Data Rate, Other Facts and Protocols

by Verity Carney

Data rate refers to the amount of data that can be transferred per second. Specifically it refers to a transmission rate through a given communications line that can be measured in bits per second (bps), bytes per second (Bps) or in baud (Stallings 2000: 94; Webnox: 2003).

Error rate refers to the rate at which errors occur. It is determined by the non-correspondence between the binary code which is sent and the code that is received – which means that an error rate measures the instances of receiving a 1 instead of a 0 or visa versa. (Stallings 2000: 95)

Bandwidth refers to the maximum amount of information that can be transferred. Bandwidth is constrained by the difference between the highest and lowest frequencies of a transmitted signal through a transmission channel. Thus "the width of its allocated band of frequencies" constitutes the bandwidth of a transmission (Webnox: 2003). Bandwidth is expressed in cycles per second, or hertz (Stallings 2000: 94).

Compare and contrast twisted pair cable, coaxial and fibre optics cable.

Both twisted wire pair cable and coaxial cable are made from coper wire. In the twisted pair cable the copper wires are insulated and then twisted together in a spiral configuration. In contrast the copper conductors of the coaxial cable are arranged concentrically. Coaxial Cable's have a higher bit rates than twisted pair cables however the latter perform better over short distances such as is used in DSL or LAN

Networking. In contrast to these types of cables, fibre optics are made from glass fibre. Rather than transmitting electrical impulses fibre optics conduct a pulses of light that allows it to support greater bit rates. Unlike copper wires, fibre optics are not affected by electrical interference. Coaxial cables are used prevalently in television transmission, whereas fibre optics and twisted wire pair are largely used in telecommunications. Fibre optics have become the backbone of the Internet, coaxial cable facilitate broadband and twisted pair are the dominant solution for high-speed LAN networking and residential dial up Internet access. (Kurose & Rose 2003: 36-37)

What are some of the physical media that Internet can run over?

The Internet can run over many physical media. Some facilitate transmission (broadcast media) such as fibre optics, copper wire cables (twisted pair or coaxial) as well as radio spectrum and microwave transmitter/receivers (satellite link to a base station). Hosts often connect to the Internet through a modem to an ISP or can be accessed with a network such as a LANs &/or WANs. All Internet transmissions run through intermediate switching devices known as routers which are also a physical media. End systems interact with other physical media such as servers that store and transmit web sites, databases and other files. (Kurose & Rose 2003: 2-4)

Describe a handshaking protocol.

A handshaking protocol is a form of transmission etiquette between two or more end systems. It is designed to maintain some form of synchronisation in the request for, transmission and receipt of data. A handshake refers to the first two messages sent by the computers that are seeking to connect for a transmission. It is analogous to a human greeting where if not reciprocated then the communication terminates or the initiator (assuming no ill will intended) may try again. In computer terms "a protocol that performs a handshaking between the communicating entities before transferring data is a connection-orientated service" (Iren 1999 cited in Kurose & Rose 2003: 13)

List dial up modem technologies that are used for residential access. Compare and contrast these modems taking into account sharing bandwidth and transmission rates.

56K modems are considered the basic technology for dialup residential access. They have largely superseded their predecessors, the 28.8K and 33.6K modems. There are 3 different modem technologies supporting 56K in the market: V.90, X2 and K56Flex . (ITSC 2003). None of these standard modems technologies allow the sharing of bandwidth. Furthermore transmission rates are lower than the configuration of the technology. "56K modem receiving speeds are limited to 53Kbps while transmission speeds top out at 31.2Kps. Line conditions and other variables often result in even lower speeds." (Capron 2002: 200)

Digital subscriber line (DSL) modems translates digital signals to analog over a traditional copper telephone wires and back again (demodulation) at the destination. DSL spreads the analog signals over a large range of frequencies, thereby increasing the transmission rate. The transmission rate varies depending on proximity to the telephone exchange (must be within 3 km) A DSL modem allows sharing of bandwidth - so that a user can use the telephone at the same time as traversing the Internet.(Capron2002: 200)

Cable Modems enable broadband access to the Internet via **Hybrid Fibre Coaxial (HFC)** Networks. These modems use coaxial television cables that already in place in a residential environment. They allow the sharing of bandwidth as they run over the same cable as the television without interrupting normal cable TV reception. In addition all users on a cable segment share its capacity (bandwidth). The speed of transmission is very fast and can reach up to 10 million bps, however as more households in a neighbourhood use the service the general speed decreases. (Capron 2002: 200-201)

List and explain the reasons for introducing as two separate layers the transport layer and the network layer.

Although the transport layer and the Network layer work in tandem and interact in the transmission of messages from source to destination, they use separate protocols and are responsible for different levels in establishing, controlling and directing transmission. It is consistent to separate them as two separate layers because at the logical level they perform different (although mutually dependent) functions. To explain

The Transport Layer's main task is "to provide reliable, cost effective data transport from the source machine to the destination machine" (Tanenbaum 1999: 479) by providing logical communication between end processes. The transport layer establishes the protocol for communication between hosts by allowing these end-to-end entities to carry on a conversation from source to destination. The transport lay can use either TCP (Transmission control protocol) or UDP(User datagram protocol). (Tanenbaum 1999: 32-36)

Network Layer, on the other hand, provides logical communication between hosts and is responsible for routing datagrams from one host to another (Kurose & Rose 2003: 56) The protocols used by this layer do not connect end-to-end entities rather they operate between each machine and its immediate neighbours by controlling the operation of the subnet in determining how packets are routed along particular transmission paths from sender to receiver (Tanenbaum 1999: 31-32). The network layer also controls congestion – by dynamically determining paths depending on network traffic. The protocol used by this layer is IP (Internet protocol).

Present the placement and role of a socket in the development and executing services provided by the application layer protocol.

A socket is the interface which is placed between the application process and the transport protocol (Kurose & Rose 2003: 83) Its role is to provide a mechanism for creating a virtual connection between processes. Sockets interface with network

communication facilities – between a client and a server. They can be either stream (bi-directional) or datagram (fixed length destination-addressed messages). The socket has associated with it a socket address, consisting of a port number and the local host's network address. (Webnox 2003)

The client process invokes a TCP connection to the server by firstly creating a socket in the client program. In creating this socket it specifies the address of the server (the IP and port number). "Upon creation of the socket, TCP in the client initiates a three-way handshake and establishes a TCP connection with the server". (Kurose & Rose 2003: 135) Subsequently the execution of services (all transmissions of data) between the application layers of the communicating entities (source and destinations) are sent through the sockets which function as memory objects (write & read) passing messages between processes.

List and discuss advantages and disadvantages of cookies.

Cookies are a means used by Internet sites to keep track of and authenticate Internet users.

An e-commerce site or an associated organisation (advertisers) can use cookies track a users activity at a particular web site or across web sites. The main advantage of this is that cookies can be used in this way to enable the use of virtual shopping trolleys for e-commerce sites.

Cookies can also be used to determine a visitor's preferences based on previous visits and purchases and thereby dynamically recommend products according to those preferences. This can make browsing and shopping on-line an easier and more simplifying experience for the user (Kurose & Rose 2003: 100 – 101)

However, if a visitor to an ecommerce site purchases something at that site then their name, credit card details, email addresses etc are then stored in a back-end database with the cookie identification number. This then enables a company to correlate the information collected by the cookie with the actual person's details. If it is unethical, a

company might then sell this information to a third party thus infringing on privacy. Cookies result in information being collected without the express consent of the Internet user, the person does not have the right to view and alter that information to ensure it is correct or in accordance with their wishes regarding privacy and the use and disclosure of personal information or profiles.

DNS is a commonly used service in the Internet. Suppose there are two servers within this environment: one local name server and one authoritative name server. Specify the roles of these servers.

A DNS (Domain Name System) is a Directory service that translates a hostname to an IP address It functions as an application layer protocol that allows hosts and named servers to communicate in order to provide the necessary translation service. A DNS operates in a distributed database that is implemented in a hierarchy of named servers. (Kurose & Rose 2003: 124) The two main types of servers in this distributed environment are known as local name servers and authoritative name servers.

The role of the local name server - which is usually located close to a particular host - is to accept a DNS query message from that host which contains the hostname to be translated. If the request is for a translation for another host that is part of the same ISP then this server will be directly able to provide the requested IP address. However if the query is for an IP address not known by the Local Name Server then this server will direct the query message to the authoritative name server. (Kurose & Rose 2003: 125)

The authoritative name sever has a DNS record of all hostnames ending with part of a particular domain name. Its records come from the authority that manages the record, and is therefore always correct (in contrast to cached records that can be out of date). (Tanenbaum 1996: 629) The role of the authoritative name server then is to respond to a request with a DNS reply that contains the mapping for the corresponding IP address. The authoritative name server will then forward the IP address requested to

the local name server, which will then forward it to the requesting host (Kurose & Rose 2003: 126-127).

Uploading and downloading

Technically in a full duplex transmission, simultaneous uploads should not slow down downloads, however the reality is that downloads can potentially be slowed down because the simultaneous transfer of packets impacts upon TCP acknowledgements upsetting the TCP flow-control algorithms. (Walker 2004). When downloading from a peer server, the sender uses the reciept of the TCP acknowledgments to pace itself on how fast to send data to the receiver. "A fast download requires not only the download packets to arrive quickly, but also for the acknowedgments to get back to the sender in a timely fashion" (Walker 2004). If a full-duplex link connected to a 128kbps modem is congested with an upload, the acknowledgements sent from the concurrent download will have to wait in a queue for a gap between the congested upload data packets before they can be sent. As a consequence, the TCP acknowledgements will be delayed getting back to the remote download server, and it will therefore be led to believe that the download reciever is on a very slow link, and it will consequently slow down the transmission of further data. (Walker 2004)

Distributed applications can be supported by either the TCP protocol or the UDP protocol. Present the reasons for selecting UDP to run applications.

User Datagram Protocol (UDP) is a connectionless protocol, which, unlike TCP, does not require connection setup (handshaking). For this reason it does not introduce any delay to establish a connection. This advantage in addition to UDPs smaller packet header overhead results in **a** minimum transaction time (RTT) for datagram transfe**r.** Another reason for selecting UDP to run applications is that by using this protocol a server dedicated to a particular application can normally support many more active clients (Kurose & Rose 2003: 198) UDP can also better support real-time applications such as broadcasting and multicasting which do not tolerate delayed segment. (Kurose & Rose 2003: 198-201)

It is very well known that UDP provides a fast but unreliable communication service. Present what should be done in order to provide reliable communication between two application processes supported by the UDP protocol.

The only feature of UDP that provides a mechanism for ensuring reliable data transfer is an error detection mechanism called checksum that checks for bit errors in transmitted packets. Checksums can be used to notify the application that data has been altered and must be discarded or else warn the application to implement a mechanism to recover from an error.

Apart from the checksum error detection, all other aspects of reliability must be built directly into the application processes when using UDP. This requires that the application layer processes packets sequence numbers and that there is some timing mechanism to determine when a packet has been delayed or lost. Thus the application processes may be required to acknowledge message receipt, correctly order received packets into meaningful messages, discard duplicate packets and request retransmission of faulty packets since UDP does not provide this service. (Thomas 2004)

Describe connection management in the TCP and UDP protocols as examples of connection-orientated and connection-less communication protocols, respectively. Connection management covers three stages: connection establishment; data transfer, and; connection termination. The UDP protocol is connectionless because it sends data without ever establishing a connection between sending and receiving hosts. TCP is connection-oriented because, before data transfer can occur, the two processes must engage in a connection establishment procedure known as a three way handshake - each host sends preliminary segments to each other to establish the parameters of the following data transfer to setup the connection and initialize "state variables". In connection termination TCP offers a graceful shutdown where FIN and ACK segments are sent between both the client and the server to terminate the connection. Data sent before a closing connection is not lost. Connectionless

protocols such as UDP have no structured procedure for acknowledging disconnection. (Kurose & Rose 2003: 250-251)

Introduce and characterise multiplexing and de-multiplexing network applications by the transport layer.

A multiplexing/demultiplexing service is required for all computer networks. Multiplexing involves gathering chunks of data at the source host from different sockets, encapsulating each data chunk with header information to create segments and passing the segment to the network layer. Demultiplexing involves the transport layer examining the destination port number in the segment header and directing (delivering) the segment of data to the correct socket (Kurose & Rose 2003: 190-191)

Briefly characterise the TCP congestion control

TCP uses end-to-end congestion control rather than network assisted congestion control. This means that TCP causes each sender to limit the rate at which it sends traffic to its connection as a function of perceived network congestion. If little network congestion is perceived the TCP sender increases the rate of transmission. TCP uses the mechanism of additive-increase, multiplicative decrease in the management of its congestion control. The idea behind this is that the sender reduces its sending rate through decreasing its congestion window size when an event of data loss occurs. And subsequently increases its sending rate when less congestion is perceived. Consequently TCP congestion control mechanisms can be characterised as fair as it enables the equal sharing of bottleneck link's bandwidth among competing TCP connections (Kurose & Rose 2003: 262-268)

Topic 9

The port number ranging from 0 to 1023 are referred to as well-known addresses and are restricted for the use of well-known application protocols. To identify the port numbers for these applications then a transport user can refer to RFC 1700 to determine wether the address of the destination transport users process has a

particular reserved port number. Alternatively the transport users can simply examine the source port number in any message received back from the destination to find out its address.

In addition to finding IP addresses, name servers are able to find the transport server access point (TSAP) which is an address corresponding to a given transport user's service name. The user invokes DNS protocol to sends a message specifying the service name, and the name server sends back the TASP address translated to an IP address. The name server provides a mapping of names onto numbers. (Tanenbaum 1996: 491-492).

Broadcast, can be used in a network topology where each node broadcasts the identities (including address components) to all other routers in the network. (Kurose & Rose 2003: 304) A transport user can find the identity (addresses) of a destination transport user by using a ping or tracert command which uses the information broadcast to the routers to identify the port and IP addresses of the destination user.

List and characterise the influence of the quality of the network in terms of the services provided by the network layer on the scope of the transport layer protocol.

The network layer is responsible for delivering datagram's from source to destination subject to pre-specified quality of service parameters. The network layer provides services, which involve upper layer interaction with the transport layer. The transport layer determines how to use the network layer to provide a virtual error-free, point-to-point connection so that a source host can send messages to a destination host that will arrive un-corrupted and in the correct order. If the quality of the network is lacking then the transport layer must compensate in terms of guaranteeing reliability of service. The network layer provides a service in which it takes segments from the transport layer, which it encapsulates into a datagram and then sends these datagram's along a path of links between routers until they arrive at their destination. At the

destination the network layer extracts the transport layer segments and delivers these segments to the transport layer at this host. The main services of the network layer are (Kurose & Rose 2003)

- Connection establishment (Call Setup) – this occurs in some network layer architectures such as ATM or other connection orientated sessions subject to certain quality of service parameters where routers along a certain path handshake with each other in order to setup state information before network-layer packets can actually be transferred. (Bashandy 1999)

- Packet determination and Route establishment– the network layer determines the route taken by a packet in its transfer from sender to receiver. It calculates this path using a routing algorithm. In better quality networks this can take the form of virtual circuits. The user specifies the destination and the quality of the service and the network layer then finds an appropriate path by invoking several central and distributed algorithms. (Bashandy 1999)

- Transmitting, Forwarding and receiving data - the network layer provides the means to ensure the delivery of data which includes switching capabilities, segmentation and reassembly, modulation and others. (Bashandy 1999)

- Providing information about the network - eg session specific information such as the number of packets lost, throughput or maximum capacity of a path and propagation delay

- Error detection and correction to ensure reliability

- Other services include Security and encryption as well as Management of multicast groups

Depending on the quality of the network architecture these Network layer services provide varying degrees of bandwidth guarantee, No-Loss guarantee, Ordering, Timing and congestion indication. (Kurose & Rose 2003: 294)

Compare and contrast datagram and virtual services.

A virtual circuit (VC) is a connection-oriented network service which is implemented on top of a network. It has three phases. 1) Virtual circuit setup in which it determines the path (series of links and packet switches) between sender and receiver through which the packets will travel. Setup involves a process that reserves resources such as bandwidth along the path of the VC. 2) Data transfer in which connection state information is maintained in the packet switches, and 3). VC teardown when a host informs the network layer that it wishes to terminate the VC. (Kurose & Rose 2003: 296-299)

Datagram service on the other hand is a connectionless service. When an end system sends a message it simply stamps the packet with the destination address and then just sends to packet into the network. This service does not involve any setup procedure and packet switches (routers) do not maintain any state information. Switches simply examine the destination address in the packet header and forward the packet in the direction of the destination. A series of packets may follow different paths and may arrive out of order Datagram service is also known as best effort service where delivery and timing between packets are not guaranteed. (Kurose & Rose 2003: 296-299)

Explain the importance of routing algorithms, and compare and contrast link state and distance vector routing algorithms.

Routing algorithms value lies in their ability to compute the least cost path that packets can follow to be transferred between a source and a destination. Link state algorithms use complete global knowledge about the network taking the connectivity between all nodes and all link costs as inputs to calculate the least-cost path. Each node broadcasts the identities and costs of its attached links to all routers in the network. Thus all nodes have an identical and complete view of the topology of the

network. The link state algorithm consists of an initialisation step followed by a loop that is executed for each node on the network. (Kurose & Rose 2003: 303-308)

Vector routing algorithms use a decentralised algorithm calculated in an iterative, asynchronous and distributed manner where a node only knows its neighbour in a least cost path and never actually knows the complete path from source to destination. Each node receives some information from one or more or its directly attached neighbours, performs a calculation and then distributes the results of the calculation back to its neighbours. Thus each node knows of the minimum cost path off each of its neighbours to each destination. (Kurose & Rose: 303, 308-316). Link State algorithms are more robust, have a higher speed of convergence and are more complex than Vector routing algorithms.

There are different intra-AS routing algorithms in use in autonomous systems. Explain whether it is necessary that every autonomous system use the same intra-AS routing algorithm.

Within a single Autonomous system (AS), all routers run the same intra-autonomous routing protocol. However different autonomous systems connected via gateway routers can use different intra-AS routing algorithms. In this case these special gateway routers connecting the different AS use an intra-AS routing algorithm that determines routing paths among the Autonomous systems so as to connect an AS to another AS. Therefore it is not necessary that every AS use the same intra-AS routing algorithm (Kurose & Rose 2003: 318-319)

Compare and contrast the IPv4 and IPv6 header fields. Do they have any fields in common?

The only header fields that Ipv4 and Ipv6 have in common are a version field (yet the content of this field indicates the different versions of the IP version) and the source and destination address fields. However Ipv6 has expanded addressing capabilities. It increases the size of the IP address from 32 to 128 bits. Apart from that, a number of Ipv4 fields have been dropped or made optional in Ipv6 headers. Some of these

include fields such as Header length, Type of service, the 16-bit identifier, flags, 13-bit fragmentation offset and time to live. This has resulted in Ipv6 having a 40-byte fixed length header, which allows for faster processing of the IP datagram. One other major difference is Ipv6 has a flow label in its header for packets that belong to a particular flow for which the sender requests special handling such as real-time service. (Kurose & Rose 2003: 334 & 369)

List and discuss the reasons for moving toward IPv6, pay particular attention to the IPv4 and IPv6 header fields

Fragmentation/Reassembly – Ipv6 performs fragmentation and reassembly only at the source and destination and not at intermediate routers. This speeds up IP forwarding within the network. The Ipv4 fragmentation offset header field is no longer required.

Header checksum – Ipv6 has dropped the Ipv4 TTL (Time to Live) field. This field required that a header checksum be recomputed at every router. Because fast processing of IP packets is a central concern, dropping this field and its associated computational requirements results in Ipv6 saving more in time and cost of message transfer.

Options – Ipv6 removes the options field and replaced it with a pointer to the next header. This has enabled Ipv6 to have a fixed length 40-byte header. (Kurose & Rose 2003: 371)

References

Capron, H. Johnson, J.(2002) *Computers: Tools For An Information Age*, Prentice Hall, New Jersey

Kurose, J.& Rose, K. (2003) *Computer Networking: A Top Down Approach Featuring the Internet* (2nd edition.), Addison & Wesley New York

Stallings, W. (2000) *Data & Communications* (6th Edition) Prentice Hall International Inc., New Jersey

Tanenbaum, A. (1996), *Computer Networks* (3rd Edition) Prentice Hall International Inc. New Jersy,

Walker, R. 2004, "Modem Troubleshooting Tips" *ntlworld* http://homepage.ntlworld.com/robin.d.h.walker/cmtips/downup.html#ethdup (accessed 17 March 2004)