Data communication reviewer

Reviewer DataCom: Chapter 1-5 Chapter 1: Intranet- Restricted group on a company and only allows internal employee access. Extranet- Type of network that allows outside vendors special access to limited info in a company. Protocols- Rules ofcommunication. * An identified sender and receiver * An agreed-upon method of communicating * Common language and grammar * Confirmation or acknowledgement requirements Elements of a Network: * Rules or agreements: protocols or how the message is semt, directed, received and interpreted. * Massages: units of info that travels Medium: means of interconnecting these devices, can transport the messages

* Devices: devices on the network exchange messages Messages- a generic term that encompasses forms of communication enabled by the Internet. Devices- several devices work to see that the message is properly directed to the source to the destination device. Icons- symbols that graphically presents network devices and media. * Desktop Computer * Laptop * Server – a computer dedicated to providing app services * IP Phone – a digital phone

* LAN media * Wireless media LAN switch – most common device for interconnect LANs * Firewall – provides security to networks * Router – helps direct messages between networks * Wireless router * Cloud – summarize a group of networking devices * WAN media IP (Internet Protocal) & TCP (Transmission Control Protocol) – most common protocols * WWW – HTTP * E-mail – SMTP * Instant messae – XMPP * IP telephony – SIP Convergence – coming together of technologies onto a digital platform. It occurs when computer communications all use the same rules to transport their messages. Network Architecture – the conceptual plans on which a physical

network is built. Fault tolerance- needs to function even if some components fail * Scalability- network's ability to grow & react to future changes * Quality of service- performance level of services. Prioritize traffic and its characteristics to manage data. * and Security Packets-single message is broken into small blocks of data. Bandwidth- measure of the data-carrying capacity of the network. Chapter 2: Elements of communication: * Message source, or sender * Destination, or receiver *

Channel- media that provides pathway Network- refers to data networks carrying massages. Segmentation- all messages are broken into smaller pieces Multiplexing- occurs when segments of two messages can shuffle into each other and share the medium. * Increased efficiency of network communication End device- a piece of equipment that is either the source or the destination of a message on a network. Host- an end device that sends or receives messages. Clients- other hosts that set up to store and share info by the host servers *The host address is a unique physical address used by hosts inside a LAN. Intermediary device- connects the individual host to the network and connect multiple individual network to form an internetwork. Network access devices

* Internetwork devices * Communication severs * Modems * Security devices Network media: Copper, Fiber-optic cable, Wireless Encoding- refers to the way data is converted to patterns of electrical, light, or electromagnetic energy. LAN- a group of end devices and users under the control of a common administrator. WAN- a network that is used to connect LANs that are geographically far apart. Internetwork- is a collection of two or more LANs connected by WANs. Proprietary – A limited-use protocol owned by a

company. Network Representations: Network interface card (NIC)- provides the physical connection to the network at the PC or other host device. * Physical port- is a connector or outlet on a networking device where the media is connected to a host.

* Interface- refers to how the device can allow 2 different networks to communicate. The organizations that standardize networking protocols are: * IEEE – Institute of Electrical and Electronics Engineers * IETF – Internet Engineering Task Force Interaction of Protocols: * Hypertext Transfer Protocol (HTTP) – common protocol that governs the way that a web server and a web client interact. Transport protocol – Transmission Control Protocol (TCP) is the transport protocol that manages the individual conversations between web servers and web clients. * Internetwork protocol * Network access protocols – describes 2 primary functions: Data-Link Management & the physical transmission of data on the media. Layered Models – describe the complex process of network communication. Open Systems Interconnection (OSI) – is the most widely known internetwork reference model.

Provides an abstract description of the network communication process. Developed by International Organization for Standardization (ISO). Application, Representation, Session, Transport, Network, Data Link, Physical TCP/IP Model – defines the 4 communication functions that protocols perform. * Application, Transport, Internet, Network Access Encapsulation- Process of adding control info as it passes through the layered model Decapsulation- process of removing extra information Protocol Data Unit (PDU) – generic term for data at each level. Chapter 3: Presentation Layer

has 3 primary functions: * Coding and conversion of application layer data * Compression of the data * Encryption of the data TCP/IP protocols: Domain Name System (DNS) - used to resolve internet names to IP address. * HTTP – used to transfer files that make up the web pages of the WWW. * Simple Mail Transfer Protocol (SMTP) – used for the transfer of mail messages and attachments. * Telnet – a terminal emulation protocol used to provide remote access to servers and networking devices. * File Transfer Protocol (FTP) – used for interactive file transfer between systems. Process – each executing program loaded on a device. Client/server model Deamon – are describes as " listening" for a request from a client. Application layer services and protocols

Peer-to-peer networking and applications * 2 or more computers are connected through a network and can share resources such as printers and files without having a dedicated server. nslookup – a utility that allows the user to manually query the name servers to resolve a given host name. ipconfig/displaydns – displays all the cached DNS entries 3 common message types are: * GET- is a client request for data. * POST and PUT- are used to send messages to that upload data to the web browser. E-Mail Server Processes: * Mail Transfer Agent (MTA) – process used to forward e-mail. * Mail Delivery Agent (MDA)

Server Message Block (SMB) – a client/server file-sharing protocol. Chapter 4: Transport Layer – provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. It enables applications on devices to communicate. * Tracking the individual communications * Segmenting data and managing each piece *

Reassembling the segments * Identifying the different applications * Performing flow control between end users * Enabling error recovery * Initiating a session Flow Control – can prevent the loss of segments on the network and avoid the need for retransmission.

Used to avoid buffer overflows. Two most common transport layer: TCP (Transmission Control Protocol) – incurs additional overhead to gain functions. * Web browsers, E-mail, File transfers UDP (User Datagram Protocol) – provide the basic functions for efficiently delivering the data pieces. Has the advantage of providing low-overhead data delivery. * DNS, Video streaming, Voice over IP (VoIP) 3 basic operations of reliability: * Tracking transmitted data * Acknowledging received data * Retransmitting any unacknowledged data Socket – refers only to the unique combination of IP address and port number.

Internet Assigned Numbers Authority (IANA) – assigns port number. Different types of ports: * Well-known ports (0 to 1023) – reserved for services and applications. * Registered ports (1024 to 49151) – are assigned to user processes or applications. * Dynamic or private ports (49152 to 65535) – also known as ephemeral ports, are usually assigned dynamically to client applications. netstat – a command that is an important network utility that you can use to verify TCP connections. It lists the protocol in use, the local address and port number… Datagram – is a UDP segment (piece).

Flags – are six 1-bit fields contain control information used to manage the TCP processes: * URG: Urgent pointer field significant * ACK: Acknowledgement field significant * PSH: Push function * RST: Reset the connection * SYN: Synchronize sequence numbers * FIN: No more data from

sender *flags have fields that the only value is 1 bit and, therefore, has only two values: 1 or 0. 3 way handshake: Step 1 – SYN, Step 2 – SYN and ACK, Step 3 – ACK. Expectational acknowledgement – occurs when TCP uses the acknowledgement number in segments sent back to the source to indicate the next byte in this session that the receiver expects to receive.

Window size – is the amount of data that a source can transmit before an acknowledgement must be received. Chapter 5: OSI Layer 3 – provides services to exchange the individual pieces of data over the network between identified end devices. The network layer describes four tasks to be performed: * Addressing packets with an IP address * Encapsulation – is the process of adding that information. * Routing – is the process router perform when receiving packets… * Decapsulation – is the process of removing encapsulation data at different layers. Source IP address – is the IP address of the sending host

Destination IP address – is the IP address of the receiving host. IP header – contains the address information and some other bits that identify the PDU as a network layer PDU. Packet – is referred when an OSI layer 4 PDU has been encapsulated at the network layer. Hop – is each route that a packet takes to reach the next device. Common network protocol: * IPv4 – most widely used network protocol. * IPv6 – currently in use in some area. * Novell IPX – a widely popular internetworking protocol in the 1980s and 19990s. * AppleTalk – Apple Computer's propriety networking protocol. Connectionless Network Service (CLNS) – a protocol used in telecommunication network. IPv4 basic characteristics: * Connectionless * Best effort (unreliable) * Media independent *Some networks have media restrictions and must enforce a

Maximum Transmission Unit (MTU). Fragmentation – is the process when the network layer builds the packets according to specification. Key fields: * IP source addressing * IP destination addressing * Time to Live (TTL) * Type of Service (ToS) * Protocol * Flag and Fragment Offset Other Key Fields: * Version * Internet Header Length (IHL) * Packet Length * Identification Header Checksum * Options * Padding *Because broadcast do not travel beyond the network boundary, the network is known as a broadcast domain. Gateway router – is the router a network uses to send and receive messages beyond the network. Hierarchical addressing – is read from the most general information to the most specific. Subnetting – the process when a large network needs to be divided into smaller subnets, additional network codes can be created using some of the bits designated for the host. *The default route is used when the destination network is not represented by any other route in the routing table.

Next hop – is the address of the device that will process the packet next. *The route info can be manually configured on the router, creating what is known as a static route. Dynamic routing – when routers learn about routes automatically from other routers in the same internetwork. Routing Protocols – are the set of rules by which routers dynamically share their routing information. * Routing Information Protocol (RIP) * Enhanced Interior Gateway Protocol (EIGRP) * Open Shortest Path First (OSPF) 3 key factors to consider when grouping hosts into a common network: * Purpose * Ownership * Geographic location