- Information gathering, processing, and distribution are the key technologies in these days.
- The demand for sophisticated information processing grows even faster than the ability to gather, process, and distribute information.
- Computer systems are interconnected by a single technology, e.g., the Internet.
- The Internet has many uses including business applications, home applications, and mobile users.
- These uses raise a number of social issues.
- The client-server model is popular for communication, e.g., email, VoIP, and e-commerce.
- Other forms of business include B2C, B2B, G2C, C2C, and P2P.
- Homes contain many networked devices connected to the Internet by cable, DSL, wireless, etc.
- Some applications use the peer-to-peer model where there are no fixed clients and servers.
- Mobile users communicate, consume content, and use sensors, with devices such as tablets, laptops, and smartphones.
- Network neutrality, content ownership, anonymity and censorship, and privacy are important issues.
- Networks can be classified by transmission technology and network scale.
- Transmission technologies include point-to-point and broadcast.
- Network scales include PAN, LAN, MAN, WAN, and the Internet.
- The Internet is a collection of interconnected networks.
- Network functions include raw data transfer, error and flow control, switching, routing, traffic control, and network security.
- Each protocol instance talks virtually to its peer, with each layer communicating only by using the one below.
- Connection-oriented and connectionless services are provided to the layer above as primitives.
- A service is a set of primitives that a layer provides to the layer above it.
- OSI and TCP/IP are two reference models used in networking.
- The physical layer determines specifications for all physical components.
- The link layer is responsible for data transfer between neighboring network elements.
- The network layer controls the operation of the subnet and provides network-wide addressing.
- The transport layer provides reliable data delivery and end-to-end error control and flow control.
- The session layer allows applications to maintain an ongoing session.
- The presentation layer allows applications to interpret the meaning of data.
- The application layer supports network applications and gives end-user applications access to network resources.
- The TCP/IP reference model is a four-layer model derived from experimentation.
- Malware can infect hosts, record keystrokes, and upload information to a collection site.
- Malware can infiltrate hosts via the Internet, through viruses and worms.
- Spyware malware can record keystrokes, visited websites, and upload info to a collection site.
- Infected hosts can be enrolled in botnet, and used for spam or DDoS attacks.
- Attackers can perform Denial of Service (DoS) attacks by overwhelming server resources with bogus traffic.
- Attackers can sniff packets and use fake addresses, a technique known as IP spoofing.
- In IEEE802.11 (WiFi), clients communicate via an Access Point (AP) that is wired to the network, using the ISM bands.
- The transport layer runs on various hosts and converts application layer messages into transport layer packets or segments.
- In the internet, two transport layer protocols are available to the application layer: UDP (User Datagram Protocol) and TCP (Transmission Control Protocol).
- The Internet's network-layer protocol, IP (Internet Protocol) provides logical communication between hosts.
- The transport layer extends host-to-host delivery to process-to-process delivery, a process known as transport-layer multiplexing and demultiplexing.
- TCP offers reliable data transfer, ensuring data is delivered correctly and in order via flow control, sequence numbers, acknowledgments, and timers.
- A TCP socket is identified by a four-tuple: source IP address, source port number, destination IP address, destination port number.
- The UDP checksum provides for error detection.
- TCP is connection-oriented and provides full-duplex service.
- The server process and the client process work through a TCP connection.
- A Python client program establishes connection with the server using the command: clientSocket.connect((serverName, serverPort)).
- The client first sends a special TCP segment, the server responds with a second special TCP segment, and finally the client responds again with a third special segment.
- The first two segments do not carry any application-layer data, the third segment might carry a payload.
- This connection-establishment procedure is often referred to as a three-way handshake.
- Once a TCP connection is established, the two application processes can send data to each other.
- TCP directs this data to the connection's send buffer, which is one of the buffers that is set aside during the initial three-way handshake.
- The maximum amount of application-layer data in a segment is limited by the maximum segment size (MSS).
- TCP pairs each chunk of client data with a TCP header, forming TCP segments. These segments are passed down to the network layer, where they are separately encapsulated within network-layer IP datagrams.
- The TCP segment consists of a data field and header fields. The data field contains a chunk of application data, the MSS limits the maximum size of a segment's data field.
- The TCP header is typically 20 bytes, segments sent by Telnet may be only 21 bytes in length.
- The header includes source and destination port numbers for multiplexing/demultiplexing data from/to upper-layer applications, and a checksum field.
- A TCP segment header also contains the following fields: a 32-bit sequence number field, a 32-bit acknowledgment number field, a 16-bit receive window field, a 4-bit header length field, and an optional and variable-length options field.
- The flag field of a TCP header contains 6 bits. The ACK bit indicates that the value carried in the acknowledgment field is valid. The RST, SYN, and FIN bits are used for connection setup and teardown. The CWR and ECE bits are used in explicit congestion notification. The PSH bit indicates that the receiver should pass the data to the upper layer immediately. The URG bit is used to indicate that there is data in this segment that the sending-side upper-layer entity has marked as "urgent."

- The sequence number for a segment is the byte-stream number of the first byte in the segment. These sequence numbers are a critical part of TCP's reliable data transfer service.
- Field in the header
- Appropriate TCP segment