Computer Networks

Malik Algazaeery

Chapter1-Computer Networks

Motivation

Two important questions:

-Why do we need computer Networks?

-Why do we study computer Networks?

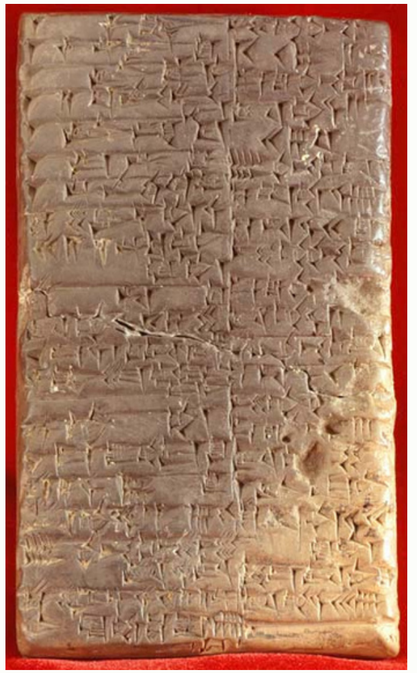
-Why do we need computer Networks?

Ans: to share messages (Information)

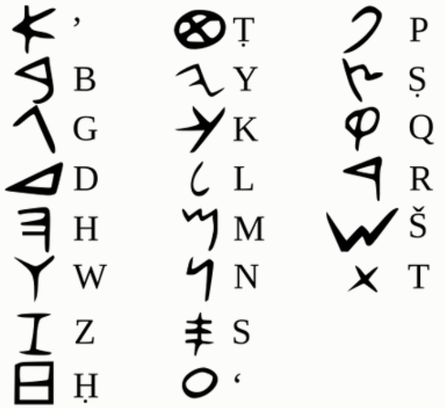
- Cuneiform Script (~3500 BCE): First written language by the Sumerians in Mesopotamia (Iraq), used for record-keeping and information sharing on clay tablets.

- Alphabet Systems (~1500 BCE): Phoenician alphabet in the levant simplified communication, leading to modern alphabetic writing systems.

- Paper and Ink (105 CE): Invented by the Chinese, paper became the main medium for written communication, replacing stone and clay.



document of salary payment:
https://de.wikipedia.org/wiki/Keilschrift

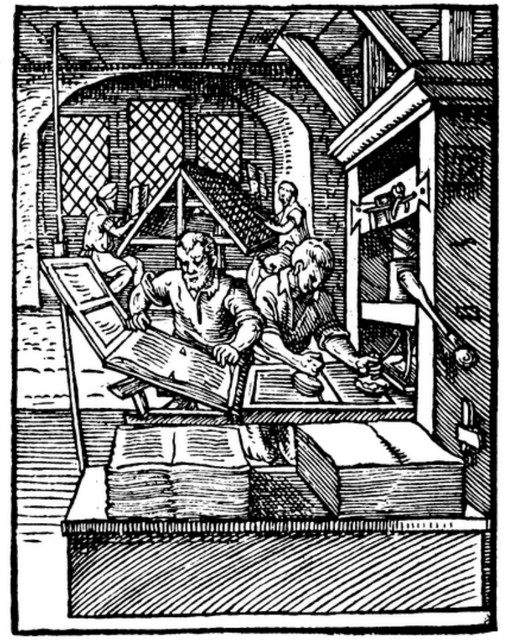


The Phoenician alphabet:
https://en.wikipedia.org/wiki/Phoenician_alphabet

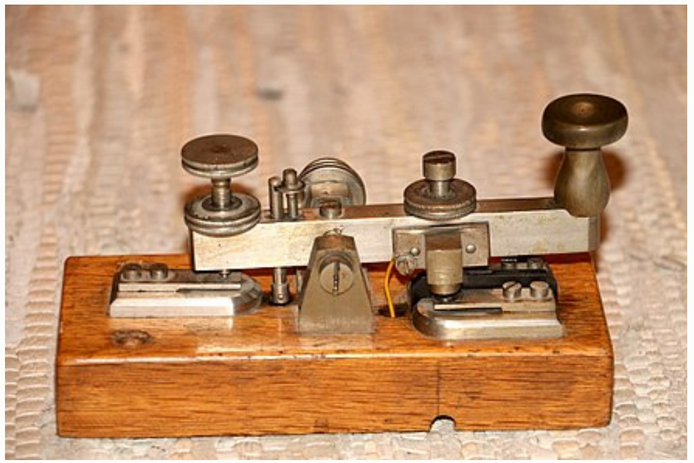
- Printing Press (1440 CE): Gutenberg’s invention (Germany) revolutionized mass communication by enabling the mass production of books and documents.

- Postal Systems (1500s): Formalized postal services developed for long-distance written communication, connecting empires and nations.

- Telegraph (1830s): First electronic communication system, transmitting messages over long distances using Morse code.



An early wooden printing press, depicted in 1568: https://en.wikipedia.org/wiki/Johannes_Gutenberg

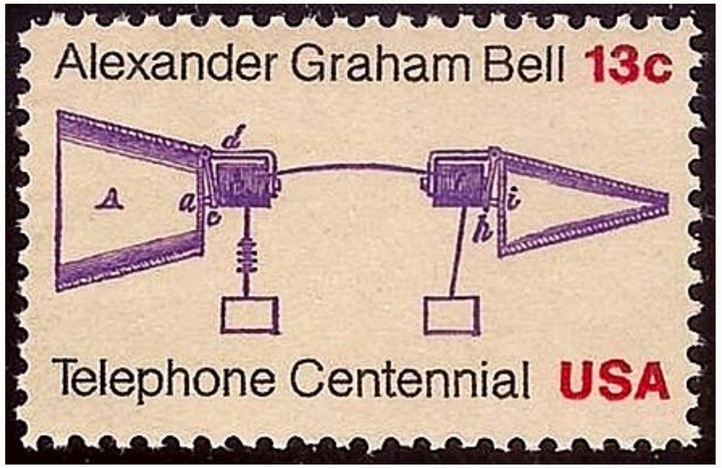


https://en.wikipedia.org/wiki/Morse_code

- Telephone (1876): Invention of the telephone by Alexander Graham Bell enabled real-time voice communication over long distances.

- Radio (1900s): Wireless transmission of sound, enabling mass communication through live broadcasts without physical connections.

- Television (1920s-1930s): Combined sound and visuals for entertainment and news broadcasting to large audiences.

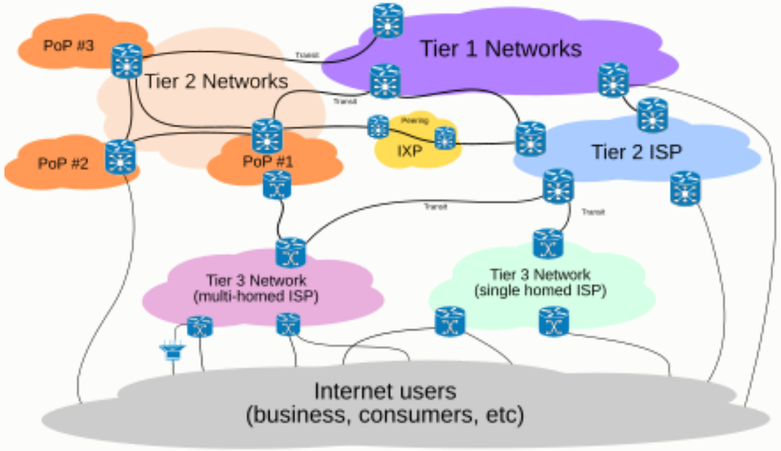


https://en.wikipedia.org/wiki/History_of_the_telephone

https://en.wikipedia.org/wiki/Television

- Satellite Communication (1960s): Allowed global transmission of television, radio, and telephone signals, linking distant regions.
- Personal Computers (1970s-1980s): Brought digital communication into homes, facilitating text-based interactions via networks.
- Mobile Phones (1980s-1990s): Made portable voice communication widely accessible, evolving into multi-functional smartphones.
- Internet (1960s-present): Now the global backbone of digital communication, enabling real-time data exchange, emails, video calls, and social media.

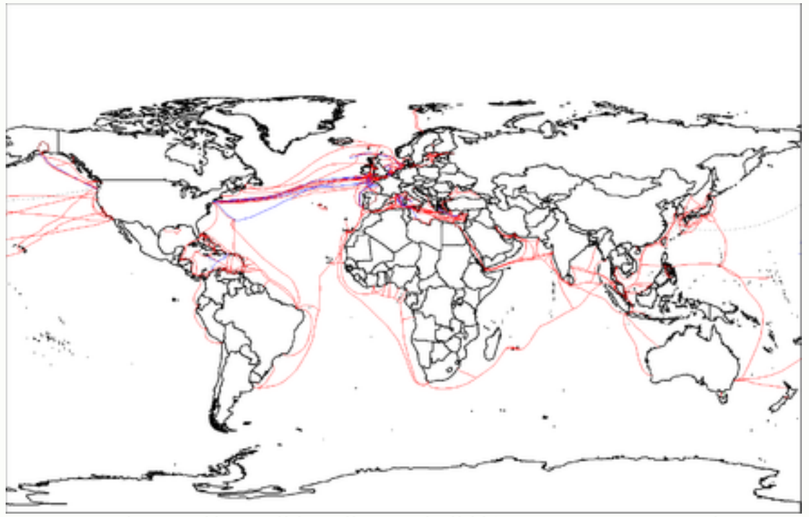
https://en.wikipedia.org/wiki/Satellite



https://en.wikipedia.org/wiki/Internet

-Why do we study computer Networks?

Ans: It helps us understand the network (Internet) infrastructure to enhance the performance in many aspects for example:


https://en.wikipedia.org/wiki/Computer_network

-Increase Efficiency:

- Optimize data transmission and network performance.
- Ensure reliable connectivity with minimal downtime.

-Enhance Security:

- Protect networks from cyberattacks and data breaches.
- Implement encryption and security protocols for safe data transfer.

-Enable Scalability:

- Design networks that grow with user and traffic demands.
- Support expansion in IoT, devices, and global users.

-Ensure Reliability:

- Design fault-tolerant systems for continuous uptime and data availability.

Important Course Information:

- Lecture Materials & Homework: Available on Moodle.
- Module Registration: Please register through the LSF system.
- Urgent Module Enrollment: If you're unable to register through LSF but need to take the module this semester, you can apply for manual admission (Handzulassung). Fill out the form here: Manual Admission Form.
- Final Exam Eligibility: To be eligible for the final exam, you must successfully submit all homework assignments. You are allowed to fail in only one out of all the assignments.
- Homework Grading: Each assignment will be graded as either 1 (pass) or 0 (fail). You will receive a 1 if at least 75% of the assignment is solved correctly.
- Previous Homework Submissions: If you've already completed the homework in a previous semester, you are automatically eligible for the final exam. Please contact the lecturer you submitted your homework to, and ask them to send me an email confirming this.
- Final Exam Weighting: The final exam accounts for 100% of the module grade.
- Homework Groups: Form groups of three students for homework assignments.

This presentation, along with all future lectures, is based on the book Computer Networking: A Top-Down Approach, Eighth Edition, by James F. Kurose and Keith W. Ross.
https://elibrary.pearson.de/book/99.150005/9781292405513

For all images, figures, and diagrams in these slides, if no source is cited directly below, the material is sourced from the book referenced earlier.

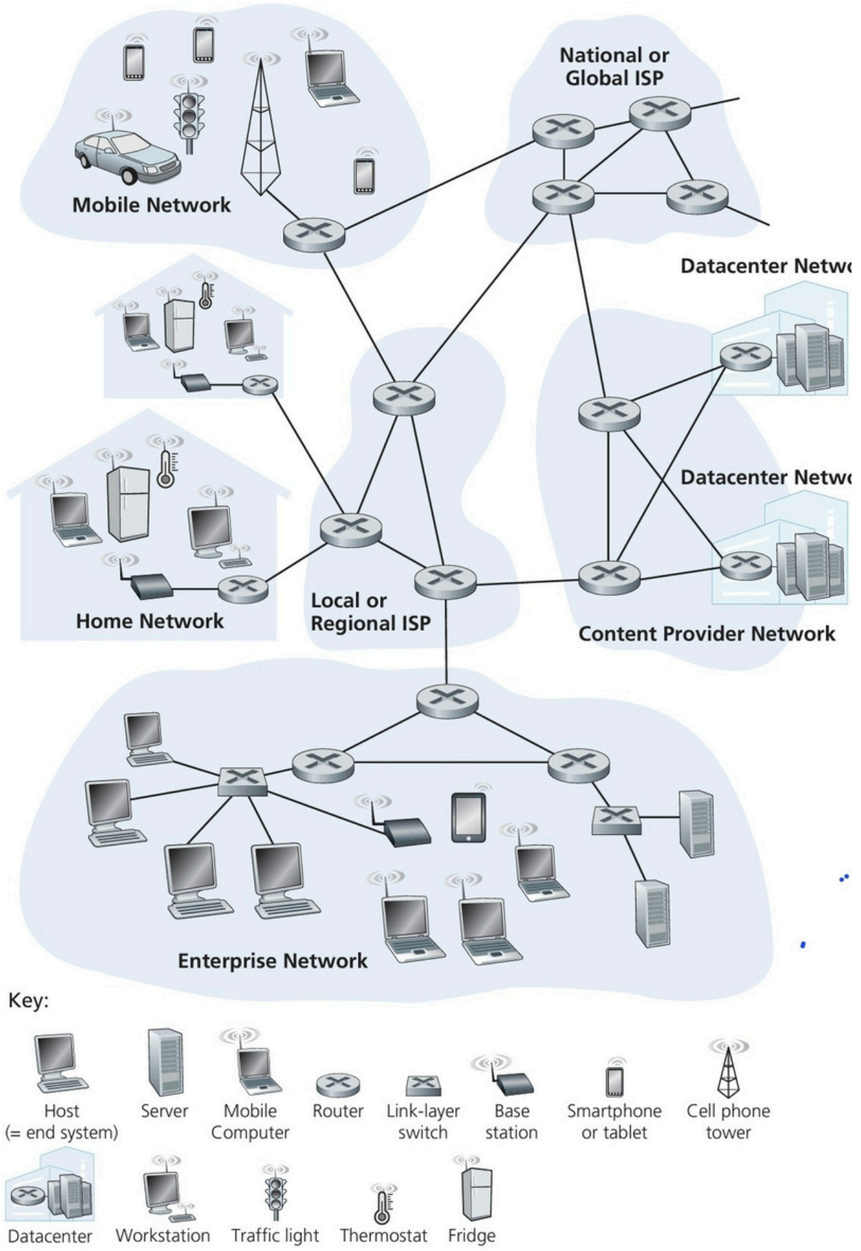
Chapter-1 agenda:

- What is the Internet.
- Eathernet and WiFi.
- Physical Media.
- Radio channels (wireless channels).
- The network core and packet switching.
- Delays and Packet loss.
- Circuit switching.
- Protocol Layers and Their Service Models.
- Networks Under Attack.

Kapitel-1: Computer Networks and the Internet

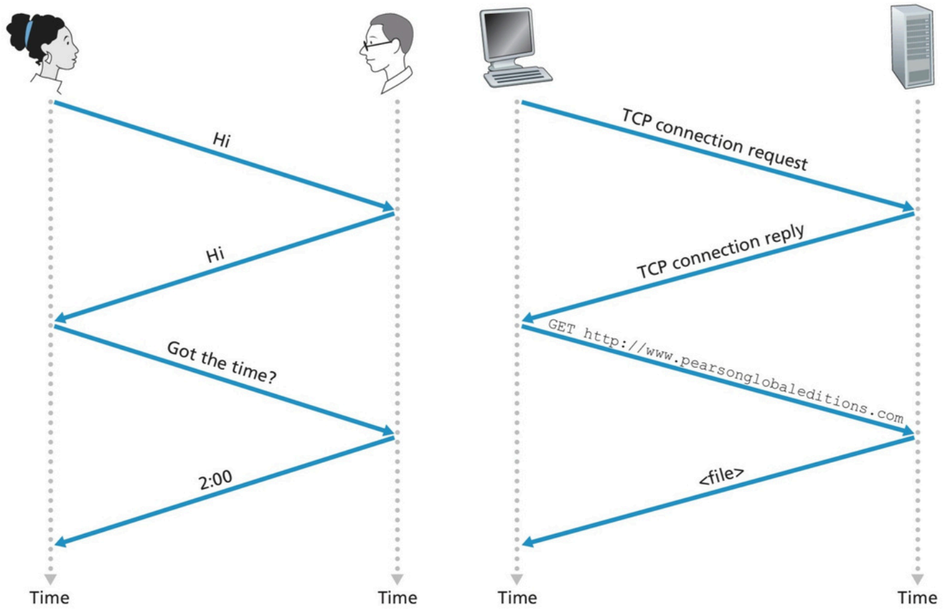
What is the Intrtnet?

- The Internet is a computer network that interconnects billions of computing devices throughout the world.
- End systems are connected together by a network of communication links and packet switches.
- Different links can transmit data at different rates, with the transmission rate of a link measured in bits/second.
- Packet switch takes a packet arriving on one of its incoming communication links and forwards that packet on one of its outgoing communication links.
- Two most prominent types in today's Internet are routers and link-layer switches.
- 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.
- Internet standards are developed by the Internet Engineering Task Force (IETF) [IETF 2020]. The IETF standards documents are called requests for comments (RFCs).



The internet as services:

- End systems attached to the Internet provide a socket interface 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.
- Internet socket interface is a set of rules that the sending program must follow so that the Internet can deliver the data to the destination program.



Internet 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.

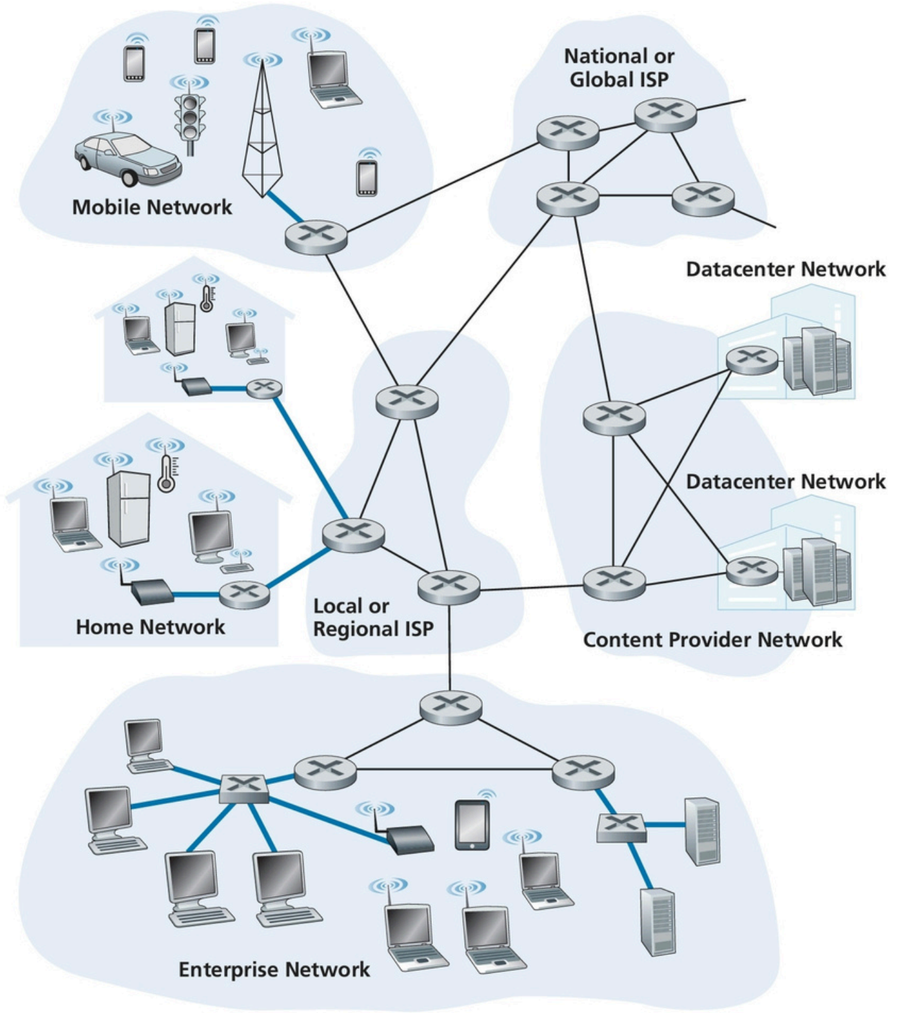
- The Internet use protocols. Different protocols are used to accomplish different communication tasks.

- example protocol with which you are probably familiar, consider what happens when you make a request to a Web server, that is, when you type the URL of a Web page into your Web browser. The scenario is illustrated in the right half of the Figure.

The network edge and access networks:

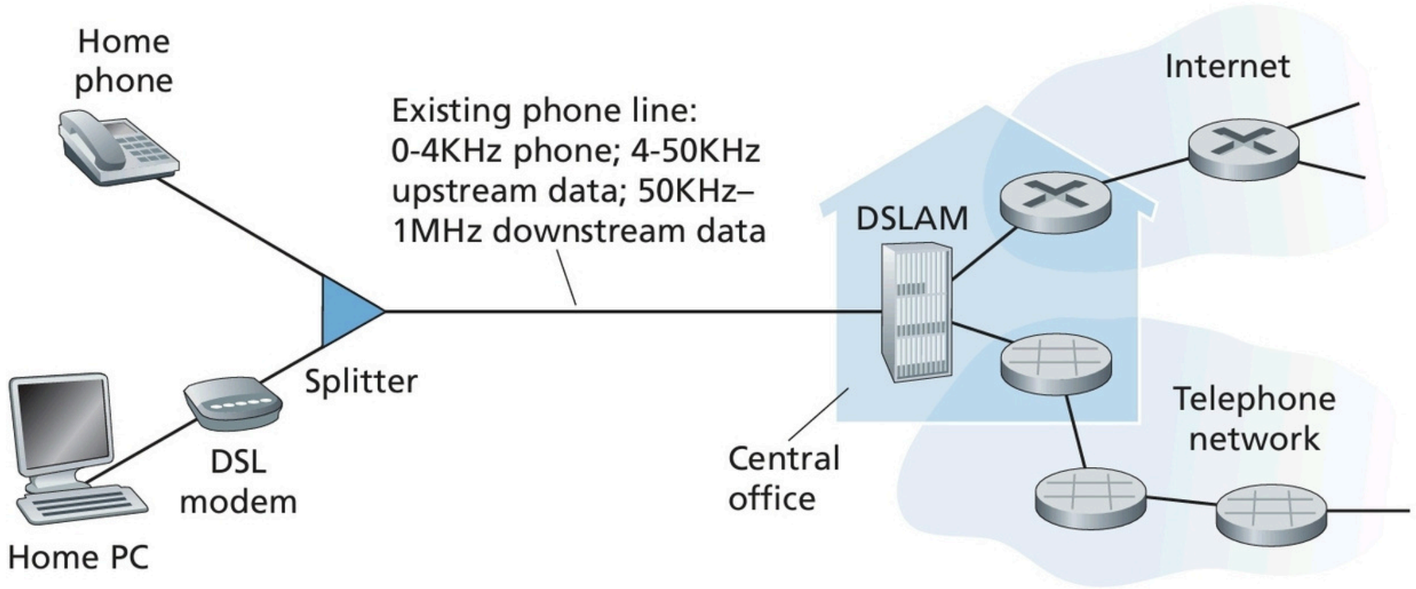
- End systems sit at the edge of the Internet, as shown in the figure. The Internet's end systems include desktop computers, servers, mobile phones etc.

- 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.



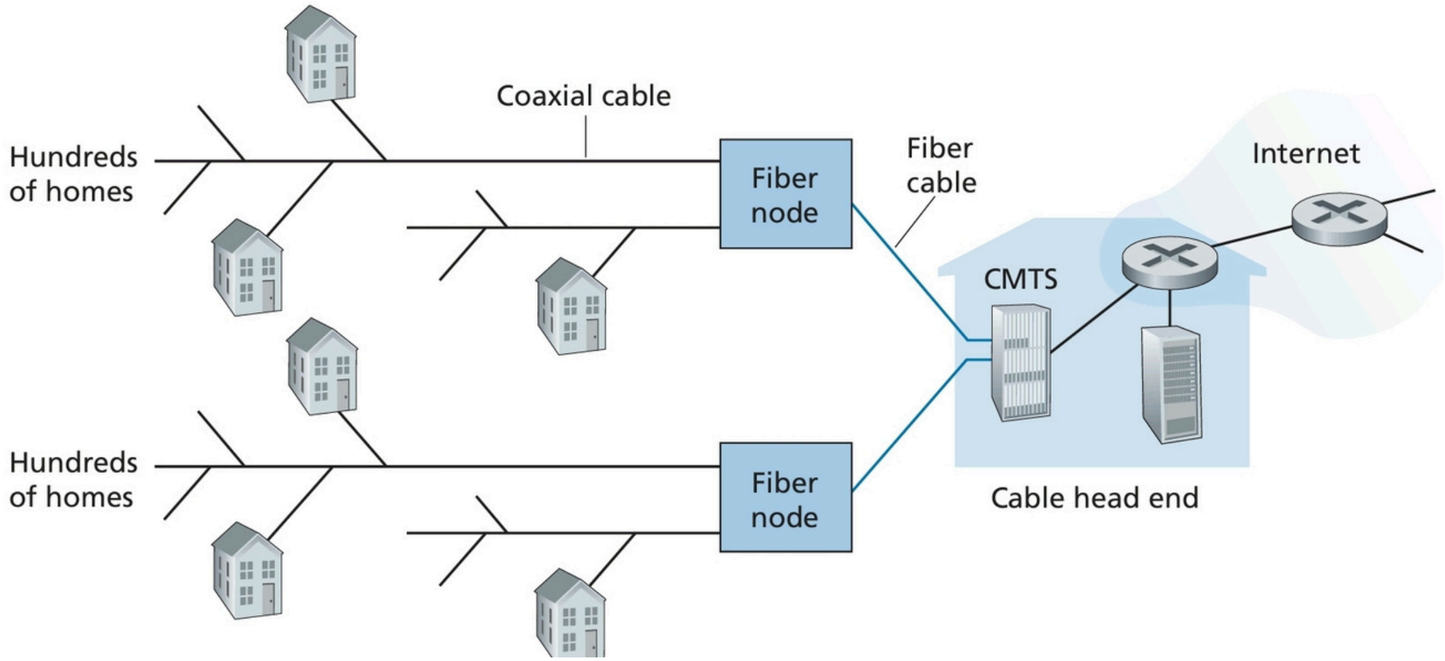
Home Access: DSL

As shown in the Figure, each customer's DSL modem uses the existing telephone line exchange data with a digital subscriber line access multiplexer (DSLAM) located in the telco's local central office (CO). The home's DSL modem takes digital data and translates it to high- 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.



Cable Internet access:

- makes use of the cable television company's existing cable television infrastructure.
- Because both fiber and coaxial cable are employed in this system, it is often referred to as hybrid fiber coax (HFC).
- At the cable head end, the cable modem termination system (CMTS) serves a similar function as the DSL network's DSLAM— turning the analog signal sent from the cable modems in many downstream homes back into digital format.
- 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.

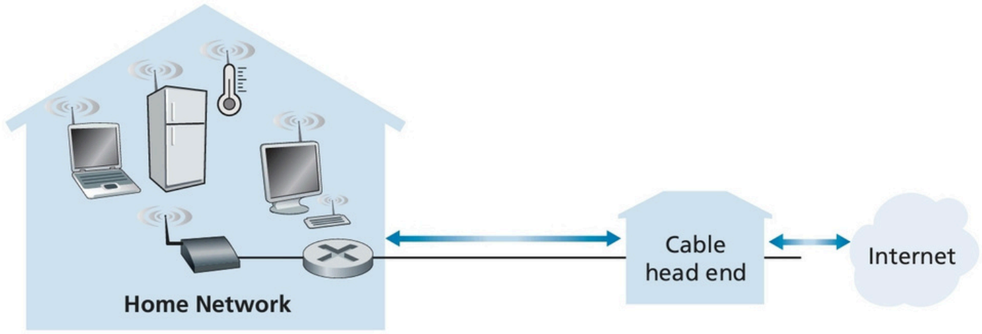


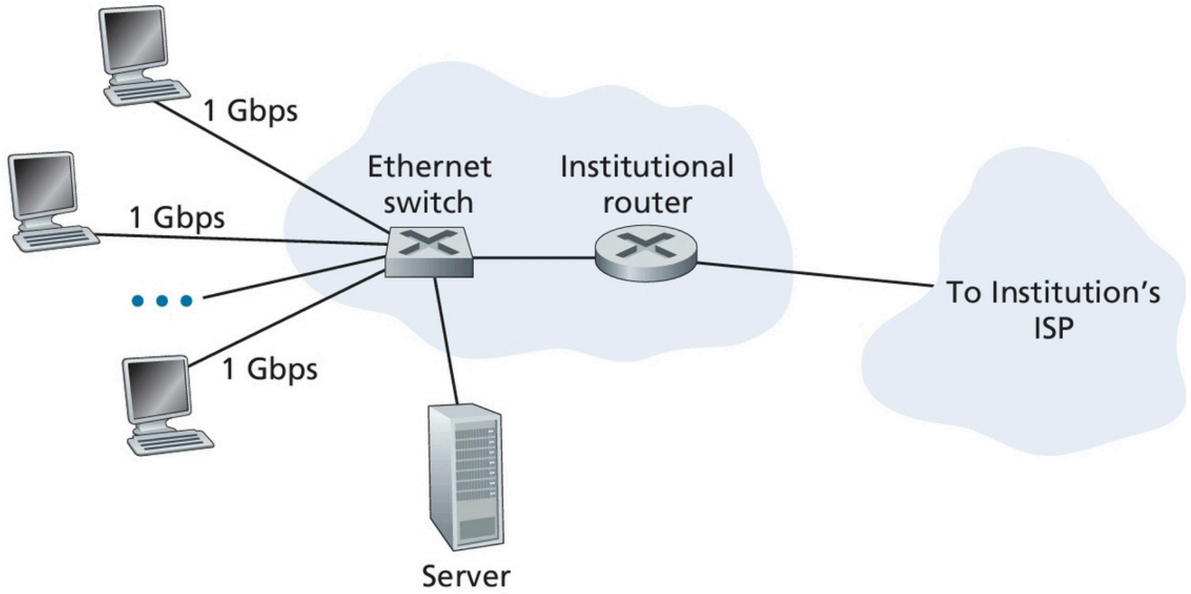
fiber to the home (FTTH):

- As the name suggests, the FTTH concept is simple—provide an optical fiber path from the CO directly to the home.
- FTTH can potentially provide Internet access rates in the gigabits per second range.
- In addition to DSL, Cable, and FTTH, 5G fixed wireless is beginning to be deployed. 5G fixed wireless not only promises high-speed residential access, but will do so without installing costly and failure-prone cabling from the telco’s CO to the home.

Ethernet and WiFi

- Ethernet is the most prevalent access technology in corporate, university, and home networks.
- Ethernet users use twisted-pair copper wire to connect to an Ethernet switch.
- In a wireless LAN setting, wireless users transmit/receive packets to/from an access point that is connected into the enterprise's network (most likely using wired Ethernet), which in turn is connected to the wired Internet.



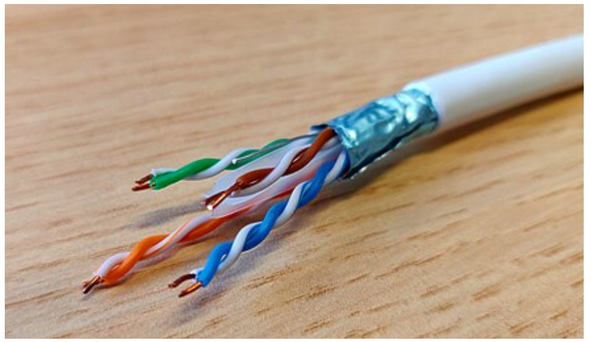


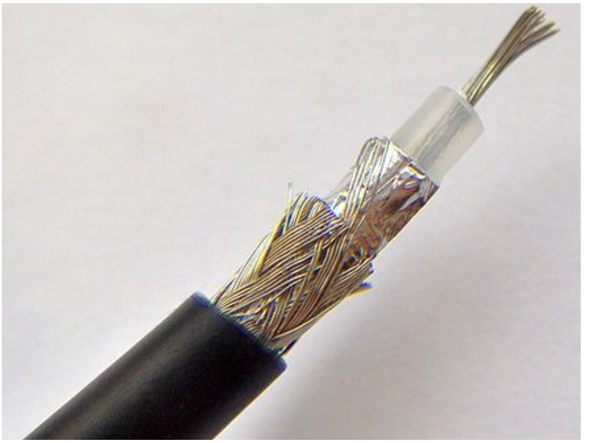
Wide-Area Wireless Access 3G and LTE 4G and 5G:

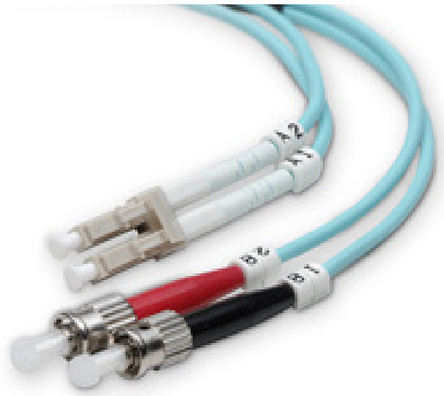
- Mobile devices are being used to message, share photos in social networks, make mobile payments, watch movies, stream music, and much more while on the run.
- These devices employ the same wireless infrastructure used for cellular telephony to send/receive packets through a base station that is operated by the cellular network provider.
- Unlike WiFi, a user need only be within a few tens of kilometers (as opposed to a few tens of meters) of the base station.
- Telecommunications companies have made enormous investments in so-called fourth-generation (4G) wireless, which provides real-world download speeds of up to 60 Mbps. But even higher-speed wide-area access technologies—a fifth-generation (5G) of wide-area wireless networks—are already being deployed.

Physical Media:

- For each transmitter-receiver pair, bits are sent by propagating electromagnetic waves or optical pulses across a physical medium.
- The physical medium can take many shapes and forms and does not have to be of the same type for each transmitter-receiver pair along the path.
- guided media and unguided media: With guided media, the waves are guided along a solid medium, such as a fiber-optic cable, a twisted-pair copper wire, or a coaxial cable. With unguided media, the waves propagate in the atmosphere and in outer space, such as in a wireless LAN or a digital satellite channel.



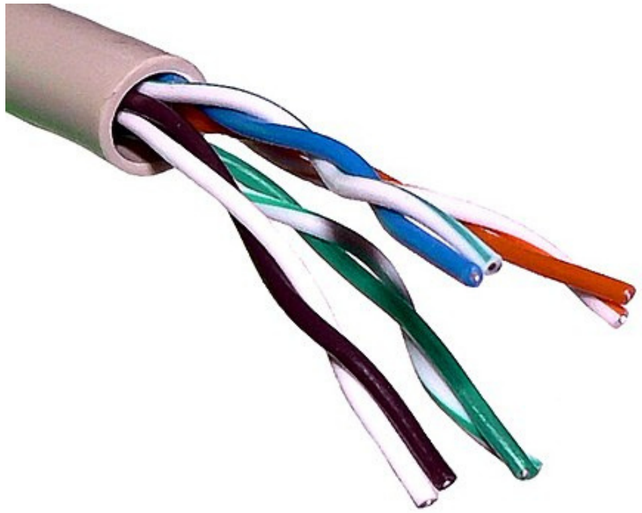




https://en.wikipedia.org/wiki/Networking_cable

Twisted-Pair Copper Wire:

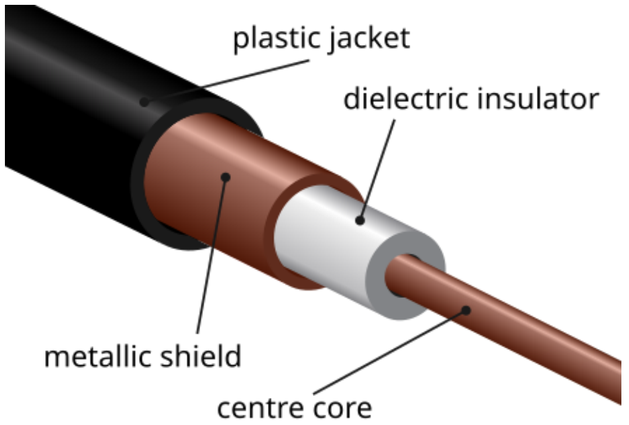
- The least expensive and most commonly used guided transmission medium.
- Over a hundred years it has been used by telephone networks.
- More than 99 percent of the wired connections from the telephone handset to the local telephone switch use twisted-pair copper wire.
- Consists of two insulated copper wires, each about 1 mm thick, arranged in a regular spiral pattern. The wires are twisted together to reduce the electrical interference from similar pairs close by.
- Typically, a number of pairs are bundled together in a cable by wrapping the pairs in a protective shield.
- Data rates for LANs using twisted pair today range from 10 Mbps to 10 Gbps.
- Modern twisted-pair technology, such as category 6a cable, can achieve data rates of 10 Gbps for distances up to a hundred meters.



https://en.wikipedia.org/wiki/Twisted_pair

Coaxial Cable:

- Consists of two copper conductors, but the two conductors are concentric rather than parallel.
- with special insulation and shielding, coaxial cable can achieve high data transmission.
- Common in cable television systems.
- Cable television systems have recently been coupled with cable modems to provide residential users with Internet access at rates of hundreds of Mbps.
- The transmitter shifts the digital signal to a specific frequency band, and the resulting analog signal is sent from the transmitter to one or more receivers.
- Coaxial cables are guided -shared medium.
- A number of end systems can be connected directly to the cable, with each of the end systems receiving whatever is sent by the other end systems.



https://en.wikipedia.org/wiki/Coaxial_cable

Radio Channels:

- Carry signals in the electromagnetic spectrum.
- Require no physical wire to be installed.
- Can penetrate walls, provide connectivity to a mobile user, and can potentially carry a signal for long distances.
- The characteristics of a radio channel depend significantly on the propagation environment and the distance over which a signal is to be carried.
- Environmental considerations:

1. Path loss: decrease the signal strength as the signal travels over a distance.
2. Shadow fading: around/through obstructing objects.
3. Multipath fading (due to signal reflection of interfering objects).
4. Interference (due to other transmissions and electromagnetic signals).

https://en.wikipedia.org/wiki/Radio_broadcasting

Satellite Radio Channels:

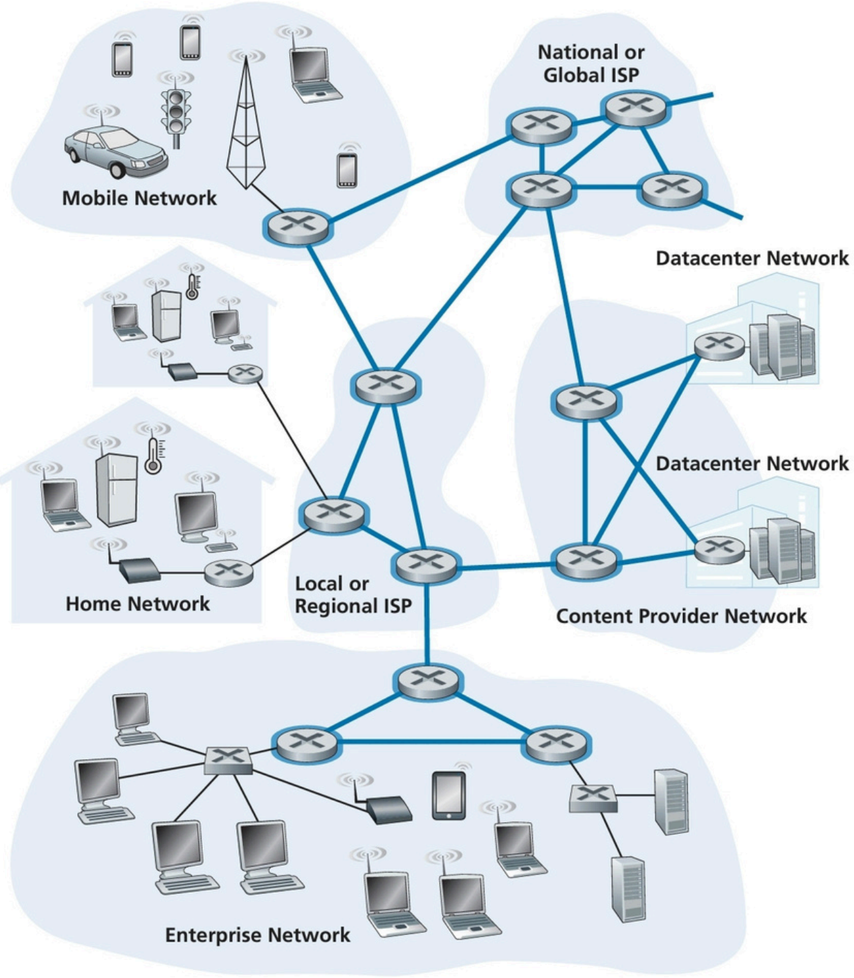
- A communication satellite links two or more Earth-based microwave transmitter/ receivers, known as ground stations.
- Two types of satellites are used in communications: geostationary satellites and low-earth orbiting (LEO) satellites.
- Geostationary satellites permanently remain above the same spot on Earth. This stationary presence is achieved by placing the satellite in orbit at 36,000 kilometers above Earth's surface. This huge distance from ground station through satellite back to ground station introduces a substantial signal propagation delay of 280 milliseconds.
- Often used in areas without access to DSL or cable-based Internet access.
- LEO satellites are placed much closer to Earth and do not remain permanently above one spot on Earth. They rotate around Earth (just as the Moon does) and may communicate with each other, as well as with ground stations. To provide continuous coverage to an area, many satellites need to be placed in orbit. There are currently many low-altitude communication systems in development.

https://en.wikipedia.org/wiki/Low_Earth_orbit

The Network Core

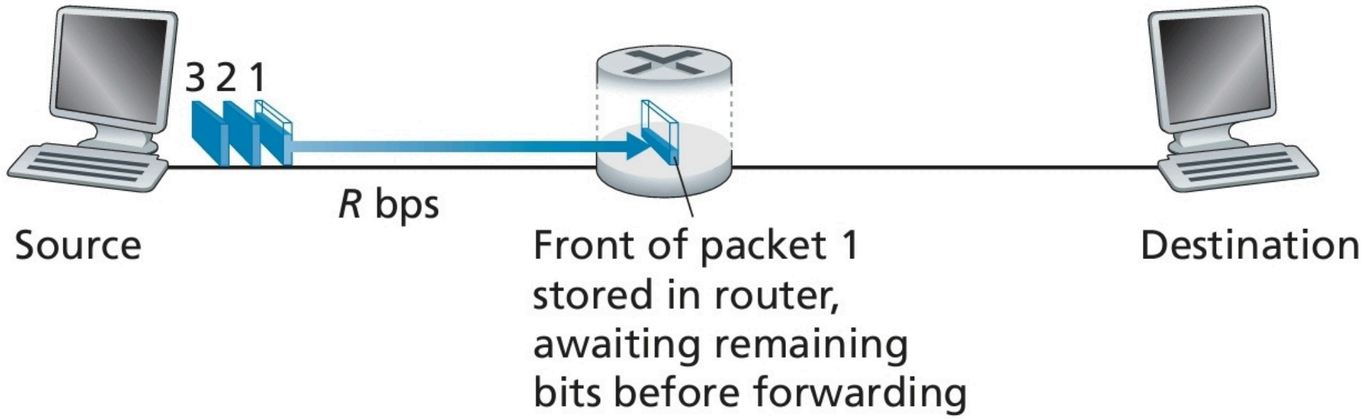
Packet Switching:

- In a network application, end systems exchange messages with each other.
- Messages can contain anything the application designer wants.
- To send a message from a source end system to a destination end system, the source breaks long messages into smaller chunks of data known as packets.
- Packet travels through communication links and packet switches.
- If a source end system or a packet switch is sending a packet of L bits over a link with transmission rate R bits/sec, then the time to transmit the packet is L / R seconds.



Store-and-Forward Transmission:

- Most packet switches use store-and-forward transmission at the inputs to the links.
- Packet switch must receive the entire packet before it can begin to transmit the first bit of the packet onto the outbound link.
- A router have many incident links, it switchs an incoming packet onto an outgoing link.
- In the Figure, the source transmitted some of packet 1. The front of packet 1 already arrived at the router.
- The router cannot transmit the bits it received. Instead it first buffers “stores” the packet’s bits.
- After receiving all of the packet’s bits, the router can begin to transmit “forward” the packet onto the outbound link.



- The source begins to transmit at time 0; at time L/R seconds, the source has transmitted the entire packet, and the entire packet has been received and stored at the router.

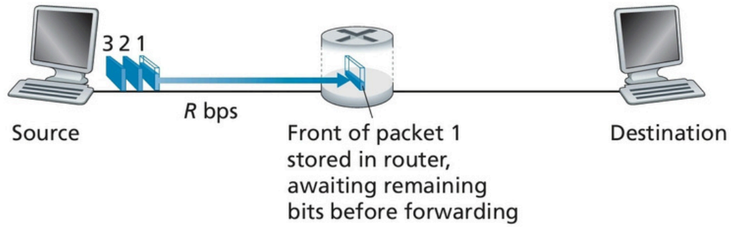
- At time L/R seconds, since the router has just received the entire packet, it can begin to transmit the packet onto the outbound link towards the destination.

- At time 2L/R, the router has transmitted the entire packet, and the entire packet has been received by the destination.

- The total delay is 2L/R.

- Sending one packet from source to destination over a path consisting of N links each of rate R (thus, there are N-1 routers between source and destination). Applying the same logic as above, we see that the end-to-end delay is:

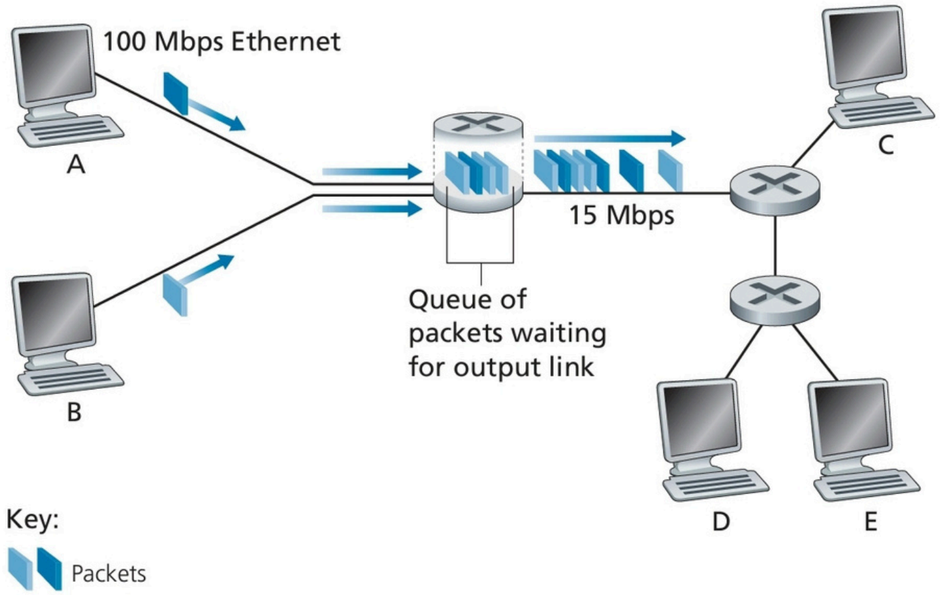
- d(end to end)= N (L/R)



d(end to end)= N (L/R)

Queuing Delays and Packet loss:

- The packet switch has an output buffer (also called an output queue), which stores packets that the router is about to send.
- If an arriving packet needs to be transmitted onto a link but finds the link busy with the transmission of another packet, the arriving packet must wait in the output buffer.
- An arriving packet may find that the buffer is completely full with other packets waiting for transmission. In this case, packet loss will occur.
- When a source end system wants to send a packet to a destination end system, the source includes the destination's IP address in the packet's header.
- Each router has a forwarding table that maps destination addresses (or portions of the destination addresses) to that router's outbound links.



Circuit Switching:

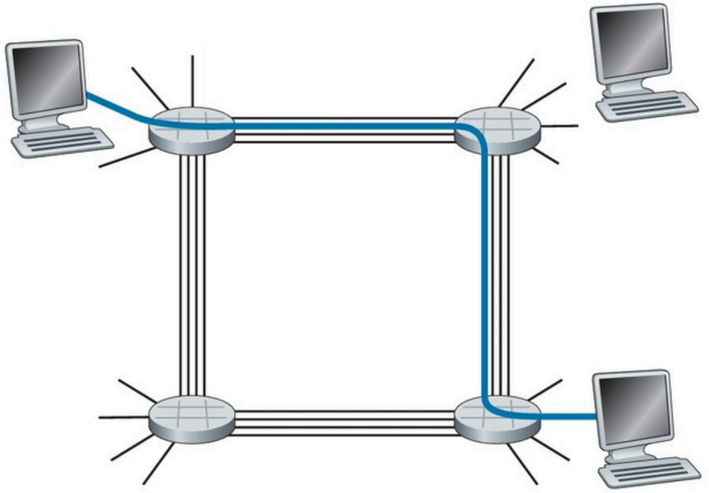
- There are two fundamental approaches to moving data through a network of links and switches: circuit switching and packet switching.

- In circuit-switched networks, the resources needed along a path (buffers, link transmission rate) to provide for communication between the end systems are reserved for the duration of the communication session between the end systems.

- Traditional telephone networks are examples of circuit-switched networks.

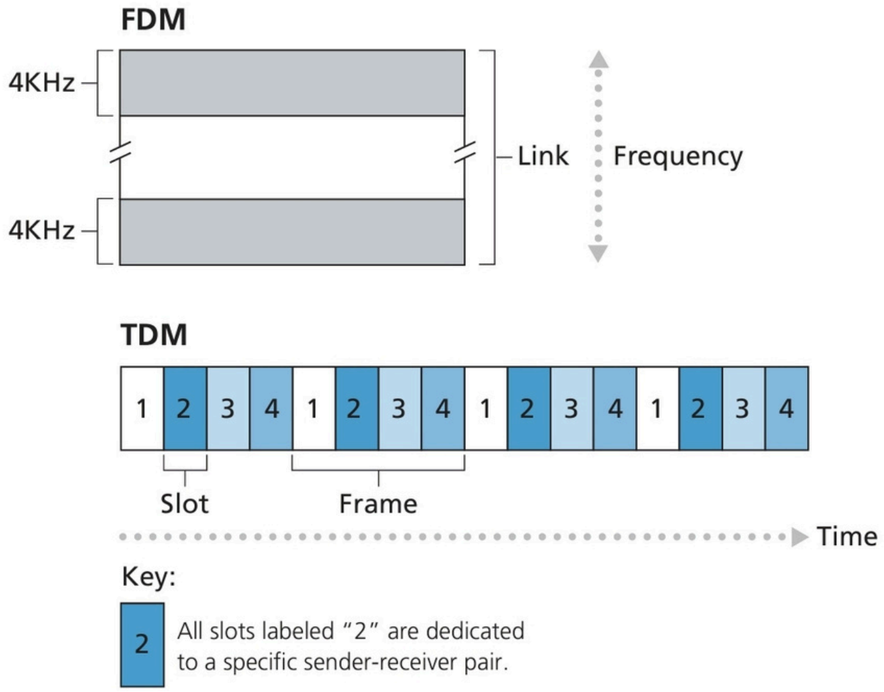
- When the network establishes the circuit, it also reserves a constant transmission rate in the network's links for the duration of the connection.

- The sender can transfer the data to the receiver at the guaranteed constant rate.



Multiplexing in Circuit-Switched Networks:

- A circuit in a link is implemented with either frequency-division multiplexing (FDM) or time-division multiplexing (TDM).
- With FDM, the frequency spectrum of a link is divided up among the connections established across the link.
- The link dedicates a frequency band to each connection for the duration of the connection. In telephone networks, this frequency band typically has a width of 4 kHz.
- For a TDM link, time is divided into frames of fixed duration, and each frame is divided into a fixed number of time slots.
- For TDM, the transmission rate of a circuit is equal to the frame rate multiplied by the number of bits in a slot. For example, if the link transmits 8,000 frames per second and each slot consists of 8 bits, then the transmission rate of each circuit is 64 kbps.



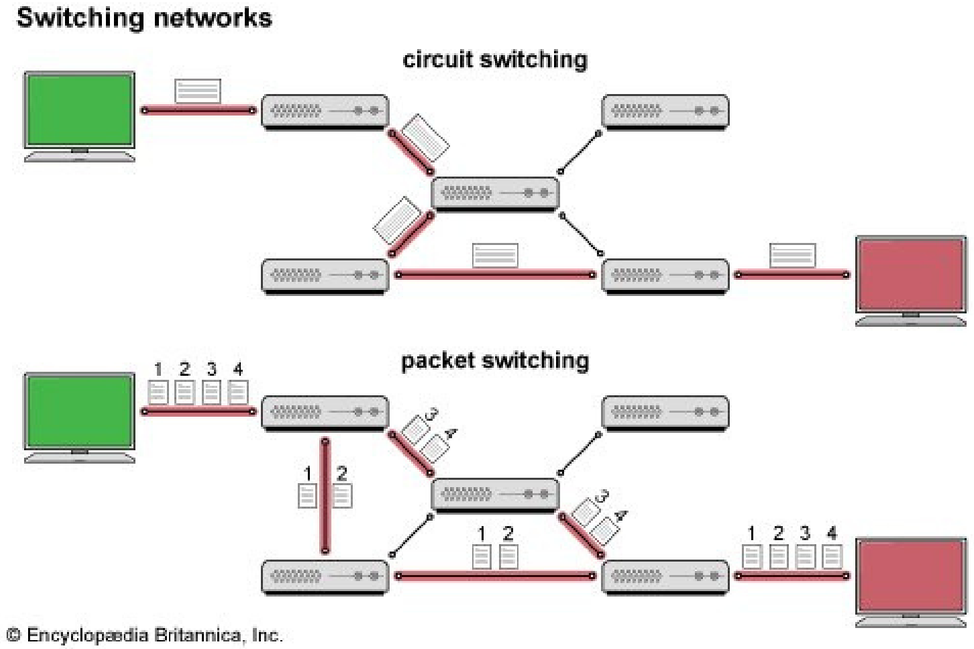
Numerical example:

- Consider how long it takes to send a file of 640,000 bits from Host A to Host B over a circuit-switched network?
- Suppose that all links in the network use TDM with 24 slots and have a bit rate of 1.536 Mbps.
- Also suppose that it takes 500 msec to establish an end-to-end circuit before Host A can begin to transmit the file.
- How long does it take to send the file?
- Each circuit has a transmission rate of (1.536 Mbps)/24 = 64 kbps, so it takes (640,000 bits)/(64 kbps) = 10 seconds to transmit the file.
- We add the circuit establishment time, giving 10.5 seconds to send the file.
- Note that the transmission time is independent of the number of links: The transmission time would be 10 seconds if the end-to-end circuit passed through one link or a hundred links. (The actual end-to-end delay also includes a propagation delay).

Packet Switching Versus Circuit Switching:

- Packet switching is not suitable for real-time services (for example, telephone calls and video conference calls) because of its variable and unpredictable end-to-end delays (due primarily to variable and unpredictable queuing delays).

- Packet switching offers better sharing of transmission capacity than circuit switching and it is simpler, more efficient, and less costly to implement than circuit switching.



Why is packet switching more efficient?

- Suppose users share a 1 Mbps link. Also suppose that each user alternates between periods of activity, when a user generates data at a constant rate of 100 kbps, and periods of inactivity, when a user generates no data. Suppose further that a user is active only 10 percent of the time (and is idly drinking coffee during the remaining 90 percent of the time).

- With circuit switching, 100 kbps must be reserved for each user at all times. For example, with circuit-switched TDM, if a one-second frame is divided into 10 time slots of 100 ms each, then each user would be allocated one time slot per frame. can support only 10 (= 1 Mbps/100 kbps) simultaneous users.

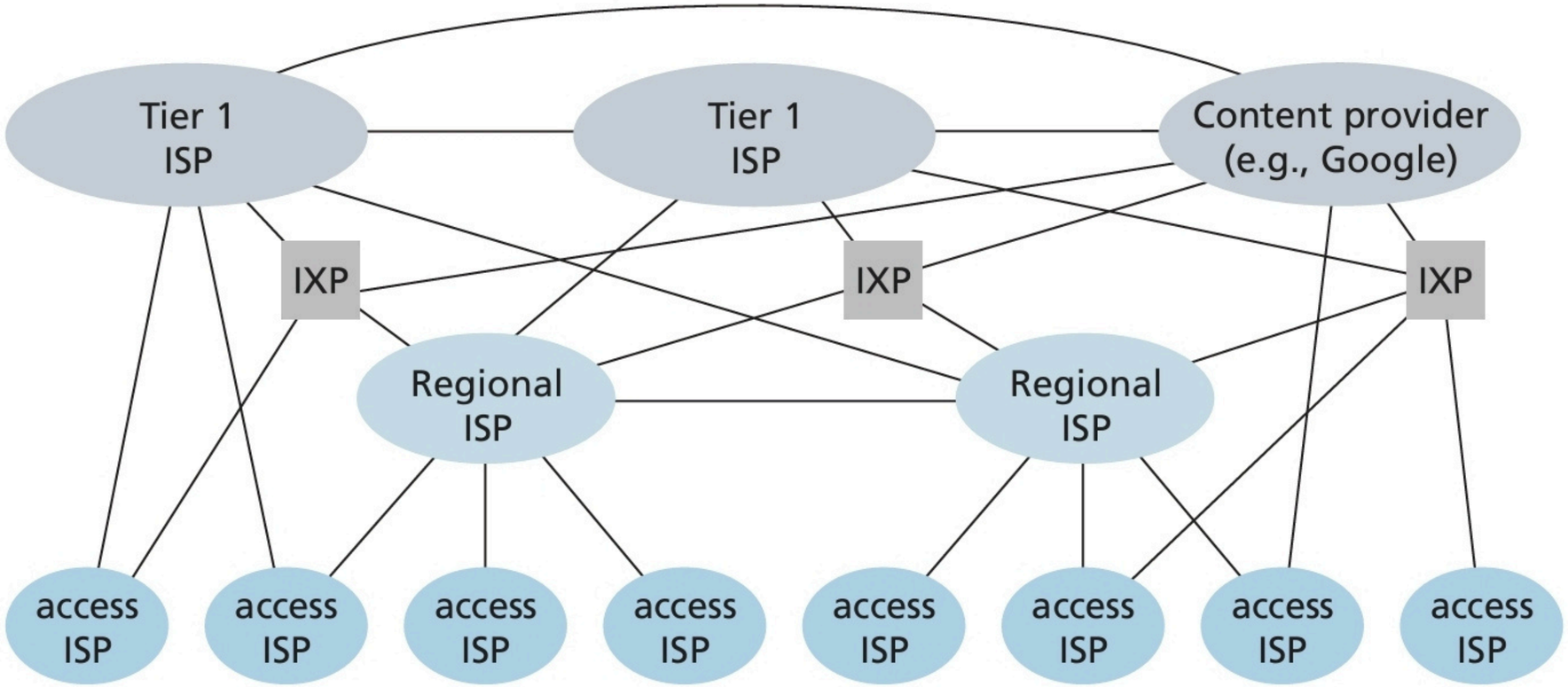
- With packet switching, the probability that a specific user is active is 0.1 (that is, 10 percent). If there are 35 users, the probability that there are 11 or more simultaneously active users is approximately 0.0004. When there are 10 or fewer simultaneously active users (which happens with probability 0.9996), the aggregate arrival rate of data is less than or equal to 1 Mbps, the output rate of the link.

A Network of Networks:

- End systems (PCs, smartphones, Web servers, mail servers, and so on) connect into the Internet via an access ISP.
- The access ISPs themselves must be interconnected. This is done by creating a network of networks.
- One naive approach would be to have each access ISP directly connect with every other access ISP.
- Hundreds of thousands of access ISPs and multiple global transit ISPs.
- the global transit ISPs themselves must interconnect.
- In any given region, there may be a regional ISP to which the access ISPs in the region connect. Each regional ISP then connects to tier-1 ISPs.
- Tier-1 ISPs are our global transit ISP.

- To reduce costs, a pair of nearby ISPs at the same level of the hierarchy can peer, that is, they can directly connect their networks together so that all the traffic between them passes over the direct connection rather than through upstream intermediaries.

- A third-party company can create an Internet Exchange Point (IXP), which is a meeting point where multiple ISPs can peer together.



Delay, Loss, and Throughput in Packet-Switched Networks:

- Processing Delay The time required to examine the packet’s header and determine where to direct the packet is part of the processing delay.

- Queuing Delay At the queue, the packet experiences a queuing delay as it waits to be transmitted onto the link. The length of the queuing delay of a specific packet will depend on the number of earlier-arriving packets that are queued and waiting for transmission onto the link.

- The transmission delay is L/R. This is the amount of time required to push (that is, transmit) all of the packet’s bits into the link.For example, for a 10 Mbps Ethernet link, the rate is R = 10 Mbps; for a 100 Mbps Ethernet link, the rate is R = 100 Mbps.

- Propagation Delay Once a bit is pushed into the link, it needs to propagate to router B. The time required to propagate from the beginning of the link to router B is the propagation delay. The propagation speed depends on the physical medium of the link and is in the range of 2 * (10^8) meters/sec to 3 * (10^8) meters/sec which is equal to, or a little less than, the speed of light.The propagation delay is the distance between two routers divided by the propagation speed. That is, the propagation delay is d/s, where d is the distance between router A and router B and s is the propagation speed of the link.

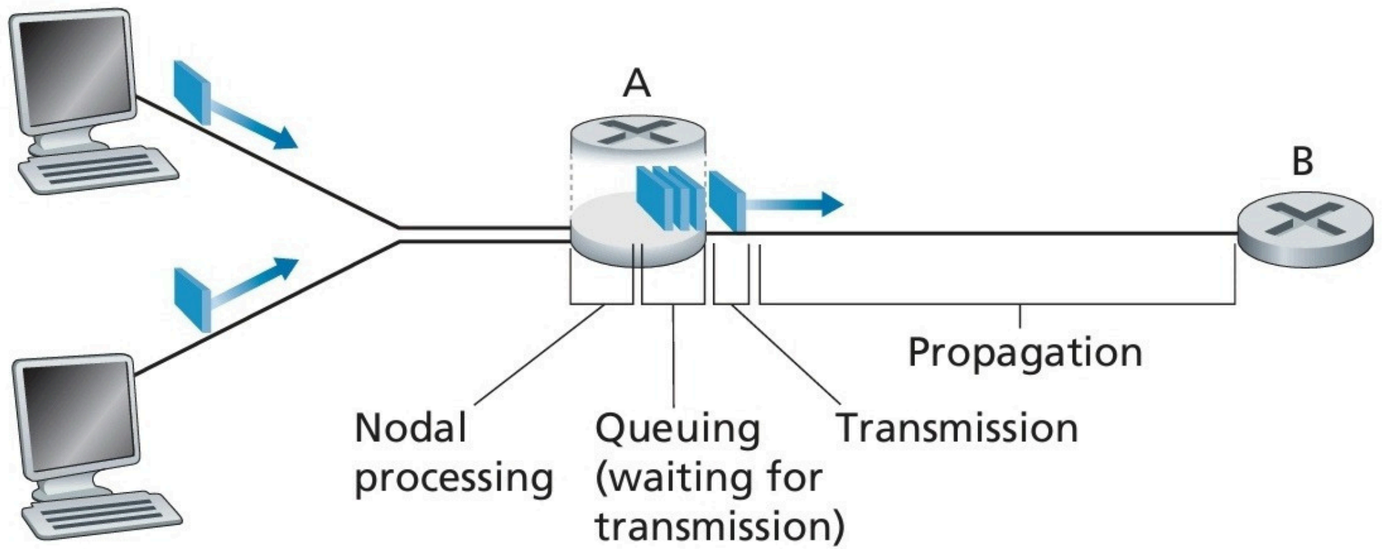
- dnodal = dproc + dqueue + dtrans + dprop

Packet Loss:

In reality a queue preceding a link has finite capacity. A packet can arrive to find a full queue. With no place to store such a packet, a router will drop that packet; that is, the packet will be lost.

End System, Application, and Other Delays:

There can be additional significant delays in the end systems. For example, an end system wanting to transmit a packet into a shared medium (e.g., as in a WiFi or cable modem scenario) may purposefully delay its transmission as part of its protocol for sharing the medium with other end systems.

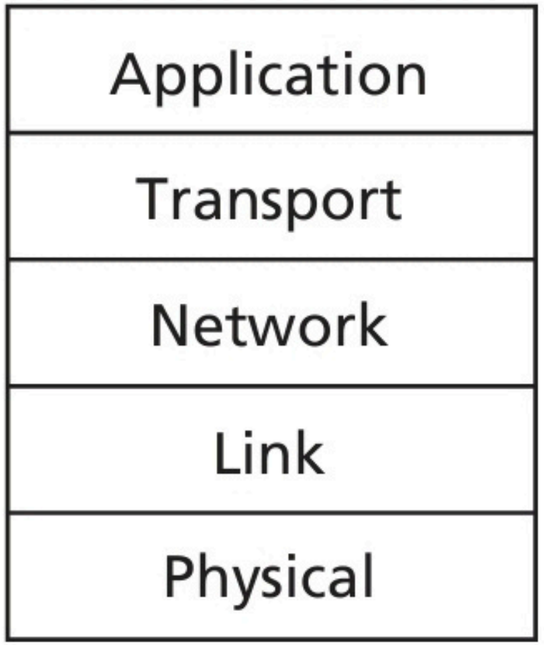


Protocol Layers and Their Service Models:

- 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. Each protocol belongs to one of the layers.

- We are interested in the services that a layer offers to the layer above, the so-called service model of a layer.

- For example, the services provided by layer n may include reliable delivery of messages from one edge of the network to the other. This might be implemented by using an unreliable edge-to-edge message delivery service of layer n- 1, and adding layer n functionality to detect and retransmit lost messages.



Five-layer Internet protocol stack

- A protocol layer can be implemented in software, in hardware, or in a combination of the two.

- layering provides a structured way to discuss system components. Modularity makes it easier to update system components.

- The protocols of the various layers are called the protocol stack. The Internet protocol stack consists of five layers: the physical, link, network, transport, and application layers

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. In this book, we’ll refer to a transport-layer packet as a segment.

Network Layer:

- Moving network-layer packets known as datagrams from one host to another. The Internet transport-layer passes a transport-layer segment and a destination address to the network layer.

- The network layer then provides the service of delivering the segment to the transport layer in the destination host.

- It includes the IP protocol, which defines the fields in the datagram as well as how the end systems and routers act on these fields. There is only one IP protocol, and all Internet components that have a network layer must run the IP protocol.

- The Internet’s network layer also contains routing protocols that determine the routes that datagrams take between sources and destinations. The Internet has many routing protocols.

- The network layer contains both the IP protocol and numerous routing protocols.

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. Examples of link-layer protocols include Ethernet and WiFi.

- We'll refer to the link-layer packets as frames.

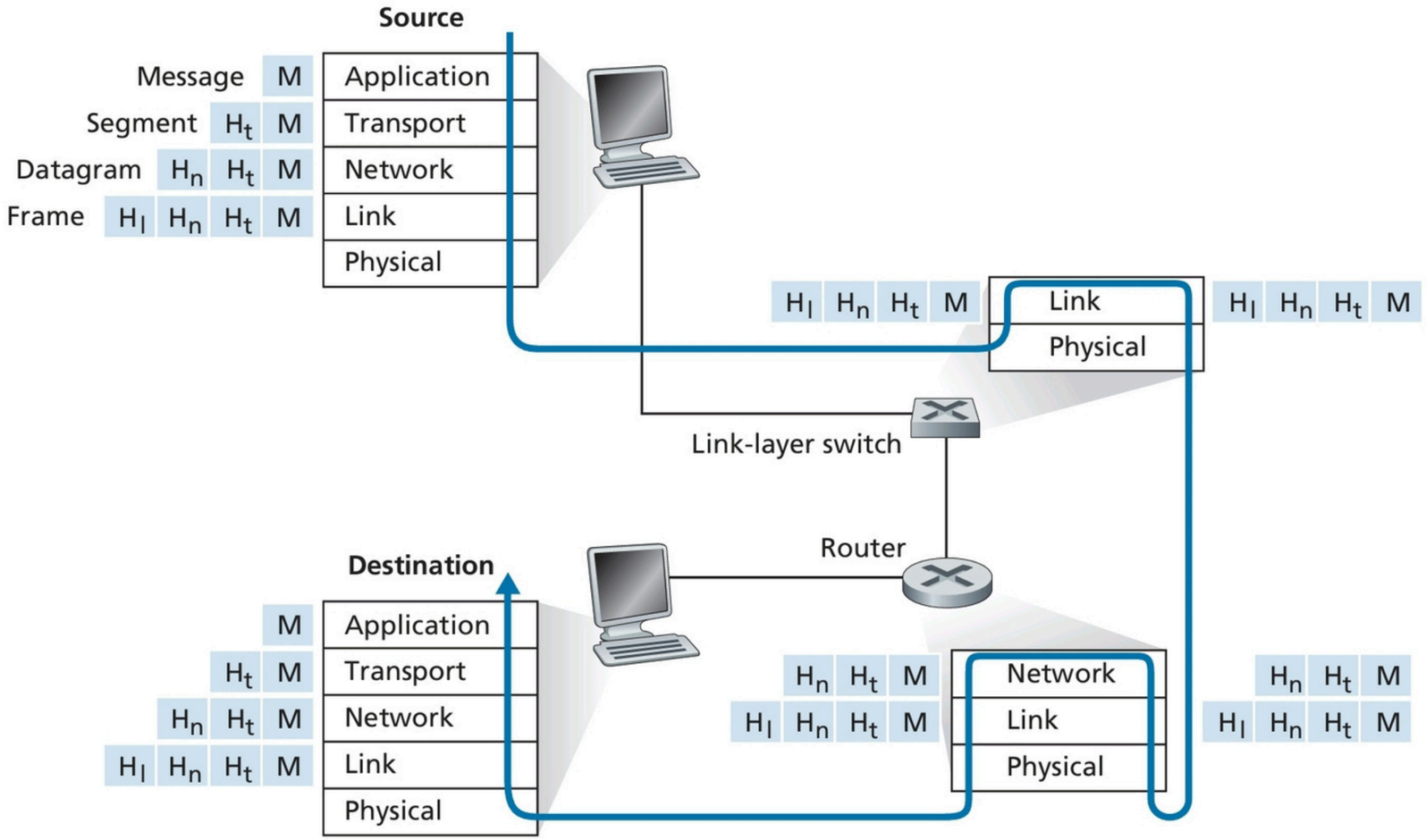
Physical Layer:

- 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). For example, 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.

Encapsulation:

The figure shows the physical path that data takes down a sending end system's protocol stack, up and down the protocol stacks of an intervening link-layer switch and router, and then up the protocol stack at the receiving end system.



Networks Under Attack:

The field of network security is about how the bad guys can attack computer networks and about how we, soon-to-be experts in computer networking, can defend networks against those attacks, or better yet, design new architectures that are immune to such attacks in the first place.

- Put Malware into Your Host Via the Internet: Once malware infects our device it can do all kinds of devious things, including deleting our files and installing spyware that collects our private information, such as social security numbers, passwords, and keystrokes, and then sends this (over the Internet, of course!) back to the bad guys.

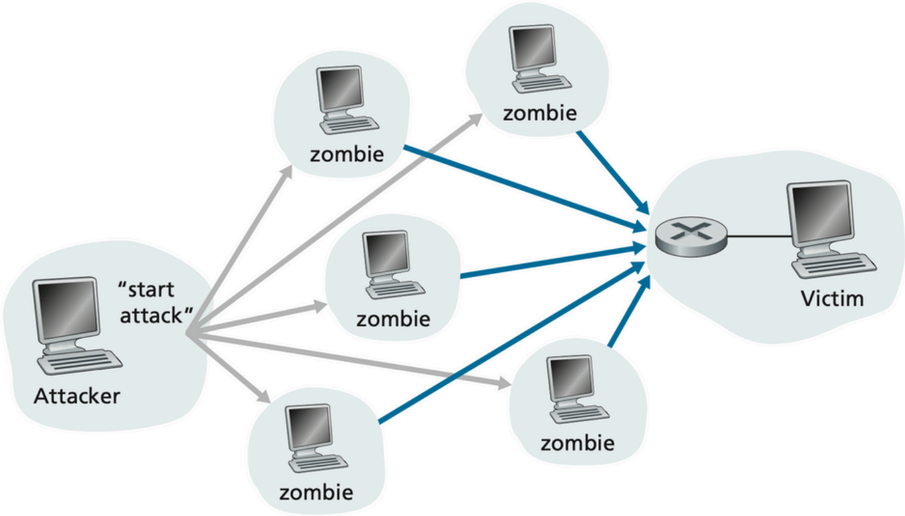
- Sniff Packets:

1. Placing a passive receiver in the vicinity of the wireless transmitter, that receiver can obtain a copy of every packet that is transmitted.
2. In wired broadcast environments, as in many Ethernet LANs, a packet sniffer can obtain copies of broadcast packets sent over the LAN.

- IP spoofing: Is the ability to inject packets into the Internet with a false source address. Imagine the unsuspecting receiver (say an Internet router) who receives such a packet, takes the (false) source address as being truthful, and then performs some command embedded in the packet's contents. To solve this problem, we will need end-point authentication, that is, a mechanism that will allow us to determine with certainty if a message originates from where we think it does.

- Denial-of-service (DoS) attacks: a DoS attack renders a network, host, or other piece of infrastructure unusable by legitimate users. Web servers, e-mail servers, DNS servers, and institutional networks can all be subject to DoS attacks.

- Distributed DoS (DDoS) attacks: the attacker controls multiple sources and has each source blast traffic at the target. With this approach, the aggregate traffic rate across all the controlled sources needs to be approximately R to cripple the service.



Summary:

- various pieces of hardware and software that make up the Internet in particular and computer networks in general.
- We looked at the edge of the network, where end systems and applications are.
- We also looked at the link-layer tech- nologies and physical media typically found in the access network.
- Packet switching and circuit switching are the two basic approaches for transporting data through a telecommunication network. And there are strengths and weaknesses of each approach.
- The Internet has a hierarchical structure, consisting of higher- and lower-tier ISPs.
- We examined the causes of delay, throughput and packet loss in a packet-switched network.
- we looked at protocol layering and service models.
- We surveyed some of the more prevalent security attacks in the Internet.
- In the following chapters, we’ll revisit all of these ideas, covering them in much more detail.