**Final Review:**

**The final exam is cumulative: 30% of the questions covers topics from weeks 1-7, 70% covers topics from weeks 8-14.**

Chapters 1 and 2:

* Protocol
  + Properties

-Specifies how to handle one aspect of communication

-Can specify:

-Low level details (such as voltage and frequency)

-High level details(such as format visible to a user)

* + Specification

-Syntax:

-Format of each message

-Representation of data items

-Encoding of bits in electromagnetic signals

-Semantics:

-Meaning of each message

-Procedures used to exchange messages

-Actions to take when an error occurs

* + Design

-The steps in protocol design:

-look at the facilities the underlying hardware provides

-Imagine an abstract communication mechanism as a user would like it to work

-Design an efficient implementation of the abstraction

-The key to success= **Choose a good abstraction**

-Why it’s difficult

- Multiple implementations of a protocol will exist

-Key Tradeoffs:

-A specification that dictates all possible details restricts implementations

-A specification that does not specify enough details is ambiguous and leads to incompatible implementations

* Internet Protocols
  + TCP/IP model:
    - 4-layer model:

Layer 1 = Network Access Layer

-Function:

-Defines how to use the network to transmit a frame(data)

-Exchange data between the computer and the physical layer

-Help deliver data b/w 2 devices of the same network

Layer 2 = Internet Layer

-Function:

-Communicates between computer across an internet addressing model

Layer 3 = Transport Layer

-Function: Communicates between applications

Layer 4 = Application Layer

-Function: Formats the representation of data and messages

* + - 5-layer model:

Layer 1 = Physical Layer

-Function: Handles host to host communication; transmission of media, hardware, and signals

-Data = “bits”

Layer 2 = Network Interface

-Function: communication between computer and network hardware;

allows computer to access the wire, wireless, or fiber optic network infrastructure and send data to other computers

-Data = “frame”

Layer 3 = Internet Layer

-Function: communication between computers across an internet addressing models, forwarding packets; responsible for logical transmissions of data packets over the internet

-Data = “packet”

Layer 4 = Transport Layer

-Function: communication between a pair of applications; to effectively control communications between two hosts

-Data = “datagram”

Layer 5 = Application Layer

-Function: methods for requesting and transferring data; provides the interfaces and the protocols needed by the users

-Data = “message” / ”information”

* + OSI model:

Layer 1 = Physical Layer

-Function: transmits raw bit stream over the physical medium

Layer 2 = Data Link Layer

-Function: defines the format of the data on the network

Layer 3 = Network layer

-Function: decides which physical path the data will take

Layer 4 = Transport Layer

-Function: transmits data using transmission protocols including TCP and UDP

Layer 5 = Session Layer

-Function: maintains connections and is responsible for controlling ports and sessions

Layer 6 = Presentation Layer

-Function: ensures that data is in a usable format and is where data encryption occurs

Layer 7 = Application Layer

-Function: Human-like computer interaction layer, where applications can access the network services

Chapters 3 and 4:

* DNS

-Means “Domain Name System

* Internetworking
  + -Interconnecting many packet switching technologies into a functioning whole
  + -Provides the basis of the global Internet
  + -More powerful than a single networking technology because the approach permits new technologies to be incorporated at any time without requiring the wholesale replacement of old technologies
* transport layer
* HTTP
* FTP
* Client Server
* A network medium of which clients access resources and services from a central computer
* Peer to peer (P2P)
* A group of computers linked together with equal permissions and responsibilities for processing data

Chapters 5, 6, and 7

* Data Communication Framework
  + Encryptor
* Also known as a “scrambler”

- Function: transforms data into and unintelligible form to prevent unauthorized use of the data

* + Encoder
* Makes sure that there’s no errors nor redundancies
* Adds “noises” to your signal
* Converts streams of data bits into a predefined “code”(which are groupings of bits used to make a predictable pattern that is recognized by the sender and the receiver).
  + Modulator
* Simplifies multiple signals
* Combining multiple signals into one
  + Decryptor
* Extracts and converts the garbled data and transforms it into words/images that is understandable by the reader and the system
  + Decoder
* Converts the data into its original format
  + Demodulator
* Recovers the ‘information content’ from the modulated carrier wave
  + Multiplexor
* Recovers the ‘information content’ from the modulated carrier wave
  + Demultiplexor
* Reconverts a signal that contains multiple signals(analog or digital) into its original separate and unrelated signals
* Analog Signal
  + Sine wave characteristics (amplitude, frequency, phase)

- Amplitude = “Height”; the difference b/w the maximum and minimum signal height

- Frequency = the number of oscillations per unit time

- Phase = how far the start of the sine wave is shifted from a reference time

* + Fourier analysis
* Method of decomposing a composite signal into its constituent(basic) parts
  + Analog bandwidth
* The difference between the highest and lowest frequency of its components.
  + Frequency Domain

- Allows to observe several characteristics of a signal that wasn’t easy to see nor visible

- Adv: A frequency domain representation is both small and easy since each sine wave occupies a single point

* Digital Signal
* A fixed set of valid levels and each change consists of an instantaneous move from one valid level to another
* Analog to digital conversion
* 2 approaches:

- Pulse code modulation

- Delta modulation

- Pulse modulation: A technique where the level of an analog signal is measured repeatedly at fixed time intervals and converted to digital form.

- Delta modulation: Instead of measured repeatedly and at fixed intervals, measured once since it’s in a 1-bit data stream

* Digital to analog conversion
* Approximation: involves building a composite signal from only a few sine waves
* Synchronization
* Deals with the problem of disturbing time and frequency among spatially remote locations
* To be able to extract original source from sender
* Transmission media
  + Guided

Twisted Pair: : 2 insulated copper wires twisted to reduce interference from other pairs

- Is twisted to have no interference with other wires

* + - Coaxial: copper core surrounded by insulating material and a braided outer conductor
    - Fiber optic: glass fiber carrying light pulses; most popular
  + Unguided

Infrared: A form of electromagnetic radiation that behaves like visible light but falls outside the range that is visible to a human eye

-Best suited where the path between sender and receiver is short and free from obstruction

Laser: Similar to infrared however, does not cover a broad area.

-Due to its narrow beam of light, the transmission of sender and receiver must be aligned precisely.

Terrestrial Radio: communication uses equipment such as radio or microwave transmitters that is relatively close to the earth’s surface.

-Typical locations for antennas: top of hills, man-made towers, tall buildings

Satellite: 3 types: low-Earth orbit(LEO), medium-Earth orbit(MEO), Geostationary-Earth orbit(GEO)

-LEO: Has the adv. of low delay; disadvantage: satellite appears to move across the sky(from an observer’s POV on the Earth)

-MEO: An elliptical orbit used to provide communication from South and North Poles

-GEO: Adv: orbital period is exactly the same rate at which the earth rotates

Disadvantage: being farthest away can cause delay to some applications

* Wireless Transmission
* Most popular to use is electromagnetic energy in the Radio Frequency range
* Radio Transmission
* Using radio waves from an antenna?(Just think like this…)
* Measuring Transmission Media

- Propagation Delay:

- Time required for a signal to traverse a medium

- Nyquist’s Theorem:

-Gives a theoretical limit on the channel capacity of transmission media when no noise is present

-Theoretical maximum data transmission rate

- Shannon’s Theorem:

- Specifies the channel capacity in realistic situations when noise is present

-Capacity of data channels with noise

Chapter 13

* LAN Technologies

- “LAN” = “Local Area Network”

-A type of packet switch category

-Key ideas to Wired LANs:

- Minimize the number of connections by sharing them among many computer

- Relatively low cost

- High “thoughput?”

- Limited to short distances

- Dominant wire LAN standard: Ethernet

-LAN operations---------🡪 between Physical and Network Interface layer (in TCP/IP model)

* Network Topology (bus, token ring, star, mesh)

-Bus

Diagram

Description automatically generated

-Single cable to which computers attach

-Problem: If cable breaks down, all will break down

-Token ring

Diagram

Description automatically generated

-Same as Bus, but in a circle

-Has same problem as Bus

Diagram

Description automatically generated-Star

-All computers attaching to central point(hub)

-The best since losses is less drastic than others

-Hub: consists of an electronic device that accepts data from a sending computer and delivers it to the appropriate destination

Diagram

Description automatically generated-Mesh

-Direct connection between each pair of computers

-Disadvantage: costly to employ

* Unicast, Multicast, Broadcast, Anycast

Chapter 15, 21, 23

* Ethernet

-A single long cable of which computer attach

-Serves as a medium

-Transmits signals down a cable instead of broadcasting radio frequency through atmosphere

-Allows all communication to proceed across the shared cable

* IPv4 & IPv6
  + Subnetting
  + CIDR
* DHCP

-“DHCP” = “Dynamic Host Configuration Protocol”

-Goal = Host dynamically get its IP address from a server when it joins the network

-Allows a computer to move to a new network and obtain configuration information, without requiring an administrator to make manual changes to a server database

* CIDR

-“CIDR” = “Classless Inter-Domain Routing”

-Only specifies addressing and forwarding

-A set of Internet protocol standards that is used to create unique identifiers for networks and individual devices

- This: /#

* ARP

-“ARP” = “Address Resolution Protocol”

-Used by computer on the physical network

-Allows a computer to find the MAC address of another computer

-Operates at Network Interface layer(Layer 2)

Chapters 9, 10, 11

* Transmission modes
  + Parallel

-Multiple bits sent on multiple waves

* + Serial (asynchronous, synchronous, isochronous)

-One bit at a time

-Asynchronous: Can occur anytime with an arbitrary delay between the transmission of two data items

-Synchronous: Occurs continuously with no gap between the transmission of two data items

-Isochronous: Occurs at regular intervals with a fixed gap between the transmission of two data items.

* + Ethernet transmission order (Big Endian, little Endian, unicast, multicast, broadcast)

-Big-endian: A system that sends the Most Significant Bit (MSB)

-Little-endian: A system that sends the Least Significant Bit (LSB)

-Unicast: Identifies a single host

-Multicast: Identifies a group of hosts

-Broadcast: All hosts

* Modulation (analog and digital)

-Analog: The process of transferring an analog baseband (low frequency) signal

-Digital: The process of encoding a digital information signal into the amplitude, phase, or frequency of the transmitted signal

* Multiplexing and demultiplexing (FDM, WDM, TDM, CDM)

-FDM: (“Frequency Division Multiplexing”); technique for sending two or more signals over the same phone line or medium.

-WDM: (“Wavelength Division Multiplexing”); the application of frequency division multiplexing to optical fiber

-TDM: (“Time Division Multiplexing”); multiplexing in time = transmitting an item from one source, then transmitting an item from another source, and so on.

-CDM: (“Code Division Multiplexing”); facilitates various signals to occupy a single transmission channel

-Optimizes the use of available bandwidth-FDM: (“Frequency Division Multiplexing”); technique for sending two or more signals over the same phone line or medium.

* Access Technologies (dialup, broadband)

-Dialup:

-Uses telephone lines to access the Internet

-Slow

-Requires a telephone connection

-Broadband:

-Uses fiber optic cable

-Fast

-Does not require telephone connection or connection

Chapter 16

* Wireless Network

-4 types of wireless networks:

-Local Area Networks (LANs)

-IEEE standard: 802.11-2007

-is associated to Wi-Fi

-3 building blocks of a wireless LANs:

-Access point (or “base stations”)

-An interconnection mechanism (such as a switch or router used to

connect access points)

-Set or wireless hosts (called wireless nodes/stations)

-2 possible types:

-ad hoc

-infrastructure

-Uses an infrastructure architecture in which a wireless computer communicates through an access point

-Metropolitan Area Networks (MANs)

-Potential for commercial success: 802.16, which was coined as WiMax

-IEEE standard: 802.16

-2 types of WiMax:

-Fixed:

-Does not provide for handoff among access points

-Designed to provide connections b/w a service provider and a fixed location such as residence/ office building

-Mobile:

-Offers handoff among access points, meaning it can be used with portable devices such as laptops and cell phones

-Wide Area Networks (WANs)

-

-Can be divided into 2 categories:

-Cellular communications systems:

-Designed to provide voice services to mobile customers

-Follows a key principle: Interference can be minimized if an adjacent pair of cells do not use the same frequency

-Satellite communications systems

-Makes it possible for business and consumers to have dish antennas on their property

-Personal Area Network (PANs)

-Provides communication over a short distance

-IEEE standard: 802.15

- 2 others for short distance: Infrared and RFID(Radio Frequency Identification)

* + Wifi

-is associated to wireless LANs

* + Ad-hoc

-Wireless hosts communicate among themselves without a base station

-A type of wireless LANs

* + Cellular network

Chapter 22, 23

* Datagram forwarding

-Also called IP Datagram Forwarding

-It is a packet sent across a TCP/IP internet

-Getting the data to the right host

-Performed by routers

-Uses IP addresses

-Route table entry specifies next hop

-Refers to an Internet packet

-What an IP datagram contains

-Begins with a header

-followed by a payload

-Size of a datagram is determined by the amount of data an application sends

-In IPv4, datagram can contain up to 64K octets

-In IPv6, datagram is slightly larger because the datagram Can carry up to 64K octets of payload plus a header

-Datagram header contains:

-Address of the source

-Address of the destination

-A field that specifies the type of data being carried in the payload area

-Datagram does not contain MAC address

-IPv4 data header has a fixed size, which makes header processing more efficient

-IPv6 data header:

-divides header info into a base header and a series of smaller, optional extension header

-Consists of a base header followed by zero or more extension headers followed by a payload

-Unlike IPv4, IPv6 places many key pieces of information in extension headers, meaning that most datagrams contain a sequence of headers

-Generally, the size of the payload is much larger than the size of the headers

* ICMP

-“Internet Control Message Protocol

-An IP companion protocol used to report errors back to the original source (for IPv4)

-is co-dependent on IP( meaning IP depends on ICMP to report errors and ICMP uses IP to carry error messages)

-

* NAT

-“Network Address Translation”

-Purpose: Extend IPv4 address space

-Allows multiple computers to share a single IP address

-Site appears to have a single host with a valid IP address

-Each host gets a private address

-Occurs on the connection between the Internet and the LAN

-Translates source and/or destination address in datagrams that pass between the site and the Internet

-Network Address and Port Translation(NAPT)

-Also translates TCP/UDP protocol port numbers

-Permits multiple computers at a site to contact the same Internet service simultaneously without interface

Chapters 24, 25, 26:

* Transport layer

-Known as “end-to-end protocols” because a transport protocol allows an individual application program to be an endpoint of communication

* UDP

-“User Datagram Protocol”

-Extends IP by adding end-to-end delivery and app demultiplexing

-Minimal overhead, computation, communication

-Connectionless service paradigm

-does not pre-establish communication

-does not inform network or other endpoint when a message is being sent

-Message oriented

-Complete message encapsulated in a single IP datagram

-No guarantee of reliability

-No congestion or flow control

-UDP segment must fit in payload area of an IP datagram(UDP message size)

-UDP checksum: detects errors (e.g. flipped bits) in transmitted segment (includes UDP header, payload, parts of IP header)

-Uses:

-DHCP

-RIP

-DNS

-VoIP (e.g. Skype) and some video apps

-Only a small percentage of Internet traffic uses UDP

* TCP

-“Transmission Control Protocol”

-90% of all Internet traffic

-One of the 2 major transport protocols

-Characteristics of TCP:

-Connection-oriented paradigm

-Reliable startup, graceful shutdown

-Point-to-point connections

-Complete reliability

-Full duplex communication

-Stream interface

-Flow and congestion control

-Provides a reliable, connection-oriented, full-duplex stream transport service that allows two application programs to from a connection, send data in either direction, and then terminate the connection

-A pair of applications must( in terms of connection-oriented):

-establish a TCP connection before communicating

-Terminate the connection when finished

-TCP connection has a pair of endpoints identified by:

-IP source address (TCP source port)

-IP destination address (TCP destination port)

-TCP communication is between a pair of applications

TCP connection does not support:

-Receiving from arbitrary senders

-Multi-port connections (more than 2 endpoints)

-Broadcast or multicast delivery

-TCP Congestion Control:

-Retransmits when excessive traffic is present causes more congestion and packet loss

-Uses packet loss to infer network congestion

-Manages congestion by adjusting the size of the sender window to slow down transmission

* Internet Routing and routing protocols:
  + IGP:

-“Interior Gateway Protocols”

-Used within an autonomous system

-choice of IGP made by each AS

-Easy to install and operate, but may limit the size or routing complexity of an autonomous system

* + EGP:

-“Exterior Gateway Protocols”

-Used between autonomous systems

-Interconnected AS’s must agree on EGP

-More complex to install and operate, but offers more flexibility and lower traffic

-Summarizes routing information from an autonomous system before passing it to another in order to save traffic

-Implements a policy constraints which allows a system manager to determine exactly what info is released outside the organization

* + BGP:

-”Border Gateway Protocol”

-Current EGP choice for the Internet

-Used by Tier 1 ISPs at the core of the Internet

-Modified Distance-Vector protocol (advertises path rather than distance)

-Characteristics of BGP-4:

-Routing among autonomous systems

-Provisions for policies

-Facilities for transit routing

-Reliable transport

* + OSPF:

-“Open Shortest Path First Protocol”

-Routing within an autonomous system

-More powerful but more complex than RIP

-Can scale to handle a much larger number of routers than other IGPs

-Uses Link-State/Dijkstra’s (SPF algorithm)

-Characteristics of OSPF:

-Routing within an autonomous system

-CIDR support

-Authenticated message exchange

-Imported routes

-Link-State/Dijkstra’s algorithm

-Support for metrics

-Extension To IPv6

-Support for Multi-access Networks

-Has hierarchical routing

-It is an Interior Gateway Protocol that uses Dijkstra’s/Link-Stats algorithm to propagate routing information

* + RIP:

-“Routing Information Protocol”

-Routing within an autonomous system (IGP)

-Distance-Vector with hop count metric

-One of the earliest IGPs

-Characteristics of RIP:

-Routing within an autonomous system

-Hop count metric

-Unreliable transport

-Broadcast or multicast delivery

-Support For IPv4 CIDR and Subnetting

-Support for Default Route Propagation

-Distance Vector Algorithm

-Passive Version for Hosts

-Extension for IPv6

Chapters 27, 28, 29

* Network Performance
  + QoS:

-”Quality of Service”

-Motivation: make it possible to run applications such as streaming videos with no interruptions

-Allow service providers to charge (much) more for better service

-3 approaches: Priority, Fine-grain QoS, Coarse-grain QoS

-Implementation of QoS:

-Classification and Policing

-Forwarding Computation

-Output queuing

-Traffic scheduling

* + DiffServ:

-A coarse-grain QoS approach.

-Divides traffic into classes.

-Service guaranteed for each class rather than per flow

-Easier to implement than fine-grain approach

-Usually implemented as a proportional guarantee rather than absolute quantities

-(Textbook) Produces a definition of how classes can be specified and how the TYPE OF SERVICE field in an IPv4 or IPv6 header can be used to specify the class of a datagram.

* + CBR (Constant Bit Rate): Data enters the flow at a fixed rate, such as data from a digitized voice call entering at exactly 64 Kbps
  + VBR (Variable Bit Rate): Data enters the flow at a variable rate within specified statistical bounds
  + ABR (Available Bit Rate): The flow agrees to use wherever data rate is available at a given time.
  + UBR (Unspecified Bit Rate): No bit rate is specified for the flow; the application is satisfied with best-effort service
* Multimedia And IP Telephony (VoIP)

-Multimedia: combines 2 or more forms of information such as photos, music, audio, and video

-IP Telephony (VoIP): Known as “Voice over IP”

-One of the most widespread multimedia applications

-Basic idea: Continuously sample audio, convert each sample to digital form, send the resulting digitized stream across an IP network in packets, and convert stream back to analog for playback

* Network Security
  + Firewalls

-Purpose: Site integrity

-Known as “Internet firewall”

-Helps protect an organization’s computers and networks from unwanted Internet traffic

-Hardware and software that isolates an internal network from the Internet

-Manages traffic flow in and out of the internal network

-implements a security policy and rejects any traffic that doesn’t adhere to it

-Stateful Firewalls

-Firewall recognizes SYN packet from host and creates a state w/ source and destination IP address

-Web server returns a SYN-ACK which the firewall allows to pass through

-State is maintained until connection ends

* + Intrusion Detection

-Purpose: Site integrity

-Monitors arriving packet streams for unusual activity or security violations

-Provides an extra layer of security awareness

-Can be configured to watch for specific types of attacks(Ex: port scanning, Dos attack)

-Difference b/w IDS and firewall: IDS includes state information, meaning it can keep a history of packets.

- However, requires more computation and memory access

* + DMZ

-“DMZ” = “demilitarized zones”

-Is created to isolate servers from the rest of the network

-End goal: to allow an organization to access untrusted networks while ensuring its private network or LAN remains secure

-Creates an extra layer of protection from external attack

* + Encryption

-Purpose: Privacy

-A function that generates a ciphertext version of the message

-Scrambles the bits of the message that only the intended recipient can unscramble them

-Encrypted message can contain info such as the message length

-Terminology used with encryption:

-Plaintext: an original message before it has been encrypted

-Cyphertext: a message after it has been encrypted

-Encryption key: a short bit string used to encrypt message

-Decryption key: a short bit string used to decrypt message

* + - Symmetric Key encryption

-“Private key encryption”

-Uses a single secret key or encrypt/decrypt with the same key

-Each side can send or receive messages

* + - Asymmetric Key encryption

-“Public key encryption”

-Encryption and decryption uses different keys

* + Digital Signature

-Purpose: Message authentication

-An encryption mechanism/technique used to authenticate the sender of a message

-To “sign” a message, sender encrypts the message using a key known only to the sender.

-Receiver uses inverse function to decrypt the message. Also knows who sent the message because only the sender has the key to perform the encryption.

* + SSL/TLS

-“SSL” = “Secure Socket Layer”, A technology originally designed by Netscape Communications that uses encryption to provide authentication and confidentiality. SSL software fits between an application and the socket API, and encrypts data before transmitting over the Internet. SSL is used on a web connection to allow users to conduct financial transactions safely(i.e. send a credit card number to a web server

-“TLS” = “Transport Layer Security”, Designed by the IETF in the late 1990s as a successor to SSL, TLS builds on version 3 of SSL. Both SSL and TLS are available for use with HTTPS.

* + VPN

-Means “Virtual Private Networks”

-Achieves confidentiality and low cost

-Uses encryptions to secure access to an organization’s intranet by using standard protocols over the standard Internet

-Emulates private network connection in software

-Purpose: Data confidentiality

-2 forms of it: Stand-alone device & VPN software

-

* + Network attacks
    - Wiretapping: Making a copy of packets as they traverse a network to obtain information
    - Replay: Sending packets captured from a previous session
    - Buffer overflow: Sending more data than a receiver expects in order to store values in variables beyond the buffer
    - Address Spoofing: Faking the IP source address in a packet to trick a receiver into processing the packet
    - Name Spoofing: Using a misspelling of a well-known name or poisoning a name server with an incorrect binding
    - DoS and DDoS: Flooding a site with packets to prevent the site from successfully conducting normal business
    - SYN flood: Sending a stream of random TCP SYN segments to exhaust a receiver’s set of TCP connections. This can be considered a sub-category of DoS and DDoS attacks
    - Key Breaking: Automatically guessing a decryption key or a password to gain unauthorized access to data
    - Port Scanning: Attempting to connect to each possible protocol port on a host to find a vulnerability
    - Packet interception: Removing a packet from the Internet which allows substitution and man-in-the middle attacks

Labs:

* LINUX basic commands learned from labs 1 through 4

Lab 1

-Pwd = print working directory

-ls = list files in current directory

-ls -A = command that shows all files in your home directory (excluding . and ..).

-wc= used to count lines, words, and characters in files or data “piped” to it from another program

-mkdir = create directory

-ls -a | wc -l = used to count the items

-cat = open file

- grep “string you are searching” = searches lines in the input stream for a specified string or pattern

- man “command” = a complete description from the manual

Lab 2-3

- chmod -x = used to remove execute permissions from a file

- ping -c 10 192.168.18.y = command is used to see if a specific IP address is online

- echo = displays a line of texts

- ifconfig = Find the Ethernet/MAC address and the IP address of the network interface card

- ifconfig enp0s3 192.168.18.x = to manually assign an IP address

- arp –n = to view the contents of the ARP cache

Homework

* Assignments from weekly learning modules

REVIEW EXAM

Review Questions - Computer Networks and Internets – Professor: Dr. Dang

1. Protocols in layer \_\_\_\_\_ specify communication between two computers across the Internet.
   1. 1
   2. 2
   3. 3
   4. 4
   5. 5
2. Three major types of protocols being used with email are:
   1. Transfer
   2. Access
   3. Representation
   4. All of the above
3. The overall purpose of the Domain Name System:
   1. to provide a service that maps human-readable symbolic names to computer addresses.
   2. to allow easy access to the network
   3. Easy to remember hostname than IP address
   4. All of the above
4. Telnet, HTTP, FTP, SMTP, POP4, VoIP, SNMP are examples of:
   1. Application layer
   2. Network layer
   3. Data Link layer
   4. Transport layer
5. TCP and UDP operate at \_\_\_\_\_\_\_\_\_\_\_ layer:
   1. Transport
   2. Network
   3. Data Link
   4. Application
6. IP operates at the:
   1. Application layer
   2. Network layer
   3. Physical layer
   4. Transport layer
7. RJ-45, Ethernet (IEEE802.3) operate at the:
   1. Application layer
   2. Network layer
   3. Physical layer
   4. Transport layer
8. A term referring to a data link header and trailer, plus the data encapsulated between the header and trailer
   1. Frame
   2. Packet
   3. Segment
   4. Protocol data unit
9. The placement of data from a higher-layer protocol behind the header (and in some cases, between a header and trailer) of the next-lower-layer protocol.
   1. Encapsulation
   2. De-encapsulation
   3. Adjacent-layer interaction
   4. Same-layer interaction
10. IPV6 includes:
    1. Unicast, Broadcast, Multicast
    2. Unicast, anycast, broadcast
    3. Anycast, multicast, broadcast
    4. Anycast, unicast, multicast
11. Which piece of a data communications system handles analog input?
    1. Information sources
    2. Encryptor
    3. Encoder
    4. Modulator
    5. Multiplexor
12. \_\_\_\_\_\_\_\_\_connect devices that can be far apart, potentially hundreds or thousands of miles apart.
    1. LANs
    2. WANs
    3. MANs
    4. Both a and b
13. The router forwarding logic include:
    1. Forward the frame
    2. Find the best route to the destination address
    3. Compare the packet’s inside a new data-link header and trailer
    4. Ensure the frame had no errors
    5. All of the above
14. TCP supports
    1. Error recovery
    2. Flow control using windowing
    3. Connection establishment and termination
    4. Ordered data transfer and data segmentation
    5. All of the above
15. UDP supports
    1. Error recovery
    2. Multiplexing using ports
    3. Connection establishment and termination
    4. Ordered data transfer and data segmentation
    5. None of the above
16. FTP, SSH, Telnet, SSL use \_\_\_\_\_\_\_\_\_\_
    1. TCP
    2. UDP
    3. Both a and b
    4. None of the above
17. DHCP, SNMP, ICPM, VoIP use
    1. TCP
    2. UDP
    3. Both a and b
    4. None of the above
18. DNS uses
    1. TCP
    2. UDP
    3. Both a and b
    4. None of the above
19. The IPv6 address of 192.168.1.3 is:
    1. ::FFF:C0A8:103
    2. ::FFF:B0A8:103
    3. ::FFF:E0A8:103
    4. None of the above
20. NAT translates \_\_\_\_\_\_\_\_\_ addresses that pass between the site and the internet
    1. Source
    2. Destination
    3. Both a and b
    4. None of the above
21. IPv6 address binding:
    1. Maintains a neighbor cache
    2. Keeps the cache up-to-date at all times
    3. Polls neighbors periodically
    4. All of the above
22. NFS uses TCP/IP to
    1. Allow easy access
    2. Allow shared file access
    3. Allow limited access
    4. All of the above
23. Which of the following statement regarding stateless packet filter is true?
    1. Tracks status of TCP connections
    2. Can admit packets that “make no sense” (e.g. dest port = 80, ACK bit set, even though no TCP connection is established
    3. Is more secure than stateful packet filter
    4. All are false
24. Demilitarized zones (DMZ) is used to:
    1. Isolate servers from the rest of the network
    2. Allow access to trusted network
    3. Block outbound traffic
    4. Block inbound traffic
25. Data Encryption Standard (DES) uses:
    1. 56 bit symmetric key and 64-bit plaintext input
    2. 64 bit symmetric key and 64-bit plaintext input
    3. 56 bit symmetric key and 32-bit plaintext input
    4. 64 bit symmetric key and 32-bit plaintext input
26. Which statements regarding Advanced Encryption Standard (AES) is true?
    1. Uses 128, 192, or 256 bit keys
    2. Uses 128 bit blocks
    3. Is considered more secure than DES
    4. Is a symmetric key standard to replace DES
    5. All of the above
27. Which of the following statement is true?
    1. Symmetric key systems encrypt and decrypt with the same key
    2. Asymmetric key systems encrypt and decrypt with different keys
    3. Asymmetric key systems are more secure than symmetric key systems
    4. Both a and b
    5. None of the above
28. Consider the following example: Alice encrypts message with her private key and sends it to Bob. Which of the followings is true?
    1. Bob decrypts message with Alice’s public key
    2. Bob knows the message was encrypted with Alice’s private key
    3. Anyone with Alice’s public key could read the message
    4. Both a and b
    5. All of the above