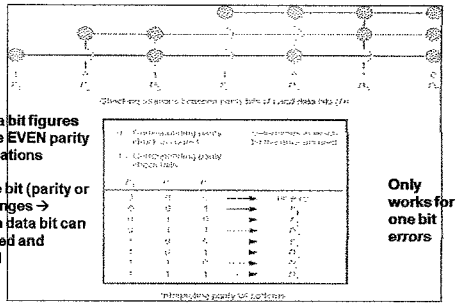
Data Communications for a Global Environment

Hamming Code – An FEC Example



Each data bit figures into three EVEN parity bit calculations

If any one bit (parity or data) changes → change in data bit can be detected and corrected

Only works for one bit *errors*

Data Communications for a Global Environment

Ethernet (IEEE 802.3)

- Most widely used LAN protocol, developed jointly by Digital, Intel, and Xerox, now an IEEE standard
- Uses contention based media access control
- Byte-count data link layer protocol
- No transparency problem
  - uses a field containing the number of bytes (not flags) to delineate frames
- Error correction: optional

April 5, 2011

Backbone Networks
- high speed
- typically fiber optic cables
- connects to other backbones, MANs, and WANs (city-wide)
- enterprise or campus-wide network
- has switches routers or gateway
- most switches operate at data-link layer, others at network layer
- routers operate at network layer; also determines the best path to send message
- gateways operate at application or network layer; has a processor; can translate messages between different protocols

Backbone Network Architectures
- access layer
- distribution layer
- core layer

*no class next Thurs 14th

April 7, 2011

[digital - discrete values ~ 1 or 0
analog - continuous values]

types
- MANs - metro ~ 3 to 30 miles
- WANs - connect BN and MANs
- usually transmit over telephone line

- phone circuits types
  - circuit switched
  - packet switched

- Ring Architecture good
- Star " better
- mesh " best, expensive

- don't have to know T-Carrier speeds

- X.25
- ATM
- Frame Relay

VPN - Virtual Private Network

April 12, 2011

Chapter 10 - The Internet

- network of networks
- made up of tiers
  - National ISPs
  - Regional "
  - Local "
    - You
- Internet is based thru movement of packets
- peering - anyone on the same level are not charged, otherwise they are
- NAP - Network Access Point
- MAE - Metro area Exchange
- Layer-2 Switch = Data Link
- most common form of DSL is asynchronous
  mismatch speed = asynchronous

- WAP Architecture is for cell phones

- Internet Governance is done ~~by~~ by nobody; the closest thing is Internet Society (ISOC)
  - ~~public~~ public policy
  - education
  - standards

- IETF is under IESG

Lecture 19

Network Security

Why Networks Need Security

Organizations vulnerable due to dependency on computing and widely available Internet access to its computers and networks

Business loss potential due to security breaches

- $350,000 average loss per incident
- Reduced consumer confidence as a result of publicity
- Loss of income if systems offline
- Costs associated with strong laws against unauthorized disclosures (California: $250K for each such incident)
- Compliance with HIPPA and Sorbanes-Oxley

Protecting organizations' data and application software

- Value of data and applications far exceeds cost of networks
- Firms may spend about $1,250/employee on network security

Financial Impact of Security

2005 Computer Security Institute/FBI Computer Crime and Security Survey

- 70% of the respondents reported security breaches in the last 12 months
- 60% reported a financial loss due to security breaches
- Average loss: $350,000

Security issues can impact consumer confidence

70% of all email sent worldwide was spam in 2006

New laws on data privacy and financial information include Sarbanes-Oxley Act (SOX) and Health Insurance Portability and Accountability Act (HIPPA)

Primary Goals in Providing Security: "CIA"

Confidentiality

- Protection of data from unauthorized disclosure of customers and proprietary data

Integrity

- Assurance that data have not been altered or destroyed

Availability

- Providing continuous operations of hardware and software so that parties involved can be assured of uninterrupted service

Types of Security Threats

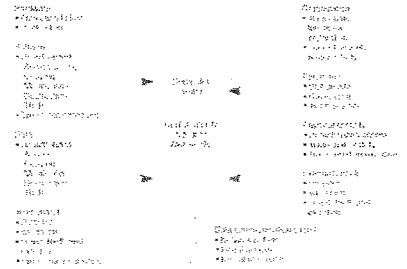
Business continuity planning related threats

- Disruptions
  - Loss or reduction in network service
  - Could be minor or temporary (a circuit failure)
- Destructions of data
  - Viruses destroying files, crash of hard disk
- Disasters (Natural or manmade disasters)
  - May destroy host computers or sections of network

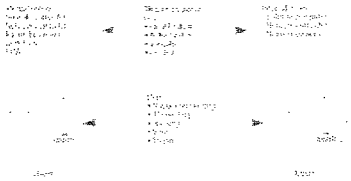
Intrusion

- Hackers gaining access to data files and resources
- *Most unauthorized access incidents involve employees*
- Results: Industrial spying; fraud by changing data, etc.

Threats to a computer center



Example of Some Threats (Cont.)



Security Threats

Identify threats

- Any potentially adverse occurrence that can
  - Harm or interrupt the systems using the network, or
  - Cause a monetary loss to an organization

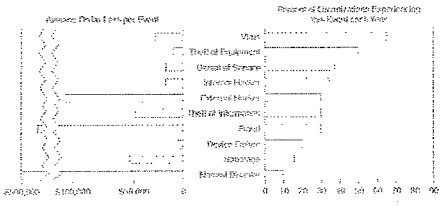
Rank threats according to

- Their probability of occurrence
- Likely cost if the threat occurs

Take the nature of business into account

- Example: Internet banking vs. a restaurant
  - Bank's web site: has a higher probability of attack and much bigger loss if happens
  - Restaurant web site: much less likely and small loss

Likelihood and Costs of Threats



Common Security Threats

THREATS:

Virus infection is most likely event

Intrusion

- By internal employees and external hackers
- High cost to recover in terms of financials and publicity

Device failure (not necessarily by a malicious act)

Device theft, Natural Disaster

Denial of Service attacks

- External attacks blocking access to the network

Big picture messages:

- Viruses: most common threat with a fairly high cost
- External intrusion is now greater threat than own employees

COST OF THREATS:

Costs may be $33,000 per virus that infects an average number of computers

External intrusion may cost an average of $100,000 per incident

Internal intrusion happens about as frequently as external intrusion, external is rising

Natural disasters happen to about 20 percent of organizations each year

Denial of Service attacks could cost Amazon.com $10 million per hour, organizations typically lose $100,000 to $200,000 per hour

Cost of lost work for a single LAN may be $1000 to $5000 per hour

Preventing Computer Viruses

Viruses

spreads when infected files are accessed

- **Macro viruses attach themselves to other programs (documents) and spread when the programs are executed (the files are opened)**

Worms

- **Special type of virus that spread itself without human intervention (sends copies of itself from computer to computer)**

A Trojan Horse

is a subset of a Virus. It does not reproduce by infecting files or does it self replicate. It may open up a backdoor for more malicious attacks.

Preventing Denial of Service Attacks

DoS attacks
- Network disrupted by a flood of messages that prevents messages from normal users
  - Flooding web servers, email servers so server cannot respond

Distributed DoS (DDoS) come from many different computers
- DDoS agents on several machines are controlled by a DDoS handler, may issue instructions to computers to send simultaneous messages to a target computer

Difficult to prevent DoS and DDoS attacks
- Setup many servers around the world
- Use Intrusion Detection Systems
- Require ISPs to verify that all incoming messages have valid IP addresses

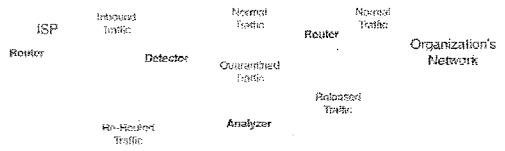
DOS and DDOS Approaches

Traffic filtering: verify all incoming traffic source addresses for validity (requires a lot of processing)

Traffic limiting: When a flood of packets are entering the network, limit incoming access regardless of source (some may be legitimate)

Traffic anomaly detectors: Perform analysis of traffic to see what normal traffic looks like, block abnormal patterns

Traffic Analysis



Firewalls

Prevent intruders by securing Internet connections
- From making unauthorized access and denial of service attacks to your network

Could be a router, gateway, or special purpose computer
- Examines packets flowing into and out of the organization's network
- Restricts access to that network
- Placed on every connection that network has to Internet

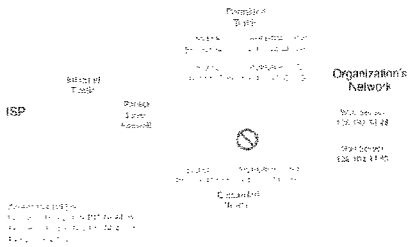
Main types of firewalls
- Packet level firewalls (a.k.a., packet filters)
- Application-level firewalls (a.k.a., application gateway)
- NAT Firewalls

Packet-level Firewalls

Examines the source and destination address of every packet passing through
- Allows only packets that have acceptable addresses to pass
- Examines IP Addresses and TCP port IDs only
  - Packet filtering firewall is unaware of applications and what the intruder is trying to do

Access Control Lists
- A set of rules for a packet-level firewall
- Can be used to
  - permit packets into a network
  - deny packets entry

How Packet Level Firewalls Work



IP Spoofing

"IP spoofing" remains a problem
- Done by simply changing the source address of incoming packets from their real address to an address inside the organization's network
  - Firewall will pass this packet as it looks like a valid internal IP address
  - Many firewalls know to discard incoming packets with internal IP addresses

Application-Level Firewalls

Acts as an intermediate host computer (between outside clients and internal servers)
- Forces anyone to login to this firewall and allows access only to authorized applications (e.g., Web site access)
- Separates a private network from the rest of the Internet
  - Hides individual computers on the network behind the firewall

Some prohibit external users downloading executable files
- Software modifications done via physical access

Requires more processing power than packet filters which can impact network performance

Network Address Translation (NAT)

Used by most firewalls to shield a private network from public network
- Translates between private addresses inside a network and public addresses outside the network
- Done transparently (unnoticed by external computers)
- Internal IP addresses remain hidden

Performed by NAT proxy servers
- Uses an address table to do translations
- Ex: a computer inside accesses a computer outside
  - Change source IP address to its own address
  - Change source port number to a unique number
    - Used as an index to the original source IP address
  - Performs reverse operations for response packets

Using Private Addresses with NAT

Used to provide additional security

Assigns private IP addresses to devices inside the network
- Even if they are discovered, no packets with these addresses will be delivered (publicly illegal IP address)
- Example: Assigned by ICANN: 128.192.55.xx
  - Assign to NAT proxy server: 128.192.55.1
  - Assign to internal computers: 10.3.3.xx
    - 10.x.x.x is reserved for private networks (never used on Internet)
  - No problem for users as handled by NAT proxy server, but big problem for intruders

Additional benefit is that it gives ability to have more internal IP addresses for an organization

NAT Proxy Servers

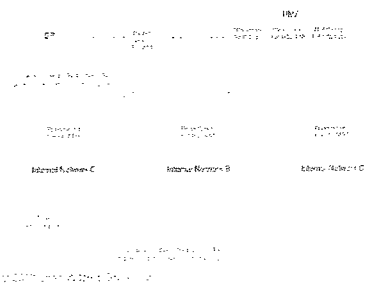
Becoming popular; replacing firewalls

Slow down message transfer

Require at least two separate DNS servers
- For use by external users on Internet
- For use by internal users (internal DNS server)

Use of combined, layered approach
- Use layers of NAT proxy servers, packet filters and application gateways
- Maintaining online resources (for public access) in a "DMZ network" between the internal networks and the Internet

A Network Design Using Firewalls



Server and Client Protection

Security Holes
Operating Systems
Trojan Horses
Encryption

Security Holes

Made by flaws in network software that permit unintended access to the network
- A bug that permits unauthorized access
- Operating systems often contain security holes
- Details can be highly technical

Once discovered, knowledge about the security hole quickly circulated on the Internet
- A race can then begin between
  - Hackers attempting to break into networks through the security hole and
  - Security teams working to produce a patch to eliminate the security hole
- CERT: major clearing house for Internet-related holes

Other Security Holes

Flawed policies adopted by vendors
- New computers come with preinstalled user accounts with well known passwords
  - Managers forgetting to change these passwords

Operating Systems

American government's OS security levels
- Minimum level (C2): provided by most OSs
- Medium Level (B2): provided by some
- Highest level (A1 and A2): provided by few

Windows vs. Linux

OS Security: Windows vs. Linux

Windows
- Originally written for one user one computer
  - User with full control
  - Applications making changes to critical parts of the system
    - Advantages: More powerful applications without needing user to understand internals; feature rich, easy to use applications
    - Disadvantages: Hostile applications taking over the system

Linux
- Multi-users with various access rights
- Few system administrators with full control

Trojan Horses

Remote access management consoles (rootkits) that enable users to access a computer and manage it from afar

More often concealed in other software that is downloaded over Internet
- Common carriers: Music and video files shared on Internet sites

Undetected by even the best antivirus software

Major Trojans
- Back Orifice: attacked Windows servers
  - Gave the attacker the same right as the administrator
- Morphed into tools such as MoSucker and Optix Pro
  - Powerful and easy to use

Optix Pro Trojan Menu

Three Types of Trojans

Spyware
- Monitors what happens on the target computer
- Can record keystrokes

Adware
- Monitors users' actions
- Displays pop-up advertisements on the screen

DDos

Encryption

One of the best way to prevent unauthorized access (more formally, cryptography)

Process of disguising info by mathematical rules

Main components of encryption systems
- Plaintext: Unencrypted message
- Encryption algorithm: *Works like the locking mechanism to a safe*
- Key: Works like the safe's combination
- Cipher text: Produced from the plaintext message by the encryption function

Decryption - the same process in reverse
- Doesn't always use the same key or algorithm.
- Plaintext results from decryption

Encryption Techniques

Symmetric (single key) encryption
- **Uses the same algorithm and key to both encrypt and decrypt a message**
- **Most common**

Asymmetric (public key) encryption
- **Uses two different "one way" keys:**
  - a public key used to encrypt messages
  - a private key used to decrypt them

Digital signatures
- **Based on a variation of public key encryption**

Symmetric Encryption

Key must be distributed
- Vulnerable to interception (an important weakness)
- Key management – a challenge

Strength of encryption
- Length of the secret key
  - Longer keys more difficult to crack (more combinations to try)
- Not necessary to keep the algorithm secret

How to break an encryption
- Brute force: try all possible combinations until the correct key is found

Symmetric Encryption Techniques

Data Encryption Standard (DES)
- Developed by the US government and IBM
- Standardized and maintained by the National Institute of Standards and Technology (NIST)
- A 56-bit version of DES: used commonly, but can be broken by brute force (in a day)
- Not recommended for data needing high security

Other symmetric encryption techniques
- Triple DES (3DES): DES three times, effectively giving it a 168 bit key
- Advanced Encryption Standard (AES), designed to replace DES; uses 128, 192 and 256 bit keys
- RC4: a 40 bit key, but can use up to 256 bits

Regulation of Encryptions

Considered a weapon by the U.S. government

Regulated its export the same way the weapons are

Present rule:

- Prohibits the export of encryption techniques with keys longer than 64 bit without permission
- Exemptions: Canada, European Union; American companies with foreign offices

Focus of an ongoing policy debate between security agencies and the software industry

- Many non-American companies and researchers developing more powerful encryption software

Asymmetric Encryption

Also known as Public Key Encryption (PKE)

Most popular form of PKE: RSA

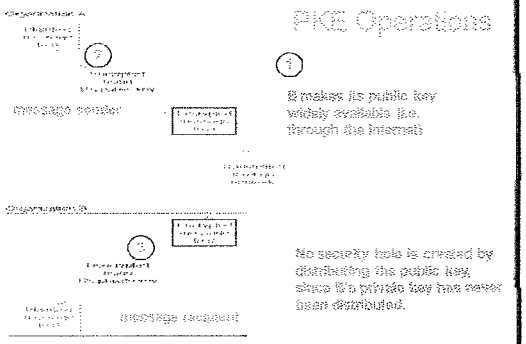
- Named (1977) after the initials of its inventors: Rivest, Shamir, and Adelman
- Forms the basis of Public Key Infrastructure (PKI)
- Patent expired in 2000; Now many companies offer it

Longer keys: 512 bits or 1,024 bits

Greatly reduces the key management problem

- Publicized Public keys easily accessible in a public directory
- Never distributed Private keys (kept secret)
- No need to exchange keys
  - **Sender uses the receiver's public key to encrypt**
  - **Receiver uses their private key to decrypt**
  - **Public key cannot decrypt public key encrypted message, only private key will work**

PKE Operations



Authentication

Provide secure and authenticated message transmission, enabled by PKE

Provides a proof identifying the sender

- Important for certain legal transactions

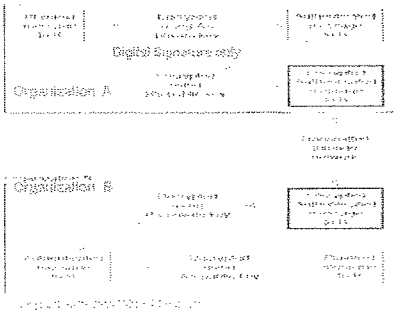
Digital Signature:

- *Includes the name of the sender and other key contents* (e.g., date, time, etc.,)

Use of PKE in reverse (applied to Digital Signature part of the message only)

- Outgoing: Encrypted using the sender's private key
- Incoming: Decrypted using the sender's public key
  Providing evidence who the message originated from

Transmission with Digital Signatures



Public Key Infrastructure (PKI)

Set of hardware, software, organizations, and policies to make PKE work on Internet

- Solves the problem with digital signatures
  How to verify that the person sending the message

Elements of PKI

- Certificate Authority (CA)
  A trusted organization that can vouch for the authenticity of the person of organization
- Certificate
  A digital document verifying the identity of a digital signature's source
- "Fingerprint"
  A unique key issued by the CA for every message sent by the user (for higher security certification)

Process with Certificate Authority

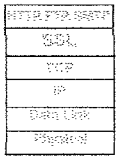
- User registers with a CA (e.g., VeriSign)
  - Must provide some proof of identity
  - Levels of certification: Examples:
    - Simple confirmation of an email address
    - Complete police style background check
- CA issues a digital certificate
- User attaches the certificate to transactions (email, web, etc)
- Receiver authenticates transaction with CA's public key
  - Contact CA to ensure the certificate is not revoked or expired

Pretty Good Privacy (PGP)

- A PKE freeware package
  - Often used to encrypt e-mail
- Users make their public keys available
  - Example: Posting them on Web pages
- Anyone wishing to send an encrypted message to that person
  - Copies the public key from the Web page into the PGP software
  - Encrypts (via PGP software) and sends the message using that key

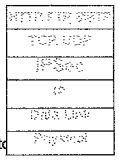
Secure Sockets Layer (SSL)

- A protocol widely used on the Web
  - Between the application and transport layers
- Operations of SSL
  - Encrypts outbound packets from application layer before transport layer
  - Negotiation for PKI
    - Server sends its public key and encryption technique to be used (e.g., RC4, DES)
    - Browser generates a key for this encryption technique; and sends it to the server (by encrypting with server's public key)
  - Communications encrypted by using the key generated by browser



IP Security Protocol (IPSec)

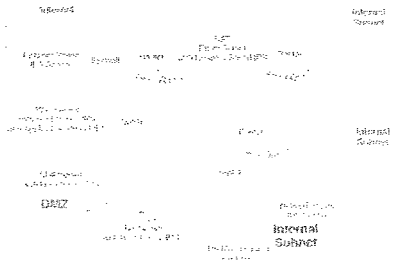
- Another widely used encryption protocol
  - Can be used with other application layer protocols (not just for web applications)
- Operations of IPSec between A and B
  - A and B generate and exchange two random keys using Internet Key Exchange (IKE)
  - Then combine these two numbers to create encryption key to be used between A and B
  - Next, A and B negotiate the encryption technique to be used, such as DES or 3DES.
  - A and B then begin transmitting data using either:
    - Transport mode: only the IP payload is encrypted
    - Tunnel mode: entire IP packet is encrypted (needs a new header for routing in Internet



Techniques Used by IPSs

- Misuse detection
  - Compares monitored activities with signatures of known attacks
  - If an attack is recognized the IPS issues an alert and discards the packet
  - Challenge: keep database current
- Anomaly detection
  - Operates in stable computing environments
  - Looks for major deviations from the "normal" parameters of network operation
    - e.g., a large number of failed logins
  - When detected, an alert is issued, packets discarded
  - Problem: false alarms (valid traffic different from normal)

Use of IPS with Firewalls



Intrusion Recovery

Must have a clear plan to respond to breaches
- Have an emergency response team (CERT for Internet)

Steps to take once intrusion detected:
- Identify where the security breach occurred and how it happened
  - Helps to prevents other doing it the same way
  - May report the problem to police
- Use Computer Forensics area techniques
  - Use of computer analysis techniques to gather evidence for trials

Entrapments – Use of honey pots
- Divert attackers to a fake server (with interesting, but fake data used as bait)
- Monitor access to this server; use it as a proof

April 19, 2011

CIA – Confidentiality, Integrity, Availability
- primary goal in providing security

- Beseness contenuity planned related threats
  - disruptions
  - destructors of dates
  - disasters (natural or manmade)
- Intrusion
  - hackers gaining access
  - unauthorized access
  - mostly done by former employee

- Viruses – usually macros attached to a file or program
- worms – they can spread themselves
- Trojan horse – similar to a virus

- Denial of Service Attacks
  - flood a web server so that they can't respond
  - Destributed DoS come from several machines

DoS and DDoS Approaches

- traffic filtering
- traffic limiting
- traffic anomaly detectors - most advanced
- Firewalls
  - router is a type of firewall (NAT)
  - looks a packet (packet level)
  - " " application gateway (application level)
- IP Spoofing
  - remove original IP with another
- NAT
  - shields private networks from public networks

April 27, 2011

Exam 3 review

ch 8 - ~~backbone networks~~ w/ components
- ~~comps~~ switch, router, gateway (com.)
  - how they work in a backbone
- backbone layers (3)
- ~~skip~~ skip virtual backbones (com.)
- comparts of backbone

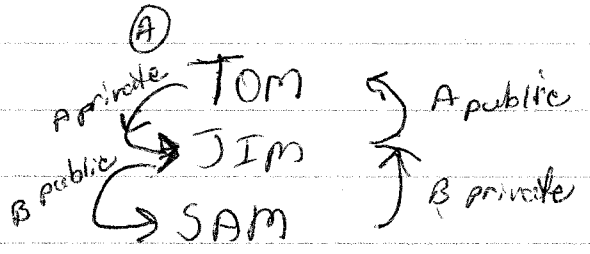
ch 9 Telephony ~~switch~~
- four circuit types (private, ~~switched~~ switch dedicated, ~~packet~~ packet ~~public~~ Public, ~~virtual~~, VPN)
  - differences between each
  - higher level info
- packet switched is multipoint
  - VPN is, characteristics, why, drawbacks
    - more secure, performance, no standardization, expensive

ch 10 Internet
-

c

Security

- CIA
- security approach
  - [redacted] potential risks, cost, and key issues
  - where security dollars are spent
- virus, worm, trojan horse
- denial of service vs Distributed DoS
  - protection: filtering, [redacted], traffic limiting (on packet, IP address, IP address source) read
  - [redacted] anomalie
- firewall - intrusion protection, usually is a router
  - packet, application, or NAT proxy server Firewall types
- encryption
  - use mathematical algorithm to decode
  - types: symetric, 1 key
    asymetric, 2 keys; can be used as public key



authenticate, then encrypt

omit IP security protocol

-33

(67)

March 31, 2011

Name: Kenneth Robinson

MIS 340 Exam II

1. (8 pts) Indicate (T/F) which of the following major functions of the Data Link Layer

Addressing	T
Message Assembly and Disassembly	F
Media Access Control	T
Routing	F
Message Delineation	T
Message Acknowledgement and Flow Control	F
Error Control	F
Session Management	F

-3

2. (6 pts) In controlling when and what computers transmit, there are two possible approaches. Name and describe each of the two approaches.

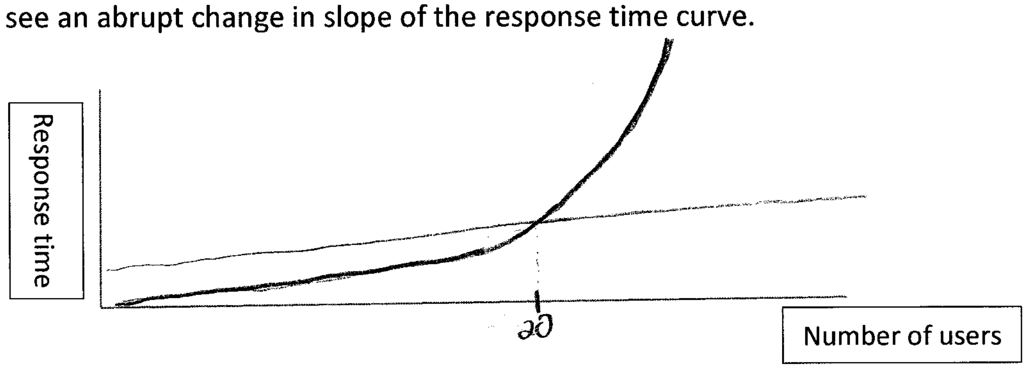
Token Ring (~~contention based~~ controlled) - each computer takes turns (holds token) transmitting data with no time limit? [must pass token after preset time — this would shut down network]

?

Time ~~Division~~ (controlled) - each computer is given a set amount of time to transmit data.

-3

3. (4 pts) One of the approaches described in question 2. is the predominant approach for more than 90% of all LANs in the US. If I were to plot response time versus the number of users what would the shape of the curve look like and at what number of users would we see an abrupt change in slope of the response time curve.



Controlled

4. (6 pts) Complete the following:
   - The Major cause of errors in network circuits are caused by line interference.
   - On average there is one error in every 500,000 bits
   - The error detection algorithm to use if we want a greater than 98% chance of detection is the Cyclic Redundancy Check.
   - If an error is detected then the primary means of error correction is called retransmit.
   - What is the specific type of error correction used in full duplex circuit retransmit Cont. ARQ
   - The major technique managing message flow control between two processors is called the flow rate Sliding Window

-2

5. (6 pts) What are the differences between a digital and analog signal and why do we prefer to use a digital signal in network transmission. Digital signal has discrete values of one and zero whereas analog does not. Digital signals are preferred because they are easier to correct errors, encrypt, mix audio, data, graphical

-1

6. (6 pts) What is the definition of multiplexing and describe how one of major multiplexing techniques operates. Multiplexing is splitting one ~~logical~~ Physical circuit into several logical circuits.

-4

7. (4 pts) Describe how we can encode a digital signal on an Analog carrier wave. In your description name the three techniques that could be used. Taking a sample from the analog signal and convert it to digital. The phase, amplitude, or sampling rate could all be changed.
AM, FM, Phase Shift

-2

8. (4 pts) Describe how we can send multiple bits at the same time on a carrier wave and what is the relationship between the # of bits sent concurrently and the number of amplitudes required. Using multiplexing, the bits are sent through the circuit at different frequencies.

-3

9. (5 pts) If we wanted to send an analog signal over a digital circuit, we would need to decode an analog signal into a digital data stream.

- What is the device that performs this function called? Codec
- What are the two main parameters that can be adjusted to control the resultant accuracy of the digital signal. amplitude and phase.
- The differences between the original analog signal and the reproduced digital signal is referred to as the sampling rate Quant Error
- The Nyquist theorem is used to determine the minimum value of one of the parameters described above.
- It is dependent on what characteristic of the original analog signal amplitude Bandwidth

-4

10. (4 pts) Why do we need LANs and what is the Business Value companies hope to achieve by their investments in LANs? LANs are used to share resources and information. Companies hope to achieve greater profits by being able to do things faster.

11. (4 pts) What are the basic components of a LAN? Cables, Network Interface Cards, Server with a Network Operating System, clients, and hub or switch

12. (6 pts) Fill in the Blanks

- What is the most common type of cable found in LANs CAT 5?
- What is the typical connector for that cable called? RJ-45?
- What are the Max data rates that can be run on that cable? 100 mbps?
- What is the name of the device used to connect components on a shared Ethernet LAN hub?
- What are the two main objects that Active Directory Service maintains information on? resources and security Principles.
- The AD Framework can be viewed at three levels: forest, tree and domain.
- Domains are identified by their tree DNS Namespace name.
- Group Policies are usually applied at the organizational unit level.
- To allow one domain to access resources in another domain the AD uses trusts.

13. (3 pts) Let's look at the characteristics of Shared and Switched LANs. Indicated whether the following characteristics are reflective of a Hub or Switch or both.

- My logical topology is a star — hub S X
- I can connect two cables with different connectors — hub B X
- I provide a level of amplification that allows longer LAN Segments — both B
- I utilize the contention protocol CSMA/CD — hub B X
- I can allow two computers to transmit at the same time — switch
- My capacity rate does not decrease with the number of users. — switch

4

14. (6 pts) What are the three modes of Switch operation and what are the characteristics of each.

1) store and forward - message is stored by switch and then forwarded to destination.
2) cut-through
3) fragment free forwarded

15. (3 pts) A dedicated LAN is experiencing throughput issues. It may result from bottlenecks in either the LAN or the Server. What would be my first step in diagnosing the problem? What criteria would you use to determine where the bottleneck lies?

If the error rate is greater than 60% then the server should be checked. If it is between 40% and 60% then the LAN should be checked. < 40% its more like Network in between could be both, have to test

16. (3 pts) If the problem was determined to be the server, then what other steps could I take to more precisely pinpoint and correct the problem. Assume replacing the server is not an option.

3

More servers could be added to increase capacity. A switch could be used instead of a hub. — how would that help the server

17. (9 pts) With respect to wireless LANs, complete the following statements:
- At the physical layer a wlan uses radio signals to transmit data.
- The device that replaces a hub in a wlan is a ~~switch~~ AP.
- A wireless LAN operates in what two frequencies ranges 2.4GHz and 5.0GHz.
- Which frequency range has the greater data capacity rate 5.0GHz?
- Which frequency range experiences the least amount of attenuation 5.0GHz?
- What device do we never place on the wireless LAN server?
- What is max range of an AP 300 ft indoors?
- If power is supplied to an AP by POE, what type of voltage is this Direct Current?

18. (3 pts) What is the "hidden node" problem and how does it occur? When one device cannot "hear" that another device is transmitting to the access point. Both devices are in range of the AP, but are not in range of each other.

19. (3 pts) At the datalink level wireless communication can utilize two protocols one is contention based the other is controlled. Identify the name of the controlled protocol and describe how it works. Why would we need this second protocol?

PCF. It works by the AP giving a clear-to-send signal when requested by the device. Otherwise the device must wait and resend another request.

20. (7 pts) Complete the following questions pertaining to Bluetooth.
- What is the typical power output of a Bluetooth device 1 milliwatt?
- A network of Bluetooth enabled devices is called a piconet?
- A Bluetooth network can consist of how many devices 8?
- What is the protocol that Bluetooth uses to avoid interference statistical?
- What is the frequency range that Bluetooth operates in 2.4GHz?
- That range is broken down into how many individual channels 79?
- How many times a second does Bluetooth change channels 1600?

February 25, 2011 Name: Kenneth Robinson

-29

MIS – 340 Exam I

1). (10 pts) The Internet reflects one of the most rapid adaptions of Technology by both the Business and the Public Sector creating a self-feeding relationship between Network Capacity and User Demand. Select one of the factors from the following list that you feel has the greatest impact on this Demand/ Capacity relationship and discuss why you think it is the most significant influence.

-Increasing Computer capacity and decreasing cost
-Geographic expansion of public network access to Local ISP's
-Business processes becoming more complex and multi-national
-Rapid consumer adoption driven by e-commerce, e-mail, socialization networks and gamers

Increased capacity is significant because it allows more work to be done faster. The decreased cost is beneficial to companies because their money can be invested in other computing technologies.

5

2.) (5 pts)The networking model we discuss almost exclusively in this course is the Internet layer model. Identify the number of layers and show them in the proper order that they would occur on the sending processor. PONTA

Application → Transport → Network → Data → Physical

3.) (4 pts) What is the definition of a protocol? Give an example of one protocol you have studied and indicate which layer it is associated with. Protocol is a standard set of rules for a given purpose, the HyperText Transfer Protocol is associated with the Application layer.

4.) (10 pts)One significant changes in the evolution of Software Development was the trend toward reusable code. Repeatable Software patterns were often employed. A repeatable pattern describing system level organization is called an Architectural Style.

a) Describe the 3-Tier Architectural Style? This style is divided into 3 levels. The User Interface, Business or Application Layer, and the Data Access Layer.

b) What is the relationship between this Architectural Style and the number of processor's that it could potentially run on? This style allows for it to be scaled up or down as much as it is needed to meet demand.

-1

c) What are the advantages and disadvantages of the 3-Tier Architectural Style.

Advantages are that it is scalable to meet needs. A disadvantage is that it creates more network traffic.

-1

5.) (5 pts)The way the World Wide Web works is an example of the Client-Server Architectural Style.

a). What is the Application Protocol used by the WWW? HTTP

b). What are the three sections that comprise the protocol request structure? Indicate what sections are mandatory and list the key fields in each section.

Header is mandatory. (only Host needed)

~~Request section is optional.~~

Body section is optional

Command line - CMD, URL, HTTP Ver# mandatory

-3

6.) (10 pts) The following questions pertain to electronic mail.

a). What is the primary application protocol for the sending client in a thin client e-mail application?

SMTP HTTP

-2

b). What is the primary application protocol for the sending client in a "fat" client e-mail application?

SMTP

c). What are the two possible protocols associated with the receiving e-mail server and the receiving client? IMAP or POP3

d). What is the main difference between these two receiving protocols.

IMAP leaves the messages on the server. POP3 downloads the messages to the client's machine.

7.) (5 pts) What are the five major functions of the Transport Layer?

To put enclose the destination, source, and segment info into the packet.

-3

8.) (3 pts)Why is TCP called a reliable protocol?

Because it will resend packets that do not reach their destination.

9.) (3 pts) The TCP header message is 24 bytes long and consists of several fields. Identify three of the most critical fields required for successful network communication.

Destination socket, source socket, and segment number
Port # Port #

-1

10.) (3 pts) What is the Transport layer protocol used in connectionless communication and provide two examples where this protocol is utilized. UDP is the protocol in connectionless communication. It is used for streaming audio and video conferencing.

11.) (4 pts) What are the two primary functions of the Network Layer? To address the message and to send it to either the data or transport layer, Routing

-2

12.) (5 pts) The host computer in attempting to translate an Application layer address to an IP address, found no matching IP address is found in its local cache. Describe how the host computer determines the IP address from the Application layer address. It would connect to the DNS server to obtain the IP address. If not available there, it would connect to the next highest DNS server.

13.) (2 pts) The IP address represents two components ID's. Name them.

The network ID and the host.

14.) (2 pts) Initially IPv4 addresses were assigned using a Classfull addressing scheme. Under that scheme, the following IP address belongs to what class?

10000000	00000000	00000000	00000000	128 -191

Class B

15.) (2 pts) Today a classless or slash notation scheme is used. In the following IP address 130.160.83.243/16, What does the /16 represent?

The number of bits that represent the network ID.

16.) (5 pts) The following range of addresses are called Private Addresses. What is a Private Address and why would I want to use one?
10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, 192.168.0.0 – 192.168.255.255

Private addresses allow for small networks to be created within a larger network. Also so that certain devices can be accessed within the network

17.) (3 pts) What is sub-netting and why would I want to do it? To share resources or components within the same network.

18.) (3 pts) With respect to the IP address, what information does a subnet mask provide for us?
Which part of the IP address is the network ID.

19.) (3 pts) From a network performance perspective, why would I want to know if the destination IP address was on the same subnet as the sending host? It would decrease the transmission time and reduce the amount of network traffic

20.) (2 pts) In network terms, what is Routing?
The path that data travels from the source to the destination. determining

21.) (4 pts) There are two types of dynamic routing. What are the two types of dynamic routing and describe what information is used as the primary input on routing decisions. Also identify which protocol is associated with each type. Primary input is which way is the fastest. based on what?

22.) (2 pts) What is an Autonomous System in networking? A system that automatically connects devices on a network.

23.) (5 pts) Fill in the following answers with respect to Routing
a) The router that connects two subnets is called gateway
b) The router that connects two autonomous systems is called gateway Border
c) RIP, OSPF, EIGRP are examples of direct routing protocols
d) BGP is an example of an streaming routing protocol
e) Two hosts on the same subnet communicate through what router? subnet

Bonus Questions

24.) (3 pts) What is an ephemeral port designation used for and would I most likely find this designation used on the sending application or the receiving server. It is used for connecting to a server based on the protocol. It would be found on the receiving server.

25. (5 pts) Describe how instant messaging works and how it differs from traditional e-mail.

Instant messaging uses the same protocol for sending and receiving messages.