you are developing a distributed Internet application, the programs running on the different end systems will need to send data to each other.
- And here we get to a central issue—one that leads to the **alternative way of describing the Internet as a platform for applications**.
- ***How does one program running on one end system instruct the Internet to deliver data to another program running on another end system?***

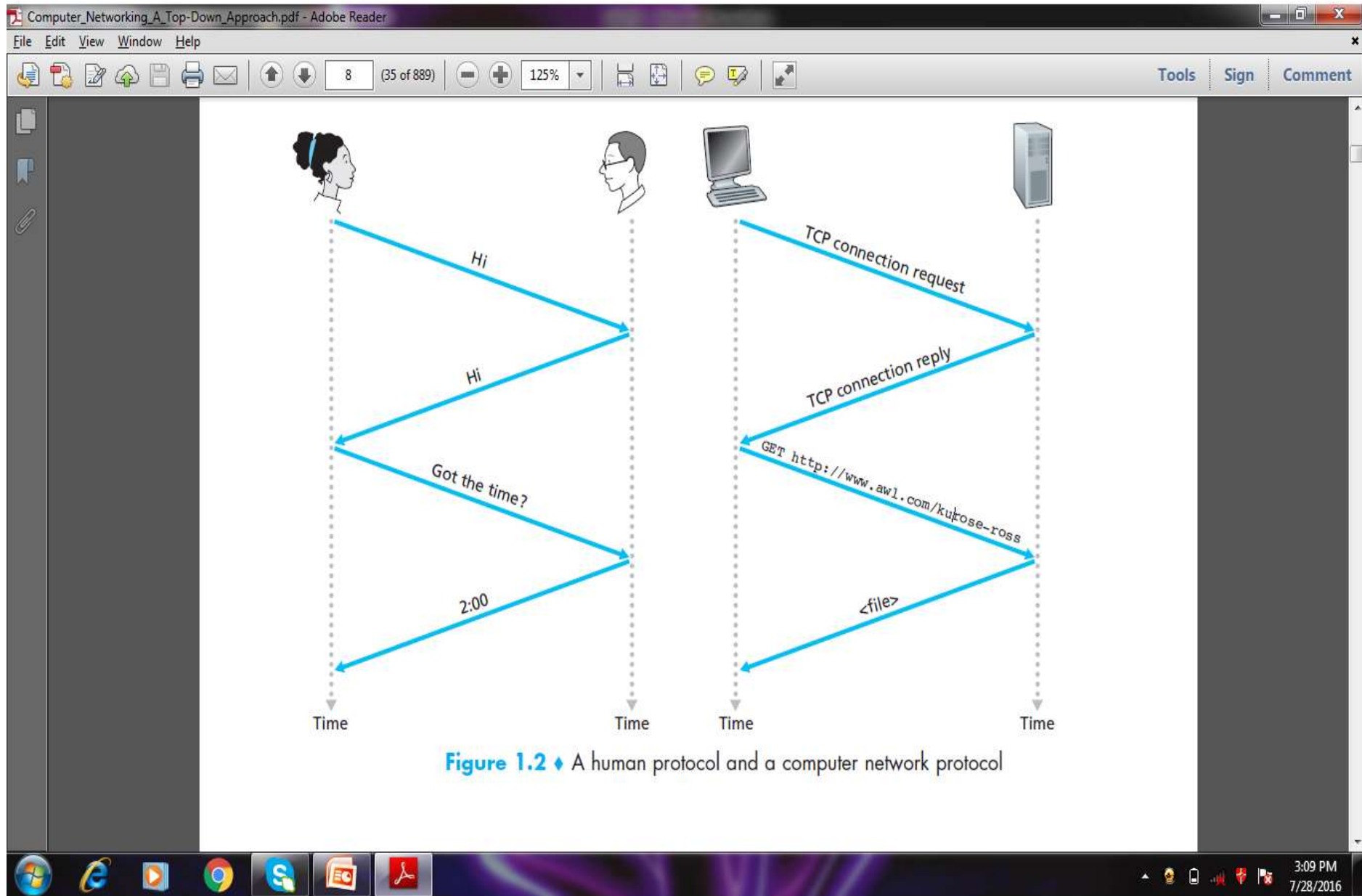
Basic communications model

- End systems attached to the Internet provide an **Application Programming Interface (API)** that specifies how a program running on one end system asks the Internet infrastructure to deliver data to a specific destination program running on another end system.
- This Internet API is a **set of rules** that the *sending program must follow* so that the Internet can deliver the data to the destination program.

What Is a Protocol?

- In our human protocol, *there are specific messages we send, and specific actions we take in response to the received reply messages or other events (such as no reply within some given amount of time).*
 - *transmitted and received messages, and actions taken when these messages are sent or received or other events occur*, play a central role in a human protocol.
- If people run different protocols the protocols do not interoperate and no useful work can be accomplished. The same is true in networking—it takes **two (or more) communicating entities running the same protocol in order to accomplish a task.**

PROTOCOL



Network Protocols

- A network protocol is similar to a human protocol, except that the *entities exchanging messages and taking actions are hardware or software components of some device* (for example, *computer, smartphone, tablet, router, or other network-capable*)

Network Protocols

- All activity in the Internet that involves two or more communicating remote entities is governed by a protocol.
- For example, hardware-implemented protocols in **two physically connected computers control the flow of bits on the “wire” between the two network interface cards;**
- **congestion-control protocols in end systems control the rate at which packets are transmitted between sender and receiver;**
- **protocols in routers determine a packet’s path from source to destination.**

Network Protocols

- *A protocol defines the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event.*
- The Internet, and computer networks in general, make extensive use of protocols.
- Different protocols are used to accomplish different communication tasks

A DIZZYING ARRAY OF INTERNET END SYSTEMS

- Beginning in the late 1990s and continuing today, a wide range of interesting devices are being connected to the Internet, leveraging their ability to send and receive digital data.
- Given the Internet's ubiquity, its well-defined (standardized) protocols, and the availability of Internet-ready commodity hardware, it's natural to use Internet technology to network these devices together and to Internet-connected servers.

A DIZZYING ARRAY OF INTERNET END SYSTEMS

- Many of these devices are based in the home—video game consoles (e.g., Microsoft's Xbox), Internet-ready televisions, digital picture frames that download and display digital pictures, washing machines, refrigerators.
- IP-enabled phones with GPS capabilities put location-dependent services (maps, information about nearby services or people) at your fingertips. Networked sensors embedded into the physical environment allow monitoring of buildings, bridges, wildlife habitats, river estuaries, and the weather.
- Biomedical devices can be embedded and networked in a body-area network. With so many diverse devices being networked together, the Internet is indeed becoming an **“Internet of things”**

End Systems

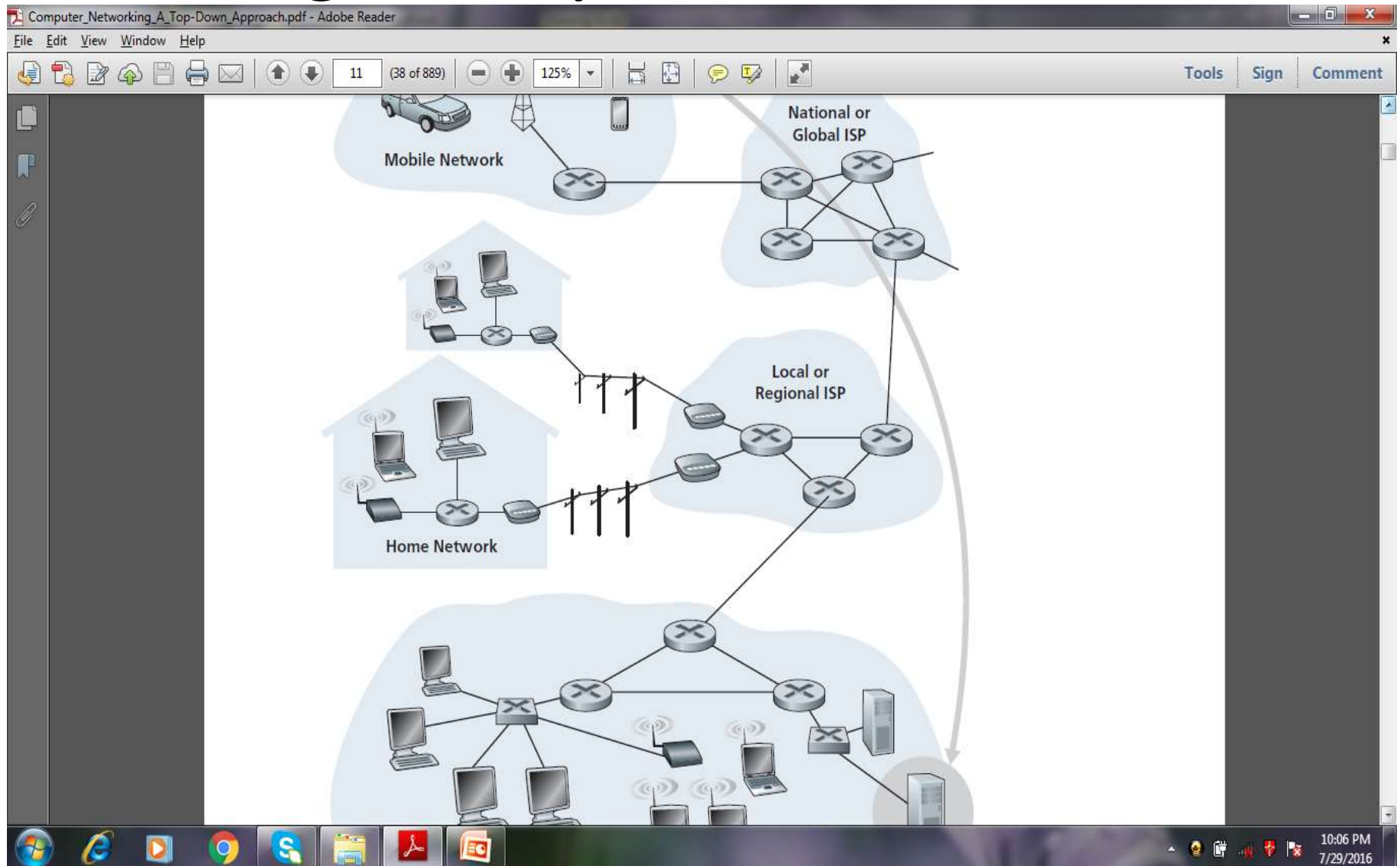
- The computers and other devices connected to the Internet are often referred to as **end systems**.
- They are referred to as end systems **because they sit at the edge of the Internet**. The Internet's end systems include **desktop computers (e.g., desktop PCs, Macs, and Linux boxes), servers (e.g., Web and e-mail servers), and mobile computers (e.g., laptops, smartphones, and tablets)**.
- An increasing number of *non-traditional devices* are being attached to the Internet as end systems

End Systems

- **End systems** are also referred to as *hosts* because they host (that is, run) application programs such as a Web browser program, a Web server program, an e-mail client program, or an e-mail server program.
- that is, *host = end system*. Hosts are sometimes further divided into two categories: **clients and servers**.

- **Clients** tend to be desktop and mobile PCs, smartphones, and so on, whereas servers tend to be more powerful machines that store and distribute Web pages, stream video, relay e-mail, and so on.
- Today, most of the **servers** from which we receive search results, e-mail, Web pages, and videos reside in large **data centers**. **For** example, Google has 30–50 data centers, with many having more than one hundred thousand servers.

Fig: End-system interaction



Access Networks

- The applications and end systems at the “edge of the network,”
- the access network—the network that physically connects an end system to the first router (also known as the “edge router”) on a path from the end system to any other distant end system networks with thick, shaded lines, and the settings (home, enterprise, and wide-area mobile wireless) in which they are used

Home Access: DSL, Cable, FTTH, Dial-Up, and Satellite

- Today, the two most prevalent types of broadband residential access are **digital subscriber line (DSL)** and **cable**.
- The residential telephone line carries both data and traditional telephone signals simultaneously, which are encoded at different frequencies:
 - A high-speed downstream channel, in the 50 kHz to 1 MHz band
 - A medium-speed upstream channel, in the 4 kHz to 50 kHz band
 - An ordinary two-way telephone channel, in the 0 to 4 kHz band

frequency tones for transmission over telephone wires to the CO; the analog signals from many such houses are translated back into digital format at the DSLAM.

The residential telephone line carries both data and traditional telephone signals simultaneously, which are encoded at different frequencies:

- A high-speed downstream channel, in the 50 kHz to 1 MHz band
- A medium-speed upstream channel, in the 4 kHz to 50 kHz band
- An ordinary two-way telephone channel, in the 0 to 4 kHz band

This approach makes the single DSL link appear as if there were three separate links, so that a telephone call and an Internet connection can share the DSL link at the same time. (We'll describe this technique of frequency-division multiplexing in

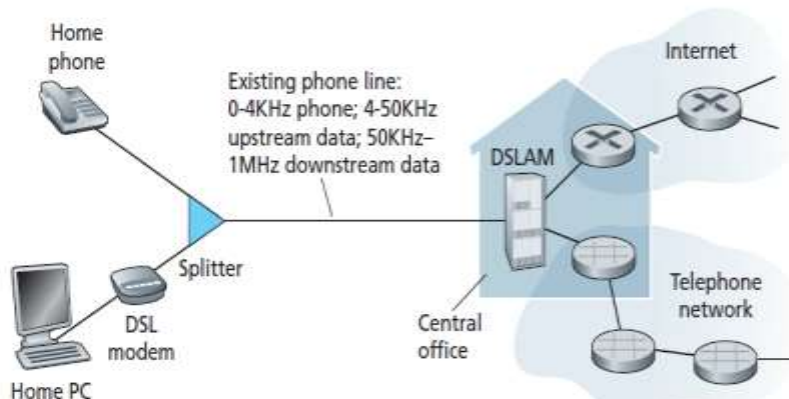


Figure 1.5 ♦ DSL Internet access

- While DSL makes use of the telco's existing local telephone infrastructure, **cable Internet access makes use of the cable television company's existing cable** television infrastructure.
- A residence obtains cable Internet access from the same company that provides its cable television.

company that provides its cable television. As illustrated in Figure 1.6, fiber optics connect the cable head end to neighborhood-level junctions, from which traditional coaxial cable is then used to reach individual houses and apartments. Each neighborhood junction typically supports 500 to 5,000 homes. Because both fiber and coaxial cable are employed in this system, it is often referred to as hybrid fiber coax (HFC).

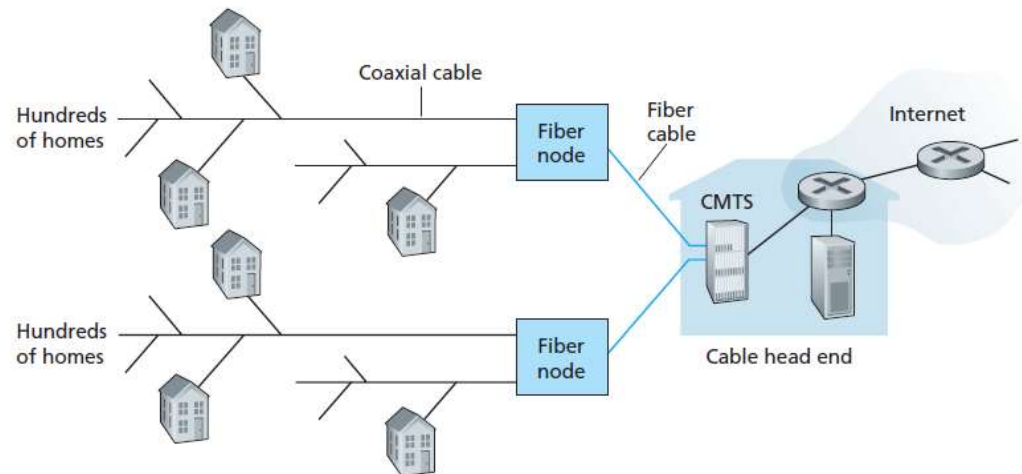


Figure 1.6 ♦ A hybrid fiber-coaxial access network

- One important characteristic of cable Internet access is that it is a shared broadcast medium.
- In particular, every packet sent by the head end travels downstream on every link to every home and every packet sent by a home travels on the upstream channel to the head end.
- For this reason, if several users are simultaneously downloading a video file on the downstream channel, the actual rate at which each user receives its video file will be significantly lower than the aggregate cable downstream rate.

- Although DSL and cable networks currently represent more than 90 percent of residential broadband access in the United States, an up-and-coming technology that promises even higher speeds is the deployment of **fiber to the home (FTTH)**.
- As the name suggests, the FTTH concept is simple— provide an optical fiber path from the CO directly to the home.
- In the United States, Verizon has been particularly aggressive with FTTH with its FIOS service

- Cable internet access requires special modems, called cable modems. As with a DSL modem, the cable modem is typically an external device and connects to the home PC through an Ethernet port.

- One important characteristic of cable Internet access is that it is a shared broadcast medium. In particular, every packet sent by the head end travels downstream on every link to every home and every packet sent by a home travels on the upstream channel to the head end.
- For this reason, if several users are simultaneously downloading a video file on the downstream channel, the actual rate at which each user receives its video file will be significantly lower than the aggregate cable downstream rate.
- On the other hand, if there are only a few active users and they are all Web surfing, then each of the users may actually receive Web pages at the full cable downstream rate, because the users will rarely request a Web page at exactly the same time.
- Because the upstream channel is also shared, a distributed multiple access protocol is needed to coordinate transmissions and avoid collisions.

Protocol layers and service definitions

- Internet is an *extremely complicated* system.
There are many pieces to the Internet:
 applications and protocols,
 various types of end systems,
 packet switches,
 various types of link-level media.
- Given this enormous complexity, is there any hope of organizing a network architecture

Protocol layers and service definitions

- To provide structure to the design of network protocols, network designers organize protocols—and the network hardware and software that implement the protocols—in **layers**.

Protocol layers and service definitions

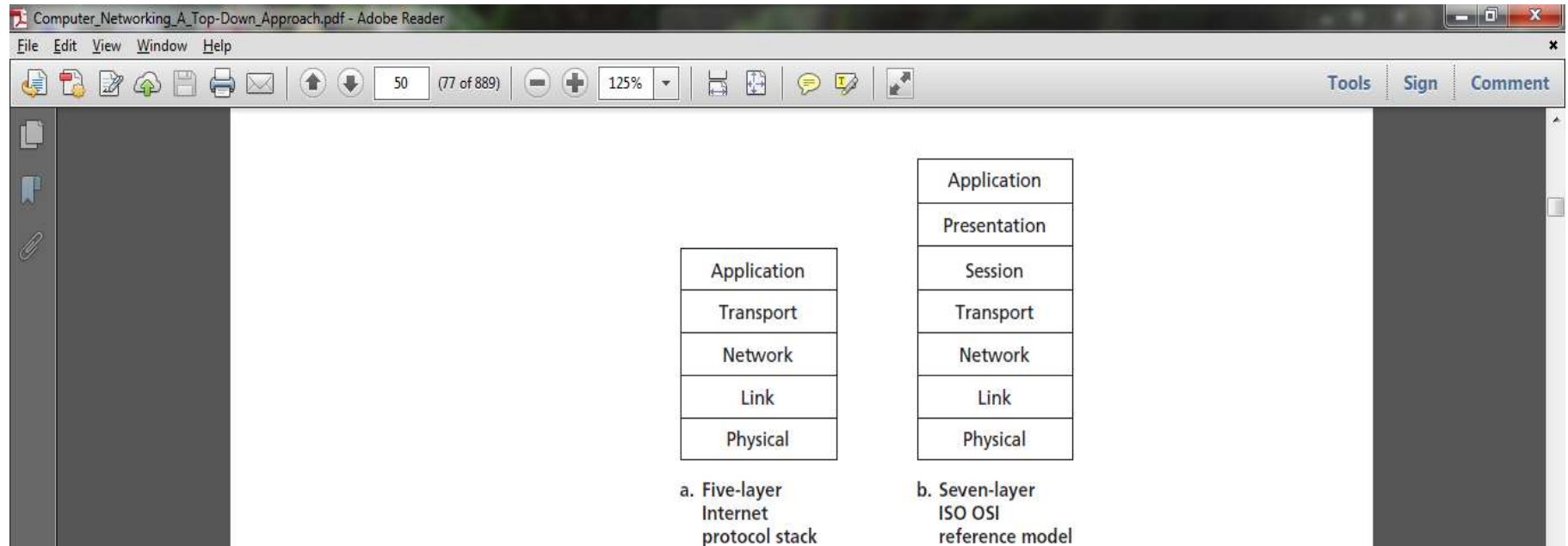


Figure 1.23 ♦ The Internet protocol stack (a) and OSI reference model (b)

always implemented in software in the end systems; so are transport-layer protocols. Because the physical layer and data link layers are responsible for handling communication over a specific link, they are typically implemented in a network interface card (for example, Ethernet or WiFi interface cards) associated with a given link. The network layer is often a mixed implementation of hardware and software. Also note that just as the functions in the layered airline architecture were distributed among the various airports and flight control centers that make up the system, so too is a layer n protocol *distributed* among the end systems, packet switches, and other components that make up the network. That is, there's often a piece of a layer n protocol in each of these network components.

Application Layer

- The application layer is **where network applications and their application-layer protocols reside.**
- The **Internet's application layer includes many protocols, such as the HTTP protocol (which provides for Web document request and transfer), SMTP (which provides for the transfer of e-mail messages), and FTP (which provides for the transfer of files between two end systems).**
- An application-layer protocol is distributed over multiple end systems, with the application in one end system using the protocol to exchange packets of information with the application in another end system.
- We'll refer to this packet of information at the application layer as a **message.**

Transport Layer

- The Internet's transport layer transports application-layer messages between application endpoints.
- In the Internet **there are two transport protocols, TCP and UDP, either of which can transport application-layer messages.**
- **TCP provides a connection-oriented service to its applications. This service includes guaranteed delivery of application-layer messages to the destination and flow control (that is, sender/receiver speed matching).**
- TCP also breaks long messages into shorter segments and provides a congestion-control mechanism, so that a source throttles its transmission rate when the network is congested.
- **The UDP protocol provides a connectionless service to its applications. This is a no-frills service that provides no reliability, no flow control, and no congestion control.**
- we'll refer to a transport-layer packet as a **segment**.

Network Layer

- The Internet's network layer is responsible for moving network-layer packets known as **datagrams** from one host to another. The Internet transport-layer protocol (TCP or UDP) in a source host passes a transport-layer segment and a destination address to the network layer, just as you would give the postal service a letter with a destination address.
- **The network layer then provides the service of delivering the segment to the transport layer in the destination host.**
- The Internet's network layer includes the celebrated IP Protocol, which *defines the fields in the datagram as well as how the end systems and routers act on these fields.*
- The Internet's network layer also contains routing protocols that determine the routes that datagram take between sources and destinations.

Link Layer

- The Internet's network layer routes a datagram through a series of routers between the source and destination. To move a packet from one node (host or router) to the next node in the route, the network layer relies on the services of the link layer.
- At each node, the network layer passes the datagram down to the link layer, which delivers the datagram to the next node along the route. At this next node, the link layer passes the datagram up to the network layer.
- The services provided by the link layer *depend on the specific link-layer protocol that is employed* over the link. For example, some link-layer protocols provide reliable delivery, from transmitting node, over one link, to receiving node. This reliable delivery service is different from the reliable delivery service of TCP, which provides reliable delivery from one end system to another.
- **Examples of link layer protocols include Ethernet, WiFi, and the cable access network's DOCSIS protocol.**
- As datagrams typically need to traverse several links to travel from source to destination, a datagram may be handled by different link-layer protocols at different links along its route. For example, a datagram may be handled by Ethernet on one link and by PPP on the next link. The network layer will receive a different service from each of the different link-layer protocols.
- we'll refer to the link layer packets as **frames**.

Physical Layer

- While the job of the link layer is to move entire frames from one network element to an adjacent network element, the job of the physical layer is to move the *individual bits within the frame from one node to the next*.
- The *protocols in this layer are again link dependent and further depend on the actual transmission medium of the link* (for example, twisted-pair copper wire, single-mode fiber optics).
- Ethernet has many physical-layer protocols: one for twisted-pair copper wire, another for coaxial cable, another for fiber, and so on. In each case, a bit is moved across the link in a different way.

Protocol layers & service definition

- **Encapsulation**
- **Routers and link-layer switches** are both **packet switches**. Similar to end systems, routers and link-layer switches organize their networking hardware and software into **layers**.
- Routers and link-layer switches **do not implement *all of the layers*** in the protocol stack; they typically implement only the **bottom layers**.
- **Link-layer switches** implement **layers 1 and 2**;
- **Routers** implement **layers 1 through 3**.
- **Internet routers** are capable of implementing the **IP protocol** (a layer 3 protocol), while **link-layer switches** are not.
- while **link-layer** switches do not recognize IP addresses, they are capable of recognizing layer 2 addresses, such as **Ethernet addresses**.
- The **hosts** implement all five layers;
 - the Internet architecture puts much of its complexity at the edges of the network.

Encapsulation

54 CHAPTER 1 • COMPUTER NETWORKS AND THE INTERNET

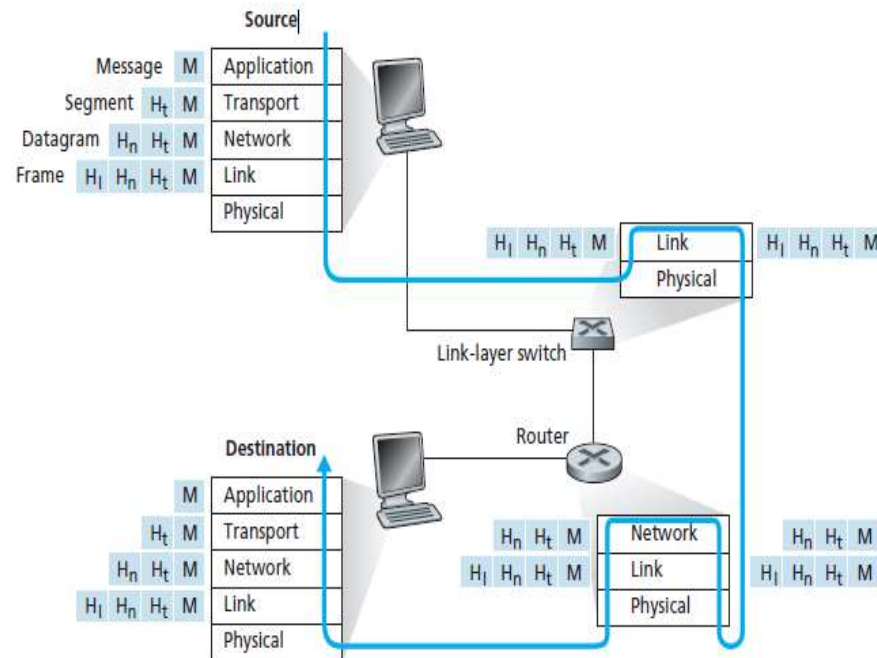


Figure 1.24 ♦ Hosts, routers, and link-layer switches; each contains a different set of layers, reflecting their differences in functionality

are capable of recognizing layer 2 addresses, such as Ethernet addresses. Note that hosts implement all five layers; this is consistent with the view that the Internet architecture puts much of its complexity at the edge of the network.

Encapsulation

- **At the** sending host, an **application-layer message(M)** is *passed to the transport layer*.
- The transport layer takes the message and appends additional information (**transport-layer header information, H_t** that will be used by the receiver-side transport layer.
- The application- layer message and the transport-layer header information together constitute the **transport-layer segment**.
- **The transport-layer segment thus encapsulates the** application-layer message.
- The added information might include information allowing the receiver-side transport layer to deliver the message up to the appropriate application, and error-detection bits that allow the receiver to determine whether bits in the message have been changed in route.
- The transport layer then passes the segment to the network layer, which adds network-layer header information **H_n such as source and destination end system addresses**, creating a **network-layer datagram**.
- **The datagram is then passed to the link** layer, which will add its own link-layer header information and create **link-layer frame**.
- **At each layer, a packet has two types of** fields: header fields and a **payload field**.
- ***Eg:**the sending of an interoffice memo from one corporate branch office to another via the public postal service*

The OSI Model

- In the late 1970s, the **International Organization for Standardization (ISO)** proposed that computer networks be organized around seven layers, called the **Open Systems Interconnection (OSI) model**.
- The OSI model took shape when the protocols that were to become the Internet protocols were in their infancy, and were but one of many different protocol suites under development; in fact, the inventors of the original OSI model probably did not have the Internet in mind when creating it.

The OSI Model

- Nevertheless, beginning in the late 1970s, *many training and university courses picked up on the ISO mandate* and organized courses around the seven-layer model.

The OSI Model

- The seven layers of the OSI reference model are:
- application layer,
- presentation layer,
- session layer,
- transport layer,
- network layer,
- data link layer,
- and physical layer.

The OSI Model

- Let's consider the two additional layers present in the OSI reference model—the presentation layer and the session layer.
- The **role of the presentation layer is to provide services that allow communicating applications to interpret the meaning of data exchanged.**
- **These services include data compression and data encryption as well as data description.**
- The session layer provides for **delimiting and synchronization of data exchange, including the means to build a check pointing and recovery scheme.**

The OSI Model

- The fact that the **Internet lacks two layers** found in the OSI reference model poses a couple of interesting questions:
 - Are the services provided by these layers unimportant?
 - What if an application *needs one of these services*?
- *The Internet's* answer to both of these questions is the same—**it's up to the application developer.**
- It's up to the application developer to decide if a service is important, and **if the service is important, it's up to the application developer to build that functionality** into the application.

The OSI Model

- The **ISO** was one of the first organizations to formally define a common way to connect computers. Their architecture, called the *Open Systems Interconnection (OSI) architecture* defines a partitioning of network functionality into seven layers, where one or more protocols implement the functionality assigned to a given layer.
- *The ISO, usually in conjunction with* a second standards organization known as the International Telecommunications Union (ITU), publishes a series of protocol specifications based on the OSI architecture. This series is sometimes called the “**X dot**” series since the protocols are given names like **X.25, X.400, X.500**, and so on.

Computer_Networks_Peterson_A_Systems_Approach_Fourth_Edition.pdf - Adobe Reader

File Edit View Window Help

27 (56 of 835) 125%

Tools Sign Comment

The diagram illustrates the OSI network architecture. On the left and right are two vertical stacks representing 'End host' systems. Each stack contains seven layers, from top to bottom: Application, Presentation, Session, Transport, Network, Data link, and Physical. These layers are connected by vertical lines. In the center, a cloud-shaped area represents the network. Inside the cloud, there are two identical vertical stacks of three layers: Network, Data link, and Physical. These stacks are connected by horizontal lines. The Physical layer of the left end host is connected to the Physical layer of the left network stack. The Physical layer of the right end host is connected to the Physical layer of the right network stack. Below the cloud, the text 'One or more nodes within the network' is written.

End host

Application

Presentation

Session

Transport

Network

Data link

Physical

Network

Data link

Physical

Network

Data link

Physical

One or more nodes within the network

Figure 1.13 OSI network architecture.

9:23 PM 8/8/2016

The OSI Model

- Starting at the bottom and working up, the *physical layer handles the transmission of raw bits* over a communications link.
- The *data link layer then collects a stream of bits into a larger aggregate called a frame*. Network adaptors, along with device drivers running in the node's OS, typically implement the data link level.
- This means that **frames**, not raw bits, are actually **delivered to hosts**.
- The *network layer handles routing among nodes within a packet-switched network*. At this layer, the unit of data exchanged among nodes is typically called a *packet rather than a frame*, although they are fundamentally the same thing. **The lower three layers are implemented on all network nodes, including switches within the network and hosts connected along the exterior of the network.**
- The *transport layer then implements what we have up to this point been calling a process-to-process* channel.
- Here, the unit of data exchanged is commonly called a *message* rather than a packet or a frame.
- The transport layer and higher layers typically run only on the end hosts and not on the intermediate switches or routers.

The OSI Model

- *Application layer protocols* include things like the File Transfer Protocol (FTP), which defines a protocol by which file transfer applications can interoperate.
- Below that, the *presentation layer* is concerned with *the format of data exchanged between peers*,
 - for example, whether an integer is 16, 32, or 64 bits long and whether the most significant byte is transmitted first or last, or how a video stream is formatted.
- Finally, the *session layer* provides a name space that is used to *tie together the potentially different transport streams that are part of a single application*.
 - For example, it might manage an audio stream and a video stream that are being combined in a teleconferencing application.

Internet protocols

- The **Internet Protocol (IP)** is the principal communications protocol in the Internet protocol suite for *relaying datagram across network boundaries*. Its routing function enables internetworking, and essentially establishes the Internet.
- IP has the task of delivering packets *from the source host to the destination host solely based on the IP addresses* in the packet headers. For this purpose, **IP defines packet structures that encapsulate the data to be delivered**. It also defines addressing methods that are used to label the datagram with source and destination information.

Internet Protocol

- The Internet Protocol is **responsible for addressing hosts and for routing datagrams (packets) from a source host to a destination host across one or more IP networks.**
- For this purpose, the *Internet Protocol defines the format of packets and provides an addressing system that has two functions: Identifying hosts and providing a logical location service*

Internet Protocol

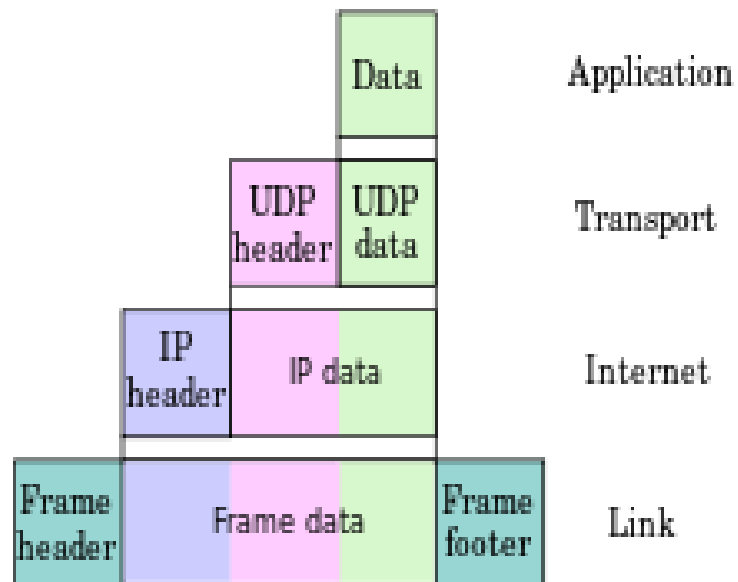
- **Datagram construction**
- Each datagram has two components:
 - a header and a payload.
- The **IP header** is tagged with the
 - *source IP address,*
 - *the destination IP address,*
 - *other meta-data needed to route and deliver the datagram.*
- The **payload**
 - the data that is transported.

This method of nesting the data payload in a packet with a header is called **encapsulation**.

Internet Protocol

- IP addressing and routing
- IP addressing entails the
 - assignment of IP addresses and associated parameters to host interfaces.
 - The address space is divided into networks and subnetworks, involving the designation of network or routing prefixes.
- IP routing is performed by
 - all hosts, as well as routers, whose main function is to **transport packets** across network boundaries.
- Routers communicate with one another via
 - specially designed routing protocols, either interior gateway protocols or exterior gateway protocols, as needed for the topology of the network.
- IP routing is also common in local networks.
 - **Ethernet switches support IP multicast operations.**
 - These switches use IP addresses and Internet Group Management Protocol to control *multicast routing*
 - **MAC addresses for the actual routing**

Internet Protocol



Internet Protocol

- IP specifies
 - the format of packets, and the addressing scheme.
- Most networks combine IP with a higher-level protocol called *Transmission Control Protocol (TCP)*,
 - which establishes a virtual connection between a destination and a source.
- *IP by itself is something like the postal system.*
 - *It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient.*
 - *TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.*

Internet Protocol

- Short for **Internet Protocol address**, an **IP** or **IP address** is a **number** used to
 - indicate the location of a computer or other device on a network using TCP/IP.
- These addresses are similar to those of your house;
 - they allow data to reach the appropriate destination on a network and the Internet.
- **IPv4 vs. IPv6**
- As the Internet and technology evolve, there has been an increasing demand for IP addresses.
- To help meet the demand for IP addresses, there are two types of addresses used today, IPv4 and IPv6.
- IPv4 address in your local home, school, or small office.
 - Example of an **IPv4** address:
 - 45.79.151.23
 - Example of an **IPv6** address:
 - 2601:681:4200:c5c0:516:f0bb:ac3b:46bd

Internet Protocol

- **IP address classes**
- With an **IPv4 IP address** there are *five classes* of available IP ranges:
 - **Class A, Class B, Class C, Class D and Class E** while only A, B, and C are commonly used.
- **Each class allows for a range of valid IP addresses**, shown in the following table.
- **Class A** 1.0.0.1 to 126.255.255.254 Supports 16 million hosts on each of 127 networks.
- **Class B** 127.1.0.1 to 191.255.255.254 Supports 65,000 hosts on each of 16,000 networks.
- **Class C** 192.0.1.1 to 223.255.254.254 Supports 254 hosts on each of 2 million networks.
- **Class D** 224.0.0.0 to 239.255.255.255 Reserved for multicast groups.
- **Class E** 240.0.0.0 to 254.255.255.254 Reserved for future use, or Research and Development Purposes.
- Ranges 127.x.x.x are reserved for the loopback or localhost, for example, **127.0.0.1** is the loopback address.
- Range **255.255.255.255** broadcasts to all hosts on the local network.

Internet Protocol

- **IP address breakdown**
 - Every IP address is broken down into four sets of octets and translated into binary to represent the actual IP address.
- For an example, let's break down the IP "166.70.10.23" in the following table.
- The first row contains the separate sections of the IP address, the second has binary values, and the third row shows how the binary value equals the section of the IP address.
- **IP:** 166 70 10 23
- **Binary value:** 10100110 01000110 00001010 00010111
- **Numerical value:** $128+32+4+2=166$ $64+4+2=70$ $8+2=10$ $16+4+2+1=23$

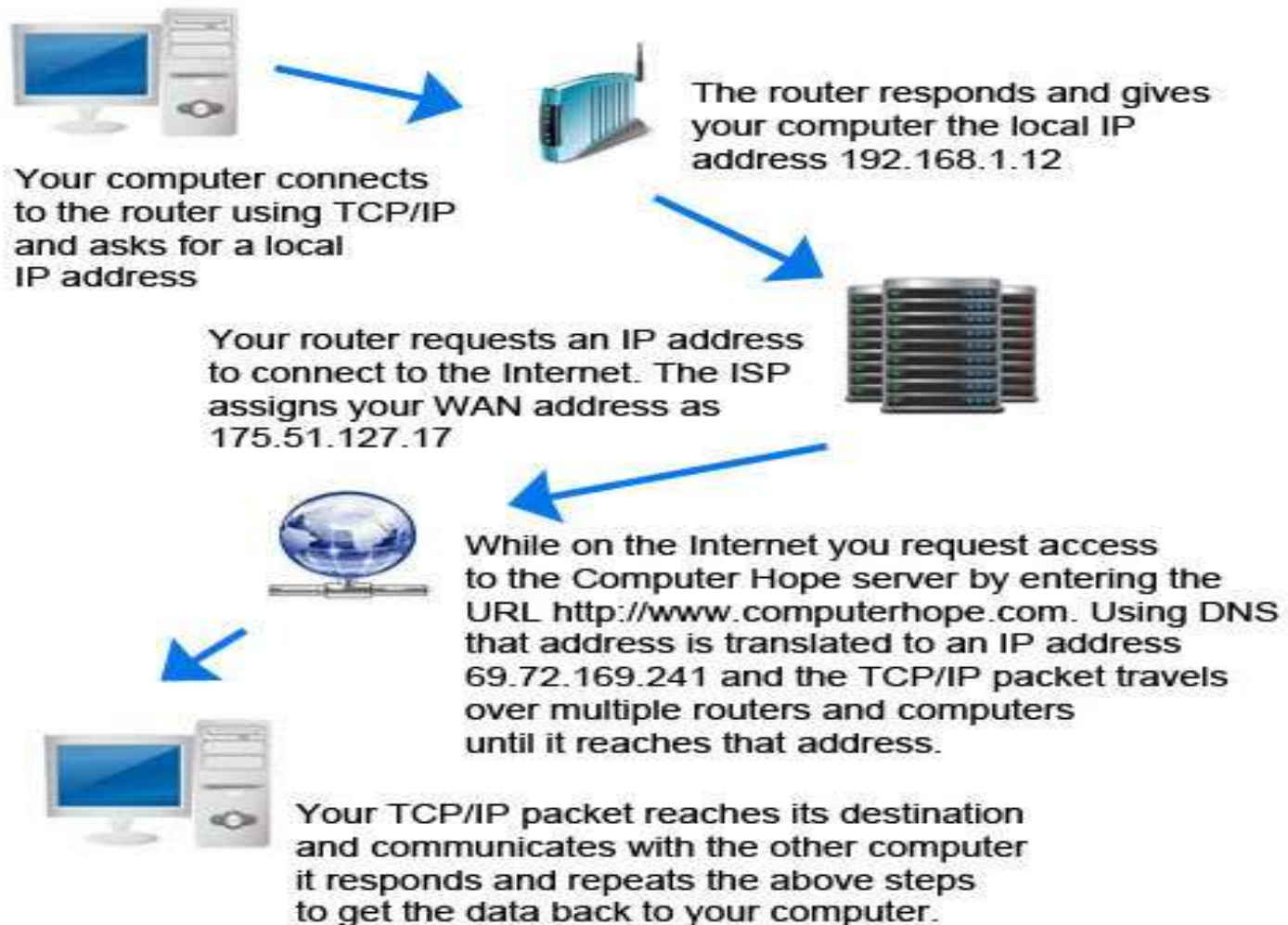
Internet Protocol

- **Automatically assigned addresses**
- There are IP addresses that are automatically assigned (dynamic allocation) when you set up a home network.
- These default addresses are what allow your computer and other network devices to communicate and broadcast information over your network.
- Below are the most commonly assigned default addresses for home networks.
- 192.168.1.0 0 is the automatically assigned network address.
- 192.168.1.1 1 is the commonly used address used as the gateway.
- 192.168.1.2 2 is also a commonly used address used for a gateway.
- 192.168.1.3 - 254 Addresses beyond 3 are assigned to computers and devices on the network.
- 192.168.1.255 255 is automatically assigned on most networks as the broadcast address.

Internet Protocol

- **Getting an IP address**
- By default the router will NAT (**Network Address Translation**) assign each of your computers their own IP address, often using to forward the data coming from those computers to outside networks such as the Internet.
- If you need to register an IP address that can be seen on the Internet, you must register through InterNIC or use a web host that can assign you addresses.
- Anyone who connects to the Internet is assigned an IP address by their Internet Service Provider (ISP), which has registered a range of IP addresses.
- For example, let's assume your ISP is given 100 addresses, 109.145.93.150-250. In this range, the ISP owns addresses 109.145.93.150 to 109.145.93.250 and can assign any address in that range to its customers.
- So, all these addresses belong to your ISP until they are assigned to a customers computer. In the case of a dial-up connection, you are given a new IP address each time you dial into your ISP.
- With most broadband Internet service providers, you are always connected to the Internet your address rarely changes. It remains the same until the service provider requires otherwise.

"How do computers connect to each other over the Internet?"



The role of standard organizations

- The rise of open standards not owned by any one company has been a great boon to customers of computer and networking products, as well as the manufacturers that sell to them.
- In order to facilitate the development of open standards,, organizations are needed that will coordinate the creation and publishing of these *documents*. Generally, these are *non-profit organizations* that specifically take a neutral stance regarding technologies and work for the betterment of the industry as a whole.
- Here are some of the standards organizations that you are likely to encounter when reading about networking and the Internet:

The role of standard organizations

- **International Organization for Standardization (ISO):** Probably the biggest standards organization in the world, the ISO is really a federation of standards organizations from dozens of nations. In the networking world, the ISO is best known for its *OSI Reference Model*.
- **Note:** The shortened name of the International Organization for Standardization is indeed “ISO”. Many people, especially in the United States, think “ISO” is short for “International Standards Organization”, but this is incorrect.

The role of standard organizations

- **American National Standards Institute (ANSI):**
ANSI is the main organization responsible for coordinating and publishing computer and information technology standards in the United States.
- While they are commonly thought of as developing and maintaining standards, they do neither. Instead, they oversee and accredit the organizations that actually create the standards, qualifying them as *Standards Developing Organizations or SDOs*.
- ANSI also publishes the standards documents created by the SDOs, and serves as the United States' representative to the ISO.

The role of standard organizations

- **Information Technology Industry Council (ITIC):**
ITIC is a group of several dozen companies in the information technology (computer) industry.
- ITIC is the SDO approved by ANSI to develop and process standards related to many computer-related topics.
- It was formerly known as the *Computer and Business Equipment Manufacturers Association (CBEMA)*.

The role of standard organizations

- **National Committee for Information Technology (NCITS):**
- A committee established by the ITIC to develop and maintain standards related to the information technology world.
- NCITS was formerly known by the name *Accredited Standards Committee X3, Information Technology*, or more commonly, just *X3*.

The role of standard organizations

- **Institute of Electrical and Electronics Engineers (IEEE):** The IEEE (pronounced “eye-triple-ee”) is a well-known professional organization for those in the electrical or electronics fields, including computers and networking. IEEE's main claim to fame in the networking industry is the IEEE 802 Project, which encompasses many popular networking technologies including Ethernet.

Electronic Industries Alliance (EIA): The EIA is an international industry association that is best known for publishing electrical wiring and transmission standards.

Telecommunications Industry Association (TIA): The TIA is the communications sector of the EIA, and is responsible for developing communications standards. Since communications, wiring and transmission are all related, and since the TIA and EIA organizations are also related, standards produced by the EIA or TIA are often labeled with the combined prefixes “EIA/TIA” or “TIA/EIA”.

The role of standard organizations

- **International Telecommunication Union - Telecommunication Standardization Sector (ITU-T):** ITU-T is another large international body that develops standards for the telecommunications industry. The ITU-T was formerly named the *International Telephone and Telegraph Consultative Committee* or *CCITT*
- **European Telecommunications Standards Institute (ETSI):** An organization with members from dozens of countries both within and outside Europe that is dedicated to developing telecommunications standards for the European market (and elsewhere). ETSI is known for, among other things, regulating the use of radio bandwidth in Europe and developing standards such as HiperLAN.

History of Computer Networking and the Internet

- The field of computer networking and today's Internet trace their beginnings back to the early 1960s, when the **telephone network** was the world's dominant communication network.
 - The telephone network uses **circuit switching** to transmit information from a sender to a receiver—an appropriate choice given that **voice is transmitted at a constant rate between sender and receiver**.
 - Given the increasing importance of computers in the early 1960s and the advent of timeshared computers,
 - how to **hook computers together so that they could be shared among geographically distributed users**.
 - The traffic generated by such users was likely to be **bursty**—intervals of activity, such as the sending of a command to a remote computer, followed by periods of inactivity while waiting for a reply or while contemplating the received response of
- ## Packet Switching

History of Computer Networking and the Internet

- Three research groups around the world, each unaware of the others' work began inventing **packet switching** as an efficient and robust alternative to circuit switching.
- The first published work on packet-switching techniques was that of **Leonard Kleinrock**.
- Using queuing theory, Kleinrock's work elegantly demonstrated the *effectiveness of the packet-switching approach* for bursty traffic sources.
- In 1964, Paul Baran at the Rand Institute had begun investigating the use of
 - packet switching for secure voice over military networks, and at the National Physical Laboratory in England, **Donald Davies** and **Roger Scantlebury** were also developing their ideas on packet switching.

History of Computer Networking and the Internet

- The work at MIT, Rand, and the NPL laid the foundations for today's Internet.
- But the Internet also has a long history of a **let's-build-it-and-demonstrate-it attitude** that also dates back to the 1960s.
- J. C. R. Licklider [DEC 1990] and Lawrence Roberts, both colleagues of Kleinrock's at MIT, went on to lead the computer science program at the *Advanced Research Projects Agency (ARPA)* in the United States.
- Roberts published an overall plan for the **ARPAnet**, **the first packet-switched computer network** and a **direct ancestor** of today's public Internet.
- The first host-to-host protocol between ARPAnet end systems, known as the network-control protocol (NCP), was completed.
- *With an end-to-end protocol available, applications could now be written.*
- Ray Tomlinson wrote the first e-mail program in 1972.

History of Computer Networking and the Internet

- **Proprietary Networks and Internetworking: 1972–1980**
- The initial ARPAnet was a single, closed network. In order to communicate with an ARPAnet host, one had to be actually attached to another ARPAnet IMP.
- In the early to mid-1970s, additional stand-alone packet-switching networks besides ARPAnet came into being: **ALOHANet**, a microwave network linking universities on the Hawaiian islands, as well as DARPA's packet-satellite and packet-radio networks; **Telenet**, a BBN commercial packetswitching network based on ARPAnet technology; **Cyclades**, a French packet switching network pioneered by Louis Pouzin; Time-sharing networks such as **Tymnet** and the GE Information Services network, among others, in the late 1960s and early 1970s; IBM's **SNA** (1969–1974), which paralleled the ARPAnet work.

History of Computer Networking and the Internet

- The number of networks was growing. With perfect hindsight we can see that the time was ripe for developing an encompassing architecture for connecting networks together.
- Pioneering work on interconnecting networks (under the sponsorship of the Defense Advanced Research Projects Agency (DARPA)), in essence creating a ***network of networks***, was done by *Vinton Cerf and Robert Kahn*
- These architectural principles were embodied in TCP. The early versions of TCP, however, were quite different from today's TCP. The early versions of TCP combined a reliable in-sequence delivery of data via end-system retransmission (still part of today's TCP) with forwarding functions (which today are performed by IP).
- Early experimentation with TCP, combined with the recognition of the importance of an unreliable, non-flow-controlled, end-to-end transport service for applications such as packetized voice, led to the separation of IP out of TCP and the development of the UDP protocol. The three key Internet protocols that we see today—TCP, UDP, and IP—were conceptually in place by the end of the 1970s.

History of Computer Networking and the Internet

- These architectural principles were embodied in TCP. The early versions of TCP, however, were quite different from today's TCP. The early versions of TCP combined a reliable in-sequence delivery of data via end-system retransmission (still part of today's TCP) with forwarding functions (which today are performed by IP).
- Early experimentation with TCP, combined with the recognition of the importance of an unreliable, non-flow-controlled, end-to-end transport service for applications such as packetized voice, led to the separation of IP out of TCP and the development of the UDP protocol. The three key Internet protocols that we see today—TCP, UDP, and IP—were conceptually in place by the end of the 1970s.

History of Computer Networking and the Internet

- In addition to the DARPA Internet-related research, many other important networking activities were underway.
- In Hawaii, Norman Abramson was developing ALOHAnet, a packet-based radio network that allowed multiple remote sites on the Hawaiian Islands to communicate with each other. The ALOHA protocol was the first multiple-access protocol, allowing geographically distributed users to share a single broadcast communication medium (a radio frequency).
- Metcalfe and Boggs built on Abramson's multiple-access protocol work when they developed the Ethernet protocol for wire-based shared broadcast networks.
- Interestingly, Metcalfe and Boggs' Ethernet protocol was motivated by the need to connect multiple PCs, printers, and shared disks. Twenty-five years ago, well before the PC revolution and the explosion of networks, Metcalfe and Boggs were laying the foundation for today's PC LANs.

History of Computer Networking and the Internet

- **A Proliferation of Networks: 1980–1990**
- By the end of the 1970s, approximately two hundred hosts were connected to the ARPAnet. By the end of the 1980s the number of hosts connected to the public Internet, a confederation of networks looking much like today's Internet, would reach a hundred thousand. The 1980s would be a time of tremendous growth.

History of Computer Networking and the Internet

- Much of that growth resulted from several distinct efforts to create computer networks linking universities together. BITNET provided e-mail and file transfers among several universities in the Northeast.
- CSNET (computer science network) was formed to link university researchers who did not have access to ARPAnet.
- In 1986, NSFNET was created to provide access to NSF-sponsored supercomputing centers. Starting with an initial backbone speed of 56 kbps, NSFNET's backbone would be running at 1.5 Mbps by the end of the decade and would serve as a primary backbone linking regional networks.

History of Computer Networking and the Internet

- In the ARPAnet community, many of the final pieces of today's Internet architecture were falling into place.
- January 1, 1983 saw the official deployment of TCP/IP as the new standard host protocol for ARPAnet (replacing the NCP protocol).
- The transition from NCP to TCP/IP was a flag day event—all hosts were required to transfer over to TCP/IP as of that day.
- In the late 1980s, important extensions were made to TCP to implement host-based congestion control.
- The DNS, used to map between a human-readable Internet name (for example, `gaia.cs.umass.edu`) and its 32-bit IP address, was also developed.

History of Computer Networking and the Internet

- Paralleling this development of the ARPAnet (which was for the most part a US effort), in the early 1980s the French launched the Minitel project, an ambitious plan to bring data networking into everyone's home.
- Sponsored by the French government, the Minitel system consisted of a public packet-switched network (based on the X.25 protocol suite), Minitel servers, and inexpensive terminals with built-in low-speed modems.
- The Minitel became a huge success in 1984 when the French government gave away a free Minitel terminal to each French household that wanted one.
- Minitel sites included free sites—such as a telephone directory site—as well as private sites, which collected a usage-based fee from each user. At its peak in the mid 1990s, it offered more than 20,000 services, ranging from home banking to specialized research databases.
- The Minitel was in a large proportion of French homes 10 years before most Americans had ever heard of the Internet

History of Computer Networking and the Internet

- **The Internet Explosion: The 1990s**
- The 1990s were ushered in with a number of events that symbolized the continued evolution and the soon-to-arrive commercialization of the Internet. ARPAnet, the progenitor of the Internet, ceased to exist. In 1991, NSFNET lifted its restrictions on the use of NSFNET for commercial purposes. NSFNET itself would be decommissioned in 1995, with Internet backbone traffic being carried by commercial Internet Service Providers.
- The main event of the 1990s was to be the emergence of the World Wide Web application, which brought the Internet into the homes and businesses of millions of people worldwide.
- The Web served as a platform for enabling and deploying hundreds of new applications that we take for granted today, including search (e.g., Google and Bing) Internet commerce (e.g., Amazon and eBay) and social networks (e.g., Facebook).

History of Computer Networking and the Internet

- The Web was invented at CERN by Tim Berners-Lee between 1989 and 1991, based on ideas originating in earlier work on hypertext from the 1940s by Vannevar Bush and since the 1960s by Ted Nelson.
- Berners-Lee and his associates developed initial versions of **HTML, HTTP, a Web server, and a browser**—the four key components of the Web.
- Around the end of 1993 there were about two hundred **Web servers** in operation, this collection of servers being just a harbinger of what was about to come. At about this time several researchers were developing Web browsers with GUI interfaces, including Marc Andreessen, who along with Jim Clark, formed Mosaic Communications, which later became *Netscape Communications Corporation*.
- By 1995, university students were using Netscape browsers to surf the Web on a daily basis. At about this time companies—big and small—began to operate Web servers and transact commerce over the Web.
- In 1996, Microsoft started to make browsers, which started the browser war between **Netscape and Microsoft**, which Microsoft won a few years later.

History of Computer Networking and the Internet

- The second half of the 1990s was a period of tremendous growth and innovation for the Internet, with major corporations and thousands of startups creating Internet products and services.
- By the end of the millennium the Internet was supporting hundreds of popular applications, including four killer applications:
 - E-mail, including attachments and Web-accessible e-mail
 - The Web, including Web browsing and Internet commerce
 - Instant messaging, with contact lists
 - Peer-to-peer file sharing of MP3s, pioneered by Napster
- Interestingly, the first two killer applications came from the research community, whereas the last two were created by a few young entrepreneurs.

History of Computer Networking and the Internet

- The period from 1995 to 2001 was a roller-coaster ride for the Internet in the financial markets. Before they were even profitable, hundreds of Internet startups made initial public offerings and started to be traded in a stock market.
- Many companies were valued in the billions of dollars without having any significant revenue streams.
- The Internet stocks collapsed in 2000–2001, and many startups shut down.
- Nevertheless, a number of companies emerged as big winners in the Internet space, including Microsoft, Cisco, Yahoo, e-Bay, Google, and Amazon.

History of Computer Networking and the Internet

- **The New Millennium**
- Innovation in computer networking continues at a rapid pace. Advances are being made on all fronts, including **deployments of faster routers and higher transmission speeds in both access networks and in network backbones.**

History of Computer Networking and the Internet

- Since the beginning of the millennium, we have been seeing aggressive deployment of broadband Internet access to homes—not only **cable modems and DSL** but also fiber to the home.
- This **high-speed Internet access** has set the stage for a wealth of *video applications*, including the distribution of *user-generated video* (for example, YouTube), *on-demand streaming of movies and television shows* (e.g., Netflix) , and *multi-person video conference* (e.g., Skype).

History of Computer Networking and the Internet

- The increasing ubiquity of high-speed (54 Mbps and higher) public WiFi networks and medium-speed (up to a few Mbps) Internet access via **3G and 4G cellular telephony networks** is not only making it possible to remain constantly connected while on the move, but also enabling new location-specific applications.
- The number of wireless devices connecting to the Internet surpassed the number of wired devices in 2011. This high-speed wireless access has set the stage for the **rapid emergence of hand-held computers** (*iPhones, Androids, iPads*, and so on), which enjoy constant and untethered access to the Internet.

History of Computer Networking and the Internet

- Online social networks, such as Facebook and Twitter, have created massive people networks on top of the Internet.
- Many Internet users today “live” primarily within Facebook.
- Through their APIs, the online *social networks* create platforms for new *networked applications and distributed games*.

History of Computer Networking and the Internet

Online service providers, such as Google and Microsoft, have deployed their own extensive private networks, which not only connect together their globally distributed data centers, but are used to bypass the Internet as much as possible by peering directly with *lower-tier ISPs*

As a result, Google provides search results and email access almost instantaneously, as if their data centers were running within one's own computer.

History of Computer Networking and the Internet

- Many Internet commerce companies are now running their applications in the “cloud”—such as in *Amazon’s EC2*, in *Google’s Application Engine*, or in *Microsoft’s Azure*.
- Many companies and universities have also migrated their Internet applications (e.g., email and Web hosting) to the cloud.
- Cloud companies not only provide applications scalable computing and storage environments, but also provide the applications *implicit access to their high-performance private networks*.

Security in the Internet

- **Types of Security**
- *Computer Security*
 - - generic name for the collection of tools designed to protect data and to thwart hackers
- *Network Security*
 - - measures to protect data during their transmission
- *Internet Security*
 - - measures to protect data during their transmission over a collection of interconnected networks

Security in the Internet

- **Goals of Security**
- **Confidentiality** – prevents unauthorized use or disclosure of information
- **Integrity** - safeguards the accuracy and completeness of information
- **Availability** – authorized users have reliable and timely access to information

Security in the Internet

- **Cryptography**- Has evolved into a complex science in the field of information security.
- Part of a field of study known as **cryptology**
- **Cryptology includes:**
 - - **Cryptography**
 - Study of methods for secret writing
 - Transforming messages into unintelligible form
 - Recovering messages using some secret knowledge (key)
 - - **Cryptanalysis:**
 - Analysis of cryptographic systems, inputs and outputs
 - To derive confidential information

Security in the Internet

- **Cryptography**
- **Encryption** – process of *transforming plaintext to ciphertext using a cryptographic key*
- **Symmetric key cryptography** – *uses a single key to both encrypt and decrypt information. Also known as private key. - Includes DES, 3DES, AES, IDEA, RC5, Blowfish*
- **Asymmetric key cryptography** – *separate keys for encryption and decryption (public and private key pairs)*
- - Includes **RSA, Diffie-Hellman, El Gamal**

Security in the Internet

- **Terminology of cryptography**
- **Cipher**
 - Cryptographic technique (algorithm) applying a secret transformation to messages
- **Plaintext / cleartext**
 - Original message or data
- **Encryption**
 - Transforming plaintext, using a secret key, so meaning is concealed
- **Ciphertext**
 - Unintelligible encrypted plaintext
- **Decryption**
 - Transforming ciphertext back into original plaintext
- **Cryptographic Key**
 - Secret knowledge used by cipher to encrypt or decrypt message

Security in the Internet

Security-Part-1.pdf - Adobe Reader

File Edit View Window Help

60 / 85 70.4%

Tools Sign Comment

Cryptography

The diagram illustrates the cryptography process. It starts with a yellow envelope icon labeled 'Plaintext'. An arrow labeled 'ENCRYPTION ALGORITHM' points to a yellow envelope icon labeled 'Ciphertext'. Below this arrow is a key icon and a box labeled 'Encryption Key'. From the 'Ciphertext' icon, an arrow labeled 'DECRYPTION ALGORITHM' points to another yellow envelope icon labeled 'Plaintext'. Below this arrow is a key icon and a box labeled 'Decryption Key'. Below the 'Encryption Key' box is a key icon and a box labeled 'Shared Key'. Below the 'Decryption Key' box is a key icon and a box labeled 'Shared Key'. To the right of these 'Shared Key' boxes is the text 'Symmetric Key Cryptography'. Below the 'Shared Key' boxes are two key icons. The left one is a padlock icon and a box labeled 'Public Key'. The right one is a key icon and a box labeled 'Private Key'. To the right of these boxes is the text 'Asymmetric Key Cryptography'.

Plaintext

ENCRYPTION ALGORITHM

Ciphertext

DECRYPTION ALGORITHM

Plaintext

Encryption Key

Decryption Key

Shared Key

Shared Key

Symmetric Key Cryptography

Public Key

Private Key

Asymmetric Key Cryptography

APNIC

Security in the Internet

- Symmetric Key Algorithm

Stream ciphers – encrypts bits of the message at a time

Block ciphers – takes a block of bits and encrypts them as a single unit

Security in the Internet

- **Cryptography**
- **Digital Signature** – sender encrypts message with own private key instead of encrypting with intended receiver's public key
- **Message digests** – produces a condensed representation of a message (hashing)
 - MD5
 - SHA-1
 - HMAC

Security in the Internet

- Secret Key Algorithms
- **DES** – block cipher using shared key encryption, 56-bit
- **3DES** (Triple DES) – a block cipher that applies DES three times to each data block
- **RC4** – variable-length key, “stream cipher” (generate stream from key, XOR with data)
- **AES** – replacement for DES; current standard

Security in the Internet

- **Triple DES**
- 3DES (Triple DES) – a block cipher that applies DES three times to each data block
- Uses a key bundle comprising of **three DES keys (K1, K2, K3)**, each with 56 bits excluding parity.
- **DES encrypts with K1, decrypts with K2, then encrypts with K3**
- **$C_i = EK_1(DK_2(EK_1(P_i)))$**
- Disadvantage: *very slow*

Security in the Internet

Security-Part-1.pdf - Adobe Reader

File Edit View Window Help

66 / 85 70.4%

Tools Sign Comment

Secret Key Encryption

The diagram illustrates the Secret Key Encryption process. It shows a flow from 'Sensitive Information (Cleartext)' on the left to 'Sensitive Information (Cleartext)' on the right. In the middle, a cloud labeled 'Internet' contains the text '(Ciphertext)'. Above the 'Internet' cloud, two yellow keys labeled 'DES' are shown, each with a red arrow pointing down to a green oval labeled 'ENCRYPT' and another green oval labeled 'DECRYPT'. The 'ENCRYPT' oval is connected to the 'Internet' cloud by a red arrow, and the 'DECRYPT' oval is connected to the 'Internet' cloud by a red arrow. The 'Internet' cloud is connected to the 'DECRYPT' oval by a red arrow. The 'DECRYPT' oval is connected to the final 'Sensitive Information (Cleartext)' by a red arrow.

Shared Secret Key

Shared Secret Key

Sensitive Information (Cleartext)

ENCRYPT

Internet (Ciphertext)

DECRYPT

Sensitive Information (Cleartext)

Common Algorithms: DES, 3DES, AES, IDEA

DOUBLE SHOT SECURITY

APNIC

3:57 PM 8/10/2016

Security in the Internet

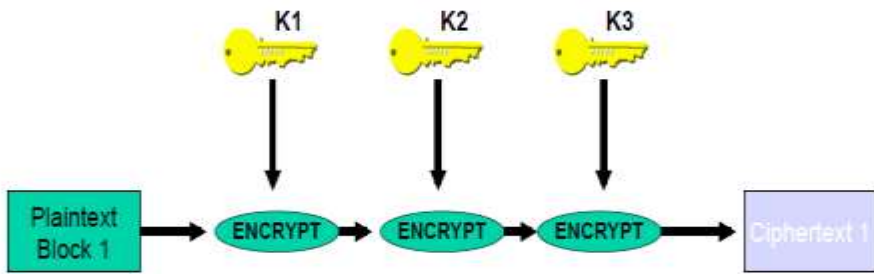
Security-Part-1.pdf - Adobe Reader

File Edit View Window Help

67 / 85 70.4%

Tools Sign Comment

Triple DES (3DES)



The diagram illustrates the Triple DES (3DES) encryption process. It shows a sequence of three encryption steps. The first step takes 'Plaintext Block 1' as input and uses key 'K1' to perform an 'ENCRYPT' operation. The output of the first step is the input for the second step, which uses key 'K2' for another 'ENCRYPT' operation. The output of the second step is the input for the third step, which uses key 'K3' for a final 'ENCRYPT' operation. The final output is 'Ciphertext 1'.

- Many applications use $K3=K1$, yielding a key length of 112 bits
- Interoperable with conventional DES if $K1=K2=K3$

DOUBLE SHOT SECURITY

APNIC

4:01 PM 8/10/2016

Security in the Internet

- DES
- Data Encryption Standard
- *Developed by IBM* for the US government in 1973-1974, and approved in Nov 1976.
- Based on Horst Feistel's Lucifer cipher block cipher using shared key encryption, *56-bit key length*
- *Block size: 64 bits*

Security in the Internet

- AES
 - *Advanced Encryption Standard (AES) Cipher*
Published in November 2001
- Symmetric block cipher
 - *Has a fixed block size of 128 bits*
 - *Has a key size of 128, 192, or 256 bits*
 - Based on Rijndael cipher which was developed by Joan Daemen and Vincent Rijmen

Security in the Internet

- **Hash Functions**
- *A hash function takes an input message of arbitrary length and outputs fixed-length code. The fixed-length output is called the **hash**, or the *message digest*, of the original input message.*
- Hashing
 - Also called a digest or checksum
 - A form of signature that represents the data.
 - Uses:
 - Verifying file integrity - if the hash changes, it means the data is either compromised or altered in transit.
 - Digitally signing documents
 - Hashing passwords

Security in the Internet

- **HASHING**
- MD5 Message Digest Algorithm
 - Outputs a 128-bit fingerprint of an arbitrary-length input
- SHA-1 (Secure Hash Algorithm)
 - Outputs a 160-bit message digest similar to MD5
- Widely-used on security applications (TLS, SSL, PGP, SSH, S/MIME, IPsec)

Security in the Internet

- **Diffie-Hellman**
- Diffie-Hellman Protocol – requires that both the sender and recipient of a message have key pairs.
- Combining one's private key and the other's public key, both parties can compute the same shared secret number.

Security in the Internet

- **Trusted Network**
- Standard defensive-oriented technologies
 - Firewall
 - Intrusion Detection
- Build TRUST on top of the TCP/IP infrastructure
 - Strong authentication
 - Public Key Infrastructure (PKI)

Security in the Internet

- **Strong Authentication**
- **Two-factor authentication**
 - - Passwords (something you know)
 - - Tokens (something you have)
- **Examples:**
 - - Passwords
 - - Tokens
 - - Tickets
 - - Restricted access
 - - PINs
 - - Biometrics
 - - Certificates

Security in the Internet

- Public Key Infrastructure
- Framework that builds the network of trust
- Combines public key cryptography, digital signatures, to ensure confidentiality, integrity, authentication, no repudiation, and access control
- Protects applications that require high level of security

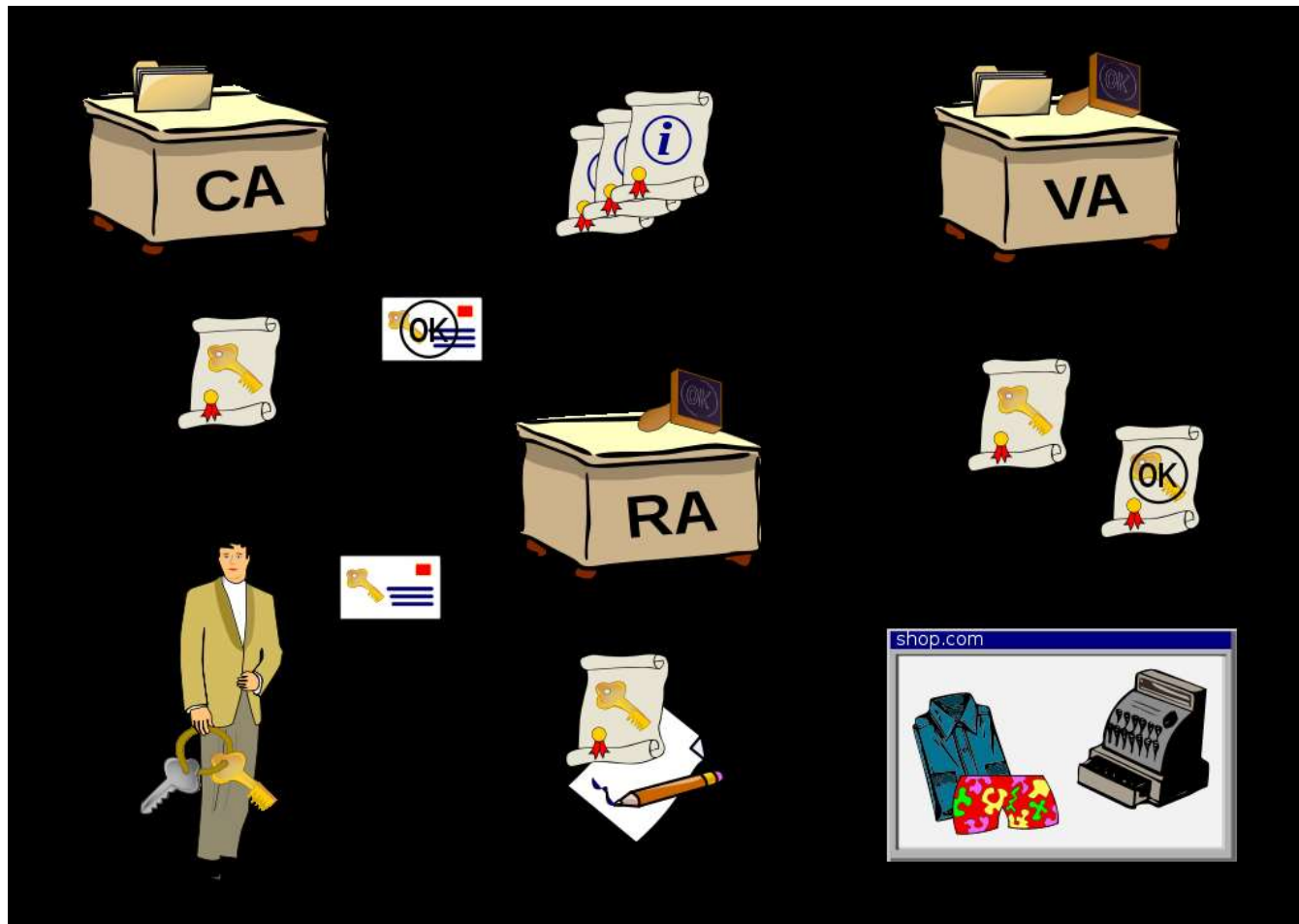
Security in the Internet

- PKI Components
- Certificate Authority (CA) – a trusted third party
 - - Trusted by both the owner of the certificate and the party relying upon the certificate
- Registration Authority (RA) – binds keys to users
 - - Users who wish to have their own certificate registers with the RA
- Validation Authority (VA) – validates the user is who he says he is

Security in the Internet

- Certificate Authority
- Components:
- Certificate Authority – a trusted third party
- Trusted by both the owner of the certificate and the party relying upon the certificate.
 - Validation Authority
 - Registration Authority

PKI Process



Security in the Internet

- **Digital Certificate**
- Digital certificate – basic element of PKI
secure credential that identifies the owner
- Also called public key certificate

Security in the Internet

- Digital Certificates
- Digital certificates deal with the problem of
 - Binding a public key to an entity
 - A major legal issue related to eCommerce
- **A digital certificate contains:**
 - - User's public key
 - - User's ID
 - - Other information e.g. validity period
- Certificate examples:
 - - X509 (standard)
 - - PGP (Pretty Good Privacy)
 - - Certificate Authority (CA) creates and digitally signs certificates

Security in the Internet

- Digital Certificates
- To obtain a digital certificate, Alice must:
 - Make a certificate signing request to the CA
 - Alice sends to CA:
 - Her identifier IdA
 - Her public key KA_PUB
- Additional information
- CA returns Alice's digital certificate, cryptographically binding her identity to public key:
- - $CertA = \{IDA, KA_PUB, info, SigCA(IDA, KA_PUB, info)\}$

Security in the Internet

- **X.509**
- An ITU-T standard for a public key infrastructure for single-sign-on and **Privilege Management Infrastructure (PMI)**
- Assumes a strict hierarchical system of Certificate Authorities (CAs) Structure of a Certificate

concept of Quality of Service (QoS)

- *Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies.*
- The primary **goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics.**
- Important is **making sure that providing priority for one or more flows does not make other flows fail.**
- QoS technologies provide the elemental building blocks that will be used for future business applications in campus, WAN, and service provider networks.

concept of Quality of Service (QoS)

- QoS features provide improved and more predictable network service by providing the following services:
 - **Supporting dedicated bandwidth**
 - **Improving loss characteristics**
 - **Avoiding and managing network congestion**
 - **Shaping network traffic**
 - **Setting traffic priorities across the network**

concept of Quality of Service (QoS)

- QoS features throughout a network to provide for **end-to-end** QoS delivery. The following three components are necessary to deliver *QoS across a heterogeneous network*:
 - **QoS within a single network element, which includes queueing, scheduling, and traffic shaping features.**
 - **QoS signalling techniques for coordinating QoS for end-to-end delivery between network elements.**
 - **QoS policing and management functions to control and administer end-to-end traffic across a network.**

concept of Quality of Service (QoS)

- Not all QoS techniques are appropriate for all network routers. Because **edge routers and backbone routers** in a network do not necessarily perform the same operations, the QoS tasks they perform might differ as well.
- In general, **edge routers** perform the following QoS functions:
 - **Packet classification**
 - **Admission control**
 - **Configuration management**
- In general, **backbone routers** perform the following QoS functions:
 - **Congestion management**
 - **Congestion avoidance**

concept of Quality of Service (QoS)

- Implementing Cisco IOS QoS in your network promotes the following features:
 - **Control over resources.** You have control over which resources (bandwidth, equipment, wide-area facilities, and so on) are being used. For example, you can limit bandwidth consumed over a backbone link by File Transfer Protocol (FTP) transfers or give priority to an important database access.
 - **Tailored services.** If you are an ISP, the control and visibility provided by QoS enables you to offer carefully tailored grades of service differentiation to your customers.
 - **Coexistence of mission-critical applications.** Cisco QoS features make certain of the following conditions:

concept of Quality of Service (QoS)

- – That your WAN is used efficiently by mission-critical applications that are most important to your business.
- – That bandwidth and minimum delays required by time-sensitive multimedia and voice applications are available.
- – That other applications using the link get their fair service without interfering with mission-critical traffic.

concept of Quality of Service (QoS)

- **QoS Identification and Marking**
- Identification and marking is accomplished through classification and reservation
- **Classification**
- To provide preferential service to a type of traffic, it must first be identified. Second, the packet may or may not be marked. These two tasks make up classification.
- When the packet is identified but not marked, classification is said to be on a per-hop basis. This is when the classification pertains only to the device that it is on, not passed to the next router.
- This happens with priority queuing (PQ) and custom queuing (CQ). When packets are marked for network-wide use, IP precedence bits can be set.
- Common methods of identifying flows include access control lists (ACLs), policy-based routing, committed access rate (CAR), and network-based application recognition (NBAR).

concept of Quality of Service (QoS)

- **QoS Within a Single Network Element**
- Congestion management, queue management, link efficiency, and shaping/policing tools provide QoS within a single network element.
- **QoS Identification and Marking**
- Identification and marking is accomplished through classification and reservation.

concept of Quality of Service (QoS)

- **Congestion Management**
- Because of the bursty nature of voice/video/data traffic, sometimes the amount of traffic exceeds the speed of a link. At this point, what will the router do? Will it buffer traffic in a single queue and let the first packet in be the first packet out? Or, will it put packets into different queues and service certain queues more often? Congestion-management tools address these questions.
- Tools include priority queuing (PQ), custom queuing (CQ), weighted fair queuing (WFQ), and class-based weighted fair queuing (CBWFQ).

concept of Quality of Service (QoS)

- **Queue Management**
- Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and will be dropped. This is a tail drop. The issue with tail drops is that the router cannot prevent this packet from being dropped (even if it is a high-priority packet). So, a mechanism is necessary to do two things:
 - **1. Try to make sure that the queue does not fill up, so that there is room for high-priority packets**
 - **2. Allow some sort of criteria for dropping packets that are of lower priority before dropping**
 - higher-priority packets
 - Weighted early random detect (WRED) provides both of these mechanisms.

concept of Quality of Service (QoS)

- **Link Efficiency**
- Many times low-speed links present an issue for smaller packets. For example, the serialization delay of a 1500-byte packet on a 56-kbps link is 214 milliseconds. If a voice packet were to get behind this big packet, the delay budget for voice would be exceeded even before the packet left the router! Link fragmentation and interleave allow this large packet to be segmented into smaller packets interleaving the voice packet. Interleaving is as important as the fragmentation. There is no reason to fragment the packet and have the voice packet go behind all the fragmented packets. Another efficiency is the elimination of too many overhead bits. For example, RTP headers have a 40-byte header.
- With a payload of as little as 20 bytes, the overhead can be twice that of the payload in some cases. RTP header compression (also known as Compressed Real-Time Protocol header) reduces the header to a more manageable size.

concept of Quality of Service (QoS)