- CN5E is authored by Tanenbaum & Wetherall, copyrighted by Pearson Education-Prentice Hall and D Wetherall in 2011.
- Information gathering, processing, and distribution are key technologies, with growing demand for sophisticated information processing systems.
- Computer systems are interconnected by technologies like the Internet, used for various applications such as VoIP, mobile use, and business applications.
- Different models for communication include client-server and peer-to-peer models.
- B2C, B2B, G2C, and C2C represent different forms of electronic commerce.
- Devices like tablets, laptops, and smartphones are popular for mobile users, with WiFi hotspots and 4G LTE providing wireless connectivity.
- Network neutrality, content ownership, and privacy are major social issues raised by these technologies.
- Networks can be classified by transmission technology (Point-to-point or Broadcast) and scale (PAN, LAN, MAN, WAN, or the Internet).
- The Internet is a collection of interconnected networks facilitated by devices called gateways.
- The Internet evolved from ARPANET and used networks like NSFNET as its backbone.
- Modern Internet consists of ISP networks serving as the Internet backbone, with traffic exchange set by business agreements.
- Internet structure comprises of hosts (end systems), communication links, and packet switches.
- Protocols such as TCP, IP, HTTP, and Skype control the sending and receiving of messages.
- Internet is a network of networks, interconnected via access ISPs.
- Network Virtualization and Virtual Local Area Networks (VLAN) are important aspects of modern networking.
- Protocols operate in layers, each with specific responsibilities and functionalities.
- The OSI and TCP/IP reference models provide structured frameworks for network protocols.
- Physical, Link, Network, and Transport layers handle data transmission and error control.
- Session, Presentation, and Application layers manage sessions, data representation, and network applications respectively.
- Network security involves defending networks against attacks and designing immune architectures.
- Malware, viruses, and spyware pose significant threats to network security.
- Malware can enter host systems through the internet via methods such as viruses and worms.
- Spyware malware can record keystrokes and visited websites, and upload the information to a collection site.
- Infected hosts can be enrolled in a botnet and used for spam and DDoS attacks.
- Attackers can overwhelm resources with bogus traffic to execute Denial of Service (DoS) attacks.
- Packet "sniffing" allows bad actors to read and record all packets passing by, including potentially sensitive information.
- IP spoofing involves sending packets with a false source address.
- In IEEE802.11 (WiFi), clients communicate via an Access Point (AP) that is wired to the rest of the network.
- The prefixes used in computing include powers of 10 for rates and powers of 2 for storage.
- The Transport Layer is implemented in end systems, not in network routers.
- The Internet provides two transport layer protocols to the application layer: UDP (User Datagram Protocol) and TCP (Transmission Control Protocol).
- The IP service model is a best effort delivery service, meaning it makes no guarantees.
- UDP and TCP extend IP's delivery service and provide transport-layer multiplexing and demultiplexing.
- TCP offers additional services such as reliable data transfer and congestion control.
- A TCP socket is identified by a four-tuple consisting of a source IP address, a source port number, a destination IP address, and a destination port number.
- The UDP checksum provides error detection.
- TCP is connection-oriented, providing full-duplex service.
- A TCP connection is always point-to-point, between a single sender and a single receiver.
- The server process and client process are distinct in the TCP connection.
- The client program, for example in Python, can connect via the command: clientSocket.connect((serverName, serverPort)).
- Three special TCP segments are exchanged in the connection-establishment procedure: a client-initiated segment, a server response, and another client response.
- The first two segments carry no payload, while the third segment may 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 breaks data into chunks and pairs each chunk with a TCP header to form TCP segments.
- The Maximum Segment Size (MSS) defines the maximum amount of application-layer data in a segment.
- TCP segments are encapsulated within network-layer IP datagrams and sent into the network.
- Upon receipt, the segment's data is placed in the TCP connection's receive buffer.
- The TCP segment consists of a data field and header fields.
- The header includes source and destination port numbers, a checksum field, 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 variable-length options field.
- The flag field in the TCP header contains 6 bits: ACK, RST, SYN, FIN, CWR, ECE, PSH, and URG.
- TCP views data as an unstructured, but ordered, stream of bytes.
- The sequence number for a segment is the byte-stream number of the first byte in the segment.
- For example, if TCP receives a data stream of 500,000 bytes with an MSS of 1,000 bytes, TCP constructs 500 segments out of the data stream.
- The first segment gets assigned sequence number 0, the second segment gets assigned sequence number 1,000, the third segment gets assigned sequence number 2,000, and so on.
- Field in the header
- Appropriate TCP segment