How does the internet work?: Computer Networking A Top-Down Approach Chapter 1

- Hosts/ End systems: Devices connected to the internet
- Communication links/ Packet Switches: Connects end systems
- Transmission rate: Rates at which links can transmit data
- 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
- Routers/ Link-layer switches: Two most prominent types of links
- Link-layer switched are typically used in access networks, while routers are typically used in the network core
- Internet Service Providers (ISPs): grants end systems access to the Internet
- 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, and mobile wireless access
- Protocols: control the sending and receiving of information within the internet
- We can describe the Internet as an infrastructure that provides services to applications
- Socket interface: a set of rules that the sending program must follow so that the internet can deliver the data to the destination program
- 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
- Access network: network that physically connects an end system to the first router on a path from the end system to any other distant end system
- The two most prevalent types of broadband residential access are digital subscriber line (DSL) and cable both usually provided by a customer's telco/ISP
- 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 1MHz band

    - A medium upstream channel, in the 4kHz to 50 kHz band
    - An ordinary two-way telephone channel, in the 0 to 4kHz band
- On the customer side, a splitter separates the data and telephone signals arriving to the home and forwards the data signal to the DSL modem
- On the telcom side, in the CO (central office), the DSLAM (Digital subscriber line access multiplexer) separates the data and phone signals and sends the data into the Internet
- The actual downstream and upstream rates achieved may be less than the rates noted above, as the DSL provider may purposefully limit a residential rate when tiered service (different rates, available at different prices) are offered
- The maximum rate is also limited by the distance between the home and the CO, the gauge of the twisted-pair line and the degree of electrical interference
- Both the DSL modem and cable modem is typically an external device and connects to the home PC through an Ethernet port
- Cable Internet access is a shared medium, 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
- So 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
- 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
- Direct fiber: each fiber leaving the central office is actually shared by many homes, it is not until the fiber gets relatively close to the homes that it is split into individual customer-specific fibers
- Two competing optical-distribution network architectures that perform this splitting: active optical networks (AON) and passive optical networks (PON)
- PON: each home has an optical network terminator (ONT), which is connected by dedicated optical fiber to a neighbourhood splitter, the splitter combines a number of homes onto a single, shared optical fiber, which connects to an optical line terminator

(OLT) in the telco's CO. The OLT, providing conversion between optical and electrical signals, connects to the Internet via a telco router

- In the PON architecture, all packets sent from OLT to the splitter are replicated at the splitter
- Satellite link: ~1 Mbps
- Dial-up access over traditional phone lines: 56 kbps
- A local area network (LAN) is used to connect an end system to the edge router
- Ethernet is the most prevalent access technology (LAN)
- With Ethernet access, users typically have 100 Mbps or 1 Gbps access to the Ethernet switch, whereas servers may have 1 Gbps or even 10 Gbps
- Third-generation wireless (3G): provides packet-switched wide-area wireless Internet access at speeds in excess of 1 Mbps
- Examples of physical media: twisted-pair copper wire, coaxial cable, multimode fiber-optic cable, terrestrial radio spectrum, and satellite radio spectrum
- Two categories of physical media: guided media and unguided media
- HFC uses a combination of fiber cable and coaxial cable
- DSL and Ethernet use copper wire
- Mobile access networks use the radio spectrum
- In a network application, end systems exchange messages with each other, the source breaks ling messages into smaller chunks of data known as packets, each packet travels through communication links and packet switches
- Packets are transmitted over each communication link at a rate equal to the full transmission rate of the link
- 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: the packet switch must receive the entire packet before it can begin to transmit the first bit of the packet onto the outbound link
- General end-to-end delay formula: dend-to-end = NLR (N = number of links in path, L = length of packet in bits, R = transmission rate in bits/sec)
- For each attached link, the packet switch has an output buffer (or output queue), which stores packets that the router is about to send into that link. 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, which stores packets that the router is about to send into that link

- Output buffer: stores packets that the router is about to send into an output link
- Queuing delay: Time a packet spends waiting in the output buffer, delay depends on the level of congestion in the network
- If the arriving packet finds that the buffer is completely full with other packets waiting for transmission, packet loss will occur
- Packet loss: when an output buffer is full and the arriving packet or one of the already-queued packet is dropped
- In the Internet, every end system has an address called an IP address. 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
- Forwarding table: a table within the router that maps destination addresses to that router's outbound links
- 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 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. In packet-switched networks, these resources are not reserved; a session's messages use the resources on demand and may have to wait (queue) for access to a communication link
- When the network establishes the circuit (reserved connection), it also reserves a constant transmission rate in the network's links for the duration of the connection --> sender can transfer to the receiver at the guaranteed constant rate
- 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 (this link dedicates a frequency band to each connection for the duration of the connection
- Bandwidth: the width of the frequency band

- For a TDM link, time is divided into frames of fixed duration, and each frame is divided into a fixed number of time slots and the network dedicates one time slot in every frame to this connection
- With FDM, each circuit continuously gets a fraction of the bandwidth. With TDM, each circuit gets all of the bandwidth periodically during brief intervals of time
- Proponents of packet switching have always argued that circuit switching is wasteful because the dedicated circuits are idle during silent periods
- Establishing end-to-end circuits ad reserving end-to-end transmission capacity is complicated and requires complex signaling software
- Critics of packet switching have often argued that packet switching is not suitable for real-time services (telephone calls and video conference calls) because of its variable and unpredictable end-to-end delays
- Proponents of packet switching argue that (1) if offers better sharing of transmission capacity than circuit switching and (2) it is simpler, more efficient, and less costly to implement than circuit switching
- Circuit switching pre-allocates use of the transmission link regardless of demand, with allocated but unneeded link time going unused. Packet switching on the other hand allocates link use on demand
- Network Structures:
    - Network Structure 1: interconnects all of the access ISPs with a single global transit ISP
    - Network Structure 2: consists of the hundreds of thousands of access SPs and multiple global transit ISPs (access ISPs prefer Network Structure 2 since they can now choose among the competing global transit providers as a function of their pricing and services, note that global transit ISPs themselves must interconnect)
    - Network Structure 3: each access ISP pays the regional ISP to which it connects, and each regional ISP pays the tier-1 ISP to which it connects
    - Network Structure 4: Ecosystem consisting of access ISPs, regional ISPs, tier-1 ISPs, PoPs, multi-homing, peering, and IXPs
    - Network Structure 5: builds on top of Network Structure 4 by adding content-provider networks

- PoP (Points of Presence): a group of one or more routers (at the same location) in the provider's network where customer ISPs can connect into the provider ISP
- Multi-home: Where any ISP chooses to connect to two or more provider ISPs, when an ISP multi-homes it can continue to send and receive packets into the internet even if one of its providers has a failure
- Peer: When a pair of nearby ISPs at the same level of hierarchy can directly connect their networks together so that all the traffic between them passes over the direct connection rather than through upstream intermediaries
- Internet Exchange Point (IXP): a meeting point where multiple ISPs can peer together
- Content-provider networks: For example the Google private network that only carries traffic to/from Google servers
- Throughput: the amount of data per second that can be transferred through a link
- Nodal processing delay, queuing delay, transmission delay, and propagation delay altogether accumulate to give a total nodal delay
- Processing delay: time required to examine the packet's header and determine where to direct the packet (includes the time needed to check for bit-level errors in the packet)
- Queuing delay: time it takes as a packet waits to be transmitted onto a 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. If the queue is empty the queuing delay will be zero and if the traffic is heavy queuing delay will be long
- Transmission delay: the amount of time require to push/transmit all of the packet's bits into the link denoted by L/R (length of packet in bits divided by transmission rate in bits per sec)
- The propagation speed depends on the physical medium of the link and is somewhat equivalent to the speed of light
- When characterizing queuing delay, one typically uses statistical measures, such as average queuing delay, variance of queuing delay, and the probability that the queuing delay exceeds some specified value
- Queuing capacity greatly depends on the router design and cost

- The fraction of lost packets increases as the traffic intensity increases. Therefore, performance at a node is often measured not only in terms of delay, but also in terms of the probability of packet loss
- End-to-end-delay = number of links * (processing delay + transmission delay + propagation delay)
- In addition to delay and packet loss, another critical performance measure in computer networks is end-to-end throughput
- In the service model of the internet each protocol belongs to its own layer
- The Internet protocol stack consists of five layers: the physical, link, network, transport, and application layers

Application layer:

- Where network applications and their application-layer protocols reside
- Includes protocols, such as HTTP (provides for Web document request and transfer), SMTP (provides for the transfer of email messages), and FTP (provides for the transfer of files between two end systems)
- Application in one end system using the protocol to exchange packets of information with the application in another end system
- We refer to this packet of information at the application layer as a message

Transport layer:

- Transports application layer messages between application endpoints
- Two transport protocols: TCP and UDP, either of which can transport application layer messages
- TCP provides a connection-oriented service to its applications; a guaranteed delivery of application layer messages to the destination and control flow
- 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
- UDP protocol provides a connectionless service to its applications; service has no reliability, no flow control, and no congestion control
- We refer to a transport layer packet as a segment

Network layer:

- Network layer packet is called a datagram
- Responsible for moving datagrams from one host to another
- Service of delivering the segment to the transport layer in the destination host
- Uses the IP protocol which defines the fields in the datagram as well as how the end routers act on these fields
- Network layer also contains routing protocols that determine the routes that datagrams take between sources and destinations

Link Layer

- Moves a packet from one node to the next node in the route
- 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, 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
- Link layer packets are referred to as frames
- Job of the link layer is to move entire frames from one network element to an adjacent network element

Physical Layer

- 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, Ethernet as many physical layer protocols: one or twisted copper wire, another for coaxial cable, another for fiber and so on

Physical path that data takes from a source end system, down a sending end system's protocol stack, and to its destination:

- Routers and link-layers do not implement all of the layers in the protocol stack; they typically only implement the bottom three layers (network, link, and physical)
- Link-layer switches can implement the bottom 2 (link and physical)
- Routers can implement the bottom 3 (network, link, and physical)
- Hosts are able to implement all 5 layers

Encapsulation:

- At the ending host, an application-layer message is passed to the transport layer
- The transport layer takes the message and appends additional information (a transport layer header) that will be used by the receiver side transport layer
- The application layer message and 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 information 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 information and create a link-layer frame
- We see at each layer, a packet has two types of fields: header fields and a payload field
- Payload: a packet from the layer above
- Malware: malicious stuff on the internet that can enter and infect our devices. Once our device is infected malware can delete our files, install spyware that collects our private information
- Botnet: a network of compromised devices, which the bad guys control and leverage for spam email distribution or DDoS attacks against targeted hosts
- Much of the malware today is self-replicating, hence malware can spread in the form of a virus or a worm
- Viruses: malware that require some form of user interaction to infect the user's device. The classic example is an email attachment containing malicious executable code. If a user

receives and opens such an attachment, the user inadvertently runs the malware on the device

- Worms: malware that can enter a device without any explicit user interaction. For example, a user may be running a vulnerable network application to which an attacker can send malware. In some cases, without any user intervention, the application may accept malware from the internet and run it creating a worm. The worm in the newly infected device then scans the internet, searching for other hosts running the same vulnerable network application. When it finds other vulnerable hosts, it sends a copy of itself to those hosts
- Denial-of-service (DoS) attacks: renders a network, host, or other piece of infrastructure unusable by legitimate users. Web servers, email servers, DNS servers, and institutional networks can all be subject to DoS attacks
- Most Internet DoS attacks fall into one of three categories:
    - Vulnerability attack: Involves sending a few well-crafted messages to a vulnerable application or operating system running on a targeted host. If the right sequence of packets is sent to a vulnerable application or operating system, the service can stop or, worse, the host can crash
    - Bandwidth flooding: the attacker sends a deluge of packets to the targeted host - so many packets that the target's access link becomes clogged, preventing legitimate packets from reaching the server
    - Connection flooding: the attacker establishes a large number of half-open or fully open TCP connections t the target host. The host can become so bogged down with these bogus connections that it stops accepting legitimate connections
- Packet sniffer: a passive receiver that records a copy of every packet that passes by via wifi or wired packet transmission
- A bad guy who gains access to an institution's access router or access link to the Internet may be able to plant a sniffer that makes a copy of every packet going to/from the organization. Sniffed packets can then be analyzed offline for sensitive information
- Some of the best defenses against packet sniffing involve cryptography
- IP spoofing: ability to inject packets into the Internet with a false source address, this is one of the many ways one user can masquerade as another user

- To solve this problem, we will need end-point authentication, a mechanism that will allow us to determine with certainty if a message originates from where we think it does
- Road map sequence of this book:
    - Computer Networks and the Internet
    - Application Layer
    - Transport Layer
    - Network Layer: Data Plane
    - Network Layer: Control Plane
    - Th Link Layer and LANs
    - Wireless and Mobile Networks
    - Security in Computer Networks
    - Multimedia Networking