About Computer Technology: Dominant Themes

by Verity Carney

A NEED FOR BROADBAND

Describe broadband and its benefits. Broadband uses analog signalling over coaxial cable and allows frequency-division multiplexing (FDM). With FDM the frequency spectrum on the cable is divided into channels or sections of bandwidth. Separate channels can therefore support data traffic, TV and radio signals. It is a unidirectional medium. The advantage of broadband is that it is able to support tremendous capacity. It can achieve a very wide coverage with the use of active amplifiers. The system is based on mature CATV technology, with reliable and readily available components.. The significance of broadband is that it represents a paradigm shift in network technology able to transmit multimedia and data transmissions simultaneously. It is incompatible with the twisted pair telephone wire infrastructure and will require a complete replacement of the cabling infrastructure.

A NEED FOR IPv6

Why has Ipv6 been developed as a successor to the Ipv4 protocol? The Ipv6 datagram format has been developed to create an expanded addressing capability, increasing the size of the IP address from 32 to 128 bits. The reason for this development was a general recognition that the 32bit address space of Ipv4 was soon to become exhausted as new networks and IP nodes being added to the Internet at an exponential rate. The 128bit address space of Ipv6 will ensure that there is an unlimited supply of IP addresses. In addition Ipv6 datagram has a simpler more streamlined structure that eliminates some of the more time consuming aspects of Ipv4 such as fragmentation and reassembly at intermediate routers. The significance of Ipv6 is that it ensures permanent scalability of the Internet by providing for unlimited growth in nodes and networks that can be possible connected around the world.(Kurose & Rose 2003: 368-372)

A NEED FOR FIREWALLS

Explain the need for a security countermeasure in the form of a firewall. A firewall allows a network administrator to control access between the outside world and resources within the administered network by managing the flow to and from these resources. It allows some packets to pass through an organisations internal network while blocking others. A firewall can be classified as a security counter measure in so far as it protects a network against malicious attacks of hackers or the contagion of viruses. At this level a packet-filtering firewall that operates at the network layer can ensure security countermeasures used to manage and enforce security access policies. In this way the type of firewall that is used is an application-level gateway, which operates at the application layer. (Kurose & Ross 2003: 640-641) The significance of firewalls is that they can protect a network against malicious or unauthorised access.

BLUETOOTH

What is Bluetooth? Bluetooth is an emerging standard for wireless links to end systems that allows gadgets and devices to communicate without being in line of sight. It is a low-power, short-range, low-rate “cable replacement” technology (Kurose & Rose 2003: 481) Bluetooth has a wide range of potential applications from portable phones to PDAs as well as from digital cameras to laptops. It is an advance from the more restricted line-of-sight technology's that previously used infrared. Instead Bluetooth uses RF wireless communications which enable it to also support multi-port and to point-point communication. It operates with the 2.45 Ghz unlicensed radio band providing data rates of up to 721 kbps as well as three 64 kbps voice channels. The significance of Bluetooth is that it enhances wireless communication and networking capabilities using the already existing radio bands to provide the flexibility to create networked communication for portable devices. (Kurose & Rose 2003: 487-488)

HISTORY AND LESSONS LEARNT FROM THE USE OF THE INTERNET

Problem statement

The Internet is often referred to as ubiquitous. What is meant by this term in terms of the services offered by the Internet?

The Internet is considered ubiquitous because it is ever present and available everywhere throughout the world. It is the largest network in existence, globally spanning and connecting millions of computers, servers, WANs and LANs. No one single entity is in control of the Internet and users have unrestrained control over what they can do once connected. The Internet provides freedom of speech, as creators of web sites don't need to go through the mediation of traditional publishing controls and official procedures to make their content available to a mass audience. Some characterise the Internet in its ubiquitous nature as anarchic and it most certainly represents one of the greatest revolutions in information distribution and person-to-person communication that has occurred in the history of human civilisation.

The **significance** of the Internet's ubiquitous nature is that it is possible for most people across the world have access to an inexhaustible source of freely available information.

LANS VERSES WANS INCORPORATING POINT-TO-POINT VS. BROADCAST NETWORKS.

Problem statement

What is the difference between the transmission technologies of LANs and WANs.

Smaller geographically contained networks such as LANs tend to use broadcasting transmission whereas the larger more widely dispersed networks such as WANs are usually point-to-point networks. In point-to-point communication, hosts are connected by a communication subnet which consist of two distinct components – transmission lines (circuits, channels) and; switching elements (nodes or routers). In a point-to-point subnet, packets are sent from one router to another using intermediate routers, which stores then forwards the packet when the required output line is free. Broadcast networks on the other hand have a single communication channel that is shared by all machines on the network Broadcasting networks use a system of addressing a packet to all destinations in the network by a code in the address field. Every machine on the network then processes the transmitted packet with its address code. If a computer is the intended destination it accepts the message, while the other computers simple read the address and ignore it. (Tanenbaum 1996: 7–13)

The significance of this difference in transmission technologies is that various typologies offer different possibilities. LANs typologies tend to be more symmetrical than the irregular typology of WANs. They are therefore more able to broadcast without congesting the network and can benefit from the faster transmission provided. On the other hand point-to-point offers a greater flexibility for wider networks.

MOBILE IP

What is Mobile IP? Mobile IP is a flexible standard that is used to refer to the Internet architecture and protocols for supporting mobile nodes capacity to invoke the services of a foreign or home agent. It is defined in RFC 3220, which specifies the use of indirect routing to the mobile node. The mobile standard also defines protocols used for agent discovery and the mobile node's registration with the home agent. The Mobile IP protocols place an emphasis on security considerations. This is important as authentication is necessary to ensure that malicious users don't intercept and redirect datagrams. The significance of mobile IP is that it allows mobile users to maintain ongoing connections while moving between networks. (Kurose & Rose 2003: 400-401)

OSI vs IEEE802 REFERENCE MODELS

What are the OSI and IEEE 802 reference models? IEEE 802 is the collective reference to standards for LANs. The various standards differ at the physical layer and MAC sub-layer but are compatible at the data link layer. The IEEE 802 standards have been adopted by ANSI as American National Standards and also by ISO as international Standards. The ISO reference model is to provide a common basis for the coordination of standards development for the purpose of systems interconnection and to provide a common reference for maintaining consistency of all related standards. The ISO reference model provides a conceptual and functional framework, which allows international teams of experts to work productively and independently on developing standards for each layer of the Open Systems Interconnection (OSI) architecture. The significance of these standards ensure interoperability within networks such that LANs WANs and the Internet can connect remote users to one another across various typologies and across the globe.

THE RELATIONSHIP BETWEEN URL ADDRESSES AND IP ADDRESSES.

Problem Statement

What is the difference between a URL and an IP address? How are they related?

URL stands for uniform resource locator. It is the address used to specifying the location of a web page on the Internet. The first part of a URL specifies the protocol used in the file transmission eg http, ftp etc. The part after the colon is the hostname. The next part is a pathname, which is usually related to the pathname of a file on the server. The last (optional) part of the URL may be a query string preceded by "?". In order to access a web site or page the hostname must be translated into its identifying IP address. This translation is performed by another application protocol called DNS. A DNS (Domain Name System) is a Directory service that translates a hostname to an IP address. The IP (Internet Protocol) address is a network layer protocol that provides the location address of each host. It is made up of a series of numbers separated by full stops. Every hostname has a corresponding IP address which must be found and used in order to connect to that host.

The significance of URL and IP addresses is that they ensure that every host has a unique identifier and can therefore be accessed by any other host connected the Internet or within some other network.

SOCKET PROGRAMMING WITH TCP

What is the process of socket programming with TCP? Client/server application development is commonly referred to as socket programming because of the importance of sockets in these applications. In the establishment of a connection between a client and a server a socket must be created which acts as the door between the application process and TCP. When the client process initiates a TCP connection to the server it connects to the WelcomeSocket(). This invokes WelcomeSocket accept () method that then creates a new door (socket) for the client which is also known as the connection socket. The TCP connection is a direct virtual pipe between the client's socket and the server's connection socket. The significance of sockets is that they provide a memory store and crossing point between transport and application layers through which received data packets can be passed. (Kurose & Rose 2003: 133-137)

SWITCHING ON THE ETHERNET

What is the nature of switching on the Ethernet? Recently new interconnection devices, namely Ethernet switches, have become widely available for LAN networks. Ethernet switches are essentially high-performance multi-interface bridges. Like bridges they forward and filter frames using LAN destination addresses as well as automatically building forwarding tables using source addresses in the traversing frames. Unlike bridges, switches have dozens of interfaces, which generate a high aggregate forwarding rate through the switch fabric. In addition most switches operate in a full duplex mode – simultaneously sending and receiving frames over the same interface. The significance of switching on the Ethernet is that it facilitates direct connection between hosts and the switch rather than a shared LAN connection.

TCP versus UDP

What is the difference between the two transport layer protocols Transmission control protocol (TCP) and User Datagram Protocol (UDP). TCP is a reliable, connection orientated deliver service. TCP involves point-to-point transmission as well as congestion and flow control. In connection establishment (handshaking) each host sends preliminary segments to each other to establish the parameters of the following data transfer and initialize "state variables". TCP also requires connection termination where FIN and ACK segments are sent to terminate the connection. UDP is a connectionless protocol, which, unlike TCP, does not require connection setup or a structured procedure for acknowledging disconnection. For this reason it does not introduce any delay to establish a connection. UDP's smaller packet header overhead results in **a** minimum transaction time for datagram transfer**.** Because of the absence of congestion and flow control UDP can support real-time applications such as broadcasting and multicasting, which do not tolerate delayed segment transmission.

THE P2P MODEL, ITS APPLICATIONS, AND VIRTUAL COMMUNICATION VS. PHYSICAL COMMUNICATION

Problem Statement

What is the P2P model? Is it possible to build a P2P file sharing application without bootstrapping nodes?

P2P file sharing is where PCs at the edge of a network can retrieve content directly from each participating peer, which are both a consumer and distributor of content (Kurose & Rose 2003: 165-166). Each peer and must be capable of simultaneously running both the client and sever sides of the file transfer protocol – acting as both a web client and a transient web server. There are three main approaches to locating content – through a centralised directory, a decentralised directory and by public domain query flooding. The later two approaches use bootstrapping nodes to learn the IP address of peers on the network. Bootstrapping nodes are an essential feature of most P2P file sharing networks. However it is possible to build a P2P file sharing application without bootstrapping nodes by establishing a centralised directory. This is where a large server provides the directory service that collects details of shared files and IP addresses from each peer creating a centralised dynamic database that maps each object name to a set of IP addresses. (Kurose & Rose 2003: 166-172)

The Significance of P2P file sharing is that content is transferred directly between peers and doesn't go through a third party server. This makes P2P networks highly scalable.