

Notes 1

August 28, 2019 1:03 PM

- ★ 7. Application - HTTP: 80 (TCP), HTTPS: 443 (TCP), SMTP: 45, DNS:53 (UDP), DHCP:67-68 (UDP), RTP:16384-32767, FTP:21
- 6. Presentation
- 5. Session
- 4. Transport - TCP, UDP
- 3. Network - IP, ICMP
- 2. Data-link - Mac address (Ethernet, Wi-Fi, 802.11, DSL, SONET)
- 1. Physical - copper wire, fiber optics

- ❖ Protocol - set of rules for communication
- ❖ Network - IP address (internet protocol)
- ❖ Dynamic Host Configuration Protocol - DHCP
- ❖ Domain Name System - DNS
- ❖ Transmission Control Protocol - TCP
- ❖ User Datagram Protocol - UDP
- ★ ❖ IETF - Internet Engineering Task Force 13
 - ★ ○ standards documents are called RFCs (Request For Comments)
- ❖ CR LF (Carriage Return) (Line Feed) 10 = 0D0A
- ❖ SP HT (Space: 32) (Horizontal "Tab": 9)
- ❖ Interface - function prototype
 - Name
 - Return type
 - Parameters
- ❖ API - Application Programming Interface
- ❖ Peer layer - a layer that is on the same level but opposite side of the layer
 - Protocol - is in the peer layer
- ❖ Peer-to-peer
- ❖ Client-server
- ❖ W3C - World Wide Web Consortium
- ❖ IRTF - Internet Research Task Force
- ★ ❖ IEEE - Institute of Electrical and Electronics Engineers
 - ❖ *Never underestimate the bandwidth of a station wagon full of tapes hurling down the highway*
- ❖ Interference
 - NEXT - Near End Cross Talk
 - FEXT - Far End Cross Talk
- ❖ 3 types of interference:
 - ★ ○ Noise - external interference
 - ★ ○ Attenuation - loses power over distance
 - ★ ○ Distortion - when parts become out of sync
- ❖ Regenerative repeater (Physical) - fixes these problems
- ❖ Full-duplex - can send and receive at the same time
- ❖ Half-duplex - can send or receive, but only one at a time
- ❖ Simplex - can only transmit in one-direction
- ★ ❖ UTP - Unshielded Twisted Pair - RJ 45 (Registered Jack)
 - ★ ○ Thin coax - BNC-T (Bayonet Neill-Concelman)
 - ★ ○ Thick coax - vampire tap
- ★ ❖ Single-mode fiber - expensive - longer distances
- ★ ❖ Multimode fiber - cheaper - shorter distances
 - ❖ ISM - Industrial, Scientific, Medical
 - ❖ U-NII - Unlicensed National Information Infrastructure
 - ❖ GEO - Geostationary Earth Orbit

- ❖ Modulate/demodulate - modem
- ❖ Baseband transmission
- ❖ Multiplexing
- ❖ De-multiplexing
- ★❖ Bit rate - usually a multiple of the baud rate
 - Signals
 - ★▪ Amplitude Shift Keying - ASK
 - ★▪ Frequency Shift Keying - FSK
 - ★▪ Phase Shift Keying - PSK
 - Binary Phase Shift Keying - BPSK
 - Quadrature Phase Shift Keying - QPSK
- ★❖ Baud rate - a baud can hold multiple bits
 - Symbol rate (signal rate)
- ❖ QAM - Quadrature Amplitude Modulation
- ❖ FDM - Frequency Division Multiplexing
- ❖ TDM - Time Division Multiplexing
- ❖ CDM - Code Division Multiplexing
- ❖ 3 Services of the Data Link Layer:
 - ★○ Framing - byte count, flag bytes/bits, coding violation
 - ★○ Flow control
 - ★▪ Hardware (RTS/CTS)
 - ★□ RTS - Ready To Send
 - ★□ CTS - Clear To Send
 - ★▪ Software (XON/XOFF)(ASCII: 17/19)(CTRL+Q/CTRL+S)
 - Error control
 - ★▪ Error correction
 - ★□ Hamming
 - ★▪ Error detection
 - ★□ Parity - count number of 1's in byte
 - ★□ Checksum - add binary values of bytes
 - ★□ CRC (Cyclic Redundancy Check) - shift and rotate the bits of the bytes
 - ACK/NAK - acknowledgement/negative acknowledgement

C0 A8 01 17

192.168.1.23/24	11000000	10101000	00000001	00010111
255.255.255.0	11111111	11111111	11111111	00000000 /24
	11000000	10101000	00000001	00000000
	192	168	1	0
	192	168	1	255

192.168.1.23/16	11000000	10101000	00000001	00010111
255.255.0.0	11111111	11111111	00000000	00000000 /16
	11000000	10101000	00000000	00000000
	192	168	0	0
	192	168	255	255

192.168.1.23/28	11000000	10101000	00000001	00010111
255.255.255.240	11111111	11111111	11111111	11110000 /28
	11000000	10101000	00000001	00010000
	192	168	1	16
	192	168	1	31

Subnet Mask:

255.255.255.0	11111111	11111111	11111111	00000000 /24
---------------	----------	----------	----------	--------------

255.255.0.0	11111111	11111111	00000000	00000000 /16
255.255.255.240	11111111	11111111	11111111	11110000 /28

/Counts the 1's

★❖ Classless Inter Domain Routing - CIDR - /22

- 240.145.253.23/22 - 11110000 10010001 11111101 00010111
- 255.255.252.0 - 11111111 11111111 11111100 00000000
- Minimum - 240.145.252.0 - 11110000 10010001 11111100 00000000
- Maximum - 240.145.255.255 - 11110000 10010001 11111111 11111111
- Host: 2^{10} - 1024

Practice:

204.258.143.77/21	11001100	10011110	10001111	01001101
255.255.248.0	11111111	11111111	11111000	00000000
204.258.134.0	11001100	10011110	10001000	00000000
204.258.141.255	11001100	10011110	10001111	11111111

★❖ NAT - Network Address Translation

- Allows us to share the router's one IP Address

Notes 2

September 20, 2019 1:10 PM

❖ Hamming code 7.4 - seven total bits/four data bits (Richard Hamming 1950)

- 0100 0001
- 010-0--
- 0101
- 01010--
- 01 0-
- 010101-
- 0 0 0 -
- 0101010
- 0101 - 0
- 01 01 - 0
- 0 0 0 0 - 0
- - 0 0 0 - 0
- 010-0-- 0100
- 0101010
- *
- 0100 - 1
- 01 01 - 0
- 0 0 0 0 - 0
- - 1 0 0 - 4
- 010-0-- 0100
- 0101010
- *
- 1101 - 1
- 11 01 - 1
- 1 0 0 0 - 1
- - 1 1 1 - 7
- 010-0-- 0100

★❖ OFDMA - Orthogonal Frequency Division Multiple Access

❖ Assumptions for Dynamic Channel Allocation

1. Independent Traffic - independent stations
2. Single Channel - one channel used for all communication
3. Observable Collisions - two frames transmitted at the same time
4. Continuous or Slotted Time - things can be transmitted at the same time because all the data is divided
5. Carrier Sense or No Carrier Sense - does not transmit if something is already being transmitted

❖ ALOHA (ALOHA's sorted best by ascending order)

★○ Pure ALOHA

★○ Slotted ALOHA - devised in the 1970s and re-used in the 2000s

★❖ Carrier Sense Multiple Access /Collision Detection Protocols - CSMA/CD

★○ 1-persistent - once transmission is clear whoever else is waiting may transmit

★○ Non-persistent - is not greedy and will wait a random amount of time to check again

★○ p-persistent - transmits with probability (best one)

❖ Physical address - not on the physical layer

❖ DIX - Digital Intel Xerox

❖ Token ring - 802.5

❖ Token bus - 802.4

- ★❖ Ethernet - 802.3
- ★❖ Wi-Fi - 802.11
- ★❖ Bluetooth - 802.15
- ❖ Bus - shared channel
 - Bus Topology - like a map of the circuitry
 - Star-Wired Bus - a component of the switch
- ★❖ Firewall - network/transport
- ★❖ Router - network
- ★❖ Switch - data link
- ★❖ Hub/repeater - physical
- ❖ Bytes
 - (a)
 - Preamble: 8 bytes
 - ★○ Destination address: 6 bytes
 - ★○ Source address: 6 bytes
 - ★○ Type: 2 bytes
 - ~Data~: 0-1500 bytes
 - Pad: 0-46 bytes
 - Checksum: 4 bytes
- ★❖ MAC address: 6 bytes
- ★❖ IPv4 address: 4 bytes
- ★❖ IPv6 address: 16 bytes
- ❖ Fixed - the fixed part of the header is 20 bytes
 - The IHL field should never be smaller than 5
- ★❖ Fragment offset
 - Every 8 bytes
- ★❖ Byte offset
 - ❖ Shifting bits to the left by 3 is the same as multiplying by 8
 - Same as: 2^3

Notes 3

Monday, October 14, 2019 11:55 AM

- ❖ Commands:
 - cd Downloads
 - javac jhttp.java
 - java jhttp . 5050
- ❖ A ServerSocket is the java object that lets me create a TCP server
- ★❖ BIND - Associate a local address with a socket (Server)
- ★❖ LISTEN - Announce willingness to accept connections; give queue size (Server)
- ★❖ ACCEPT - Passively establish an incoming connection (Server)
- ★❖ CONNECT - Actively attempt to establish an incoming connection (Client)
- ★❖ SOCKET - Create a new communication endpoint (Both)
- ★❖ SEND - Send some data over the connection (Both)
- ★❖ RECEIVE - Receive some data from the connection (Both)
- ★❖ CLOSE - Release the connection (Both)
- ❖ HTTP protocol:
 - Header
 - Blank line (\r\n\r\n)
 - Body (data)
- ❖ ICMP - Internet Control Message Protocol
- ❖ ARP - Address Resolution Protocol
- ❖ ICMP RFC:
 - Obsoletes: 1788
 - Updates: 792, 950
- ❖ Network security problems:
 - Secrecy
 - Authentication
 - Nonrepudiation - if it is signed then it cannot be refuted
 - Integrity control - part of integrity control is authentication
- ❖ Cryptology - the study of:
 - Cryptography - secret writing
 - Cryptanalysis - the analysis of secret writing
- ❖ Passive intruder - just listens
- ❖ Active intruder - can alter messages
- ❖ Plaintext - $P = D(k, C)$ - decrypt the ciphertext
- ❖ Ciphertext - $C = E(k, P)$ - encrypt the plaintext
- ❖ Code - replaces letters with symbols
- ❖ Cipher - changes numbers
- ❖ Key
 - (Secret-/public/private-)
- ★❖ Kerckhoff's principle - all algorithms must be public: only the keys are secret
- ❖ Principals - main characters
- ❖ Monoalphabetic - the general system for the symbol-for-symbol substitution
- ❖ Digram - two-letter combination
- ❖ Trigram - three-letter combination
- ❖ Transposition
- ★❖ One-time pad - immune to computational power attacks (unbreakable cipher)
 - ★• The way that the key and the algorithm apply to each other means that every possible plaintext is equally probable
01000001 plaintext
10100101 key (random bits)
----- XOR

11100100 ciphertext
10100101 key
----- XOR
01000001 decrypted plaintext

❖ Quantum cryptography

- Bases (filters)
 - Rectilinear basis
 - Diagonal basis

❖ Cryptographic principles:

- ★• Redundancy - Messages must contain some redundancy
- ★• Freshness - something that identifies when the messages was sent

❖ Symmetric-key algorithms

- ★❖ 3DES - Data Encryption Standard - symmetric
- ★❖ AES - Advanced Encryption Standard - symmetric
- ★❖ RSA - Rivest, Shamir, Adleman - asymmetric
- ★❖ Public key cryptography - can protect the data really well, but it costs too much computing power

Java/Multichat

Monday, November 4, 2019

12:16 PM

- ❖ local loopback
 - localhost - 127.0.0.1
- ❖ Server
 - Server Handler
 - Multiple Connection Handlers
- ❖ Client - Connection Listener
 - Connection Handler
- ❖ Border Layout
- ❖ JFrame - parent class/super class
- ❖ Instance - a constructed version of a class
- ❖ Inheritance - define a class and the objects inherit the behavior
- ❖ MultichatClient.java: "this" - refers to the instance of the MultichatClient

1. What is similar to the StringTokenizer() in the jhttp application? split()
2. What does split() do? Splits data into multiple pieces
3. What activates the Scanner in a program? nextLine()
4. What was the Scanner being used for its place? (BufferedReader)
5. What do we use instead of nextLine()? readLine()
6. What are the layers of the OSI model?
 - ★ 1. Application - HTTP - Multichat app
 - ★ 2. Transport - TCP/UDP - port numbers
 - ★ 3. Network - IP/ICMP - routers
 - ★ 4. Data link - Ethernet/WiFi - MAC address/switches
 - ★ 5. Physical - cables/radio - hub/modem/ repeater
- ★ 7. What does the router mainly do? Computing routes, forwarding packets
8. What else does computing routes mean? "shortest" path
- ★ 9. What does computing routes do? Collect route information, the algorithm
- ★ 10. What means to stay the same and not move? Static, non-adaptive
- ★ 11. What means to move and constantly change? Dynamic, adaptive
12. What do forwarding packets do? Sends the packets
- ★ 13. What is the difference between a host and a network? Networks are only concerned about other networks while hosts only care about the individual machines
- ★ 14. What is it called when every packet is sent out on every outgoing line except the one it arrives on? Flooding
15. Why do we need flooding? To get information out, it is not used just to find the shortest path
16. What does distance vector routing do? It operates by having each router maintain a table giving the best known distance to each destination and which link to use to get there
- ★ 17. What is the settling of routes to best paths across the network? Convergence

Notes Final

Wednesday, November 27, 2019 12:01 PM

Header - 16 bytes

- 27 - packet number
- 0 - number of the first elementary fragment in this packet
- 1 - end of packet bit

```
27 0 1 ABCDEFGHIJ
27 0 0 ABCDEFGH    27 8 1 IJ
27 0 0 ABCDE       27 5 0 FGH    27 8 1 IJ
```

```
27 0 0 ABC
27 3 0 DEF
27 6 0 GHI
27 9 1 J
```

1. What is something that has to do with making sure the network is able to carry the offered traffic? Congestion control
2. Congestion is generated by lots of traffic creating lots of nodes on the network
3. To ease congestion you can either increase the resources or decrease the load
- ★ 4. Load shedding is the dropping of packets
- ★ 5. Network provisioning provides more network bandwidth for traffic
- ★ 6. What states that a node **J** is along an optimal path from **I** to **K** then the optimal path from **J** to **K** is optimal? Optimality principle
- ★ 7. The Count-to-Infinity Problem is part of the distance vector algorithm
- ★ 8. KNOW PAGE 439 IP HEADER!
- ★ 9. HTML - define elements (Hyper Text Markup Language)
- ★ 10. CSS - format elements (Cascading Style Sheets)
- ★ 11. JavaScript - interact elements