We are using @aludra.usc.edu

TA Office Hours:  
Hao Feng

Friday 3pm-5pm

Message Length

Transmission time = Rate (bits/sec)

Distance

Propagation delay = Transmission speed

Nodal Processing time

Queing delay

Throughput

Message Size L

Transmission Delay = Bit Rate R

Message Size

Throughput = Run Trip Time

Nodal Time = Transmission time + Propagation time

Start watching Lecture and Discussion slides

**Lecture 1/15/13**

TCP/IP Protocols- Internet protocols

Lab1 criteria could be defined as a protocol.

No need to read the entire book.

Simply look over slides for reference

Networks talk to each other through links

They may not be connected on a one to one basis

Topology- How the nodes are connected

**INTERNET**

-Internet is the network of network

-Internet is dynamic

**REVIEW C++: learn in 21 days, cplusplus.com**

**Lecture 1/17/13**

Unit 0

Stuff here will be covered in detail later

Connected with wires (guided) less prone to noise

Wireless (unguided) more prone to noise

Difference in connections is determined by frequency

Medium is also known as the communication channels

EXAM will not be determined on memorizing abilities but rather BASIC CONCEPTS

KNOW WHAT LAN stands for

Network Topology-

-bus

-ring

-star Observe the differences carefully

-line

-tree

-partially connected mesh

-fully-connected mesh

Central connection device such a router is necessary to use less links because the links are costly.

NODES  
  
end-systems (hosts) The actual devices that are the original sources or ultimate destination  
switches (routers, bridges, hubs, gateways) These are connecting devices rather than the end destinations

FULLY CONNECTED MESH IS BEAUTIFUL BECAUSE EVERY NODE IS CONNECTED TO EACH OTHER

HOWEVER THIS FULLY CONNCECTED MESH IS VERY HARD FOR LONG DISTANCES SUCH AS IN US, CHINA, AND US. OR WHEN THERE ARE MANY NODES.

Using a fully connected mesh to connect 20 nodes we need

20! .

(2!)\*(18!)

For 6 nodes we need 15 connections for a fully connected mesh

(6!) .

(2!)\*(4!) = 15

Fully Connected mesh could be used in a small local setting because it could be faster and links are not that long

A network with loops not not loop parts will be called PARTIALLY CONNECTED MESH or MESH

Computer costs are lowering but costs of links are increasing!

Partially connected- use more than one router for redundancy and this will create loops.

Red and blue center nodes are routers

There are two for repetition because having just one is risky.

So we have two for redundancy

When we do this we create loops

INTERNET IS A PARTIALLY CONNECTED MESH

Client calls for information

Server gives the information

Google- is a server

Firefox- is a server

Nodes: End-systems (Host) -> end-systems could be client or servers

Only the software parts are called client or servers

Routers are called (connections)

Don’t think of my laptop as one client but rather a device with multiple clients (Since clients are pieces of software) such as firefox, internet explorer

Protocol for accessing internet uses WWW (World Wide Web)

Implement WWW means to implement client code and server code.

Peer-to-Peer network:  
  
Any video or filesharing application is a peer-to-peer network

Goes to central server that tells you where your peers are

Then you go to that peer to get your video or data.

Also someone can ask you for data then you become a server.

If you see something like this than it is a peer-to-peer network.

CLIENT-SERVER MODEL (SERVER NEVER BECOMES CLIENT)  
  
PEERS MEANS THAT NODES CAN BE SERVER OR CLIENT

WWW: Someone writes client code, someone server code and connect

EE450 we don’t really look at peer-to-peer model because we can create it by copying client/server code into one node.

ANOTHER Property of Server model

SERVER ALWAYS has to be on to provide services. THEREFORE WE NEED A LOT OF REDUNDANCY. GOOGLE has multiple servers running for back up so if one crashes, then the entire network doesn’t crash.

For peer to peer model we need a central server that keeps a list of the peers

THIS IS CALLED A DEDICATED SERVER p.17 This servers should be POWERFUL to provide fast and reliable service as a lookup director

EVERYNODE NEEDS A PROCESSOR: ROUTERS NEED PROCESSORS

ALWAYS LOOK FOR THE BOTTLENECK AND GIVE IT THE MOST POWERFUL PROCESSOR BECAUSE THE CENTRAL NODES CONNECT TO MANY OTHER NODES  
  
REVIEW THE DIFFERENT TYPES OF SERVERS p. 18-19

Software or Hardware discussion

Hardware could change: such as PC, MAC,

Firefox code should not change

This is why there are many different layers between Software and Hardware

TOP MOST: SOFTWARE PIECE

Referred to as NOS (Network Operating System)

NOS manages network

OS manages local resources

CLIENT SOFTWARE- referred as shell, redirector, or requestor

Takes request and decides if client is requesting a piece of shared resource on the network or a local resource on hardware

Directed to OS or directed to Network Protocol. Page. 21

So keyboard is directed to OS and web browsing requires Network Protocol

NIC (Network Interface Card) or adaptor card is an expansion card used to connect hosts to the network

NIC design is based on the network type, for example wireless NIC has different design than Ethernet NIC

Network Cards communicate by sending signals through transmission facilities/medium/link

NIC is needed for guided AND unguided!

NIC includes transmitter and receiver

Network Classification Based on Coverage

SEE page 23

PAN-bluetooth, (few meter)

PAN, LAN, MAN, WAN

LAN (few km)

As size increases noise increases

LAN could be as big as a building, 2 buildings, or 3 buildings. All are applicable

BACKBONE NETWORKS Connect LANs p.27

Could be cables. USC backbone

Highbandwidth cable that are connected to other LANs. Maybe same protocol to keep end-systems connected such as on p.26 could be used to keep LANS connected.

(67:50 in lecture video)

The network (LAN) has to listen to bus first before sending. If overall bus is busy then, there is no point in sending!

Bus backbone, star backbone

Backbone is a LAN in itself and uses LAN

Connections to Backbone are LANs in themselves

Ethernet is a network protocol for LANs

Ethernet is the most popular LAN

It uses a shared network. When you send the data. Everyone receives it.

Microsoft makes Internet explorer for free. Advertisements on websites rakes in money.

Free to use.

Receiving many customers makes it public.

MAN- Metropolitan

Spans over a city

USC network is a definitely not a LAN but rather a bunch of LANs

Should we call a bunch of LANs a MAN?

DOESN’T matter. We could call it a MAN or bunch of LANs.

Downtown, USC, Koreatown -> MAN

Small network p.25 could be called “internet” with a lowercase i. If a note is connected to the internet it could be called Ethernet because it is using the protocol

A LAN can have other LANs inside

LAN is a network of networks

Why are there different connecting devices: Bridges, Routers, Hubs, Gateways

HUBS – Hubs are the cheapest because they are very primitive devices and don’t filter as much. Responsibility of Hub is to copy message and relayed to remaining terminals. Only filter is to not send packet back to sender.

If you’re not happier with this then you need a router.

Hubs are easy to design and cheap. May be used for 3 nodes which would cheaper.

LAN network consists of printer and computers.

If we use we connect Hub directly to Internet then the whole world would know what you are sending. INTERENT DISCONNECTS HUBS TODAY.

If two incoming signals arrive at Hub at the same time the Hub sends collision signals to everyone.

Hub (level 1 switch -> physical layer)

If a Bridge (level 2 switch) switchbased LAN, ethernet

Router (level 3 switch)

WAN- is Internet and PSTN (BIGEST NETWORK NOT Internet) BIGGEST WAN is PSTN some parts of the world don’t have Internet but have phone access

Internetworking involves connecting two or more computer networks using a common routing technology. The result is called internetwork (often shortened to internet) p. 39

Only routers and gateways work for internetworking

Hubs and switches not used

Internet uses Internet Protocol Suite, TCP/IP

Now we know our network. How do we communicate between networks?

To send messages you need:  
1) Protocol

2) Medium

Type of transmission

a. Simplex (TV, Radio)

b. Half-duplex (Walkie Talkie)

c. Full-duplex p.45

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | | **shahin nazarian** |   Feb 15 (5 days ago) |  |  |
| |  | | --- | | to undisclosed recipients | |  |  |

Dear All,

Please watch today's discussion video, if you did not attended the class. Project phase I is due in 3 weeks (March 8 at 11:59pm.) Please start early.

Also plan wisely for the next three weeks, as you need to prepare for your first EE450 exam while working on the project.

The main topics of Quiz (on March 5)are the latency/throughput, switching technologies, network addressing and DHCP/DNS/ARP protocols and the physical layer. Please check the syllabus for the general information regarding exams. The exam rooms are listed in the updated syllabus. I will send a detailed guideline a week before the exam.

Have great long weekend,

Shahin

2/15: Project

Project (3 phases) assigned

**Discussion 01/18/2013**

Use nunki.usc.edu port 22

“pwd” command used to see current directory you are in

vim “filename” you can get into file

if you press “I” you can see that at the bottom “Insert” this puts you in editing mode

“wq” to save changes and quit

g++ compiler

and

gcc compiler

to run file just type executable

Filezilla is FTP software

C++ uses the classes which are more powerful than structs

This lecture talks about classes which I should review

Lecture 01/22/2013

Transmission is always in one direction

Physical layer means the signal processing part

People are more interested in software part

Maybe physical layer questions will not on test.  
We will mainly be focusing on the software side

5 Components of communications

1) Protocol

2) Medium type

3) Message type (Depends on the what medium it is sending through

4) Sender

5) Receiver

Shannon-Weaver Simple Communication Model 1949 p. 47

MODEM (Modulator and Demodulator) – is a transmitter that converts data from digital to analog which is suitable for the medium that the message is being transferred through.

D-> D, A -> D, A-> A, D-> A

Modem is FDX

PSTN (Public Switched Telephone Network) and Internet are switched networks and used point-to-point links

Point-to-point vs. Multipoint

Discussion about Multipoint

Almost everything is digital nowadays

Insert message into physical link until it hits the cable end where the message is absorbed

Gives message to all stations. In the Data Link Layer it waits for the entire message waiting for the head and tail header.

Physical Layer (Processing and relaying exact number of bits) (Used for synchronizing data) (send one bit, you expect one bit to be received)

You can combine physical and data link layer like combining a 5 functions in main into one function in main for programming.

This is not necessarily good

Data link Layer -> Network Layer Layer

Looks for **frame** **packet** is frame minus header

-> Transport layer -> Application Layer

Wouldn’t message relay to ALL NODES

Job of physical layer is to receive exact number of bits (signal processing)

Data link layer is where the dropping of the message occurs

What if somebody attempts to read the message? (hacking) yes this is possible but is violating the protocol. That is why there is some security mesures.

These days PSTN is connected to Internet

But assume we’re in the old days where the PSTN is not connected to the Internet

PSTN uses switches so as not use unnecessary links (not fully connected mesh)

Links between switches are highbandwith because there are other nodes may be using the same links

Highbandwith allows for multiplexing the data which can use different frequencies which allow for many different channels.

So two pairs of hosts sending and receiving can be using the same link and it would be fine

Say we have N nodes. If we add one more node we would most likely not need new routers. THEREFORE WE WOULD ADD ONE LINK.

This link attaching you to the network would be short and attached to the nearest link to you called “**the central office”**

**Trunks** are highbandwidths and also called (**shared facilities**)

The link attaching one node to the rest of the network is called **dedicated** and is not shared. Since it is only connecting one node, therefore only used by that node, it doesn’t need highbandwidth. Only one node is using it

Lecture 26:04

Network cloud: a network cloud that connects two nodes. Shared networking. We don’t really care what path the message traverses within the network cloud

Adding one node: dedicated. Adding two nodes: use maybe a router

Using shared network going from 6 -> 7 we add one link

Using fully-connected going from 6-> 7 nodes we would add

7! . 6! .

2!\*(5!) - 2!\*(4!) = 21 – 15 = 6

Network cost is per connection

VOIP

PSTN (optimized for voice)

Internet (optimized for data)

NIC (Network Interface Card) Error detection

Check frame to see if it is erroneous

Broadcast: Wanting to send a message to everybody

Unicast (one receiver)  
Multicast (send to group)

What destination address should be sent so everybody reads it?

Write Public Announcement (Use all 1s for broadcast address)

No node can have (all 1s address)

All NIC cards receive message bit by bit and is synchronized

When local network you don’t need router to broadcast to everyone

Swtiched network: (Also known as shared network)

PSTN nodes are called switches

Nodes in Internet are referred as routers

Looks at area code and then starts routing

If we see a in state area code we simply look for routers that are in the states

Different kinds of routing

Shortest

Fastest Different goals

Best Quality

Cheapest

Dial Tone indicates that network understands that N1 has requested service and that it is ready to accept its destination number (address)

Once route has been established the destination node receives ringing tone and then a ring back tone is sent back to source node

Once the path/route of a telephone call is established. The channel within the trunk remains dedicated throughout the phone call (dedicated circuit)

Per demand it is dedicated. Dedicated if requested.

Internet design says dedicated is no good. Therefore in Internet nothing is dedicated.

If you don’t hang up the line will always be dedicated

The quality of PSTN is very high quality.

If N1 demands connection to N15, the circuit (channel) will be dedicated between N1 and N15, (as if N1 were connected to N15 in a fully-connected topology)

The idea of per demand dedicated circuits makes the network feasible.

PSTN Connected to ISP (Internet Service provider)

Internet piggy backed off of PSTN using dialup services

ISP has a modem to be connected to PSTN like any other nodes.

1000 Modems used in ISP per 100K customers using Internet example because Internet monitors its connections

Internet monitors activity so if it is not active for a certain amount of time, then the modem is disconnected

N customers then N modems right?

Well not all the customers constantly use dialup Internet constantly!

4KHZ is given to a dedicated line and sends digital data

56-64Kbps (very slow)

4KHZ is for voice only

if we send voice and data at the same time then 2KHZ each which is very poor quality.

For this reason we said we can only do one at a time. Make a phone call or use dialup.

SO ISP KNEW THAT USERS CAN’T USE DIALUP AND MAKE PHONE CALLS AT THE SAME TIME SO THE NUMBER OF MODEMS PER CUSTOMER WERE DECREASED ACCORDINGLY

Page 70 for Introduction Presentation

Go over rest of slides in Introduction presentation

Private vs Public Networks

Access network: they are the physical links that connect an end system to its edge router. Access network classes are residential access, company access, and wireless access.

DSL (Digital Subscriber Line) faster than ISP

Faster downstream 8Mbps (typically < 750 kbps) than upstream 1 Mbps (typically < 6 Mbps)

Upstream (home to router) downstream (router to home)

DSL and HFC (Hybrid Fiber Coax) require special modems, called cable modems

For DSL, HFC, and satellite access service is always ON, ie, the user PC can remain permanently connected to an ISP while simultaneously making and receiving phone calls

Company access: Connecting LAN to an edge router. Many types of LAN but Ethernet is currently by far the most prevalent.

Like HFC, Ethernet uses shared medium.

End systems connect into Ethernet switch

Wireless Access Networks: Predicted that wireless handheld devices will overtake wired computers as the dominant Internet access devices throughout the world

Shared wireless access network connects endsystem to router via base station aka Access Point (AP)

1. Wireless LANs: base station within radius of a few tens of meters
2. Wider-area wireless access. 4G technology used for cellular phones.

Two main 3G standards are EVDO (Evolution-Data-Optimized) and HSDPA (High-Speed Downlink Packet Access

WiMAX aka (IEEE802.16) ver similar to 802.11 (WiFi)operates independently of cellular network and provides higher speeds with higher distances.

Future: Mobile Ad hoc NETwork (MANET) and sensor Networks

MANET also called a mobile mesh network. Involves mobile devices communicating with each other with not access point. P. 78

Home Networks (Are private Networks) p.79

Dialup, DSL, or cable modem. Slowest is dialup

Router/firewall/NAT\*

Physical (Transmission) Media p. 80

Autonomous systems p. 88 Determine protocol for routing within each network

Only on routing protocol handles routing between autonomous systems.

Protocols (TCP, IP, HTTP, and Ethernet) p. 89

Intranet is a private network that uses the same set of protocols (TCP/IP) as

Internet Protocols and Standards (Cont)

RFC (Request for Comments) for new protocols so that people can comment on them, IETF (Internet Engineering Task Force) p. 90

Tier-1 ISP (Backbone Service Providers) are the biggest and provide national/international coverage. p.93 The need each other’s help so they treat each other as equals even if their competitors in the market.

Tier-1 peers treat each other equally by carrying each other’s Internet traffic without paying each other

POP (Point of Presence) is a switching center where traffic is exchanged.

Tier-2: are smaller (often regional ) ISPs. They connect to one or more tier-1 ISPs as their customer (paying Tier 1s) they possibly have private connectivity to other tier 2 ISPs. Tier-2 is a customer of Tier-1 p.95

Tier-3: ISPs or local ISPs are the last hop (“access”) network and are the closest to end systems. They can be directly connected to tier-1 to have faster and more reliable connection, however they have to pay more than they would have to pay if they connected with tier-2

Network Structure. P.99 Network edge-application and hosts, Access networks- are the smaller tiers, with wired or wireless communication links, network core-are ISPs or backbone service providers, such as tier-1, interconnected routers mostly via fiber optics network of networks.

Network Edge: Reliable Data Transfer Service (Connection Oriented Service) p.100 Data transfer between end systems.

Handshaking (to ensure reliable transmission) setup (prepare for) data transfer ahead of time. Hello established

Setup “state” in communicating hosts

Supported by TCP/IP (Transmission Control Protocol and Internet Protocol)

Application using TCP: HTTP (Hyper Text Transfer Protocol) (web), FTP (file transfer), Telnet (Terminal Network) (remote login), SMTP (simple mail transport) (email)

TCP (Transport Control Protocol) service [RFC 793] p.101

Reliable, in-order byte-stream data transfer. LOSS: acknowledgements and retransmissions

Flow control:

Sender won’t overwhelm receiver with too many packets that the receiver cannot handle

Congestion control:

Senders “slow down (or stop) sending rate” when network is congested

UDP (User Datagram Protocol) Service [RFC768] p.102

Goal is still data transfer between end systems, however supported by

Connectionless

Unreliable data transfer

No flow control

No congestion control

UDP does not do any of above the TCP does

Applications using UDP

Streaming media

Teleconferencing, DNS (Domain Name Service), internet telephony

Dialup connection: p. 103

Dialup customers are residential customers (service providers are AOL, Netzero, Earthlink, etc)

The Internet speed with this type of connection can be at most 56kbs

Both packet and circuit switching techniques, use switching from node to node, however

In packet switching the traffic is stored in every node, processed and forwarded to another node

In circuit switching, once the path is set, there is no processing any longer.

T-Carrier (T-CXR) is the generic designator for any of several digitally multiplexed telecommunications carrier systems originally developed by Bell Labs and used in North America, Japan, and Korea.

The basic unit of T-carrier system is DS-O (DSO or Digital Signal O) which is a signal channel of 64Kpbs

CSU/DSU is like a MODEM for PSTN but for T1 it is digital. T3

Optical Carrier Specifications (Optical Carrier OC) p.107

SONET (Synchronous Optical NETwork)

OC-n speed is nX51.8Mbps

Bigger companies use higher Ocs

DONE WITH INTRODUCTION SLIDE

NEXT PRESENTATION: NETWORK PERFORMANCE AND LATENCY MEASURES

NETWORK PERFORMANCE AND LATENCY MEASURES

Network Performance Measure

Delay/Latency: How fast is the network (measured in terms of second)

Throughput: Measured by Bits per second

Just because a network is fast, it doesn’t mean the throughput is high.

Speed can be high but throughput can be low

I THINK I UNDERSTAND NODAL DELAY UP TO PAGE 18. SKIPPING THE DEN

Lecture 01/24/2013

End-to-end delay: is delay from the time it takes to be processed by source to time destination receives the last bit of information

Queue delay and processing delay are random

Example of Dexter p.21 (45:50)

Uploading is usually slower than downloading (upstream vs. downstream)

Round Trip Time (RTT) (aka Response Time)

Time it takes for packet to be sent and then an acknowledgement sent from destination back to source

RTT depends on link length, message length, propagation speed, nodal processing, network load, link direction (upstream, downstream). Etc.

RTT = d(transmission of message) + d(processing) + d(propagation) + d(queue) + d(processing) + d(transmission of ACK) + d(propagation)

Assuming that Propagation delay is the only significant component, then

RTT = 2(N+1)\*d(propagation)

Where N is the number of links //p25

Throughput (applies to reliable networks)

L (bits) / RTT (sec)

Roughly acknowledged as

L .

(delay of transmission message)\* 2(N+1)\*(propagation delay)

Message length does not include ACK

RTT is good to wait to send next message

If there is error detection than throughput decreases

SEE page 27

Time Out policy. Message is sent again if source does not receive ACK signal after a certain amount of time

ACK needs to be sent within Time Out policy

Make ACK time longer or shorter to increase or decrease RTT

Wait increases RTT

But not waiting might also increase RTT because ACK might not reach the source within the Time Out

Because Timeout is > RTT then it makes sense to send NAK  
Which is faster than waiting for Timeout to not receive an ACK

The number of bits that are sent per unit time (offered load) is not equal to the number of bits actually delivered (carried load or throughput)  
  
Offered load depends on the overall traffic while throughput is what is delivered.

Both are bits per second or packets per second

Maximum load is called “Capacity”

We don’t know capacity of everything because there are so many random variables with many different routers

Look at 70% of capacity

Bandwidth vs. Throughput

Bandwidth has two definitions:  
1) It is the width of the frequency band

2) Bit rate: number of bits that can be transmitted per second in a link

\*Bandwidth does not deal with reliability while Throughput does

Usually Throughput < Bandwidth but never reversed

Finished with Bandwidth vs. Throughput

Page 34

Bandwidth-Latency product

Optimize Bandwidth

Minimize Latency

R\*RTT

Bandwidth (bps) \* Latency (seconds) = maximum number of bits in pipe

Latency can be considered as RTT or one way

Not a good idea to send something and wait

Go for maximum number of bits that you can transmit which is equal to Bandwidth Latency

Make sure to always send something to keep system busy

Should we maximize or minimize Bandwidth\*Latency? Not a good question to ask

We prefer Low Bandwidth\*Latency over a High Bandwidth\*Latency

This means we can send smaller message rather than larger messages

LFN (Long Fat Networks) Like “Elephant” Propagation delay is too high. Hard to utilize. Submarine signals?  
  
Bit width or Bit length = length of pipe / total number of bits

= distance / (Bandwidth\*delay)

**Discussion 1/25/2013**

The number of cables (links) for each of the following topology with n nodes

1. Star n-1
2. Ring n
3. Bus one backbone with n drop off links
4. Fully Connected n\*(n-1)/2 = n!/(2!\*(n-2)!)

Throughput orientated algorithms

Backpressure Algorithm (deals with queuing delay and maximizes throughput)

Gets its inspiration from:

Lyapunov drift-designed for control systems and is also useful for network and throughput performances

Lyapunov drift + Penalty

Michael Neely (Professor about Backpressure Analysis

EE649 Deals with network organizations

**Lecture 1/29/2013**

Bandwidth vs. Throughput

While we wait for acknowledgment signal we want to send more messages.

Rate\*RTT = most bits we can send (15:15)

Rate\*2prop (1 prop for message 1 prop for acknowledge)

We don’t want dead time to JUST wait for acknowledgement

Expect two questions:  
1) For reliable transmission: Bandwidth\*2d(propagation) waits for acknowledgement

1. For unreliable transmission: Bandwidth\*d(propagation) does not wait for acknowledgement

Bit width = d/(R\*2d(prop)) = meters/bit. Tells you length of each bit

Bit width = d/(max # of bits)

Bit width = d/(R\*d(prop))

Bit width = S/R or S/(2R) since d(prop) = d/S

NETWORK PROTOCOLS AND LAYERING SLIDE

Review slides (Unit 0, Unit 1, Unit 2, Unit 3) (Unit 4 is when we actually start)

See page3

TCP connection request. TCP connection response. File

Synchronize. Rules to be on time,

See page 5 for history. ISO (International Standards Organization)

OSI (Open Systems Interconnection) uses 7 layers

Internet uses TCP/IP uses 5 layers (EE450 focuses on this)

Connect many devices through one network.

Making a standard and convincing people of the standard takes a long time by which the technology could have changed.

Interface is the most important form of communicating.

Why not have 10000 layers?

Performance decreases and more time to go through all these functions.

It is important to have the layers be independent so they don’t have too much interface. This is possible by the designer

Nazarian skips 13-15

We’ll look at these layers in more depth with TCP/IP later on

The real physical link is the only solid connection.

The abstract links such as communication between the languages of two nodes such as the code between the two nodes (applications such as firefox)

Routers simply have Network, Data link, and physical links but no higher layer links (48:00)

Headers tell you what you are sending. Header includes the details of a certain protocol. (such as if I am using a specific routing, program, FTP or HTTP). This header is for the interpretation of the receiving node. (49:00)

The Second layer has a header and trailer part (51:25)

Upper layers would not be seen by intermediate nodes. These are called end-to-end layers. Top 4

Network layers are bottom three.

Peer layer of A is the corresponding layer of B

Layer 4 of A -> to Layer 4 of B

Interface between is called Layer 1 to layer 2 or layer 4 to layer 5 interface

These interfaces are Surface Access Interface

Network layer of A peer is network layer of router 1 (54:20) p.24

Interface is Bidirectional

OSI Model is FDX

Goes through top to bottom layers. p.25

Adjacent layers are layers in the same node but different layer

Peer layer are layers of the same layer but different node p.26

SDU (Service Data Unit) is the payload

PCI (Protocol Control Information) the header which has the protocol information

SDU (the payload) + PCI (the header) is called the PDU (Protocol Data Unit) the name implies that PDU is the combination of protocol data. P. 27

See p.28 PDN (N+1) = SDU (N)

Physical layer just passes it

To send a message a node first:

Start at higher layer (layer 7) goes down to lower layer where a header is added until it hits the physical layer which transfers it to the next node.

When the destination node receives the final PDU, the data traverses from low level to high level decoding the header.

High levels have less number of bits.

For the second layer: the whole PDU in that layer is called the FRAME

The whole PDU in layer 3 is called the PACKET  
The whole PDU in layer 4 is called the DATAGRAM (for UDP which is unreliable) or SEGMENT (For TCP which is reliable) (61:40)

For physical layer: there is no term. It’s main job of physical layer is synchronization. Physical layer does not do error detection. Success is measured by synchronization (receiving and sending the same amount of bits)

Read slides 29-54 IN DEPTH REVIEW OF LAYERS

Caught up

Stopped at (64:27)

Internetworking – TCP/IP View p. 54

Physical links have different technologies

Sometimes people call the real channel as layer 0

(maybe changing from wireless to cable)

Layer 1 is the protocol used synchronize

Sometimes people call the user layer 8. (mac, windows)

Data link and Physical are dependent of technology

But the rest are technology independent

TCP/IP

5) Application

4) Transport layer TCP/IP refers to 3 and 4

3) Network Layer

2) Data Link Layer

1) Physical Layer

End systems may have different Data link and Physical layer but both end systems must have the same TCP/IP which refers to 3 and 4

Of course application must be the same such as (Firefox to Firefox, Skype to Skype, Oovoo to Oovoo)  
  
ROLES OF 5 LAYERS IN TCP/IP

Name of set of bits with data + header

Unstructured set of bits in Physical layers

In application layer: it is just calling Data

HTTP (Hypertext Transfer Protocol)

Application of http is World Wine Web

There are some application that don’t need headers

Page 62

In TCP Segment in Transport level

In UDP Datagram in Transport level

UDP is unreliable- used for web conferences since we want speed. This might lead to lower quality but we want less delay

TCP- we want to use for email for to makes sure it is reliable

**Lecture 1/29/2013 Continue**

Midterm II on 4/25 Check

Don’t like midterm I on 4/11

HTTP is an application

TCP is not used for conference call because it means that it would have to wait for receiver to acknowledge.

Page 63 look at how headers/trailers are added and subtracted

Headers/trailers change: added and then subtracted

Left side you have OSI and right side is TCP

Page 66

DNS is an underlying layer

Next class covered these things

1) Focus on Local network (Intranetwork communication)

2) Internetwork Communication

3 protocols to cover

a) DHCP

b) ARP

c) DNS

**Lecture 1/31/2013**

Final project

Three Types of Addresses

1) Physical Address: little to do with physical layer but it is part of the addressing of the second layer. MAC address = DLC address = Physical address

(Data Link Control) (Medium Access Control)

Has 48 bits (2^48 possible addresses)

2) IP address = Logical address

Has 32 bits (version 4), 128 bits (Version 6) (2^128 possible addresses)

3) Port addressing using port numbers 16 bits (2^16 possible addresses or about 64,000 bits)

We use different addressing

Example: mailing: has first name, last name, the address of the place.

Address of place is similar to the IP address to make sure it gets to the place.

Look at last name for local apartment number which matches the MAC address

Now it is in the apartment. Use the first name or port address to identify the person in the apartment which the letter should be given too.

2^10 = 1024 about 1000

Kilobyte is actually 1024 bits

Even if we had a population of 8 billion we would need much more than 8 billion IP addresses because we need to include the IP addresses of routers!

Port numbers represent applications: Applications require 2 numbers/bits

32,000 applications, which require 2 bits (However we are still fine right now)

MAC address is safest right now. It is the main identity of address of an interface (NIC) 256\*10^12 this is A LOT.

LOCAL NETWORK (NO ROUTER NEEDED)  
REMOTE ACCESS (ROUTER NEEDED)

READ slides he skipped. (Addresses go into headers) p.1-10

MAC is the physical address of NIC

MAC address is in layer 2 or Data Link Layer or MAC layer

MAC header goes into frame

(frame, Packet, Segment/datagram, message)

IP addresses

Network id: 128.125 represent net id for USC First two byte starts with MSB

Host id: lower part starts with LSB

Numbers range from:

0-255

Network Id don’t always have to be first two chunks. Could be 1 or not a multiple as well.

My IP address of my computer changes when it moves from the USC network to Ellendale 2801 address

MAC address is the identity of the NIC

MAC address doesn’t represent computer. A computer could use two NIC cards. Wireless NIC card and Ethernet NIC card

MAC address is about the interface not node. PERMANENT ADDRESS THAT CAN BE BURNED INTO NIC CARD TO MAKE SURE IT IS UNIQUE

They assign different organizations create their own NIC cards

If we see another address beside 128.125 in USC then it is PRIVATE  
  
PRIVATE addresses are addresses being reused (addresses issue of running out of addresses in IPV4)

Host id can be the same and net id to be different it is okay because the whole IP address is unique

Static addresses - permanent as long as you are connected

Dynamic addresses – Changes as soon as you turn off your device (part of solution to capacity issue)

Certain amount of IP addresses is allocated to a room/location

PUBLIC IP ADDRESS: globally unique address. At one instance only one node can have a specific address

PRIVATE ADDRESSES: cannot be used outside the private network

p.12

Port Address: Addressing inside the node to identify the correct application. Transport layer does this. To port numbers: Sender and receiver (a, j) on page 12

Sending and receiving address is for replies.

During transmission physical addresses change (computer, to router, to iphone) but port and IP address stay the same

Server: well known port number

Client: doesn’t have a name (randomly generated number)

If you are using http (NOS (Network Operating System) generates a random number which is sender code number) We use 80 as well-known number should know what 80 stands for

(36:00) Not about direction

Specific addresses are easier to remember than IP addresses. Example: [www.usc.edu](http://www.usc.edu), [trojan@usc.edu](mailto:trojan@usc.edu), (HOST NAME) (URL) (Universal Resource Locator)

The conversion of specific address to port and IP addresses is through DNS

Page 18

Network Communication

Local addressing (intranetwork communication)

NO ROUTER for local

How would E1 know E3 is connected located to E1

Use Host Address to ask DNS to receive IP address of E3. If Net IP address of E1 and E3 are the same then they are of the same network. This process is called subnet masking

Subnet masking-> getting the net ID

Only use MAC addresses if we use local addressing

ARP (Address Resolution Protocol)  
Give IP address and it will return the MAC address

IP address does not play major role in Local Addressing. No Router

Specific Address -> DNS -> IP

DNS is only for host names not routers

Hosts do not have a permanent IP address but rather it is dynamic

How would DNS be updated with different IP addresses?

For Local Networks MAC address plays major role

For Remote Networks IP address plays major role p.37

p.37 Routers determine routing route by asking the neighboring routers if they are connected to the destination node

Routers should have same net id with the network that it is connected to. But Router are connected to different networks right so how can a router have the same Net id to 10 different networks? Well, this is solved by having multiple NIC cards in a router.

(60:00) VERY IMPORTANT AND INSIGHTFUL OVERVIEW OF REMOTE

Inside each NIC card is it’s own IP address and the IP address of the DEFAULT ROUTER (EDGE ROUTER)

E7 knows R1’s IP address because it is configured in E7’s NIC

(72:00)

Cache-remember MAC or IP information

ARP is a local protocol page 39

In network Cache should store 10-20 minutes

Page 39-

Layer 3 expects a packet

ARP is a layer 3 protocol

Use ARP to BROACAST frame in request. BAD! But necessary

Reply is unicast though one sender to a specific location so this is good

**Discussion 2/1/2013**

**Maybe rewatch but it is just examples**

**Lecture 2/5/2013**

All ones to broadcasted in local address

ARP is distributed

NOT like DNS server

If we want the ARP to have a server, then each local system would need an ARP server

Request address leaves it with zeros. Look at page 43

Data link layer always processes it because physical layer is always

ARP packet has a question mark, IP of source, IP of destination, MAC address of source, and set MAC address of destination with all 1s.

Cache table could have local server, your node, or in some node in your link

NO POINT IN HAVING ARP SERVER

Downside of ARP

Broadcast

Proxy ARP

There is a router in the local network

Router is not going let it pass by sending it’s own MAC address instead of the destination address.

This idea could be extended to firewalls

Application or network layer firewalls

Host Configuration

DHCP

IP address of source and default router is configured in the NIC card

It is configured by DHCP

Say you are a new node in the room, then for you to connect to the wireless then you would need the network adminstrator to manually write the default router

OR

Use DHCP

What are the addresses that you need?

1) IP addresses of default router, 2) your own IP address, and 3)local DNS server 4) Subnet mask (different net ids have different lengths so someone would have to tell me how long the net id is)

host = end systems

page 54

can port numbers be identical for client machines?

Yes it is possible that two randomly generated numbers are the same

Combination of Port and IP address which is called socket number

DHCP (Dynamic Host Configuration Protocol) is plug and play protocol- it is just done automatically

4 phases (for local and remote

1) Discovery phase broadcast send all zeros to indicate a lack of zeros

Use DHCP data NOT LAYER 3 When a router has a DHCP then it includes a layer 5 protocol. DHCP is a layer 5 protocol since it is an application protocol.

DHCP needs a port number just like HTTP

DHCP packed has to be broadcast has a all zero’s source as IP

DHCP frame has own MAC address

Compare DHCP and ARP broadcast

ARP packet:

Known: IP address of source and destination

Unknown: MAC address of Destination. Frame is broadcast in local addresses

DHCP packet: DHCP packet is broadcasted because destination IP address is not known

2) Second phase: Offer phase DHCP will offer an IP address that is dynamic for maybe 24 hours. This is just an offer and if N wants it, it needs to request it. This offer is broadcasted.

IP of server and broadcast offer. What if another node grabs it? Inside the offer message DHCP server offers IP address and lease time.

Destination IP address is all ones. Also destination MAC address could be all ones

There could be multiple offers

3) Request phase New client broadcasts it’s request if there are multiple offers p.63

4) Ack phase

Say during the discovery no DHCP is found, then it goes to a router and then the router goes directly to the DHCP server

Proxy means substitute: Router substitutes for DHCP or Router substitutes its MAC address for an end system’s MAC address

Multiple hosts request IP address: To prevent confusion there is a TRANSACTION ID.

DNS FTP, http Lab will be one of these

ALL EXAMS WILL REMAIN UNCHANGED!

Could take exam at 2 OR 3:30pm

I already read p. 67-68

Name Space: 2 ways to organize

Flat- is not practiced in big organizations because it is not as powerful as hierarchical-

Top parts will be assigned but bottom parts can still be assgined

Domain Name Space- .edu, .org, .com p.72

USC

A domain can be a superset of domains called subdomains

Hierarchy of DNS Server like domains p.75

Each DNS servers can be in charge of a large or small domain

What a server is responsible for is called a ZONE. P.76

Types of DNS servers p. 77

Root (name) servers ONLY 13 of them WORLDWIDE (sounds like a bottle neck but they only direct the queries) Mainly in US

Top-level domain (TLD) servers

Authoritative name servers

Local name servers

Protocols are usually client-server based

Recursive DNS (Domain Name System) p.79-82

Local server should cache the IP address. (If server becomes client)

Iterative DNS

Same steps but no bottleneck

Pure Iterative: Client becomes the direct client, instead of asking the local server. The only downside is that the local server doesn’t get to cache it. P.86

(76:55)

Socket Programming

Designing an Application to connect to the network. That door is connected to the outside world which is called the SOCKET

**Lecture 2/7/2013**

Two end systems with server and client

We need to create an entry point

Door N for N application

Server might have more than one door because it has multiple clients

After creating an interface you would create an address

After the service is done you should close the door and this is THE LAB

Process is run in application layer

Client process

Server process

Peer to peer program

Two client to server pairs

Each socket has both client and server

Model Peer-to peer as client server model

No process in routers

All nodes are end systems for which processes are run

Programs can be on any layer but process is running on a host

Inter-process communication (within same node)

Socket

It is always client asking server. Server does not ask EVERY client “do you need my service?” this doesn’t make sense.

Whoever wants the services has to initiate or ask which is the client in this case.

This is why it is called client server

Server process waits to be contacted (passively open server process)

Should be always open or on

Client should know address of server (Well known) Port number

However we don’t know the IP address

We use DNS for this

How would server know the address of the Client? Once the Client contacts the server, the server will know the address of the client.

Open the door for communication

Socket is interface from process (socket = network API) interface 5-4

Socket is an abstraction and not a real door (virtual interface)

Page 7

Process is analogous to house and socket is its door.

Application data is person that wants to leave the house

It needs a means of transportation.

Program designer designs socket with application

TCP is a streaming socket (Streaming)

Datagram sockets use UDP

Designer parameters for designing the socket

Decide Transport Layer: TCP or UDP

Maximum buffer and maximum segment sizes

We’re using UNIX sockets for now. But it isn’t that hard to convert to Windows socket.

Sockets are independent of TCP/IP

Two kinds of network applications:

1) RFC-based (follows RFC standards)

2) Proprietary (You are responsible for both client and server sides because you made up your own protocol)

Raw sockets: don’t need a transport layer (we are not looking at these)

Stream sockets (connection-orientated, handshaking, reliable)

Datagram sockets (connectionless, unreliable

Client socket initiates contact

Server is always on (passively on server socket)

Page 14

Commands on the server side include (Create, Bind, Listen, Accept, Send/Receive, Close (the Child Socket) Although parent socket should NEVER close

Commands on the client side include Create, Connect (only for stream sockets) Send/Rev, Close socket

Three-way handshaking process: When connects, listens, and accepts

Page 15

Socket domain (family)  
Socket type (Sock\_stream) (Sock\_dgram)

Protocol (TCP, UDP)

Related to 5 and 4

Is socket type and protocol repetitive

There other PROTOCOLS other than TCP and UDP

For us it is repetitive because we only use TCP and UDP in this course

DHCP, and DNS are application protocols but are not really used by users

In our convention, bottom boxes give their services to upper boxes

HTTP and FTP are common application

Port number is well know for servers

There are a network of servers. (servers are distributed)

[www.mit.edu](http://www.mit.edu) (DNS decides)  
[www.google.com](http://www.google.com) (DNS decides which server out of the network of servers it is going to give)

Some applications works on TCP and UDP (DNS is one of these applications)

IP + well known port + UDP or TCP is a socket address which is a combination of these three

Creating a socket

Int Socket(PF, Type, Protoco)

If it is success the network will give a nonzero number

Parent (listening) socket is always passively open. This does have an address yet. Bind gives an address. The address length is 16 bits and 32 bits.

If everything goes fine then it returns a 0.

Bind (Binds an address to a socket) I have an interface with an address

To let network know that this socket it is ready then it creates Listen (Only for TCP not UDP)

Queue limit (max number of clients can use this socket)

If listen command is successful then there is parent socket that is able to listen to a request. (return 0 is successful)

If a request comes and we have not gone over the queue limit

Then server can accept the connect command from the client side.

Parent socket has main door. Accept gives you a child socket descriptor

Accept returns a non zero descriptor for a socket called the child socket.

How do we know the remote address? (the connect of the client server gives it)

Welcoming socket opens more doors.

Parent socket is never closed

Child socket is created in the Accept command by the server

Child socket is duplicate of parent socket. (known as communication socket)

Big open door (parent door is always open) opens small doors

Child sockets have identical well-known port number and IP address p.23

Send and Rev and Close commands

Server side: Socket is Client

How can you distinguish between child sockets by their addresses? You can’t

Client socket:

Int Socket (PF, Type, Protocol)

Actively open (only open when it wants services)

Int Connect  
remote address is well known port number, IP address uses DNS

Listen, Connect, Accept

FDX (Full Duplex)

TCP is this

UDP is the less complicated process.

Mainly uses Send and Rev

When the client is done the descriptor is destroyed. If client side closes but server sends data? This is possible. Client has no more request so client closes but server keeps open then if data is sent from server then the data is sent.

Connection is released with socket is symmetric. When both close commands are executed then the connection is closed.

SEE PAGE 26

TCP is a point-to-point protocol

SYN -> ACK\_SYN -> ACK

Say Hello -> Acknowledges Hello by saying Hello -> I heard that you said hello to my hello

SCTP is third most important

Congestion control is quiet complicated (uses prediction)

UDP doesn’t use congestion control

If you want something in between then we use these protocols. (these are connectionless but have congestion controls)

PAGE 30

DCCP, SCTP, SST

These are optional (not tested, usually in general not tested on terms)

UDP there is no initial handshake (no connect, listen, accept) not applicable or required

Pipe is logically connected

UDP is message orientated

TCP is byte orientated programming (can rely on channel)

UDP needs to rely on address. It needs to have address

Best effort protocol (It may work, it may not)

TCP is slower because it needs handshaking procedure.

No child or parent in UDP

Only one socket is created

N clients and 1 socket on the server side so N+1 sockets

2N +1 sockets for TCP (N+1 sockets on server side and N on Client side

**Discussion 2/8/2013 IMPORTANT FOR HTTP and FTP I finished looking at it**

Review on http and FTP Protocols

Application layer: HTTP, SMTP and FTP

Web page consist of objects

HTML file (writing)

Base object is HTML file

Reference object is all other files

Each object is addressable by URL

Host name for Web page

Path name is for each reference

Nonpersistent HTTP (At most one object can be sent) HTTP 1.0  
Persistent (multiple objects can be sent) HTTP 1.1 supports HTTP 1.0

Sends HTTP message and sends TCP message

If we have 10 objects on an HTML file then there is 11\*(2RTT) time

Persistent HTTP: Server leaves TCP connection open.

(23:50) Persistent with pipelining

(26:23)  
HTTP/1.1 has persistent and nonpersistent version

Connection: close //indicates that it doesn’t want to use persistent connection

HTTP response messages is sent by server

HTTP has port 80

FTP has port 21

(control connection) Password, user name, file requested is transported in initial connection

FTP has two TCP connection for each object while HTTP has only 1 TCP connection

First TCP is for uploading

Second TCP for downloading (I think)

Only one file is sent the connection is closed (similar to http nonpersistent)

LOOK TO DOWNLOAD BEEJ doc

(39:00)

IMPORTANT OVERVIEW (39:00)

use getaddress info(function)

feed address into socket(function)

Socket function gets file descriptor

Use bind function

(what port am I on)

Binding socket to port number

Use Listen(function)

(will somebody call me?)

(server is ready to listen)

Accept(function)

(usually in infinite loop to monitor again again)

Done for server side

Receives the connect(function from client side)

Breaks loop from accept function

Goes to send(function) or receive(function)

Client side

Get address info

Socket (create its child socket)

Connect(function)

This signal should detected by accept(serverside function)

Send(function) or receive(function)

Maybe there are thread program that encapsulates accepts, send, and receive function.

This thread program is in the main program.

This is utilized so that the server can set up multiple connections at once.

**Lecture 2/12/2013**

Switched (or Switching) Technologies

Packet-switched

-connectionless (does not wait for ACK)

-connection-oriented (virtual circuits) more reliable. Act like dedicated but it is not. Asks for ACK

Packets –switched are not as reliable but circuit-switch is more reliable

TCP connection orientated on IP which is connectionless

UDP which is connectionless ontop of IP

Different protocols can work together even if they don’t belong to the same class

What is to point of switching technologies: to send a message form one node to another.

From A to B we can’t assume there is a direct link

This is not a good assumption because this means that the network is fully connected but this is not a realistic network

Page 3

Typical implementation: Circuit-switched, Virtual circuit, Connection packet-switched

What layer should we do this?

The idea for circuit-switch is to this in physical layer

Virtual circuit- done in data link layer

Connectionless packet-switched- (IP) network layer

Definition of Switched Network

Traffic of message goes from one switch to another

Means that switches have shared links

Trunks are not dedicated.

How do they give circuits. So time, frequency, and wavelength division. This is how trunks are shared

Phone network maximized for voice which is stream (continuous

Data is not a stream type. Rather it is discrete.

Streaming data (dedicated)

You already know next hop

Less queuing and processing delay between routers

Router to router is going to remember path

Now it cannot see the difference between circuit-switched and fully connected mesh

internet (not dedicated) Not always listening, sending, receiving

Not store and forwarding. You need to route as you go from router to router

Storing and forwarding- store the message in the first node and then queue and process. Then send it to the next node

Real time: short: short packets are preferred

Email: not real time ( long packets are preferred)

If we have many packets then our queuing and processing will most likely be less

If we have long packets than transmission delay will be shorter but queuing and processing delay will be less.

As processing queuing goes down then transmission goes up

Long packets: short transmission delay, and longer queuing and processing delay

Short Packets: long transmission delay, and short queuing and processing delay

Store-and-Forward Delay is same as transmission delay

Virtual Circuit Switching

These routers are decided by path so that the subsequent packets will use the same path. The cost is that the routers will not use routing but virtually dedicate a path. Advantage is that the final destination will see an ordered message. Or not receive a message at all.

We create reliability with virtual dedication

The packets WILL BE IN ORDER.

Virtual Switching is not part of EE450

**Lecture 2/14/2013**

Frame Relay and ATM

See (29:50)

Given m packets and n routers

Packet-Switched

1) Connectionless: (m+ n)\*(transmission + queuing + processing) + propagation

2) Connection-orientated: (m + n)\*transmission + propagation

POP QUIZ WAS 0.5%

PHYSICAL LAYER! ALMOST THERE!

Periodic Signal

Fundamental frequency- f

2f – second harmonic

higher harmonics are weaker than lower harmonics as in they show up more in the signal

Even harmonics do not exist in square signals

The amplitude of the signal decreases exponential as we go to higher powers

Therefore just use the ones that are significant and ignore the negligible signals.

Instead of sending the first three most significant then send parameters then send A1, A3, A5, and then sums them up

If I want to send a signal to the other side: (53:40)

If there is a periodic signal then you don’t send it forever. You just send the a snapshot to the other side and the other side can reconstruct it.

MEMORIZE PAGE 10 FOURIER SERIES

NO FOURIER SERIES ON QUIZ (OPTIONAL!)

Bits or voltage number

Internet can digitize or use analog

Internet has finite number of elements to send

Change over a short span of time means high frequency

Change over a long span of time means low frequency

Information value is associated with predictability

Non-periodic signals are more unpredictable which means they have more data

Check out units on page 14 (exam will be noted or given to you so no need to memorize it)

W = (2pi)\*f

Root mean square

Peak amplitude = square root of 2 multiplied by RMS p15

Frequency domain is Amplitude vs. Frequency p.19

Frequency domain = Spectrum of a signal

Time domain to frequency domain that conversion tool: Oscilloscopes

Even harmonics do not exist for square wave

First harmonic has highest amplitude and then decreases exponentially

So finite amount of harmonics is sufficient to represent the sine wave as the higher frequencies are insignificant

Frequency Multiplexing.

Passband frequency is somewhere in the middle frequency.

Baseband can be converted to a Passband (it is simply shifted)

(80:45)

Broadband transmission: allows two or more channels

Composite signal: A signal that is a summation of sine waveforms.

Page 23

If composite signal is periodic then the decomposition gives a series of signals with discrete frequencies (less information, predictable)

If the composite signal is non-periodic, the decomposition gives a combination of sine waves with continues frequencies. (more information, less predictable the frequencies are continuously changing or staying the same)

**Discussion 2/15/2013 REVIEW**

Describe big picture of final project

**Lecture 2/19/2013 Could look over but I think I got the gist**

Highest frequency of human ear.

200KHz is the channel

Not tested on Bandwidth calculation

Actual Bandwidth vs. practical Bandwidth (19:00) look at total power of the signal

Rate is bits/second (duration of one bit)

Bit duration (transmission delay of one bit)

Rate = 1 bit/ Tbit

Practical bandwidth is the bit rate of the signal

SNR for analog

BER for digital

SNR (DB) = 10 log(10) SNR

Use medium with higher bandwidth to for better transmission

Bandwidth of medium should be higher than bandwidth of source

R < C = B\*log(2)(1+ SNR)

Analog to Analog: PSTN voice to electric

Digital to Analog: PSTN (within Central office)

Digital to Digital: 0 and 1 converting to voltage

Modulation: Vary the parameter so that the demodulator can decode the signal in a readable form

Could be modulating any of the three.

Bit rate R = R(baud) \*K

Bit rate R = fs \* log(2)(MQ)  
MQ = quantization (represents voice quality)

Fs represents accurate sampling

p/65

The higher the number of symbols the more chances for noise

**Lecture 2/21/2013**

Page 72 (clocks)

Multiplexing

FDM and TDM and WDM(optical fiber cables with different lights

Frequency Division Multiplexing

Sharing at same time but only a bit

We want the transmission channel to have a high band width

Time Division Multiplexing

One person has all of the channel for himself but only a short time

If incoming signals are slow but channel is fast

**Discussion 2/22/2013**

Review the Physical layer slide and help on PhaseI on Final Project

**Lecture 2/26/2013**

TDM

Inputs have 10bps with four signals into a MUX

Then the channel should be 4\*10bps

Mux picks up data of first and then the second and then the third and then the fourth

By the time it goes back to the first the first one starts on the second set of data

Look at mux as a rotating switch

Can I be faster than 3 times? Only if we have an idle mode which is timed at a certain interval

It wouldn’t matter the size of the packets but the rate is fixed

**Lecture 2/28/2013 (NOT DONE)**

Check email from Nazarian from last night.

Review Physical layer part

DATA LINK (LINK LAYER)  
Local source local destination

Point to point

Error detection is implemented on second layer in the NIC card

Frame synchronization

Gives services to Network layer

There is redundancy in error detection

See page 5

**Discussion 3/1/2013**

**Lecture 3/5/2013**

EXAM

**Lecture 3/7/2013**

**Discussion 3/8/2013**

**Should be caught up to Lecture 3/14/2013**

**Notes for Midterm 1 (3/14/2013)**  
FDM (Hz) Analog  
TDM (bps) Digital

WATCH DHCP AND HTTP from discussions

LOOK FOR COLLISION PROTOCOLS HW

Maybe review Discussion 3/1? For TDM?

Discussion 3/8 is Quiz review 53:20

ACK4 shits window that includes 4 because 4 has not been acknowledged yet

ALOHA-MA(Multiple Access)

CSMA (Carrier Sense Multiple Access) (Listen before talk)

There can still be collisions if both people happen to talk at the same time

Vulnerable time-(dpropagation of a message is the time that the link is vulnerable to collision

CSMA/DA  
  
802.3 - Ethernet

802.5 – Token Ring

802.11 – Wireless

Usually we design for worst cast scenarios! The worst propagation delay on page 77 is N1 and N6

Detecting and responding to a collision. SEE page 78.

Worst Case is N1 colliding at N6 and then that collision notification returns to N1 and lets it know that there is a collision.

Therefore the delay is 2dprop

Assigned waiting time is not a good idea because this could cause the same collision to happen over and over again.

Can nodes detect if the collision that occurred was it’s own frame? NO.

(22:40) 3/14/13

Because of this, the solution includes this statement.

Dtrans-fram >= RTT = 2dprop

Making sure that L is long enough so L/R >= 2\*dprop

You can’t have short frames (lower bound) for ethernet

Page 83

There also must be an upperbound so one node doesn’t hog the network.

HOW DOES P-PERSISTANT WORK?

Propagation delay doesn’t depend on type of signals traveling in medium

Propagation speed will always be the same.

47:50 REFERENCE!

Hub has only one layer.

CSMA/CD works even for a hub. Because hub can detect and send a collision detection (CD) signal.

Switches are layer 2 so CSMA/CD can be implemented on switch.

Page 94 -. Just means physical signal is different.

48 bytes for the MAC address

**Lecture 3/14/2013**

Token Ring 802.5

Collision cannot occur in Token Ring