Kevin Chen

11/23/16

Foundations of Networks Notes

Networking Topologies

* Understanding logical and physical network topologies
  + Two types: Physical (physical layout of the wires in a network) and logical topologies (how data moves through the network and the pattern of data flow in a network)
  + Networks can have different physical and logical topologies.
* Mesh, Bus, and Ring Topologies
  + Two types of mesh topologies: full mesh (all devices are directly connected to all other devices: full redundancy but most expensive because requires multiple NICs and cables for each node. Most likely found in WAN environment) vs. partial mesh (all devices directly connected to at least two other devices. Provides strong but not full redundancy. Not as expensive. Multiple NICs and cables runs on each machine, most likely found in WAN environment (e.g. Internet)).
  + Bus Topology: all nodes directly connected to main cable called the bus. Very simple. Only one node (computer) can get to send a signal at a time. Contention is used to determine which node sends the signal. Nodes listen to the network, and if they don’t hear a signal, then they send a signal. If two nodes listen at the same time and don’t hear anything, then they send a signal at the same time, resulting in a collision and cancelling each other out. The more nodes active, the more collisions on the network. After collision, all nodes again contend to send signal. Too many collisions (network storm) overload and bring down network. 30 nodes or less recommended. Least expensive, but a single bad node/cable can bring down the whole network. Also not part of the current TIA EIA 568-C standard.
  + Ring topology: connected in a circle. Packets move in ring around network, giving opportunity for node to send a signal. No contention between nodes. Heavy traffic will not bring down network, but will slow it down. Single damaged node or cable can bring down the network. Not part of the current TIA EIA 568-C standard.
* Star and Hybrid Topologies
  + Hierarchical star topology: most common used in LANs, more expensive than bus b/c needs more cables, but won’t bring down network with one damaged node. All nodes connected to a central hub or switch. Easy to troubleshoot. Susceptible to a single point of failure. If the whole network goes down, you know that the central devices is the problem. If only single node goes down, that node is the problem. This is the only topology recognized in TIA/EIA 568-C standard for LAN networks.
  + Hybrid topologies: combines normal star topology with some other topology. Physical hybrid topologies: network containing two or more physical topologies. Physical-logical hybrid star topology: network physically looks one way but functions differently (e.g. ring network that looks like a star).
* Point-to-Point and Point-to-Multipoint Topologies
  + Point-to-Point: connects two nodes directly to each other with no intervening device. Used to connect two ends of a WAN connection, connect computer directly to switch, connect switches or routers to each other. Can also be in the form of a cross-over cable connecting two computers. Often part of a hybrid system.
  + Point-to-Point multipoint: one device connects directly to more than one device.
* Client Server and Peer-to-Peer Network Management Models (for LAN)
  + Peer-to-Peer Network: computer responsible for own security and management. Each computer managed as separate device. Usually only used for very small network. Homegroup and Workstation are peer to peer. Used in small businesses and most home networks.
  + Client Server: all devices access resources through central server. Devices needing access to network are called clients. Device/devices controlling access are called servers. Network management overseen by server. Security built around the server. Server allows or restricts access to network resources and controls who is allowed to log on to network. If server goes down, no one can access the network.
* CSMA/CD and CSMA/CA: allows computers to access the network directly
  + Contention-based network access: computers competing for network access. CSMA/CD and CSMA/CA are two types of contention-based access.
  + CSMA/CD: method most commonly used by wired Ethernet. Node listens for traffic on network. If no traffic is heard, node releases packet onto network. If two nodes release packets at the same time, the packets each other and a collision occurs, resulting in a power spike heard by all the other nodes on the network and destroying the data contained in the two packets. If no collision, then transmission was successful, and network is freed up for another node to transmit. If collision occurs, all nodes start internal clock set to a random number of milliseconds. When time runs out, each node can attempt to send a new transmission.
  + CSMA/CA: method most commonly used in Wi-Fi networks. Difference from CSMA/CD is that nodes release warning packet before releasing data packet. If other nodes hear warning packet, they won’t transmit until they hear the data packet go by. However, two warning packets transmitted at the same time cause a collision. Collisions handled the same way as CSMA/CD.
* Internet vs Intranet vs Extranets
  + Internet: worldwide publically accessible infrastructure of cables, routers, switches, and servers. Not the World Wide Web, which runs on top of the Internet. Used to carry a wide variety of services: WWW, email, FTP, VoIP (voice over IP), streaming video, online gaming, etc.
  + Intranets: privately accessible infrastructure of cables, routers, switches, and servers. Generally limited to a single company, organization, or group of companies. Used to carry a wide variety of services.
  + Extranets: Privately held WAN infrastructure. Generally owned by one company or organization. May allow others access for a fee for specific purposes. Examples: MSFT Azure and Amazon Web Services

Network Implementations

* WANs and MANs
  + WANs: wide area networks. One large network that covers a large geographic area. Ex: Internet. Can be many smaller networks linked into one large one. Called an enterprise network when owned by one org. Use routers and switches to connect up network b/c of its large size.
  + MANs: metropolitan area networks. A smaller version of WAN.
* LANs, WLANs, PANs
  + LAN: local area network. Limited in size. Single room, single building, or span several buildings close together. TIA/EIA 568-C standard defines characteristics of LANs. Normally uses twisted pair cabling to connect devices. Use CAT 6 or 6A cabling in current LAN builds. LAN nodes tied together with switches or hubs. Can use fiber optic cables to connect switches.
  + WLAN: wireless local area network. Uses wireless technologies, which is often referred to as Wi-Fi. Wi-Fi technologies defined by IEEE 802.11 standard. IEEE 802.11ac is the most current Wi-Fi standard. (IEEE 802.11ax being developed.)
  + PAN: personal area network. Defined by IEEE 802.15 standard group. Primarily uses Blue Tooth technologies for connecting. Limited range of 30 feet. Requires less power to generate a signal. Uses: Keyboards and mice to connect to a computer, earbuds to use phones while driving, watches to connect to smartphones. Infrared (IrDA) can be also used instead of Blue Tooth.
* SCADA/ICS and Medianets: specialized network technologies
  + SCADA/ICS: refer to networks and technologies used to control industrial application. SCADA is a subset of ICS: SCADA describes systems that span large geographic areas. Ex: pipelines, power distribution, water management. ICS is more generic in use: normally refers to small scale systems. Ex: industrial automation, control system for power plants and factories.
  + Medianets: networks optimized for distributing large video applications and similar technologies. Ex: Hulu, Netflix. Uses smart bandwidth detection systems, which allow medianets to adjust to higher or lower bandwidth devices, allowing it to provide smooth video transmission on any platform.

OSI Model

* Intro to OSI Model
  + Open Systems Interconnection Reference Model.
  + Model for organizations when creating new protocols.
  + 7 layers: Application, Presentation, Session, Transfer, Network, Data Link, Physical. All People Seem To Need Data Processing / Please Do Not Throw Sausage Pizza Away.
  + Two parts of the OSI Model: abstract model (actual model with its seven layers) and set of specifically created protocols (protocols not actually used in any network system)
  + OSI Model published as ISO 7498 standard and under ITU-T X.200.
* Layer 1: Physical Layer
  + Concerned with physical transmission of raw data. Transmits data in the form of 1s and 0s (digital transmissions). Defines encoding methods to transmit data. Defines how bits are placed on media. Defines how to know when bits start and stop.
  + Defines specifications for media usage. Defines kinds of media permitted. Defines how physical connections are made. Defines pin usage in physical connections. Specifies standards that apply to specific types of media.
* Level 2: Data Link Layer
  + Provides error-free transmission from one node to the next over physical media by establishing and terminating links between nodes.
  + Responsible for traffic control. Transmits and receives frames (packets) sequentially. Responsible for frame acknowledgment. Provides and expects frame acknowledgment.
  + Detects and recovers from errors on physical layer by retransmitting nonacknowledged frames and handling duplicate frame receipt.
  + Responsible for delimiting, which means that it creates and recognizes frame boundaries (when a frame starts and a frame stops). Responsible for error checking: checks received frames for data integrity. Provides media access management: determines when node is allowed to use physical media.
* Level 3: Network Layer
  + Controls the operations of the subnetwork it is on. Determines best physical path for data by using network conditions, priority of service, etc.
  + Several functions: routes frames among connected networks, subnet traffic control (allows routers to send instructions to sending nodes to “throttle back” frame transmissions when are filled), frame fragmentation (determines frame size of routers located downstream. Frame size called maximum transmission unit size. Allows router to fragment frame into smaller sizes if needed and then reassembling the full frame at destination), logical-physical address mapping (translates logical addresses into physical addresses), subnet usage accounting (has function that allows device to keep track of frames forwarded by subnet intermediate systems, uses this to produce billing information).
  + Network layer communication subnets: build headers used by network layers on other devices to route packets to destination. These headers relieve higher layers of the need-to-know data transmission and switching technologies. Use protocols on lower layers to send data to destinations separated by intermediate nodes by sending information between adjacent nodes.
* Level 4: Layer
  + Ensures messages delivered error-free and in sequence and with no loss or duplication.
  + Relieves higher protocols of concern for transfer of data. Size and complexity of transport protocols dependent on services provided by network layer.
  + Message segmentation: accepts messages from session layer. Splits message into smaller units. Imposes message size limits on network layer protocols. Prepares header for each smaller unit created, passes smaller units to network layer, and then reassembles message at destination. The header for smaller units contain certain elements: start and end flags (when the segment starts and ends), sequence information (rearranges sequence of smaller units if they are received out of order).
  + Message acknowledgement (provides reliable end-to-end delivery of messages. Delivery accompanied by acknowledges)
  + Message traffic control (controls rate of traffic sent when no buffers available)
  + Session multiplexing (breaks all the data coming in on one link into separate data streams. Those data streams called sessions. Tracks which message belongs to which session)
  + Transport layer and above layers are not responsible for transmission between nodes (that is the job of the network layer). Transport and above layers responsible for source-to-destination (or end-to-end) transmission. Upper layers not concerned with underlying communications facility (this is job of transport layer).
* Layer 5: Session Layer
  + Establishes sessions between processes running on different computers. Provides several functions to accomplish this: session establishment, maintenance, termination and session support.
  + Establishment maintenance termination: allows application process on different machines to establish a connection, use a connection, and terminate a connection. (Connections are called sessions.)
  + Session support: performs the function of allowing processes to communicate over network. Performs security, name recognition, logging on, etc.
* Layer 6: Presentation Layer
  + Formats data to be presented to the application layer. Translator for the network. At sending station translates data from application layer format to common format. At receiving station translates data from common format to format used by application layer.
  + Functions: character code translation (e.g. ASCII to EBCDIC), data conversion (e.g. changing bit order, CR-CR/LF, Integer-floating point), data compression, data encryption
* Layer 7: Application Layer
  + Serves as a window for uses and applications to access network services by providing a variety of commonly used functions: resource sharing, device redirection, remote file access, remote printer access, network management, directory services, email, instant messaging.
* Encapsulation and De-encapsulation
  + Each layer of OSI model adds a header to the data. Layers also create a unit used to send or receive data. The process of moving data down the OSI model is called encapsulation. Moving up is de-encapsulation.
  + Encapsulation units: Information on application layer through session layer called data. Transport layer converts data to segments. Network layer converts segments to packets. Data link layer converts packets to frames. Physical layer converts frames to bits.
* How the Layers Work Together
  + Data coming out of applications running on the operating system. Each layer adds its own unique header. Application header tells the computer on the other end what applications are being used for the data. Presentation header contains info about encryption, compression, translation, etc. Session layer presents information needed by the session layer. Transport layer contains info about the protocol. Network layer provides info about overall final destination of the data that’s being transmitted. Data link layer provides the address of the next node that the data needs to pass on to reach the ultimate destination. All this info is then converted into ones and zeros and put on the media being used to transmit the data.
  + Data section becoming larger and larger as you go down the layers since it adds more and more headers. This is called overhead.
  + In the sending OS, you go down layers, adding a new header each. In the receiving OS, you go up the layers, peeling off a header each time.

TCP/IP Model

* Understanding the TCP/IP Suite
  + Group of protocols designed to work together to send data across a network.
  + TCP-Transport Control Protocol. IP-Internet Protocol
  + Contains a large number of additional protocols that are able to carry many different network functions.
  + An open protocol suite (suite is free for all to use). New protocols can be freely developed as needed. It is the protocol used by the Internet. Pretty much all existing networks use TCP/IP as their main transmission protocol.
* TCP/IP Model
  + A reduced version of the OSI model. Based on/around the TCP/IP protocol suite, which means that different protocols on the suite will match perfectly with the different layers of the model.
  + Has four layers: Application layer, Transport layer, Internet Layer, Network access or network interface layer.
  + All TCP/IP protocols are located on the top three layers. Protocols located on bottom layer are not part of the TCP/IP suite. Each layer corresponds to one or more OSI model layers.
* TCP/IP Application Layer
  + Defines protocols, services, and processes that allow programs and users to interface with the network. Defines how programs interface with the transport layer services to use the network
  + Common Application layer protocols: HTTP (transport web pages across Internet), Telnet (remotely access other computers using command line), FTP (move large files), TFTP (has a few less services than FTP), SNMP (network admins can remotely manage computers on a network), DNS (convert URLs to IP addresses), SMTP (used by email to move messages between email servers), X Windows (used by Linux/Unix to generate GUIs common to those OS’s).
* TCP/IP Transport Layer
  + Provides communications session management between host computers. Defines level of service and status of connections used when transporting data.
  + TCP, UDP (similar to TCP, but has fewer services), RTP (allows real-time communication between users)
* TCP/IP Internet Layer
  + Internet layer packages data into IP datagrams called packets. Header of packet contains source and destination of info. Internet layer uses this information to forward packets between hosts across the network. Performs routing of IP packets.
  + IP (find the best route and move packets across that route), ICMP (sends out control messages across the internet. Also used by ping tool and trace route tool), ARP (takes an IP address and finds the physical address that matches to it), RARP (converts physical address to IP address)
* TCP/IP Network Interface Layer (aka Network Access layer or link layer)
  + Specifies how data is physical sent through a network by specifying how bits are electrically signaled by hardware.
  + Defines how hardware devices interface with network medium (e.g. coaxial cable, optical cable, twisted pair cable)
  + Standard defined by this layer: Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, V.35
* TCP/IP Model vs. OSI Model
  + Application layer of TCP/IP Model handles application layer, presentation layer, and most of the session layer of OSI model. Transport layer of the TCP/IP Model handles the transport layer and some of the session layer of the OSI Model. Internet Layer handles the Network layer and upper half of the data link layer. Network Interface layer handles the physical layer and lower half of the data link layer.

Commonly Used Network Devices

* NICs: Network interface controller/card
  + Allows a computer or other device to access the network
  + Can come in the form of an expansion card or be built into the motherboard.
  + Works on layers 1 and 2 of the OSI model.
  + NIC Must Match Technology being used: needs to match media technology (e.g. 802.11n NIC for 802.11n Wi-Fi, UTP NIC for UTP cabling), needs to match the speed being used, needs to match network architecture (e.g. Token Ring or Ethernet)
* Hubs
  + Older technology falling out of use in favor of switches.
  + Work on layer 1 of the OSI model. Logically function as a bus topology, so uses contention. Too many hosts on a single hub can result in constant collisions.
  + Three main types: passive hubs (work like a cable splitter: the more devices, the weaker the signal to each device), active hubs (need a power source: power added to a signal when passed through a port, which prevents weakening of a signal by multiple devices being attached. Repeats signal to all hosts connected to hub. Can be used to connect multiple hubs as long as you follow the 5-4-3 rule: no more than 5 segments can be linked together, up to 4 linking devices, up to 4 linking devices can be used to form segments, only 3 segments can be populated by computers), intelligent hubs (active hubs with additional features, such as network diagnostic abilities and management abilities)
* Bridges
  + Device used to break up a network into smaller segments
  + Works on layer 2 of the OSI model.
  + Can read frames (looking at their addresses) to determine if they are allowed to pass.
* Switches
  + Connect multiple computers together.
  + Work on layer 2 of the OSI model (though some can work on higher levels as well. If it can work on more than one layer, it is called a multilayer switch)
  + Basic switch: most common switch. Essentially a multiport bridge. Used to separate larger networks into smaller segments called collision domains by using ports to set up point-to-point connections between devices connected to the affect ports. Results in no collisions on network. Allows different ports to communicate at full speed. Makes it harder to listen in to traffic on the network. Commonly used to convert media from one type to another. Some switches have fiber coming into them but copper twisted pair wires coming out.
  + Managed switches: programmable. Used to control how data behaves on the network. Most often found in corporate environments.
  + Unmanaged switches: not fully programmable, instead coming with a default configuration. Most can only be changed within predefined limits. Some cannot be changed at all. Most home or SOHO switches are unmanaged.
* Routers
  + Move data around large networks (e.g. WANs)
  + Primarily use layers 3 and 4 of the OSI models
  + Are intelligent since they make independent decision about sending data
  + Criteria used to determine route: hops (number of nodes a packet has to pass through to get to its destination), network traffic, network throughput (how fast data can move through a particular connection), network reliability. All this data is used to create and update tables.
  + Are programmable: Have to have their interfaces configured. Have to be told which networks they are connected to. Have to define criteria for what is not allowed through routers. Can be programed for multiple protocols.
* Access Points
  + Devices that allow computers to access the network. Commonly used to connect home computers to Internet. Can either be wired or wireless. Home and SOHO access point are commonly wireless. Wireless access point = WAP.
  + Wireless public access points are very common: libraries, restaurants, airports, etc.
  + WAPs also used as a type of connectivity device: used to offer wireless access to a network. Can offer several features like authentication and encryption. Combine the role of switches and routers. Can be programmed to a limited extent.