- Key technologies today are information gathering, processing, and distribution.
- Demand for sophisticated information processing is growing rapidly.
- Computer systems are interconnected by technologies such as the Internet.
- Applications of these technologies include business applications, home applications, mobile usage.
- Technologies raise social issues including network neutrality, content ownership, anonymity, and censorship.
- Popular uses include communication (email, VoIP), e-commerce (B2C, B2B, G2C, C2C), auctioning second-hand products online, and peer-to-peer networks.
- Homes contain many networked devices connected to the Internet by various means including cable, DSL, and wireless.
- Mobile users use devices like tablets, laptops, and smartphones to communicate, consume content, and use sensors.
- Networks can be classified by transmission technology and scale, with the Internet being the largest network.
- Personal Area Network (PAN), Local Area Network (LAN), Metropolitan Area Network (MAN), and Wide Area Network (WAN) are types of networks.
- An ISP (Internet Service Provider) network is a type of WAN.
- A VPN (Virtual Private Network) is a WAN built from virtual links running on top of the Internet.
- Networks are connected through devices called gateways.
- Before the Internet was the ARPANET, the early Internet used NSFNET as its backbone.
- The modern Internet uses ISP networks as the backbone, with traffic exchange set by business agreements.
- The Internet consists of millions of connected computing devices, communication links, and packet switches.
- Internet standards include RFC (Request for comments) and IETF (Internet Engineering Task Force).
- OSI (Open Systems Interconnection) reference model and TCP/IP reference model are used for understanding and designing network protocols.
- The physical layer sends bits as signals over the channel, link layer manages data transfer between neighboring network elements, network layer controls operation of the subnet, transport layer provides reliable data delivery, session layer allows applications to maintain ongoing sessions, presentation layer allows applications to interpret meaning of data, and application layer gives end-user applications access to network resources.
- Each layer in a network communicates only with the one below it, adding its own header to the message to transmit.
- Network security focuses on how to defend networks against attacks and design architectures that are immune to attacks.
- Malware can infect hosts via the Internet, recording keystrokes, visiting websites, and uploading info to a collection site.
- Infected hosts can be enrolled in a botnet, used for spam.
- Malware can infect hosts via the Internet through methods like viruses and worms.
- Infected hosts can become part of botnets and be used for spam or DDoS attacks.
- Attackers can also disrupt server and network infrastructure through Denial of Service (DoS) attacks.
- Attackers can sniff packets and use fake addresses for IP spoofing.
- In IEEE802.11 (WiFi), clients communicate through Access Points (APs) that are wired to the network.
- The transport layer protocol is implemented in end systems, not network routers. It converts application layer messages into transport layer packets or segments.
- More than one transport layer protocol may be available to network applications, such as TCP and UDP in the case of the internet.
- The internet's network-layer protocol, IP (Internet Protocol), provides logical communication between hosts.
- The transport layer extends the host-to-host delivery to process-to-process delivery through multiplexing and demultiplexing.
- TCP and UDP segments have source and destination port number fields for demultiplexing.
- In TCP, a socket is identified by a four-tuple: source IP address, source port number, destination IP address, destination port number.
- TCP is connection-oriented, providing full-duplex service and ensuring data is delivered correctly and in order.
- UDP is connectionless, allowing the transport layer to automatically assign the port number.
- For reliable data transfer, techniques like error detection and correction and loss detection and recovery are used.
- The UDP checksum provides error detection.
- The process involves a server and client process.
- A Python client program can connect to a server using the command: clientSocket.connect((serverName, serverPort)).
- The identification of the process on the server is done with TCP in the server.
- The establishment of a TCP connection involves a three-way handshake which includes the client first sending a special TCP segment, followed by a response from the server, and finally a response from the client.
- The first two segments in the handshake carry no payload, while the third segment may carry a payload.
- Once a TCP connection is established, the two application processes can send data to each other.
- The data sent is directed to the connection's send buffer, which is one of the buffers set aside during the three-way handshake.
- The amount of 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 which are then encapsulated within network-layer IP datagrams.
- The TCP segment structure consists of a data field, header fields, source and destination port numbers, and a checksum field.
- The header also contains a 32-bit sequence number field, a 32-bit acknowledgment number field, a 16-bit receive window field, and a 4-bit header length field.
- The options field is used when a sender and receiver negotiate the MSS or as a window scaling factor for use in high-speed networks.
- The flag field contains 6 bits which have different uses such as indicating that the segment contains an acknowledgment or for connection setup and teardown.
- TCP views data as an unstructured, but ordered, stream of bytes, with the sequence number for a segment being the byte-stream number of the first byte in the segment.
- Field in the header
- Appropriate TCP segment