CA169: Week 1

What is a Network?

Networks

- Two or more computers linked together to share resources, such as:
    - Files, printers, processing power, communicate, etc
- Computers communicate with each other by
    - cables, telephone lines, radio waves, satelites, infrared beams
- Networks are LAN MAN PAN WAN

Local Area Network (LAN)

- Network confined to a relatively small geographic area.
- Typically lab in computing school, office etc.
- Typical LAN has a central server which controls the network.
- Can share resources ….printers, files.
- Most common LAN is a house !

Metropolitan Area Network (MAN)

- Covers larger geographic areas, cities, schools, local libraries, government offices
- Typically uses dedicated phone lines, coaxial cabling, fibre optic cable and wireless communication

Personal Area Network (PAN)

- Lately, we have seen the growth of PAN's
- Small Networks around you. Typically connects devices together
- Mainly use Bluetooth.
- These (simple) networks becoming ubiquitous

Wide Area Network (WAN)

- Connects larger geographic areas, such as global companies.
- Local and global networks are connected to form larger network.
- Typically uses transoceanic or satellite links
- Protocols used can be ATM networks or MPLS (carrying Ethernet) or others.
- Typically use special hardware and special fibres.
- Physical layer can be DWDM - https://en.wikipedia.org/wiki/Wavelengthdivision_multiplexing
- Main use – telephones !

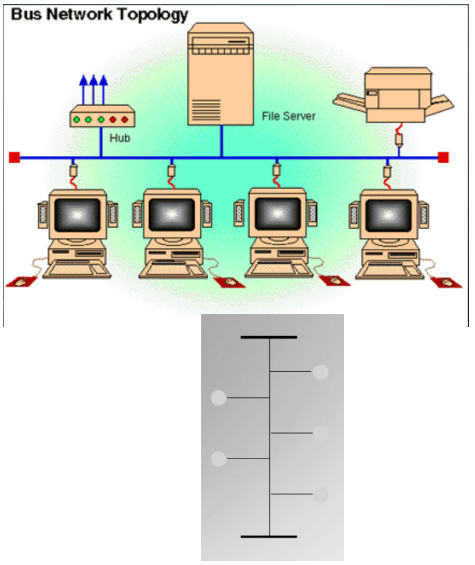
The Internet

- All of the previous network types can connect to the internet
- Infrastructure software needed – TCP\IP
- Global services available through Internet
- Internet aware applications
- Network aware devices

Network Topologies

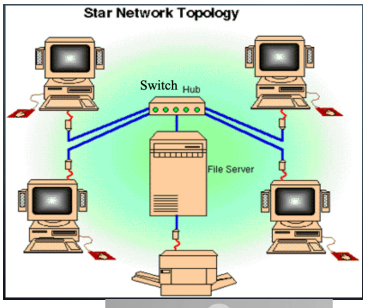
- Topology is how the cables, computers and other peripherals are connected
- Different types of topologies:
    - Star, Ring, bus, tree, Complete, irregular

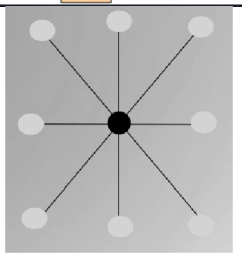
Bus Topology



- Computers share the same bus (cable) with a terminator at each end.
- Each client is connected
- to the bus.
    - Old Ethernet on coaxial cable utilises a bus
- Simple and reliable, not much hardware needed.
- Inexpensive cable and easy to expand
    - Uses the least cable
    - Management more problematic
- Heavy traffic slows overall throughput
- A break in the network brings the whole thing down.
    - Can be difficult to detect.

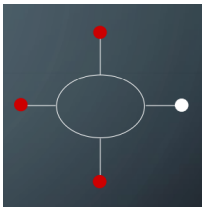
Star Topology

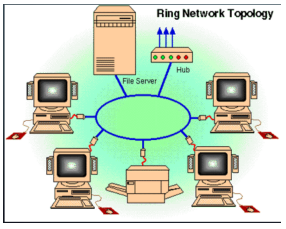




- Each node connected directly to central computer.
- All data must go through central node (hub/switch)
- Relies heavily on central computer
- Each device has a separate wire.
- Easy to install new devices.
- Disconnecting / Adding devices does not interrupt network.
- Easy to detect breaks/faults
- More cable is required (look at our cabinets)
- If central node fails, network falls over
- Commonly uses twisted pair, also uses co-axial (rare now) cable and fibre optic

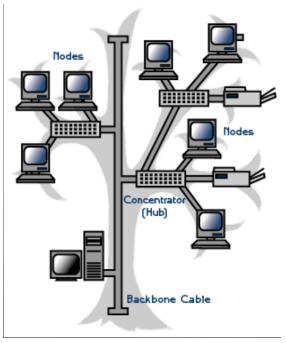
Ring Topology





- Computers tied together in a ring
- Each device is connected to the next one in line
- Circle of cable
- Signal travels in one direction
- When a device receives control (token)
    - It acts on it
    - or passes it on
- Not common these days for LAN.

Tree Topology



- Modern LANs utilise Switches tobuild a tree topology, even when the network looks like a mesh.
- Need to ensure that loops are not introduced, special protocols built into switches (STP)

Topology Considerations

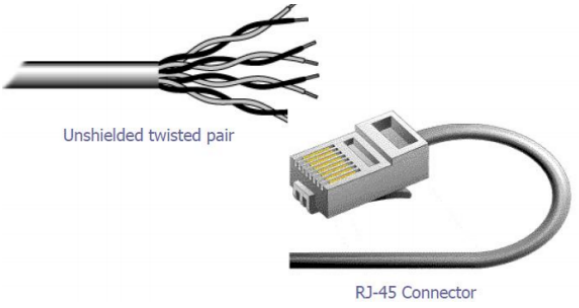
- Money
  - Bus cheapest, no need for central node
  - But what about management cost?
- Length of cable
  - Bus uses shortest cable, but how expensive is cable anyhow?
- Efficiency
  - Star topology easies to add new nodes
  - Manage existing infrastructure
- Cable type
  - Most common cable is twisted pair, most often used with star topologies

Communications Media

- Before we get into how networks work
- We need to look at how they can talk to each other
- These are the physical devices a computer uses to talk to others on a network
- Each type of media has their own strengths and weaknesses
- E.g.
  - Possibility of electronic interference
  - Length of cable/signal strength before it degrades
  - Cost to install and maintain
- No “one size fits all” solution

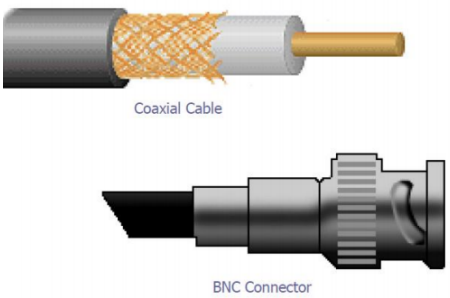
Unshielded Twisted Pair

- Cable has 4 pairs of wires, twisted in pairs
- UTP can be telephone grade to high speed cable
- 5 categories
  - 1 voice only
  - 2 Data up to 4 Mbps
  - 3 Data up to 10 Mbps
  - 4 Data up to 20 Mbps
  - 5 Data up to 100 Mbps
- Can be susceptible to radio and electrical interference.
- Shielded Twisted Pair exists, but extra shielding makes it bulky



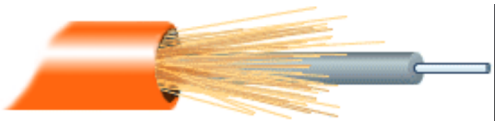
Coaxial Cable

- Like your TV cable at home
- Single copper conductor at centre with plastic layer providing insulation between conductor and braided metal shield.
- Shield prevents interference
- Supports longer cable length the UTP (Twisted Pair)
- Thin coaxial (10Base2)
- Max segment length 185M
- Thick coaxial (10Base5)
- Max segment length 500M

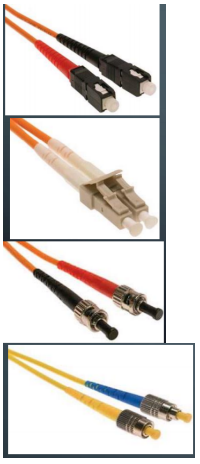


Fibre Optics

- Centre glass core surrounded by layers of protection
- Transmits light rather than electrical signals
- Not susceptible to electrical interference
- Capable of transmitting data over longer distances and at higher speeds than coaxial and TP
- 10BaseF
- Outer coating is made from Teflon or PVC
- Plastic helps cushion glass core
- Kevlar around plastic strengthens cable and prevents breakage
- From a security perspective, one of the great advantages of fibre networks is that they do not radiate any electromagnetic signals
- There is a prevalent myth that fibre networks cannot be tapped: with physical access to the cable, they can
- However, it is considered impossible to tap an optical cable without introducing a detectable increase in attenuation.
- A secure system should continuously monitor received optical signal strength and should alert on any abrupt change



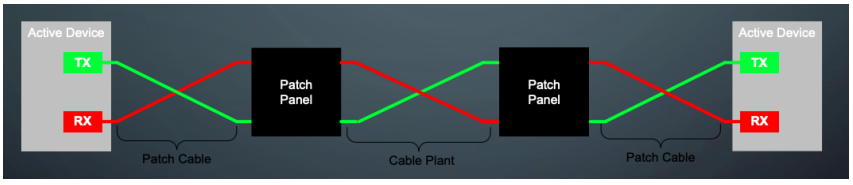
Fibre Connectors



- SC – In widespread use. Used on the original Gigabit Ethernet GBICs
- LC – Used in newer cabling installations. Used on new small form factor (SFP) GBICs
- ST – "Bayonet" mount, often used on older fibre installations
- FC – Screw mount. Only ever found on carrier-grade equipment (and usually with higher-powered lasers…don't look into these)

Patch Panels

- Fibre within or between buildings are typically terminated on patch panels like these
- Fibre patch cables are used to link active equipment to the patch panels
- In order to ensure that Transmit is always connected to Receive in each direction, patch leads and internal cable plant are always (supposed to be) crossed over this means that you can use a patch cable on its own to link two physically adjacent devices



Laser Safety

- Lasers are categorised into various classes according to the amount of optical power they emit.
- It is important to know what these mean:
- Class 1
    - The output power is below the level at which it is believed eye damage will occur.
    - Exposure to the beam of a Class 1 laser will not result in eye injury and may therefore be considered safe
- Class 2
    - A person receiving an eye exposure from a Class 2 laser beam, either accidentally or as a result of someone else's deliberate action (misuse) will be protected from injury by their own natural aversion response
- Class 3R
    - The laser beams from these products exceed the maximum permissible exposure for accidental viewing and can potentially cause eye injuries, but the actual risk of injury following a short, accidental exposure, is still small.
- Class 3B
    - Class 3B lasers may have sufficient power to cause an eye injury, both from the direct beam and from reflections.
- Class 4
    - Have an output power greater than 500 mW (half a watt).
    - There is no upper restriction on output power.
    - Capable of causing injury to both the eye and skin and will also present a fire hazard if sufficiently high output powers are used.
- In “enterprise” communications equipment, lasers more powerful than Class1 are rarely encountered (but always check !).
- Class 3 lasers are sometimes encountered in long-haul, DWDM carrier networks.

Radio

- Wireless LAN
- No cables
- High frequency radio signals
- Each workstation has a transceiver / antenna
- Also includes mobile phone technology, microwave transmission, satellite for longer distances
- Expensive, history of poor security (now down to ignorance, strong encryption available now),
- Susceptible to interference
- More on this later

CA169: Week 2

Encoding, Transmission Errors and Protocols

Recap from week 1

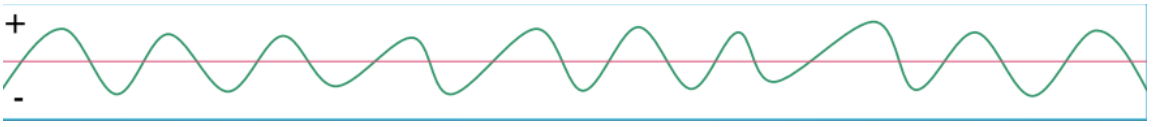
- Last week we looked at the physical ways we can transmit data
    - Unshielded Twisted pair (Phone & Ethernet)
    - Coaxial (Aerial TV, fibre to home)
    - Fibre optics (Fibre internet)
    - Radio
        - Bluetooth
        - Wifi
        - NFC

Transmission & Encoding

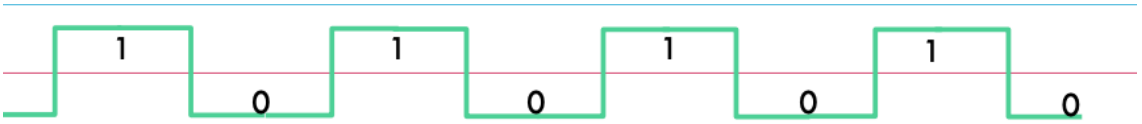
- How do we get 1's and 0's from electrical signals?
    - Encoding
- How do we deal with errors from these signals ?
    - Checksums

Analog v Digital

- Physical cables deal with voltage
- Digital systems prefer binary (1's and 0's)
- Our goal is to turn a signal from a line (analog) into a signal a computer can understand (digital)
- Essentially, turn this:



- Into this:



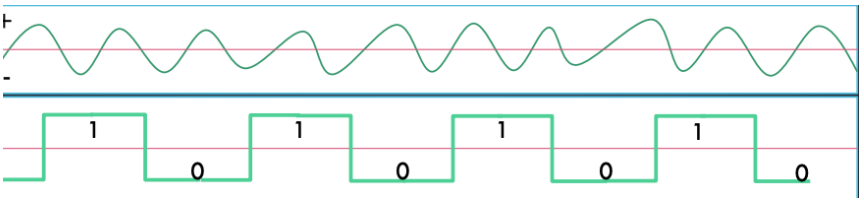
- This problem is harder than it seems
- What about a weak signal

- Or a signal with a lot of interference?

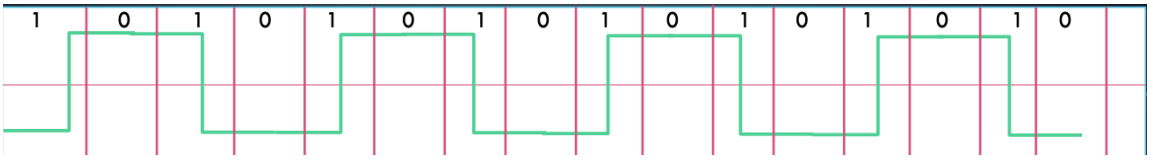
- We use an encoding algorithm
- There is no one size fits all solution
    - But some are better than others
- There are a number of factors to consider when choosing one
    - Physical medium (ethernet, wifi etc…)
    - Distance
    - voltage

Algorithm 1: NRZ-L & NRZ - I

- Non Return Zero Level (NRZ-L) is an encoding scheme where high voltage becomes a 1 and low voltage becomes 0
- This is used for short connections (e.g. to a printer)



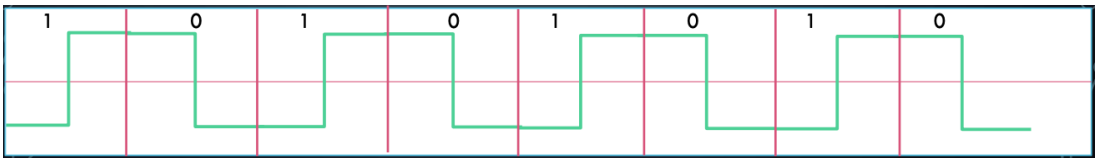
- Non Return Zero Inverted (NRZ-I) doesn't work off high-low voltage
- It looks at the transitions between positive and negative voltage
- If there is a transition, we use 1
- If there is no transition, we use 0



- Which to choose?
  - NRZ-I can deal with noise better
  - It is easier to check if voltage went from – to +
  - Than to say "if voltage >5"
  - Problem
  - What if I wanted to send the data 111111111

Clock Information

- So we clearly have to introduce a time component (clock)
- Manchester encoding does this
- We cut our signal into segments (based on time)
- We call this Biphase
- If we go from + to – we use a 0
- IF we go from – to + we use a 1



Why Manchester Encoding

- More difficult to operate
- More resistant to noise
- Requires twice as much bandwidth to send the same data as other methods
- But much more reliable

\4B/5B Coding

- 50% more efficient than Manchester (we use it in 100Mb internet)
- Take four bits from signal
- Encode them as 5 bits (we call this a cell)

Data		4B5B code
(Hex)	(Binary)	
0	0000	11110
1	0001	01001
2	0010	10100
3	0011	10101
4	0100	01010
5	0101	01011
6	0110	01110
7	0111	01111

- By mapping 4 bits onto 5 bits we have better control over the data
- This makes it more resistant to noise
- If there are only 4 bits, there are 16 possible frames (2^4)
- In short, we have a much more reliable signal

Modems

- This process of converting from analog to digital (and back again) is called modulation
- In the real world we use MODEMs to do this
- MODEM is short for:
    - MOdulator
    - DEModulator

Transmission Errors

- We know how to convert our analog signal into a digital one
- But how do we know we converted it right?
- A number of factors can influence our transmission
- We call these noise
- Noise can come in many forms
    - Electrical interference
    - Walls
    - Long distance

How to Tell if Data is Incorrect

- How can we tell if our data is incorrect?
- By adding extra check bits onto the end of our transmission
- And doing a bit of maths

Cyclic Redundancy Code (CRC)

- Error detecting codes
- Not error correcting codes
- Idea: represent binary as a polynomial

F = 110001

F(x) =$(x^5 * 1) + (x^4 * 1) + (x^3 * 0) + (x^2 * 0) + (x^1 * 0) + (x 0 * 1)$

F(x) = $x\ 5^+\ x^4 + 0 + 0 + 0 + x^0$

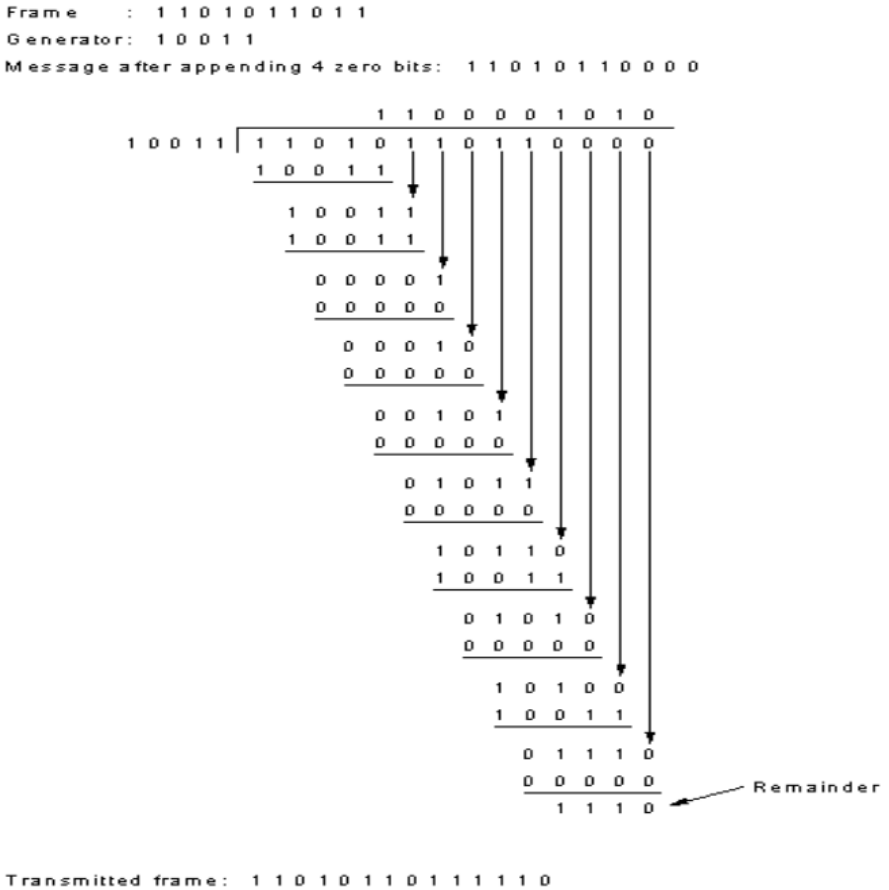
F(x) = $x\ 5^+\ x^4 + x 0$

F(x) = $x\ 5^+\ x^4 + x^0$

CRC Algorithm

- Compare using Modulo 2 arithmetic (x%2)
    - This is the same as the XOR operation ⊕
- Sender & receiver agree on G(x) generator polynomial.
- Append R 0 bits to M(x), the message, where R is the degree of G(x), this yields
- $x^R * M(x)$
- Divide G(x) into $x^R * M(x)$.
- Add reminder to $x^R * M(x)$, result T(x)
- Example

    M(x) = 1101 0110 11
    $x^R * M(x)$ = 1101 0110 1100 00
    G(x) = 10011 or x 4 + x1 + x0
    Remainder should be 1110
    T(x) transmitted message should be
    1101 0110 11 1110
    This will be evenly divisible by G(x) !



- Standard CRCS
    - CRC-12
        - $x^{12} + x^{11} + x^3 + x^2 + x + 1$
    - CRC-16
        - $x^{16} + x^{15} + x^2 + 1$
    - CRC-CCITT
        - $x^{16} + x^{12} + x^5 + 1$
    - CRC-32
        - $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

How Data is Transmitted

- I want to send a document to another device
- This document is converted into 1's and 0's
- It is sent to the other device
- The other device then converts the 1's and 0's back into the documen

IRL

- In reality, this is much harder
- The document isn't converted into one long stream of 1's and 0's
- It is broken down into packets/frames of information
- These packets are then sent to the other device
- Each packet contains only one part of the document
- Why do we do this?
    - If we sent the entire document in one go
    - We can't handle sending multiple things at once (multiplexing)
    - Your computer sends a lot of information at once all the time
    - See netstat
- What's the problem?
    - How do we tell when one packet/frame ends and another begins?
    - We call this the framing problem

Possible Solutions to the Framing Problem

- Time delay:
    - Every 1 second send a new packet
    - Data may be lost if signal is interrupted, or a delay in transmission
- What if we include the length of the packet at the end
    - Add on another bit to the CRC
    - If the count is corrupted, we would never know how long our data is

Actual Solution

- At the start and end of our packet we add in special markers
    - We call this character stuffing
- DLE STX (meaning start of packet)
    - Lets pretend this is: 1001 in binary
- DLE ETX (end of packet)
    - Lets pretend this is 0110 in binary

Examples

- If I want to send 11010101 to another computer
    - We add on our DLE STX to the start
        - 100111010101
    - Then we add on our DLE ETX to the end
        - 1001110101010110
- The computer we are sending the data to knows that a start packet is 1001 and an end packet is 0110
- When it gets this data it removes them
- This leaves us with our original data

Double Stuffing Example

- If I want to send the data 110101011001010
- Find bits that match STX or ETX 110101011001010
- Duplicate them 1101010110011001010
- Now add on the STX and ETX to the packet
- 100111010101100110010100110
- If we see a duplicated pattern, only remove one of them!

What Does Protocol Mean

- We now know how to change data from signals into nice 1's and 0's
- We can also be sure that the data we sent is correct
- But there are a number of questions we still have to answer
- What do we do if we do get an error?
- How do we signal that we have finished sending data?

Need for Protocols

- Protocols dictate how we communicate
- They control
    - Data format
    - Data content Timing/synchronisation of communication
    - How the communication is managed

Why Use Protocols

- In networking a protocol is like a language
- It provides a common way of devices to understand each other
- There is no magic
- They are designed by programmers
- They are only useful if they are widely adopted
- They are refined through trial and error

Making a Protocol

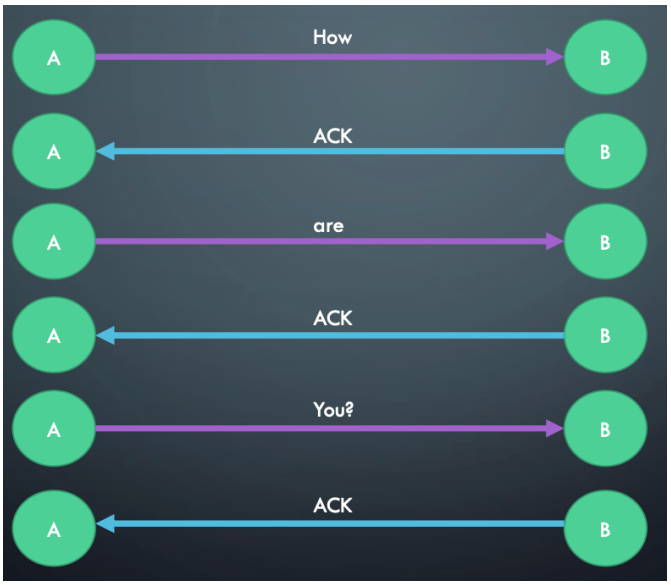
- Lets first make some assumptions:
    - Transmission will be simplex (only one computer can speak at a time)
    - Computers are always ready to receive data
    - Processing time is negligible and we have unlimited space
    - Our physical medium is error free!

Utopia Protocol

- Make all assumptions, a, b, c, d.
- For this protocol the control header and checksum are unnecessary.
- The transmitting host simply takes packets from host A (which always has one ready) and pumps them as fast as it can onto the physical link.
- The receiver accepts the frames and passes them straight to host B

Stop & Wait

- The UTOPIA protocol is nice but…
- Processing time is not negligible, and we do not have infinite space
- So we drop assumption c
- In practice the receiving computer needs time to process the packets
- Only has a fixed amount of space to store incoming packets for processing
- The receiver needs a way to prevent it from getting more data then it can handle
- When the receiver processes a packet, it sends one back requesting more data (we'll call this a control frame)
- Only after receiving this control frame will the sender fetch and transmit the next packet
- E.g Let's send the data "How are you"?



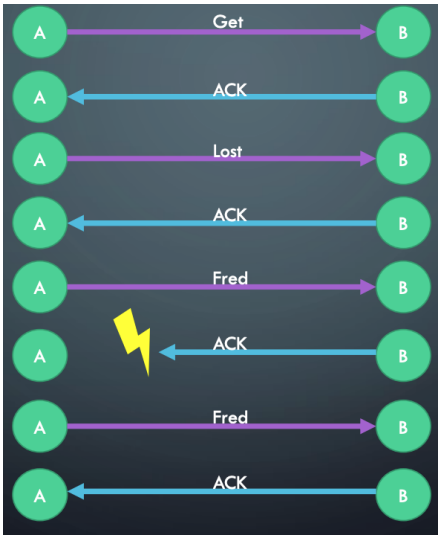
- Issues?
    - Can anyone see any problem with this method?
    - What about a failed transmission?

Positive Acknowledgement With Retransmission (PAR)

- Noisy channel simplex protocol: drop some assumptions
    - c) [processing time, buffers pace] and
    - d) [error free link]
- With error prone physical link, frames may be either damaged or lost completely.
- However,
    - Damaged frames can be detected by the checksum.
    - Lost frames will not be acknowledged.
    - Eventually the sender will tire of waiting for an acknowledgement, timeout, and retransmit the frame.
- Same as Stop-and-Wait, except that
    - damaged frames are not acknowledged,
    - causing a timeout and subsequent retransmission

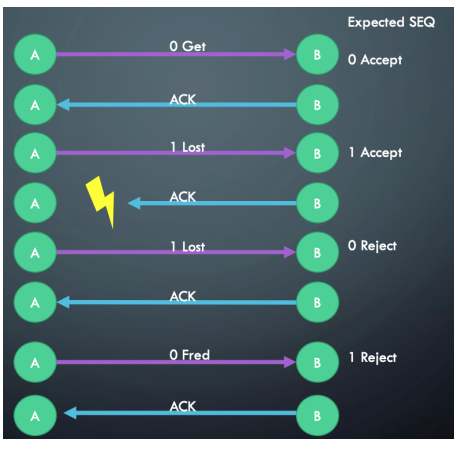
Examining Another Protocol

- Suppose the message “Get Lost Fred” is being sent from A to B, one word per packet



- What happened?
- B receives “Get lost Fred Fred” and the protocol has failed !
- Basically what has happened is that the receiver has accepted a duplicate frame.
- The solution is to use SEQ, a sequence number in the control header to differentiate between frames and allow duplicates to be discarded.
- As a frame must be acknowledged before the next one is sent, a one-bit sequence number [0,1] is sufficient.
- The receiver will expect alternatively numbered frames (0 1 0 1 0 1 ... etc.).
- Any frame with the wrong sequence number is rejected as a duplicate
    - (but still acknowledged).

- What about time outs



Timesouts

- The message “Get Lost” is received and the protocol has failed

Solution

- Include in the ACK field of the acknowledgement control frame the SEQ number of the last frame received without error.
- Then if this number (0 or 1) differs from the transmitted frame, the sender transmits it again.
- The resulting PAR simplex protocol will now work in the face of any combination of
    - garbled frames,
    - lost frames and
    - premature timeouts.

Summary

- After transmitting a frame and starting the timer, Host A waits for a response.
- There are three possibilities:
    - 1. an acknowledgement frame arrives undamaged
    - 2. a damaged acknowledgement arrives, or
    - 3. the timer goes off.
- If a valid ACK comes in, A fetches the next packet and puts it in the buffer
    - overwriting the previous packet, and advancing the sequence number.
- If a damaged frame arrives or no frame at all arrives,
    - neither a buffer nor the sequence number are changed, so that a duplicate can be sent

Bi-Directional PAR

- The control header of all frames contains the three fields KIND, SEQ and ACK.
- Sending data packets/acknowledgements in both directions is no problem –
    - by looking at the KIND bit in the header, the receiver knows which it is dealing with.
- However, this would be inefficient.
- Consider an Host B which is about to acknowledge a data frame received from
- Host A, and also about to send off a data frame to A.
- Instead of sending two frames, the acknowledgement can hitch a lift on the data frame, using the ACK field in the header.
- This is called piggybacking.
- As we are still making assumption b)
- [Transmitting and receiving hosts always ready to transmit & receive data]
- All acknowledgements can be piggybacked. Thus, data packets are bounced back and forth between A and B.
- Notes:
    - For the protocols considered so far, only one frame is in the wire at any one time.
    - The sender needs to keep a copy of each frame in a buffer for possible retransmission until the frame has been successfully acknowledged.
- Assumption b)
- [Transmitting and receiving hosts always ready to transmit & receive data]
- Easily dealt with.
    - If there is no outgoing data frame, the host will wait a short while to see if one comes along to provide a piggyback.
    - If not, a separate acknowledgement frame will be sent.
    - It must not wait too long to avoid unnecessary duplicates being sent due to the sender timing-out.
- Up until now, lost and damaged frames have been dealt with in the same way.
- No ACK is sent, leading to timeout and retransmission.
- The timeout period is usually set quite long in order to avoid complications caused by premature timeout.
- This is inefficient, as while the timeout is expiring, the link is not being used.
- A partial solution is NAK, a negative acknowledgement.
- This is sent immediately a damaged frame is received and elicits immediate retransmission.
- The NAK may also be piggybacked.
- If the NAK is damaged, no harm is done as the sender will eventually timeout and retransmit as before.
- A damaged frame is Nak'd only once.

Pipelining

- When propagation delay is not negligible, these previous methods are wasteful of bandwidth.
- The solution is to 'fill up the pipe'.
- However, doing this entails sending off frames before ACKs for previous frames have arrived.

Sliding Window Protocol

- Each outbound frame is given a sequence number in the range of 2^n-1 using an n-bit field, e.g. if n=1, then range is 0.....1 as in ABP or PAR protocols.
- Both sender and receiver keep windows informing them of which frames can be validly sent and which validly received.

Rules

- Sender :- The upper edge of sender is advanced when a frame is sent (up to max. window size).
- The lower edge advanced when ACK received for lowest numbered frame in the window.
- Receiver :- Both edges are advanced when the lowest numbered frame in window is correctly received and ACK sent.

Notes

- Buffering requirements at both sender and receiver depend on the size of the sending and receiving windows respectively.
- Each transmitted frame has its own separate timeout clock.
- In these protocols, an acknowledgement for frame N is accepted as acknowledging all transmitted frames numbered up to N (counting circularly).
- Thus, if ACK(0) and ACK(1) were both destroyed, but ACK(2) now arrives, it implicitly acknowledges 0 and 1 also.

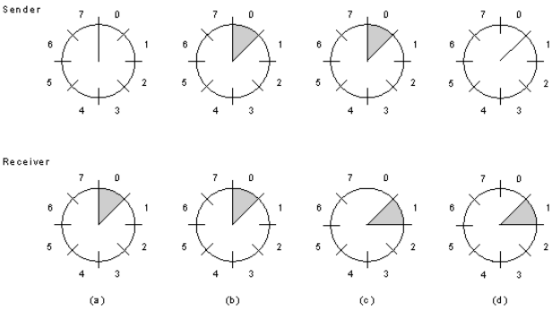
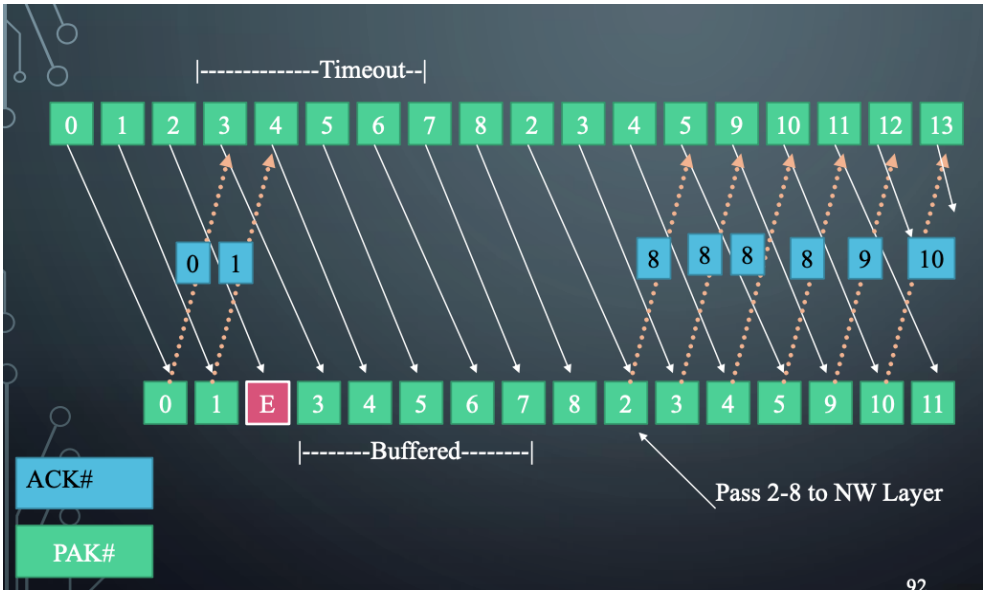


Fig. 3-12. A sliding window of size 1, with a 3-bit sequence number. (a) Initially. (b) After the first frame has been sent. (c) After the first frame has been received. (d) After the first acknowledgement has been received.

Session With Recovery



Stopping the Problem

- A Data-Link cannot be stopped.
- Consider a session termination.
- Neither terminal knows that other has sent last packet, the last packet must be ACK'd.
- In practice the data-link is dropped after the link is sensed as being dead for a prolonged period

CA169: Week 3

Layered Architectures, OSI & TCP/IP

The Need for a Layered Architecture

- Think about everything that has to happen when you load a webpage
- There are a lot of parts at play
    - Chrome
    - Operating System
    - LAN/Wifi
    - The internet
    - Servers

Layered Architecture

- To accomplish all of this we break the problem into different parts
- E.g. your network card turns 1's and 0's into something understandable
- Your router knows where it needs to send your requests to
- Chrome knows how to load and display a webpage
- We call this setup a layered architecture
- The bottom layer is the 1's and 0's
- The top layer is a webpage
- And there are many parts in-between
- In networking there are two main architectures you need to know
- OSI (Opsn Systems Interconnection) Model
- TCP/IP Model
- One is real the other is theoretical

OSI

- OSI is not real
- It is more a blueprint on how to build a network architecture from scratch
- There are 7 layers to the OSI model
- These will be on your exam !
- (They also come up in job interviews!)

OSI Model

7. Application Layer (Top Layer)
6. Presentation Layer
5. Session Layer
4. Transport Layer
3. Network Layer
2. Data Link Layer
1. Physical Layer (Bottom Layer)

OSI Application Layer

- Represents the level at which applications access network services.
- This layer represents the services that directly support applications such as software for file transfers, database access, electronic mail.
- TLDR; Applications that use the web; chrome, mobile apps etc…

OSI Presentation Layer

- Translates data from the Application layer into an intermediary format.
- This layer also manages security issues by providing services such as data encryption.
- It also provides compressed data so that fewer bits need to be transferred on the network.

OSI Session Layer

- Allows two applications on different computers to establish, use, and end a session.
- This layer establishes dialog control between the two computers in a session, regulating which side transmits, plus when and how long it transmits

OSI Transport Layer

- Handles error recognition and recovery.
- Repackages long messages when necessary into small packets for transmission and, at the receiving end, rebuilds packets into the original message.
- The receiving Transport layer also sends receipt acknowledgments.

OSI Network Layer

- Addresses messages and translates logical addresses and names into physical addresses.
- It also determines the route from the source to the destination computer
- Manages traffic problems, such as switching, routing, and controlling the congestion of data packets.

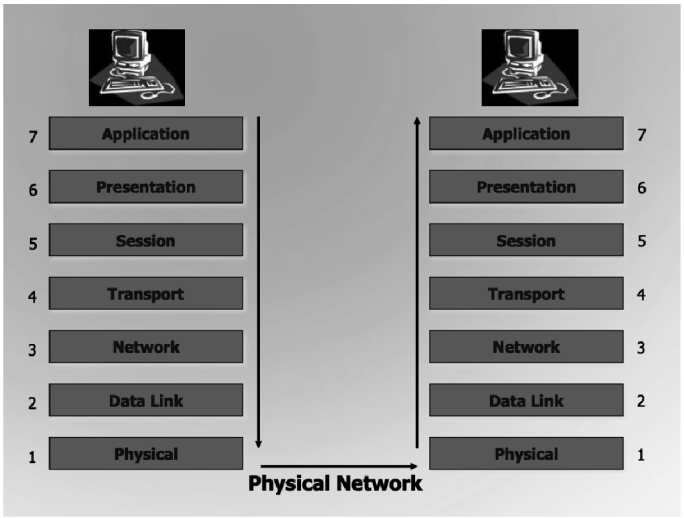
OSI Data Link Layer

- Packages raw bits from the Physical layer into frames (logical, structured packets for data).
- This layer is responsible for transferring frames from one computer to another, without errors.
- After sending a frame, it waits for an acknowledgment from the receiving computer

OSI Physical Layer

- Transmits bits from one computer to another and regulates the transmission of a stream of bits over a physical medium.
- This layer defines how the cable is attached to the network adapter and what transmission technique is used to send data over the cable.
- TLDR: What we covered last week!

OSI Model



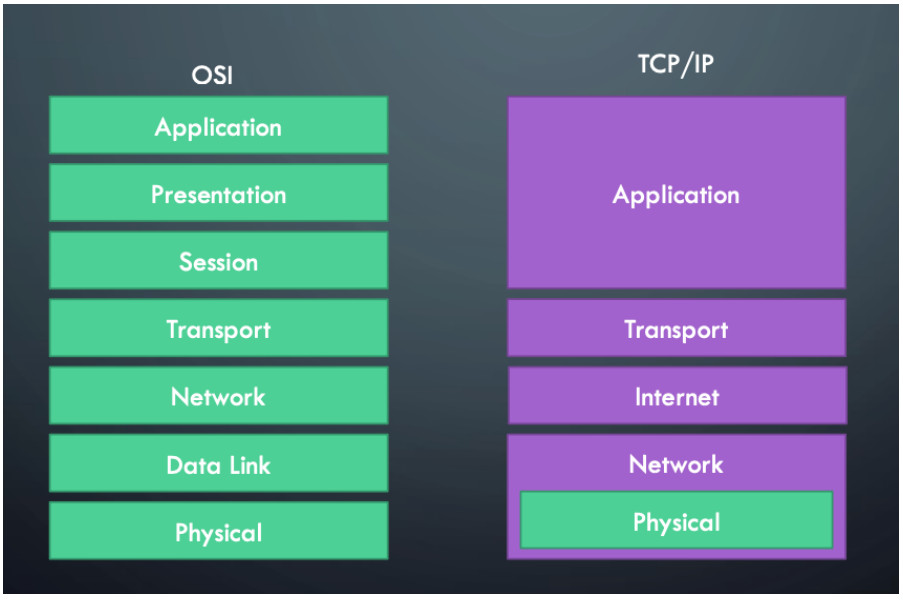
OSI Summed Up

- 7 Layers
- Guidebook on how to build a network from
- scratch
- Not real !
- Will be on your exam !

TCP/IP

- OSI is a theoretical architecture for building a network
- TCP/IP is the real version
- TCP/IP is how the internet works
- The OSI model has 7 layers
- The TCP/IP model has 5 layers
- This is because some layers in the TCP/IP model can do the work of two layers in the OSI model
-

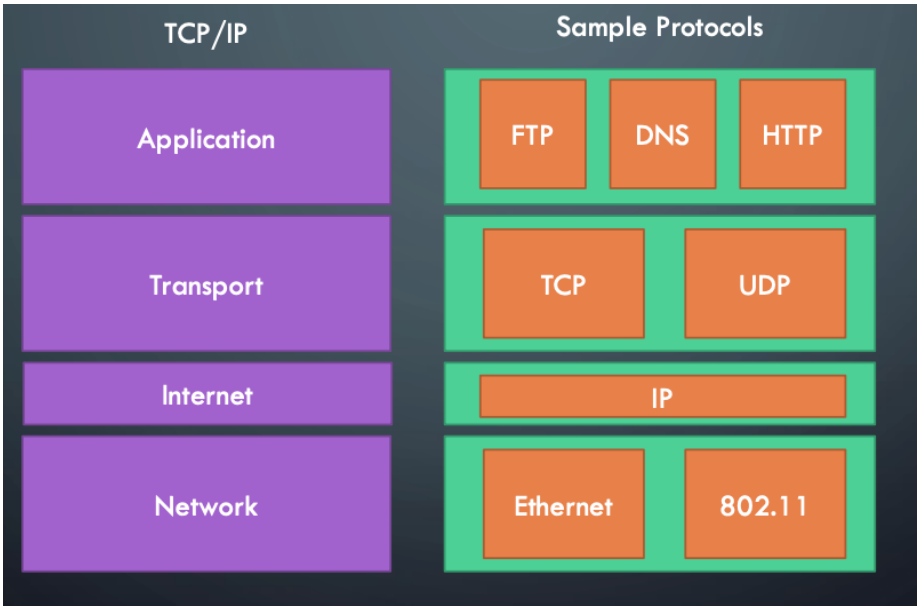
TCP/IP v OSI



TCP/IP & OSI

- Transmission Control Protocol / Internet Protocol (TCP/IP) is the protocol on which the Internet is based upon.
- It has five layers and they are related to the OSI model.
- Information is transmitted around the Internet in packets.
- These packets contain among other things the destination and source addresses of the packet and the data
- The protocol used is TCP/IP.
- Internet Protocol is protocol, which sends packets around the Internet.
- TCP sits on top of IP and it guarantees reliable delivery of packets for applications such as FTP and Telnet.
- An end-to-end connection is open for the delivery session between two applications

TCP/IP Family



Why Have Two Models

- OSI concepts
  - Services (definition)
  - Interfaces (how to access)
  - Protocols (peer protocols, private)
- Kind of OO approach, encapsulation.
- Prescriptive & Descriptive origins
  - Simple services, interfaces, protocols

OSI - TCP/IP Physical & Network Layers

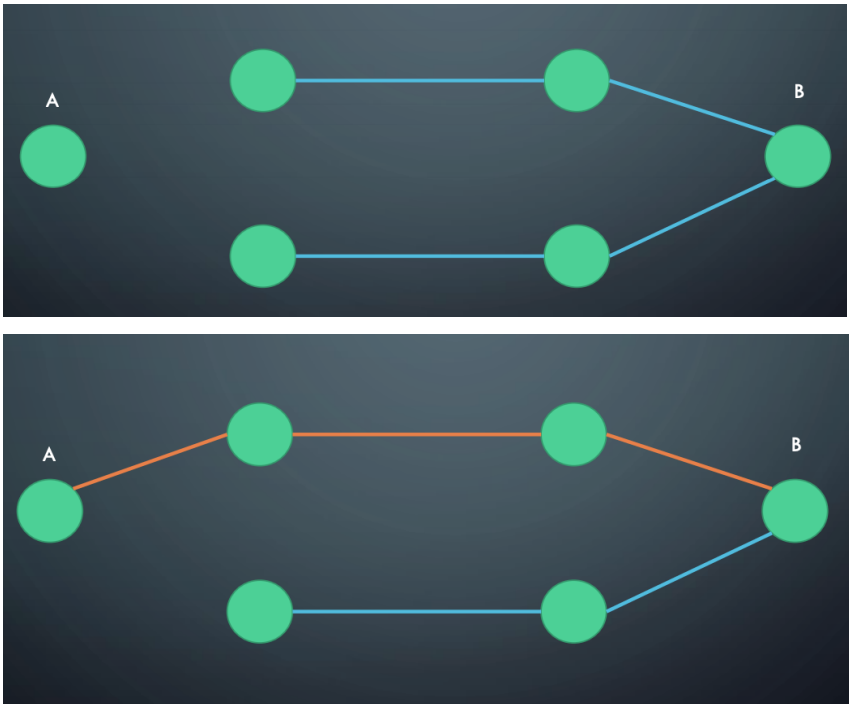
- Last week we looked at how we can transmit data
- We learned how modems turn electrical signals into digital and vice versa
- We looked at how we can detect errors, and why we need protocols
- Finally we looked at the sliding window solution for packets arriving out of order
- Now we are going to examine how a packet travels across the internet
- We will look at real world physical and network layer protocols
- 802.3 LAN
- 802.11 WiFi

Switching

- When you send a packet across a network, how does it actually get to its destination
- This process is called switching
- There are three kinds of switching:
    - Circuit Switching
    - Message Switching
    - Packet Switching

Circuit Switching

- Like old fashioned terrestrial telephone system.
- Try to form dedicated physical path from source to destination.
- Path remains dedicated until session is terminated.
- Not typical operation of bursty comms.



Message Switching

- No physical path established.
- Large bursts of data transmitted from sender to receiver.
- Each burst stored and forwarded from host to host throughout network.
- No limit to burst size, may encounter memory\buffering and link availability problems.
- Not really used anymore
- Data is sent as one large “chunk” across the network
- Used in older technologies
    - E.g. telegrams, teletype

Packet Switching

- Upper limit set on size of blocks to be transmitted.
- Ideal for bursty computer communications.
- May utilise pipelining to improve throughput.
- Large packet size will emulate message switching, small emulates circuit switching.

Packet vs Circuit Switching

Item	Circuit Switched	Packet-Switched
Call Setup	Required	No
Dedicated Physical Path	Yes	No
Each packet follows same route	Yes	No
Packets arrive in order	Yes	No
Is crash fatal?	Yes	No
Bandwidth Available	Fixed	Dynamic
When can congestion occur	During Setup	On every packet
Potentially wasted bandwidth	Yes	No
Store and forward information	No	Yes
Transparency	Yes	No
Charging	Yes	No

Local Area Networks and 802

- IEEE formulated 802 standard for LAN.
- ITU (CCITT) adopted 802 as 8802
- Common media types are UTP and Co-axial cable.
- Topologies may be Ring\ Bus\ Star or Wireless.

802 Organisation

- Layered within the Data-link and Physical layers of OSI protocol stack.
- Composed of
    - Physical Medium Dependent (PMD) layer.
    - Medium Access Control (MAC) layer.
    - Logic Link Control (LLC) layer.

802 Standards

• 802.2 LLC (HDLC based)
• 802.3 CSMA/CD Bus (Ethernet)
• 802.4 Token Bus
• 802.5 Token Ring
• 802.6 DQDB
• 802.7 Broadband LAN using Coaxial Cable (disbanded)
• 802.8 Fiber Optic TAG (disbanded)
• 802.9 Integrated Services LAN (disbanded)
• 802.10 Interoperable LAN Security (disbanded)
• 802.11 WiFi
• 802.12 demand priority (disbanded)
• 802.13 Not used (officially)
• 802.13ah Defines "Copper for the first mile" for Metro Area Networks (proposed)
• 802.14 Cable modems (disbanded)
• 802.15 Wireless PAN
• 802.15.1 Bluetooth certification
• 802.15.2 coexistance of 802.15 and 802.11
• 802.15.1 (Bluetooth certification)
• 802.15.4 (ZigBee certification)
• 802.16 Broadband Wireless Access (WiMAX certification)
• 802.16e (Mobile) Broadband Wireless Access
• 802.16.1 Local Multipoint Distribution Service
• 802.17 Resilient packet ring
• 802.18 Radio Regulatory TAG
• 802.19 Coexistence TAG
• 802.20 Mobile Broadband Wireless Access
• 802.21 Media Independent Handoff
• 802.22 Wireless Regional Area Network

Ethernet Networks 802.3

- May operate over several cable types.
- 10 Base 2 Thin wire coax, bus topology.
- 10 Base 5 Thick wire coax, bus topology.
- 10 Base T Twisted pair, star topology.
- 10 Base F Optical fibre, star topology.
- 100BASE-TX fast Ethernet over 100Mbps 802.3u
- 1000BASE-T Gbit/s Ethernet over twisted pair
- Today many types of Gbps versions over fiber depending on type of lasers used.

Ethernet Uses MAC Addresses

- 48 bit unique identifier
- Tied to a network card
- Written in hexadecimal
- Written as: D4-3B-04-1F-AD-88

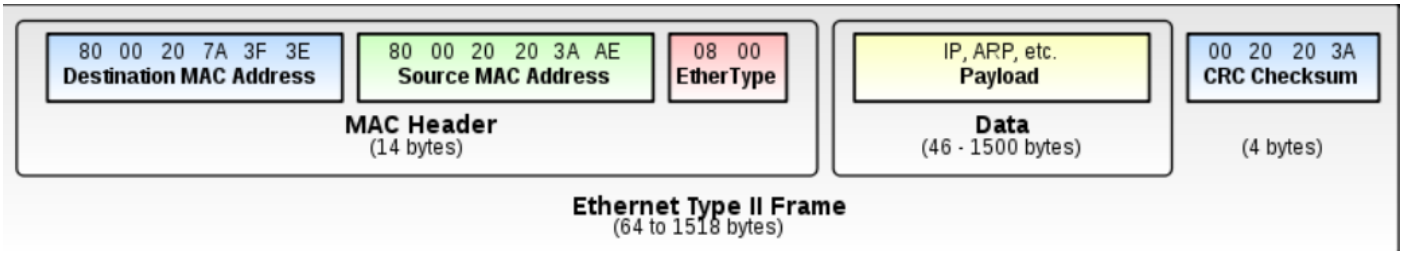
802 Frame Format

Preamble	SD	Dest Addr	Src Addr	LD	Data	Pad	CRC

- Preamble (7 bytes): Sine wave, clock synch.
- SFD – Start Frame Delimiter (1 byte): 10101011 denoted.
- Dest Addr: 6 byte unique 802 address.
- Src Address: 6 byte address, 248 possible.
- LD: Size of payload.
- Data: Payload max 1500 bytes.
- Pad: Ensures min size of 64 bytes.
- CRC: As discussed previously.

Ethernet II or DIX Frames

- Defines the 2 octet Type field (LD previously), defining the upper layer protocol encapsulating the frame data
- 0x0800 indicates IP V4
- 0x0806 is ARP
- 0x06DD is IP V6
- Must be greater than 0x0600 (1,536 decimal, > 0x05DC or 150010 the max payload of Ethernet)



Coexistence of Ethernet & Etherent II

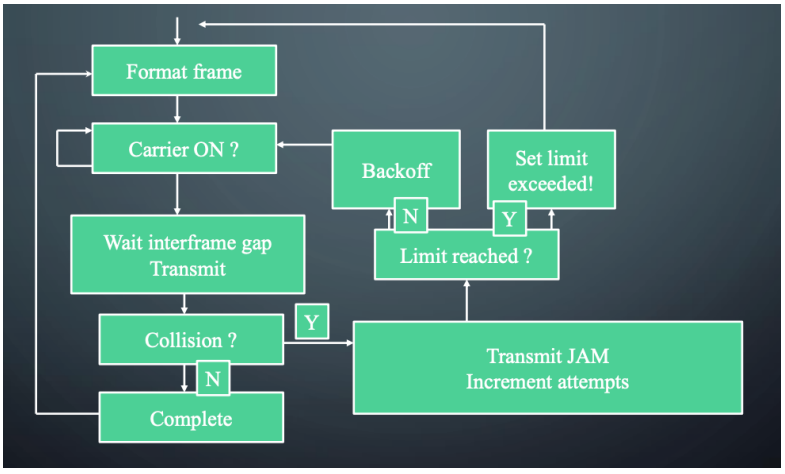
- Both types can exist on the same Ethernet network.
- Distinguish V1 and V2 by value in type field
- For V2, value in type field must be >=1,53610 or 0x600
- Maximum payload for Ethernet is 0x05DC or 1,50010
- For V1, value must be <= 150010 or 0x05DC

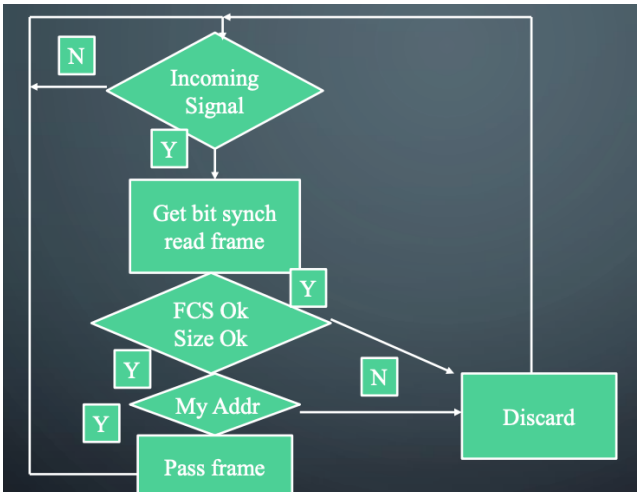
Ethernet II Types

- EtherType value
- 0x0800 signals that the frame contains an IPv4 datagram
- 0x0806 indicates an ARP frame,
- 0x8100 indicates an IEEE 802.1Q frame (Virtual Lan)
- 0x86DD indicates an IPv6 frame.

802.3 MAC

- Carrier Sense Multiple Access with Collision Detection CSMA\CD
- Allows multiple stations to share transmission medium.
- Senses carrier to see if medium is quiet.
- Be able to detect if another station is interfering by continuing to listen to carrier while transmitting.





Truncated Binary Exponential Backoff

- When collision is detected, two stations wish to transmit simultaneously.
- Need to prevent continuous collisions between this pair.
- Better to have graceful degradation of throughput.

Algorithm

- The number of slot times before the Nth retransmission attempt is chosen as a uniformly distributed random integer in the range
  - $0 \leq R \leq 2^k$
  - where K = min(N, backoff limit),
  - e.g. for a backoff limit of 20, possible ranges of K will be 0..2, 0..4, 0..8, 0..16, 0..20, 0..20, 0..20 for successive attempts at retransmission up to a maximum number of attempts.
- The backoff limit of 20 is imposed and prevents the series continuing 8, 16, 32, 64, etc, etc and thus the heuristic is called truncated binary exponential backoff.

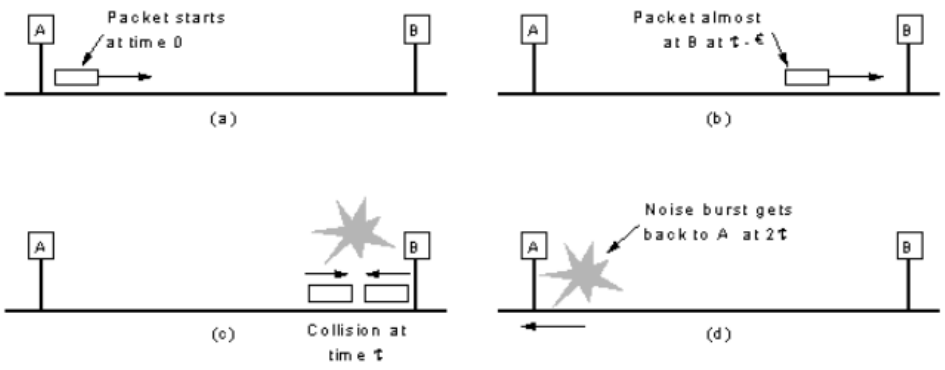
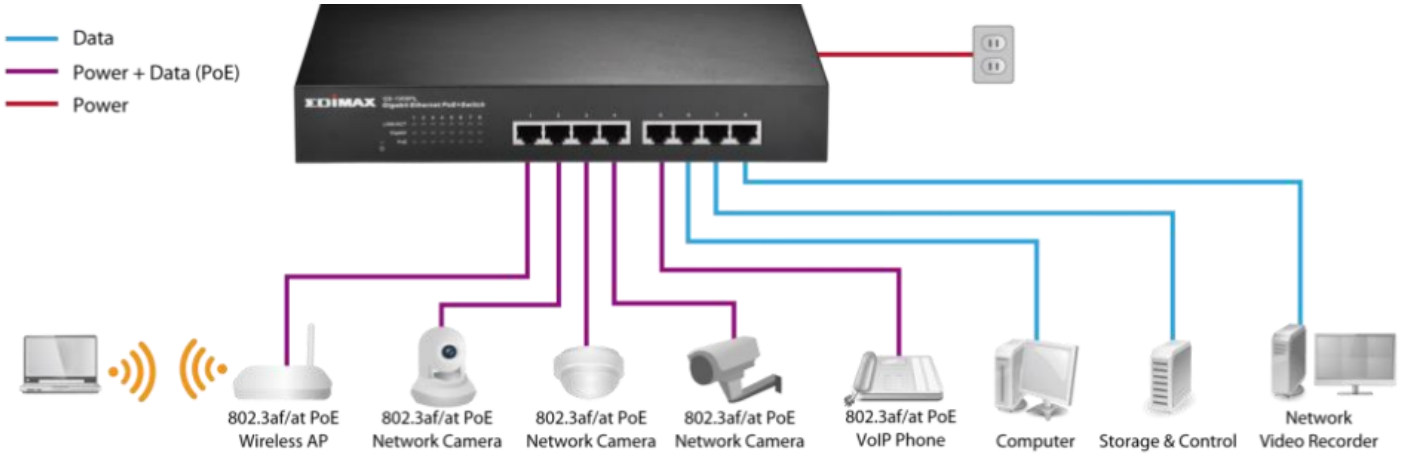


Fig. 4-22. Collision detection can take as long as 2τ.

802.3 Modern Implementations

- Most modern implementations of Ethernet use Switched Ethernet.
- There are almost no collisions
- Packet paths can cross over the switch without colliding, provided each “conversation” has no receivers in common
- Improved throughput and better utilisation

A Switch



CA169: Week 5

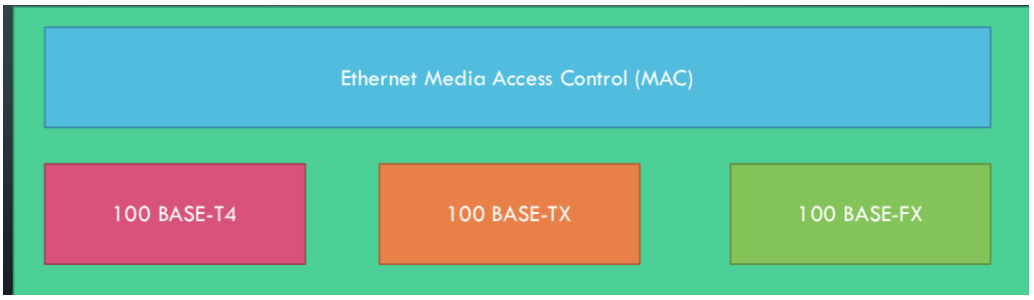
FAST Ethernet, Gigabit Ethernet & WIFI

FAST ETHERNET

-
-

FAST ETHERNET – CABLE STANDARD

- Originally Ethernet had a max speed of 10 Mbits/ second
    - 10 megabits every second
- This is pretty slow (4G LTE can reach ~50Mbits/s)
- A new standard for Ethernet in was introduced in 1995
- This standard (802.3u) can achieve speeds of 100Mbits/s
- This is called Fast Ethernet
- The only difference between Fast and normal internet is the speed
- The structure of the Frame, Payload and MAC are all the same
- If a Fast Ethernet card talks to a normal ethernet card
- The fast card changes its speed to accommodate the slower ethernet
- There are three cable standards for fast ethernet



100 BASE-TX

- This is the standard that is used today The others are basically obsolete
- 100 is the speed (100 Mbits/second)
- BASE – stands for baseband
- T4 – 4 pairs of Twisted Pair cables
- TX – 8 pairs of Twisted Pair cables
- FX – Fibre

ETHERNET COMPONENTS

- There are three main parts of an ethernet port • PHY (short for physical layer)
- MII (Media independent interface)
- Data Terminal Equipment (DTE)

ETHERNET PHY

- Short for physical layer
- A chip on an ethernet card used to implement the physical layer components
    - Analog-Digital
    - Allows the hardware to send/receive frames
- Does not handle addressing !

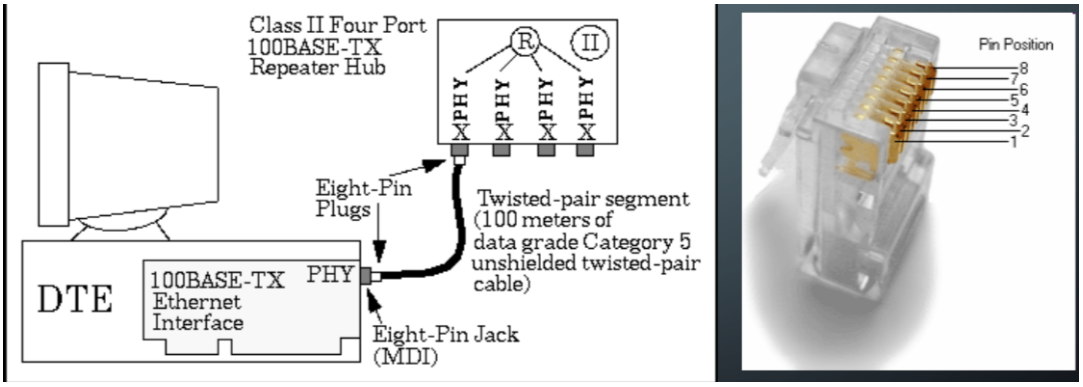
ETHERNET MII

- Media Independent Interface
- Interface to connect to fast ethernet
- Part of the ethernet standard
- Connects to the PHY chip
- Provides flexibility

DATA TERMINAL EQUIPMENT

- This constitutes the network card as a whole
- For ethernet this is layers 1 & 2 of the OSI model
- Physical (1's and 0's)
- Data Link

THE 100 BASE-TX SYSTEM



- 100BASE-TX system operates over two pairs of wires
- One pair for receive data signals and the other pair for transmit data signals.
- Most popular wiring is unshielded twisted-pair.
- The two wires in each pair of the cable must be twisted together for the entire length of the segment
- Must be kept twisted to within approximately 1/2 inch of any connector or wire termination point

100 BASE TX COMPONENTS

- Network Medium
- 100BASE-TX Repeaters
- 100BASE-TX Crossover Wiring
- 100BASE-TX Link Integrity Test

NETWORK MEDIUM

- Allows segments of up to 100 meters in length
- EIA/TIA standard recommends segment length 90 m between the wire termination equipment in the wiring closet, and the wall plate in the office
- This provides 10 m of cable allowance to accommodate patch cables at each end of the link
- Accommodate for signal losses in intermediate wire terminations on the link, etc.

NETWORK MEDIUM - PIN LAYOUT

TABLE 0.1 100BASE-TX eight-pin connector

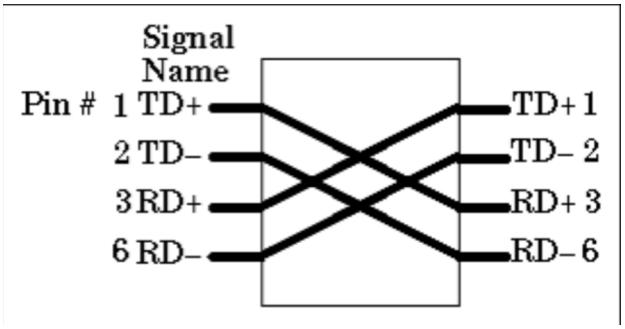
Pin Number	Signal
1	Transmit+
2	Transmit–
3	Receive+
4	Unused
5	Unused
6	Receive–
7	Unused
8	Unused

100 BASE TX-REPEATERS

- Two types of repeater: Class I and Class II.
- A Class I repeater allowed to have larger timing delays, and operates by translating line signals on an incoming port to digital form, and then retranslating them to line signals when sending them out on the other ports.
- Possible to repeat signal between media segments that use different signaling techniques, such as 100BASETX/ FX segments and 100BASE-T4 segments
- Class II repeaters:- restricted to smaller timing delays, and immediately repeats the incoming signal to all other ports without a translation process ;connect only to segment types that use the same signaling technique

100 BASE TX - CROSSOVER WIRING

- Wiring multiple segments in a building.
- Easier to wire cable connectors "straight through" do crossover wiring inside the repeater hub
- For single segment connecting 2 PCs, build special crossover cable
- transmit pins on eight-pin plug at one end wired to receive data pins on eight- pin plug at other end of crossover cable.



100 BASE TX - CONFIGURATION

- Connect the Ethernet interface in your computer to one end of the link segment, and the other end of the link segment is connected to the hub.
- That way you can attach as many link segments with their associated computers as you have hub ports, and the computers all communicate via the hub.

100 BASE-TX SEGMENT CONFIG GUIDELINES

100BASE-TX segment configuration guidelines

Maximum Segment Length		Maximum Number of MAUs	
100BASE-TX	100 m (328 ft.)[a]	Per Link Segment	2

a. 100BASE-TX segments are limited to a maximum of 100 m.

GIGABIT ETHERNET

- We first had ethernet which could handle 10Mbits/s
- The we had fast ethernet which could handle 100Mbits/s
- Now we have gigabit ethernet which can handle 1000 Mbits/s
- 1000 Mbit = 1 Gbit
- Why scale up more?
- New applications requiring more bandwith
- The explosion of the web
- Easy to migrate to

MIGRATION ISSUE – FRAME FORMATS

- Same variable length (64 to 1514 byte) frames
- Allows seamless integration
- No frame translation necessary
- Where to install the upgrade (desktop to switch to backbone) ?

PHYSICAL LAYER

- 1000 Base-X based on Fiber Channel Physical Layer (FCPL)
- Proven technology
- 1000 Base-SX :- 850 nm laser multimode
- 1000 Base-LX :- 1300 nm laser single and multimode laser
- 1000 Base-CX copper Shielded Twisted Pair
- 1000 Base-T:- long haul 4 pair category 5 UTP cable (802.3ab task force)

MAC LAYER – CARRIER EXTENSION

- 10 times faster than Fast Ethernet, 10m would be max slot size.... Problem
- Slot size of 1512 bytes employed, with pads.
- Carrier Extension allows longer distances
- Transparent to LLC (Logical Link Control)

CARRIER EXTENSION DIAGRAM

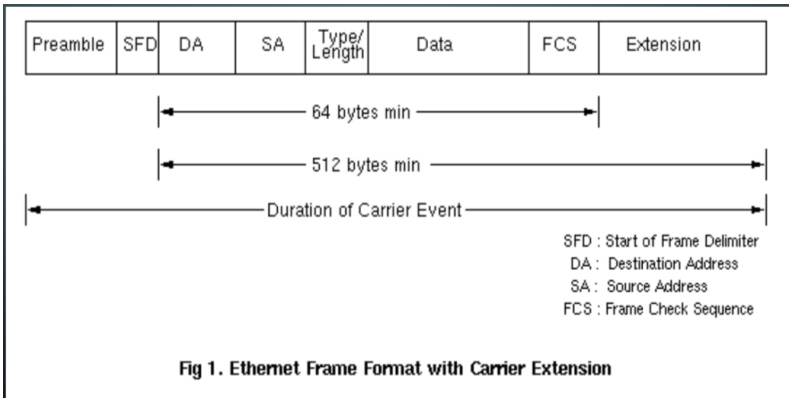


Fig 1. Ethernet Frame Format with Carrier Extension

MAC LAYER – PACKET BURSTING

- Carrier extension wastes bandwidth, with 448 pad bytes in small packets.
- For small packets, throughput only marginally better than fast Ethernet, 802.3X.... Problem !
- Solution:- extend the Carrier Extension
- Pad 1st packet to slot time (512 bytes), subsequent packets back to back with minimum inter-packet-gap until burst timer (1500 bytes) expires.

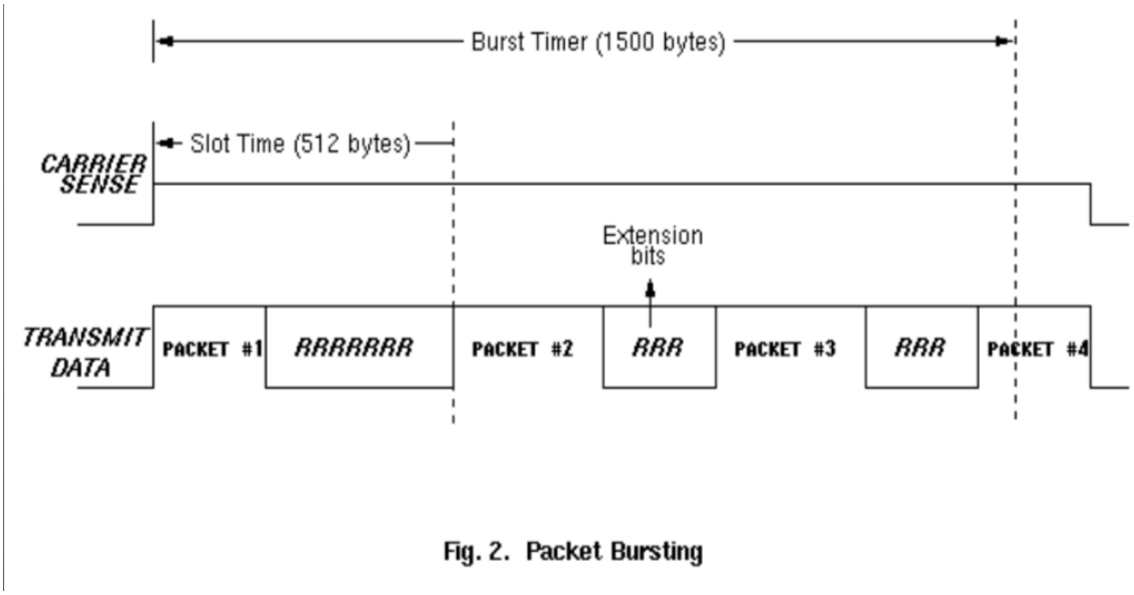
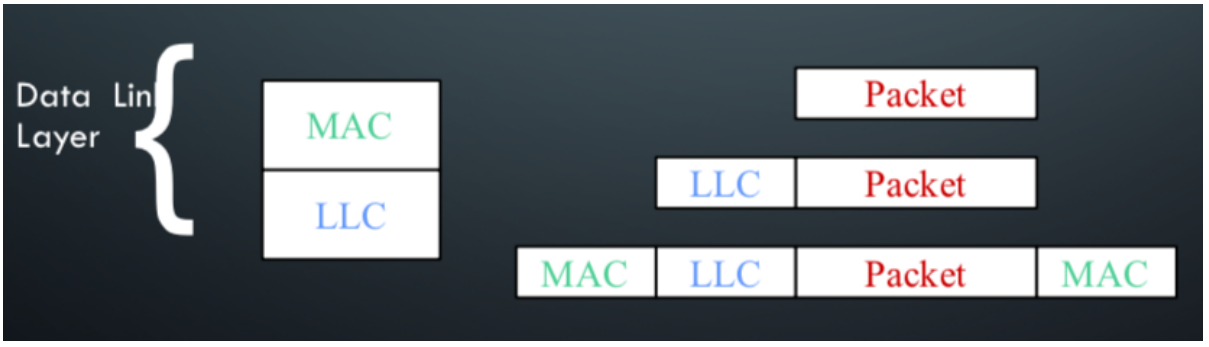


Fig. 2. Packet Bursting

ENCAPSULATION AND PROTOCOL HIERARCHIES

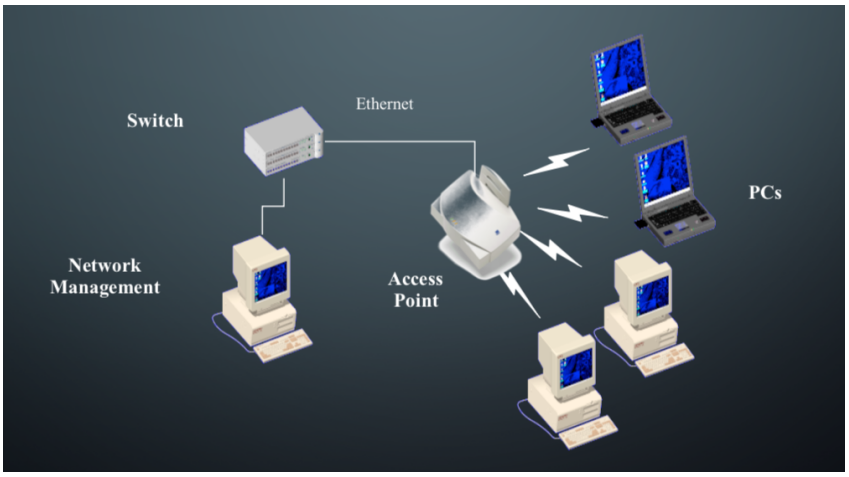
- Ethernet is layer 1 & 2 of the OSI model
- Higher layer entities build packets and provide these as a bit\byte stream to lower layer entities.
- Wrapping like Russian Dolls.



WIRELESS TECHNOLOGIES

PAN	LAN	MAN	WAN
"Personal Area Network"	"Local Area Network"	"Metropolitan Area Network"	"Wide Area Network"
Bluetooth	802.11b 802.11a HiperLAN2	802.11 MMDS LMDS	GSM GPRS CDMA 2.5-3 G
Low Data Rates Short Distances Notebook/PC to Devices/ Printer/Keyboard/Phone	Higher Data Rates Medium Distances Computer-Computer and to Internet	Higher Data Rates Med-longer Distances Fixed, last mile access	Lower Data Rates Longer Distances PDA Devices and Handhelds to Internet
< 1 Mbps	2 to 54+ Mbps	22+ Mbps	10 to 384 Kbps

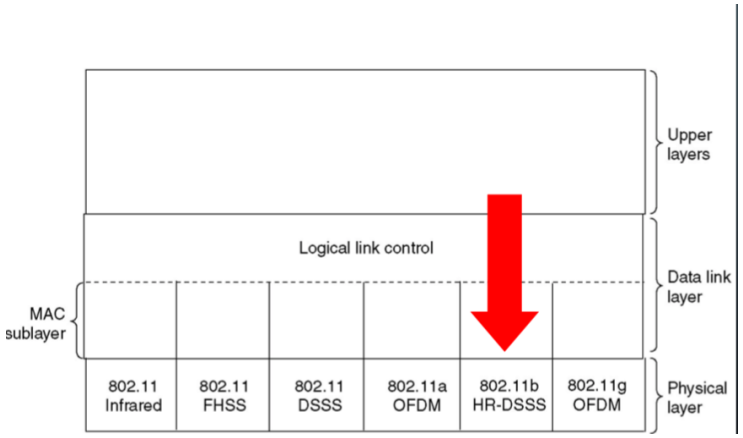
802.11B WIFI



WIRELESS LANS

- The 802.11 Protocol Stack
- The 802.11 Physical Layer
- The 802.11 MAC Sublayer Protocol
- The 802.11 Frame Structure

PART OF THE 802.11 SET OF PROTOCOLS



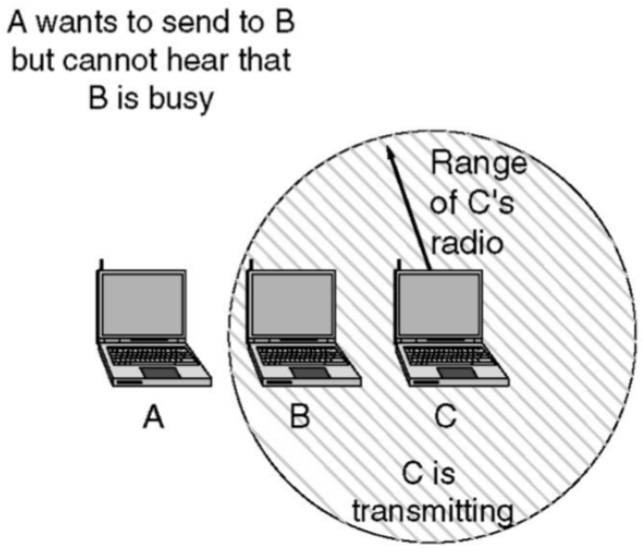
802.11 HR-DSS

- High Rate - Direct Sequence Spread Spectrum (HR-DSSS) • Speeds
- 1, 2, 5.5, 11 Mbps
- Dynamic speed adaptation
- Same bandwidth as cordless phones, Bluetooth and microwave ovens
- ISM Band
- Usually reserved for science, but we can use the 2.4 GHz band

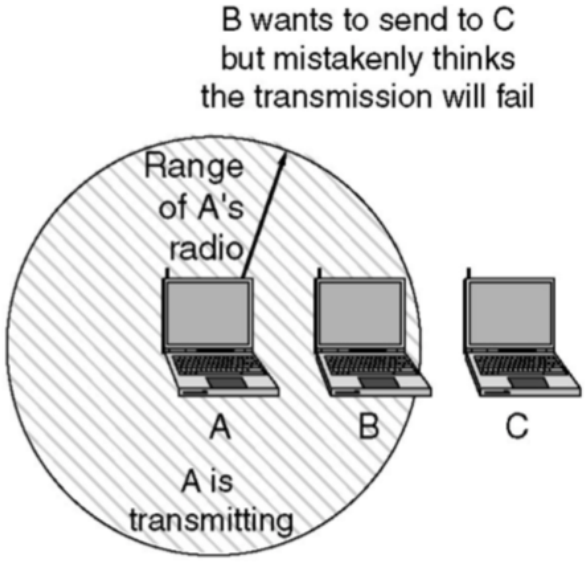
802.11 MAC PROBLEMS

- The hidden station problem.
- The exposed station problem.

HIDDEN STATION PROBLEM



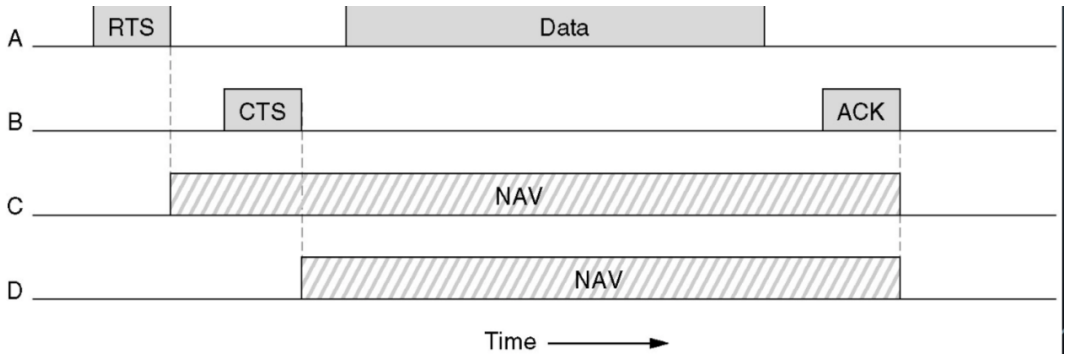
EXPOSED STATION PROBLEM



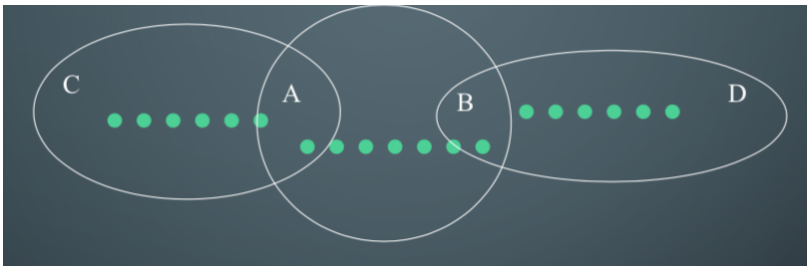
HOW DO WE OVERCOME THESE PROBLEMS?

- Some new protocols
- CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) • Some terminology
- RTS = Request to send
- CTS = Clear to send
- ACK = Acknowledgement

CSMA/CA



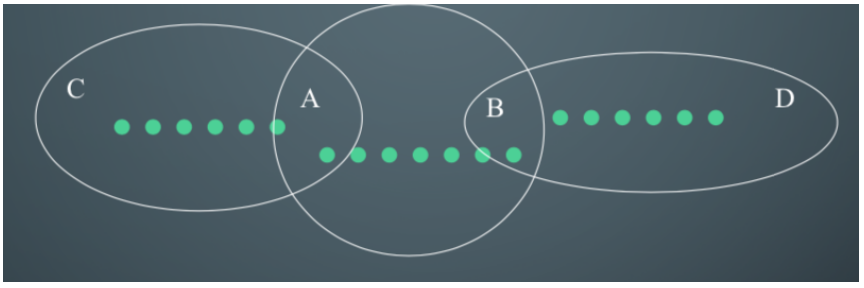
CSMA/CA EX - 1



- Example...
  - A wants to send to B, sends RTS
  - B says Ok with a CTS frame
  - A sends its frame & starts ACK timer.
  - B gets frame Ok and sends ACK frame.
  - If A's ACK timer expires, start again

OTHER STATIONS

- C within range of A... may receive RTS, if so Hush. This is Network Allocation
- Vector NAV
- D doesn't hear RTS but hears CTS... assert NAV
- All fine & dandy!



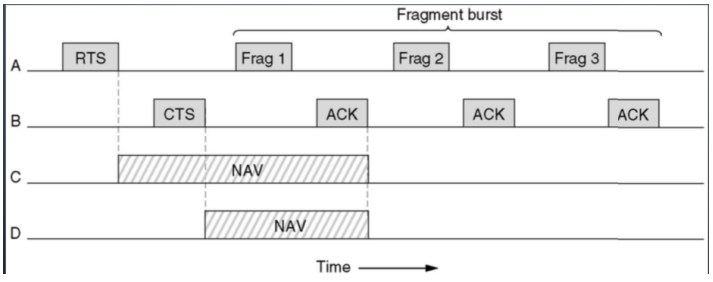
BUT ISM IS NOISY

- Probability of 1 bit error is p
- Probability of n bit frame arriving uncorrupted is $(1-p)^n$
- So, for $P = 10^{-4}$, 12144 bit frame has <30% probability of arriving correct.
- If 10^{-5}, roughly 1:9 will be damaged.
- If 10^{-6}, roughly >1:100 will be damaged.
- Bigger frames more susceptible to damage!

DEALING WITH NOISE

- Smaller frames have less change of being corrupted
- Solution:
- Break large frames into fragments and send them

FRAGMENT BURSTS



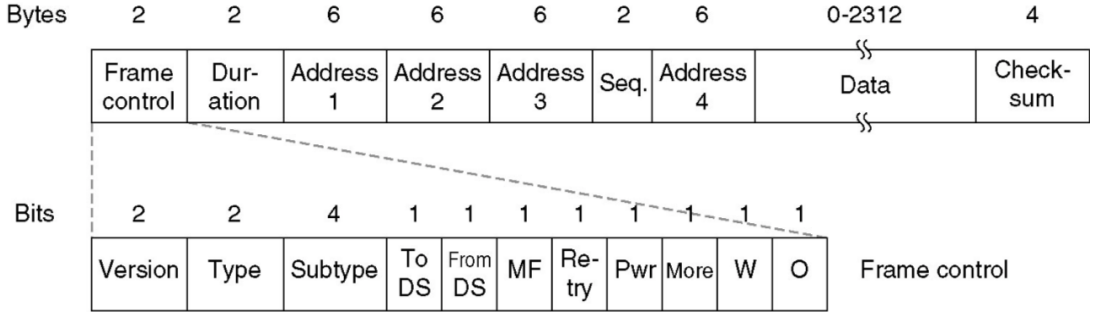
DEALING WITH NOISY CHANNELS

- Fragment frames, use checksums & number
- Acknowledge using Stop & Wait
- Once channel is acquired (RTS & CTS), send fragment burst, ACK each fragment.
- This is what is called Distributed Coordination Function (DCF) Mode

POINT COORDINATION FUNCTION - PCF

- Sits on access point
- Monitors network
- Base station polls... central control.
- Beacon frame transmitted periodically.
- There cannot be any collisions.
- Beacon frame contains system parameters.
- PCF and DCF (Distributed Coordination function) may coexist

802.11 FRAME STRUCTURE



FRAME STRUCTURE

- Data Control & Management Frames • Control has 11 Fields
- protocol version [PCF | DCF]
- Type - [Data | Control | Management]
- Subtype [RTS | CTS]
- To DS and From DS indicate to\from intercell distribution system (e.g. Ethernet)
- MF More Fragments
- Retry - this is a retransmission
- Pwr - power management [go asleep | wake up]
- W - encrypted with WEP
- O - process this frame sequence in order
- Duration field says how long frame & acknowledgement will occupy channel.
- 4 addresses - Source & Dest, also Source & Dest. Base stations for intercell traffic.
- Sequence is for fragment numbering, 12 bits for frame, 4 for fragment
- Data contains payload, up to 2312 bytes
- Checksum is CRC
- Mgmt frames operate within single cell
- Control frames are RTS, CTS and ACK

802.11 DISTRIBUTION SERVICES

- Association
- Disassociation
- Reassociation (roaming)
- Distribution (wired or wireless)
- Integration (protocol translation)

802.11G – HIGH SPEED WIRELESS

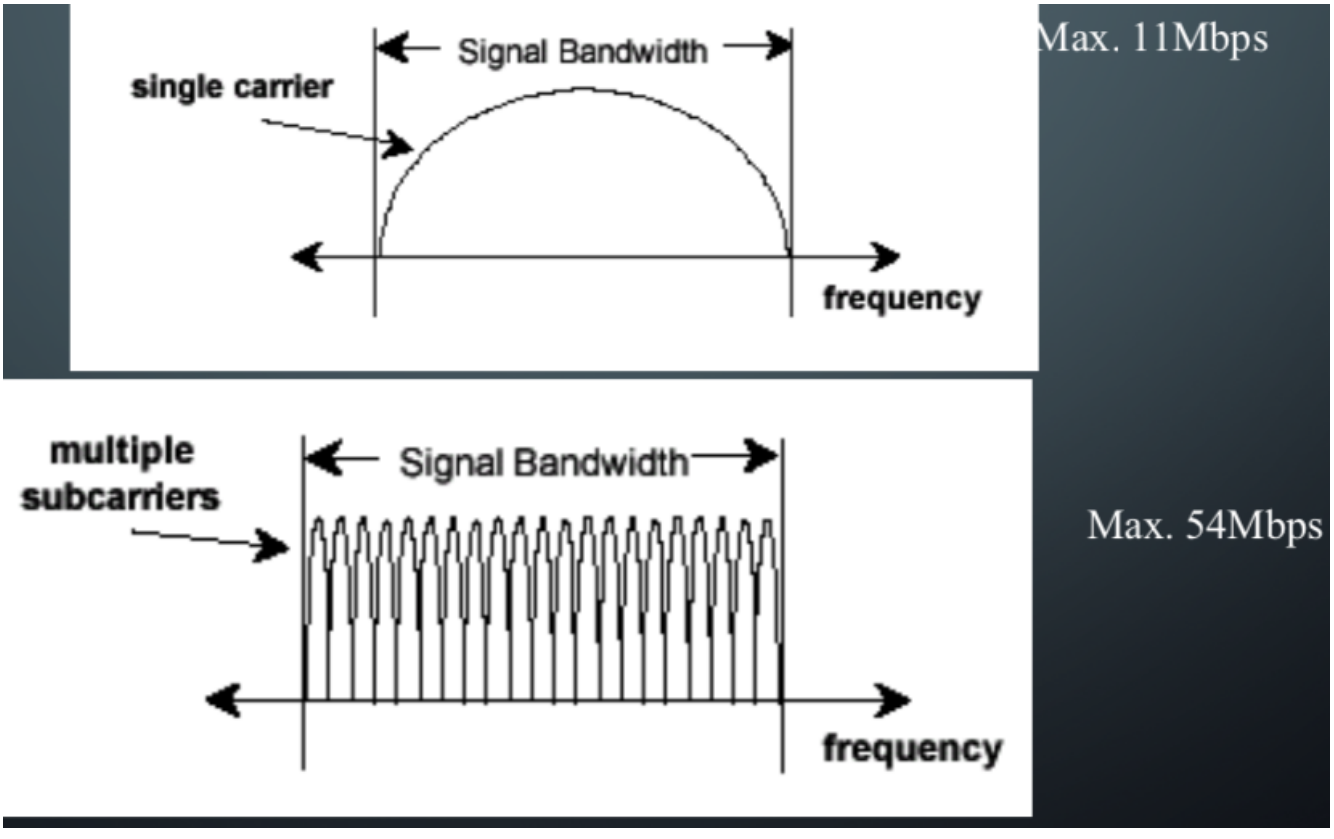
- 2.4GHz is still the frequency band with 54Mbps
- Compulsory…
    - Orthogonal Frequency Division Multiplexing (OFDM) used for rates > 20Mbps.
    - Complementary Code Keying (CCK) required for backward compatibility.
- Optional
    - CCK\OFDM Hybrid Header\Payload
    - PBCC Hybrid Header\Payload (Texas Instruments)

802.11G PACKET PREAMBLE AND PAYLOAD

Preamble/Header	Payload

- Preamble warns of forthcoming packet
- Header contains length of packet.
- Payloads vary from 64Byte to 1500Byte.
- Generally CCK used to transmit header and payload, usually!

CCK & OFDM



WIFI INTEROPERABILITY

- CSMA\CA will be used again.
- RTS\CTS will be used
- Headers may be transmitter using CCK and payloads may use OFDM

CCK	CCK

CCK	OFDM

OFDM	OFDM

802.11G SECURITY

- Wired Equivalent Privacy (WEP)
  - Garbage
- Service Set Identifier (SSID)
  - Disable broadcasts
- WiFi Protected Access (WPA)
  - Stronger than WEP
- MAC Address Authentication
- 802.1x Network Authentication
  - EAP

COMPARING WIRELESS TECHNOLOGIES

	Infrared	Bluetooth	802.11b
Frequency	10^{13} - 10^{14} Hz	2.4 GHz	2.4 GHz
Transmission Method	Line-of-sight	Frequency Hopping	Direct Sequence Spread-Spectrum
Speed	4 Mbps	1 Mbps	11 Mbps
Range	1 meters	30 meters	100 meters
Network	PAN	PAN/LAN/WAN	LAN
Signal	Data or Voice	Data & Voice	Data
Security	None	Authentication, Encryption	Authentication, Encryption

CA169: Week 6

The Internet

OVERVIEW

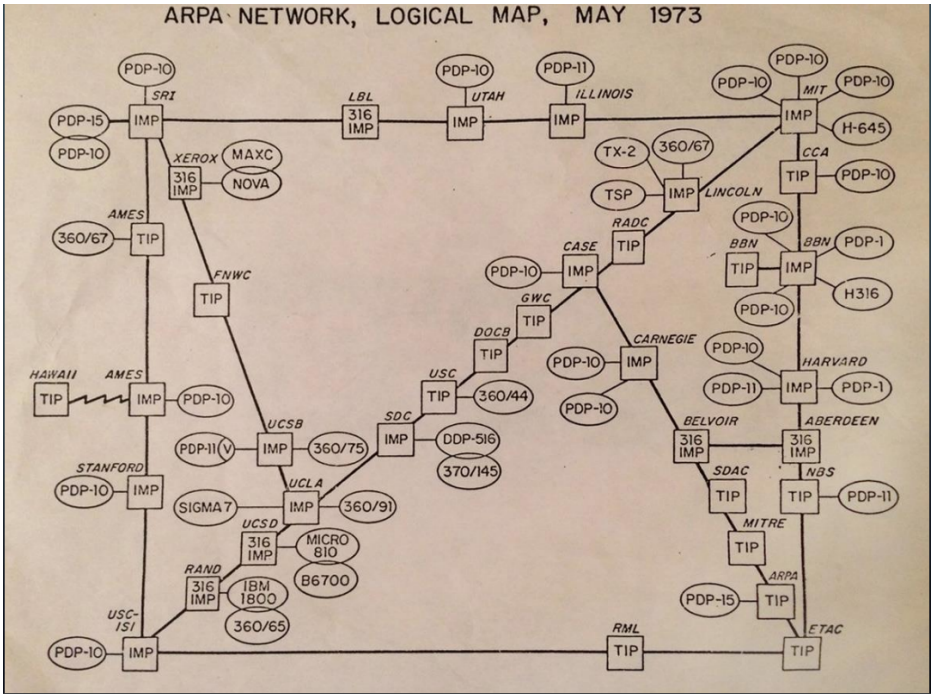
- History of the internet
- How the internet is structured
- Addressing & routing
- TCP & UDP

WHAT IS THE INTERNET?

- Global communication network
- Millions (if not billions) of computers connected
- Number of protocols to manage communications
- Websites ≠ Internet

HISTORY OF THE INTERNET

- Originally called the ARPANET in 1969
- ARPA became DARPA
- Developed during the cold war
- Linked universities & military installations



- ARPANET was the first packet switched network
- However it was only in America
- The network grew
- Other networks were created
- In order to create the internet they had to have a common form of communication
- By the end of the 1970s the transmission control protocol (TCP) was created
- This provided a common means of communication between computers
- Later on the Internet Protocol (IP) was added
- This is why we call it TCP/IP
- With TCP/IP the internet was globally connected
- However it was only used in universities for researchers to send data to one another
- They could read papers from the libraries of other organisations

THE HISTORY OF THE INTERNET – THE WORLD WIDE WEB

- In 1991 Tim Berners Lee invented the HTTP protocol
- HTTP stands for HYPERTEXT TRANSFER PROTOCOL
- This could be used to easily send data to any computer
- Along with HTTP , HTML was created
- HTML is the markup language used to create web pages
- Before HTML the internet was only used within a terminal
- HTML required a web browser to use
- Since then we are now on HTML5 & CSS3

INTERNETWORKING

- TCP/IP is the de-facto internet standard.
- Major issues to be addressed in Internetworking are…
    - Service type.
    - Addressing
    - Routing
    - QOS
    - Max. packet size
    - Flow & congestion control
    - Error reporting

SERVICE TYPE

- Connection oriented TCP
    - Provides reliable error free transport.
    - Utilises sliding window protocol.
- Connectionless UDP
    - Provides best effort datagram delivery.
    - Unreliable, packets may be discarded, not acknowledged.

ADDRESSING

- How do we address processes running on hosts ?
- How do we ensure unique addresses ?
- How do we map LAN addresses to TCP/IP addresses ?
- How do we interpret addresses ?
- How do we know where to send packets, i.e. route packets ?

ROUTING

- Issues include …
- How does host determine address of router attached to its network.
- How does host select a particular router when sending a packet.
- How does router determine addresses of other routers attached to the same network
- How does router select another router to which to send packets given destination host address.

QUALITY OF SERVICE

- Issues include…
- Transit delay expected when delivering packets to destination.
- Security and privacy required.
- Cost of delivery.
- Probability of error.
- Priority of transfer.

MAXIMUM PACKET SIZE

- Prevailing conditions may determine size.
- High bit error-rates: smaller packets better.
- Large transit delay: large queuing delays at each intermediate router, reduces efficiency.
- Buffer requirements at routers may dictate that it is easier to store smaller than larger packets..
- Processing overheads used in processing large numbers of small packets are larger than processing smaller numbers of larger packets.

TCP/IP

- Four layer Architecture
- Developed in 1960's
- Open System
- Not just one protocol, whole family.
- Many programming interfaces available.
- Standardised protocol set.

INTERNET PROTOCOL

- Main protocol for the internet
- It's job is to send packets from one address to another
- There are two main protocols in use
- IPv4
- IPv6

INTERNET PROTOCOL - IPV4

- The main transport mechanism for the internet (at the moment)
- Made up of IP addresses
- Each address is 32 bits (4 bytes)
- 32 bits = 2^{32} addresses.
- Written as decimal dot notation
    - E.g. 136.206.48.94
- Each byte can range from 0-255
- First IP address = 0.0.0.0
- Last IP address = 255.255.255.255
- ~4 Billion IPv4 addresses!
- IPv4 addresses translate into binary
- 32 bits = 4 bytes = 4 sets of 8 binary digits
    - E.g. what is 153.206.48.94 in binary
- 

BINARY (A REFRESHER)

- Base 2 number system (1's and 0's)
- We use Decimal – base 10 (0-9)
- There is also Octal – base 8 (0-7)
- Finally Hexadecimal – base 16 (0-9A-F)

BINARY TO DECIMAL

- Based on powers of two
- Exponents go right to left from 0
- Each exponent has base 2
- Multiply by binary (1or 0)
- Add them all together
- N.B. anything times 0 = 0
- Anything to the power of 0 = 1 (even $0^0 = 1$)

Binary	1	0	1	0
Exponent	3	2	1	0
	2^3	2^2	2^1	2^0
	$2^3 \times 1$	$2^2 \times 0$	$2^1 \times 1$	$2^0 \times 0$
	$(2^3 \times 1) + (2^2 \times 0) + (2^1 \times 1) + (2^0 \times 0)$			
	8 + 0 + 2 + 0			
	10			

- Convert 13 to binary
- Use whole number division
- Keep dividing the number by 2 and keep track of the remainder
- Stop once you reach 0
- Read the remainder from bottom to top

Equation	Answer	Remainder
$13 \div 2$	6 r 1	1
$6 \div 2$	3 r 0	0
$3 \div 2$	1 r 1	1
$1 \div 2$	0 r 1	1
0		

BACK TO IP ADDRESSES

- A machine can have many IP addresses
- An IP address can address only one NIC
- IP addresses broken into classes
  - A, B, C, D
- Class derived from the binary of the IP address

HOW TO FIND THE CLASS OF AN IP ADDRESS

- Convert the IP address into binary
- Look at where the first 0 is in the ip address
- If the first digit is 0 -> Class A
- Second digit -> Class B
- Etc..

Starting 0	Class
0	A
10	B
110	C
1110	D
1111	E

- What class is 192.168.0.0?
- Convert to binary
    - 11000000 . 10101000 . 00000000 . 00000000
- First 0 appears in the 3rd place Class C address

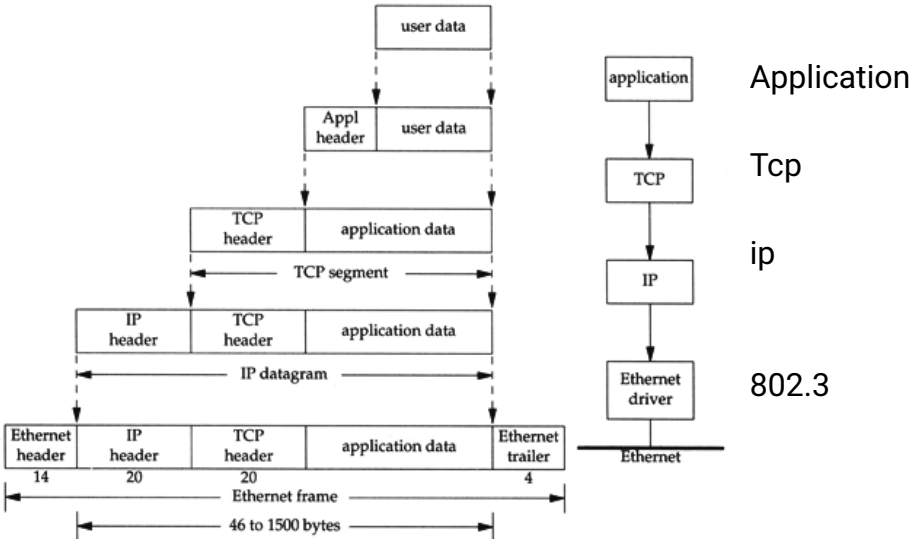
CLASSES, NETWORKS AND HOSTS

- Each class contains blocks of IP addresses called networks
- Each network contains a number of hosts
- These are the amount of machines that can be on the network.
- Class A – most hosts
- Class D – Least hosts

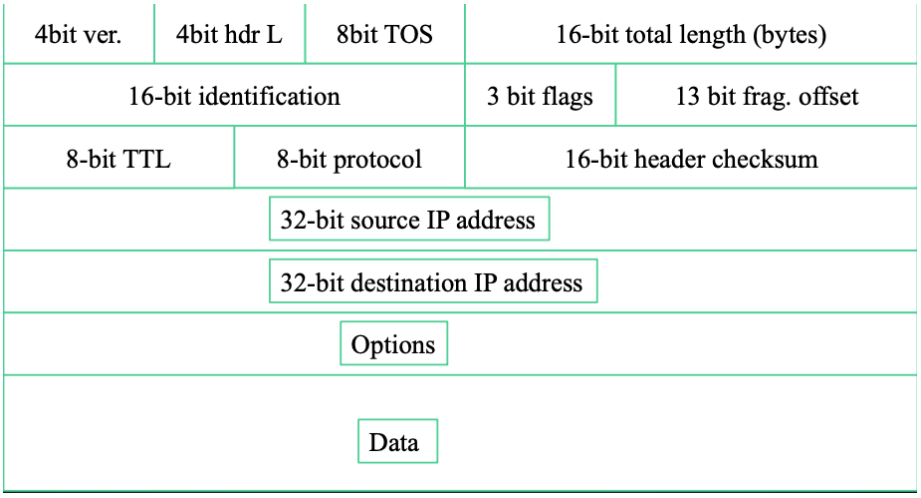
WHAT ABOUT CLASS E?

- Class E is a special class:
- It was never really defined what class E should be for
- It says reserved for “future use” (been reserved since the 90’s)
- Most networks will ignore class E addresses (there are exceptions)
- Some addresses are reserved (e.g. 255.255.255.255 – broadcast)
- Some have been set aside for “Research”
- The US Military also took a few (214.x.x.x, 215.x.x.x)

TCP/IP ENCAPSULATION



IP PACKET HEADER



IP HEADER DESCRIPTION

- Version: Currently V 4.
- Header Length: Specifies length of header as some fields are optional.
- Type of Service: This is the same as the QOS mentioned previously.
- Total length: Specifies the length of the datagram.
- Identification:Used to identify a set of datagrams which were formed from a single user message, but which got fragmented while traversing possibly several networks.
- D bit: Indicates that routers should not fragment a datagram i.e. Don't fragment bit.
- M bit: Indicates that there are more fragments to follow in later datagrams.
- Fragment offset: Where this fragments fits into the original fragmented datagram
- Time to live: Datagram loses a life (or some time to live) on each hop across the internet. Datagram destroyed when time\lives run out. Prevents Datagrams from wandering endlessly.
- Header Checksum: Checks header only.
- IP addresses (Source, Destination): As described previously

IP ROUTING

- Central function of IP is routing along with fragmentation and re-assembly of data across an internet.
- Routing information organised in a hierarchy. With hosts and gateways involved.
- ARP address resolution protocol maps IP to Ethernet addresses, an Interior Gateway Protocol (IGP)
- Exterior Gateway Protocol (EGP) knows about other routers on the internet and can route from network to network.
- Distance Vector and Link State routing are most popular, Link State is superior.
- Subnet addressing may be performed on a group of related networks (owned by one organisation).
- More on Routing later…

SPECIAL IP ADDRESSES

- Some addresses are reserved for special use.
- IP address composed of all 0 means this host.
- Network part all 0, Host part not, host on this network.
- All 1s broadcast on LAN
- Host part 127.0.0.x is Loopback, useful for debugging.
- 192.168.0.0 and 10.0.0.0 are reserved by IANA and are private addresses
- 172.16.0.0 up to 173.31.255.255 are reserved /12 or 16 class B addresses also reserved.

CREATING SUBNETS

- Address space
  - [network#, host#]
  - [network#, subnet#, host#]
- Subnet mask used to find the host part of IP address and distinguish it from the NW part.

Class	Format	Default subnet mask
A	nw.node.node.node	255.0.0.0
B	nw.nw.node.node	255.255.0.0
C	nw.nw.nw.node	255.255.255.0

SUBNETTING – WHY?

- Reduces Network traffic
  - Routers create smaller broadcast domains, more smaller domains limits the span of a broadcast.
- Optimizes NW performance
  - Less traffic, things run faster.
- Simplifies management
  - Easier to do fault analysis on a smaller self-contained NW than with a single huge NW
- Facilitates spanning of large geographical distances
  - Single large NW over large distance incurs big overhead of resources. Smaller NWs which keep much traffic local will incur less overhead over the long haul.

CIDR

- Classless Inter Domain Routing -
- Give the IP address space some breathing room!
- Basic idea: allocate the remaining IP addresses in variable-size blocks without regard to classes
  - original name: Supernetting, the opposite of Subnetting (sortof)
- A site needing 2000 addresses receives a block of 2408 addresses
  - i.e., 8 contiguous class C networks.
  - If need 8000 hosts, then allocate a block of 8192 addresses, i.e., 32 contiguous class C networks.

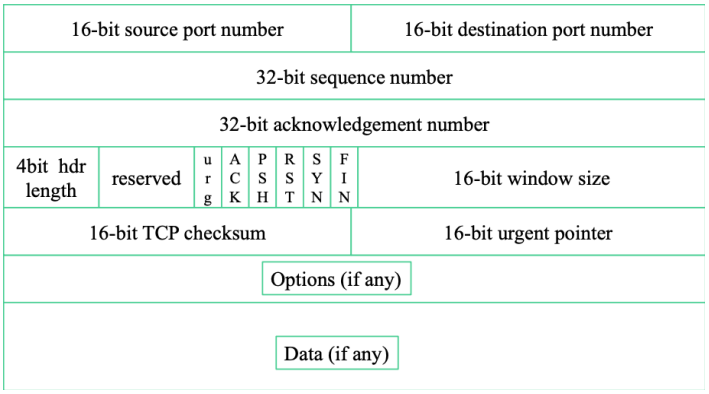
VARIABLE LENGTH SUBNET MASKS

- Only works with routing protocols which support CIDR
- Different masks on each router interface. Small number of bits for routers so they have few hosts, few routers. Keep big numbers for LANs
- Match required number of hosts to appropriate mask on each interface.
- Requires careful design so that blocks do not overlap
- Routes may be summarised, providing a hierarchy.

TCP SERVICES

- Provides connection-oriented, reliable, byte stream service.
- Segments passed to IP for routing, timer attached for each segment.
- Sliding window protocol utilised with go-back-n or selective-repeat for retransmission.
- All TCP segments acknowledged.
- TCP segments may arrive out of order, sliding window will sort order.
- TCP segments may be duplicated, duplicated are discarded.
- TCP provides flow control, no process\host will be swamped, helps avoid congestion.
- TCP utilised by many internet applications such as Telnet, Rlogin, FTP, E-mail, WWW Browsers.

TCP SEGMENT HEADER



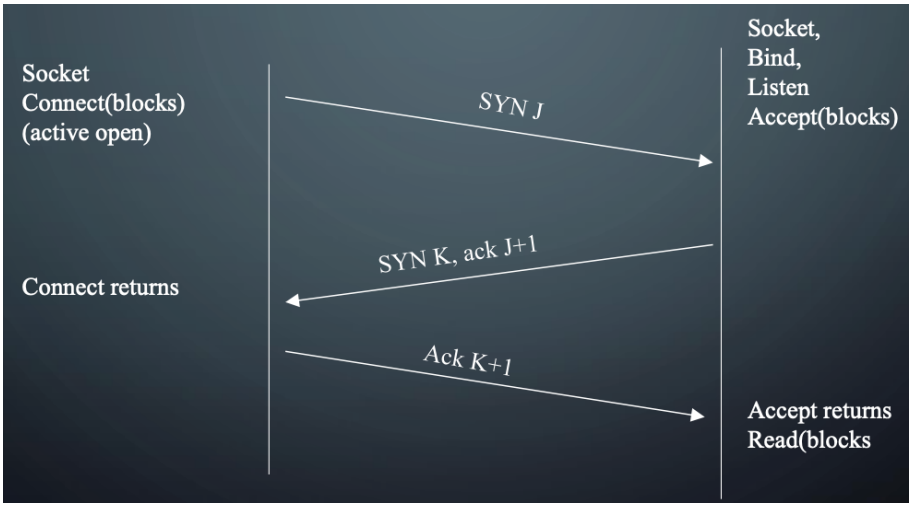
TCP HEADER DESCRIPTION

- Source Port and Destination Port identify transport end-points of connection.
- Sequence Number and Acknowledgement Number perform usual functions, Ack numbers next byte expected.
- TCP Header Length indicates number of 32 bit words in header. Length varies because of options.
- Not used. No bug fixes required !
- Six one bit flags…
- URGent pointer in use, used for indicating interrupts and offset from seq no. to urgent data.
- ACK bit used to indicate piggybacked acknowledgement.
- PSH requests that receiver does not buffer but to deliver.
- RST is reset connection, means problems !
- SYN used in conjunction with ACK to request connection.
- FIN release connection
- Window size used for variable-sized sliding window. Size of zero indicates a choke packet.
- Checksum checks header.
- Options field for things like specification of maximum TCP payload. Negotiated at startup lowest bid wins.
- A selective repeat instead of go-back-n sliding window protocol may be specified as an option.

TCP ADDRESSING

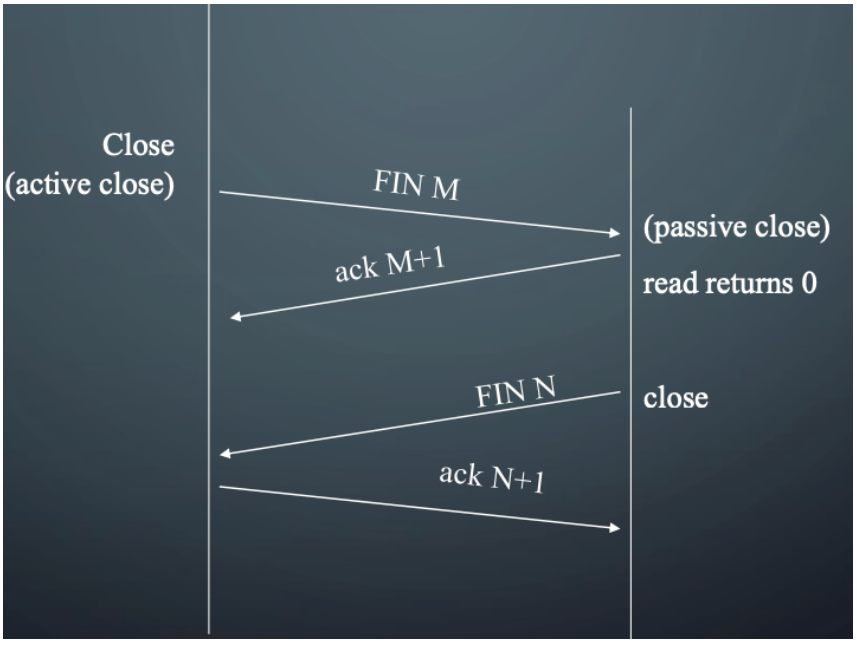
- TCP uses notion of Port Number to access transport endpoint on a single host.
- Many Ports may be in use simultaneously.
- Combination of IP address and port number uniquely identifies a port for process running on a particular machine.
- Process may even have several ports open.

Three Way Handshake



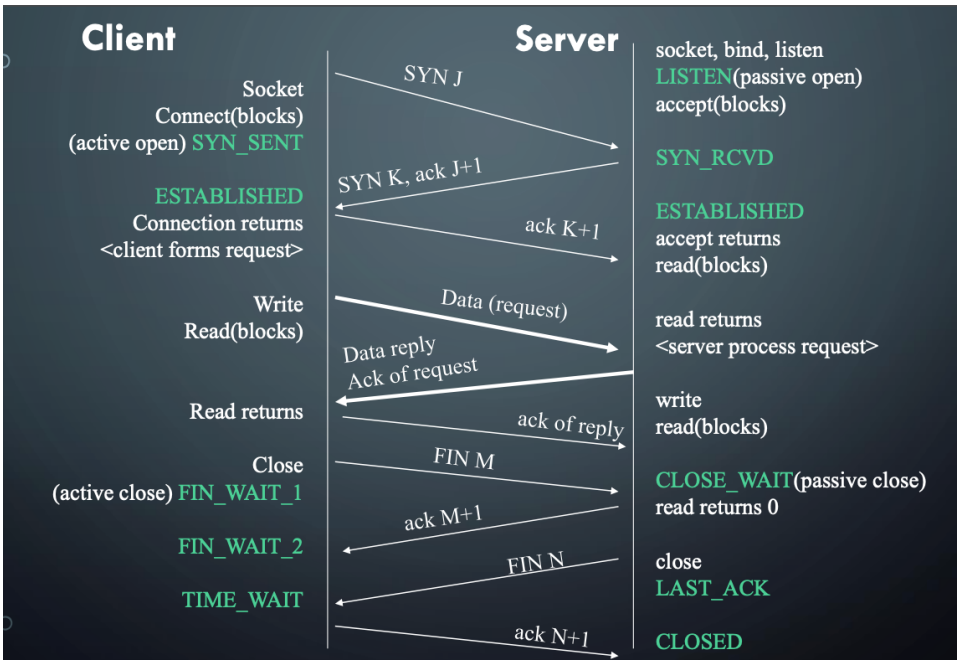
TCP CONNECTION TERMINATION

- If application calls close first, this is an active close.
- Sends FIN segment, meaning finished sending data.
- Server performs passive close.
- Clients FIN is ack'ed and sent to application as EOF, after any queued data to receive.
- When application receives its EOF, it will close its socket. TCP sends FIN.
- The server on receiving final FIN acks that FIN.



TCP CONNECTION & THE PACKETS

- A complete TCP connection involves many packet exchanges.
- Connection establishment
- Data transfer
- Connection termination
- TCP states are also shown as client and server enter them.

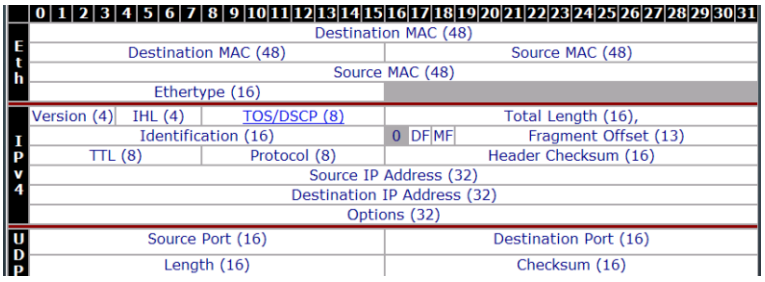


THE INTERACTIONS

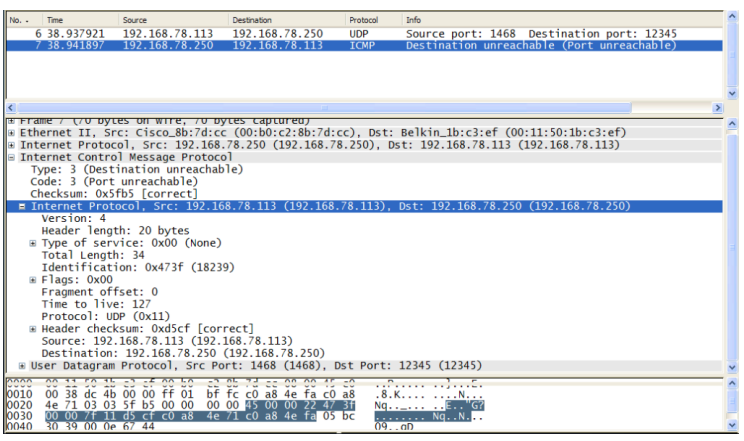
- Once connection established, clients forms request for server.
- Server processes request and replies with piggybacked ack.
- Termination by client (active close)
- Waits 2MSL (Maximum Segment Lifetime) to deal with lost or wandering IP packets.
-

UDP

- The User Datagram Protocol. Its characteristics are:-
- Packet-oriented
- Connectionless
- Unreliable
- UDP adds almost nothing to the IP network layer over which it is transported. It just introduces the concept of a port (a concept it shares with TCP as we will soon see).
- A port is an abstraction which can be regarded as a transport-layer address (remember the role of the transport layer) which uniquely identifies a particular process (or endpoint) on the destination node
- The UDP header is very brief…



- The checksum is sometimes ignored…
- Most datalink layer protocols include some form of error-checking (e.g. Ethernet CRC)
- For some data types (e.g. VoIP), timely but (slightly) corrupt data is better than late but accurate data
- Services listen on well-known ports.
- DNS on UDP port 53
- Syslog on 514
- SIP on 5060 (e.g. whatsapp voice calls)
- These are administered by IANA (the Internet Assigned Numbers Authority) and the definitive list is maintained at http://www.iana.org/assignments/port-numbers
- Another good place to look these up is the /etc/services file on a Linux box or the %WinDir%\system32\drivers\etc\services file on Windows
- When a client wants to communicate with a UDP server, it starts by allocating a randomly-chosen UDP port > 1024.
- This will be the source UDP port.
- It will then transmit to the server on the destination port (e.g. one of the well-known ports mentioned on the previous slide).
- The server will reply with a UDP packet from the well-known port back to the port the client transmitted the request from
- The combination of (source IP address, source UDP port, destination IP address, destination UDP port) uniquely identifies this “session” (although the concept of a session is artificial with the connectionless UDP protocol)
- When the client transmits its packet to the server, it has no way to know if there actually is a service (i.e. process) listening on this port at the destination
- If not, the network (IP) layer on the server will return an ICMP “Port Unreachable” message



CA169: Week 7

Computer Security

TYPES OF SECURITY

- Network security
- Network traffic security
- Physical Security
- Application Security

NETWORK SECURITY

- Stop hackers from getting into network
- Penetration testing (pen testing) to determine weak points in network
- Cryptography service for passwords
- Firewalls
- White/Blacklisting

SECURING NETWORK TRAFFIC

- Provide encryption for all traffic
- HTTP v HTTPS
- Prevent hackers from getting access
    - Man in the middle attach
- Prevent network disruption
    - DOS or DDOS

SECURITY ISSUES

- Confidentiality
    - Only authorised people should have access to information.
    - The General Data Protection Regulation (GDPR) covers data protection for individuals.
- Authentication
    - Provide correct identification of the source of a message which is verifiable and reliable
- Integrity
    - Only authorised people with correct access privileges should have access to viewing, altering, delaying or filtering data held or transmitted in an information environment
- Nonrepudiation
    - Neither the sender or the receiver of information may be able to deny that a transmission took place. Useful for financial transactions.
- Access Control
    -
- Availability
    - Information and media should be available to authorised people when needed
- Legal Issues
    - Many countries in Europe do not even allow the transmission of encrypted data, it may be a criminal offence to be involved in such activities, so check before sending encrypted email and such.
    - The US does not allow the export of cryptographic software or hardware, they regard such systems to be armaments, with severe penalties for infringements.

HACKERS

- Black Hat
  - Entirely for financial gain
  - Malicious
- Grey Hat
  - Good or bad
- White Hat
  - Ethical Hacker
  - E.g. Works as security penetration tester

YOU CAN PROTECT YOURSELF

- Know your enemy
  - Open Web Application Security Project™ https://www.owasp.org
- Defend yourself
  - Set traps: (E.g. honeypots https://us.norton.com/internetsecurity-iot-what-is-a-honeypot.html)
- Develop your expertise:
  - Facebook capture the flag
  - DEFCON: https://www.defcon.org/
  - Hack this site: https://www.hackthissite.org/

ATTACKS

- Hacking requires in depth knowledge of the target setup
- Windows or Linux?
- What language (php, python, javascript)
- What web framework ? (Node, Django, Rails, Wordpress…)

CRYPTOLOGY

- Cryptography – writing or solving codes
  - Devise encryption and decryption methods
- Cryptanalysis – analysing codes and breaking them
  - Find out patterns in the code

CRYPTANALYSIS - PROBLEMS

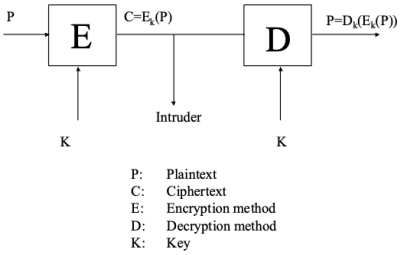
- Ciphertext only
  - Only have encrypted data and nothing else
  - Hardest kind of problem to solve
- Known plaintext problem
  - Some matching plaintext and ciphertext
- Chosen plaintext
  - Arbitrary amounts of plaintext and ciphertext available

A CRYPTOGRAPHIC SYSTEM

1. Plaintext P is passed to an encryption module
2. P is then encrypted using encryption key K making the ciphertext C
3. (optional) an intruder intercepts C but it is encrypted
4. C is then decrypted with a decryption key K to produce the plaintext P

CIPHERS

- One of the oldest methods of encryption
- Push letters up (or down) a number of spaces on the alphabet
- Oldest cipher (Caesar cipher) replaces text by 3 places (A becomes D, B -> E etc..)
- Key K = 3
- Zhofrph wr frpsxwhu qhwzrunv wz.

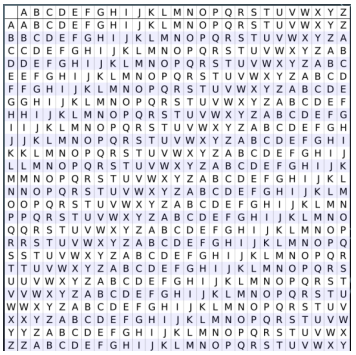


CIPHERS - SUBSTITUTION CIPHERS

- One of the oldest methods of encryption
- Push letters up (or down) a number of spaces on the alphabet
- Oldest cipher (Caesar cipher) replaces text by 3 places (A becomes D, B -> E etc..)
- Key K = 3
- Welcome to computer networks two.
- Replacing one letter with another is called monoalphabetic substitution
- There are 26 letters, the means that there are 26! Possibilities (4 × 1026)
- Generating all possible answers is called brute force cracking
- The time taken to brute force the cipher “khoor zruog” (hello world) is 31,000 years ! (2019-2020 computing power)
- However, language exhibits statistical properties that can be exploited
- Frequency analysis examines common letters and pairs to crack the password

CIPHERS – POLYALPHABETIC CYPHERS

- Use multiple Caesar ciphers
- Vigenère cipher
- Use repeating phrase as key (phrase repeatsmuntil its length matches the plaintext)
- E.g “Hello world” with key “howareyouh”
- Becomes: “oshlf amffk”



CIPHERS - TRANSPOSITION CIPHERS

- Reorder the letters but otherwise do not change them
- E.g. encrypt “Hello World”

4	5	1	2	3
H	E	L	L	O
W	O	R	L	D

4	5	1	2	3
H	E	L	L	O
W	O	R	L	D

4	5	1	2	3
H	E	L	L	O
W	O	R	L	D

4	5	1	2	3
H	E	L	L	O
W	O	R	L	D

4	5	1	2	3
H	E	L	L	O
W	O	R	L	D

- LRLLODHWEO

CIPHERS – PRODUCT CIPHERS

- Mix and match multiple substitution and transposition ciphers back to back
- Work off the binary representation of ASCII
- The Data Encryption Standard (DES) uses a product cipher system
- DES can be broken due to its small key size 56 bits
-

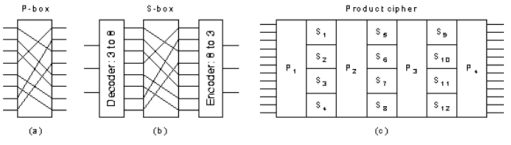


Fig. 7-4. Basic elements of product ciphers. (a) P-box. (b) S-box. (c) Product.

From: *Computer Networks*, 3rd ed. by Andrew S. Tanenbaum, ©1996 Prentice Hall

DES – DATA ENCRYPTION STANDARD

- Adopted by US Gov. in 1977
- No longer secure in original form, modified form still useful however
- Uses 19 stages product cipher, 56 bit key
- Uses S-box and P-box mixing

IDEA – INTERNATIONAL DATA ENCRYPTION ALGORITHM

- Lai and Massey in 1990,1992
- 128 bit key, immune to brute force attacks
- What else has 128 bits?
- Input is the same as DES, 64 bit blocks of plaintext

IDEA - STRENGTHS

- 64 bit blocks, enough to stop statistical analysis
- 128 bit key length stops brute force attacks (for now)
- Can be further strengthened using cipher feedback
- Confusion introduced by adding dependencies between the plaintext and ciphertext
- Three different mathematical operations (DES only uses 1)
    - Bitwise XOR
    - MOD 2^{16} addition
    - MOD 2^{16} + 1 multiplication
- Diffusion each plaintext bit has influence over each ciphertext bit. Plaintext is spread over a large amount of ciphertext, so statistical structure of the plaintext is hidden

PUBLIC KEY CRYPTOGRAPHY

- The key used must be kept secret
- In PKC the decryption key is kept secret, but the encryption key is public
- Practically impossible to guess the decryption key from the encryption key

PKC – STRONG ENCRYPTION

- Based on trap door functions, easy to solve in one direction but extremely difficult to reverse
- Multiply two prime numbers p and q which is easy to solve
- But working backwards is incredibly difficult

RSA ALGORITHM

- Pre-compute the parameters
- Divide plaintext into blocks (bit-strings) P s.t. 0<=P<n
- To encrypt
    - $C = P^e \text{ MOD } _n$
- To decrypt
    - $P = C^d \text{ MOD } _n$

CA169: Week 8

ARP, DHCP, DNS AND ICMP

RECAP

- Last week we covered TCP & UDP
- Two of the main protocols for TCP/IP communication
- TCP – 3 way handshake
    - SYN
    - ACK
    - SYN/ACK
- UDP – Fire and forget

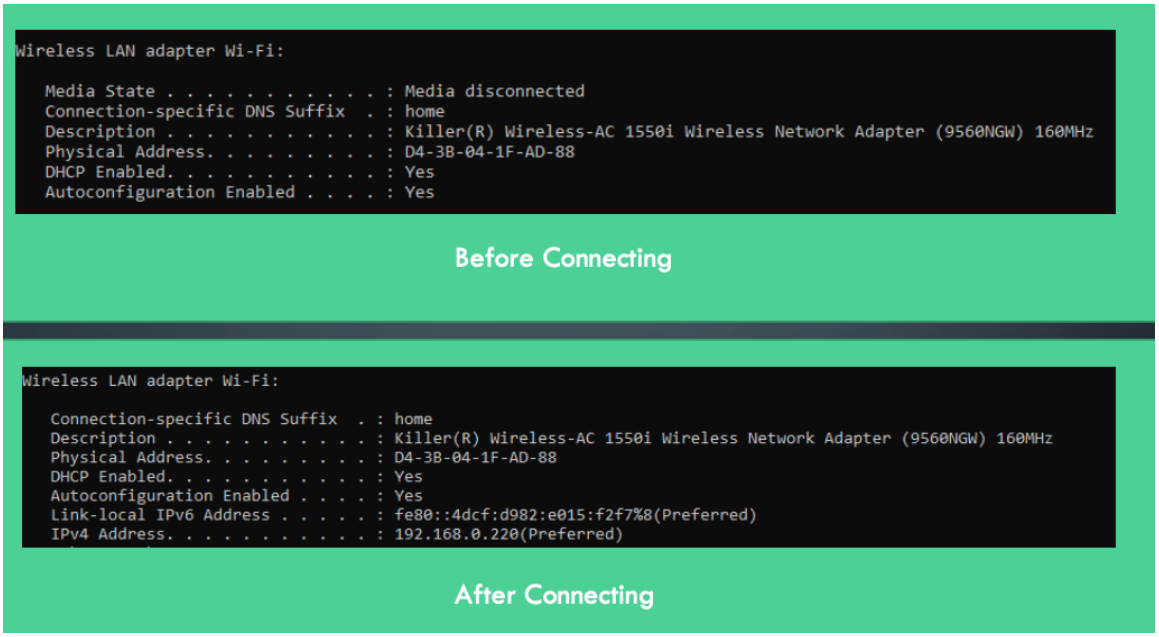
TODAY

- Helper protocols
- ICMP – general helper messages
- ARP – So your router knows who you are
- DNS – What is the ip address of www.google.com ?
- DHCP – How do I get an IP address on my network?

WHAT'S A DHCP?

- DYNAMIC HOST CONFIGURATION PROTOCOL
- On your home network you connect to your router
- Once you're connected you will see that you have an IP address

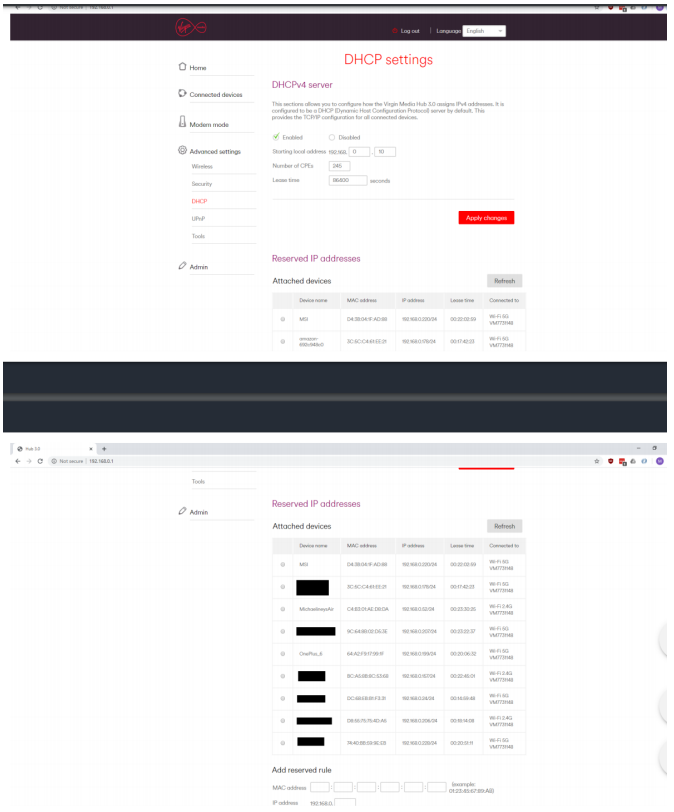
CONNECTING TO NETWORK BEFORE AND AFTER



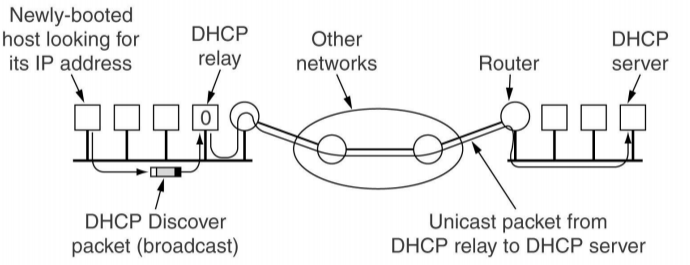
DHCP

- Allows manual IP assignment & auto assignment
- Replaces RARP & BOOTP
- Uses RARP server, not necessarily on same LAN
- DHCP relay agent exists on each LAN
- Normal operation – connection
- Workstation sends over MAC address
- Router adds IP + Mac to list of connected devices
- Machine is give IP

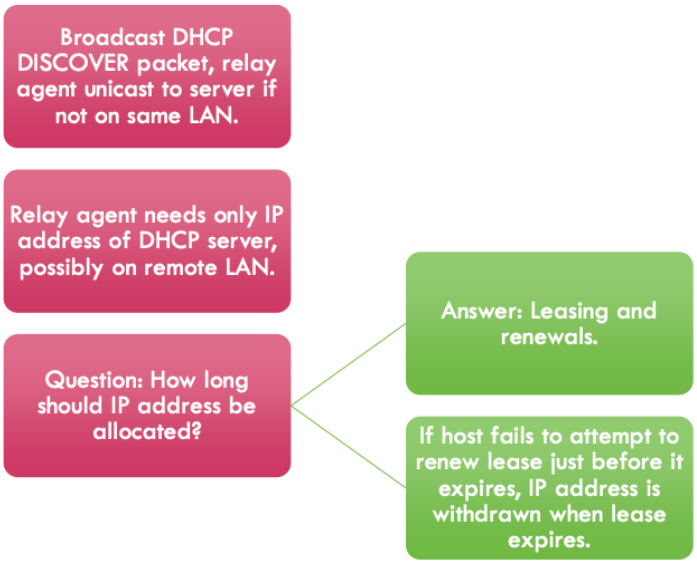
Connected Devices		
Name	**MAC**	**IP**
Printer	F6:AA:…	192.168.0.10
iPhone	AE:10:9F….	192.168.0.9
Workstation	64:5C:…..	192.168.0.11



- Allows manual IP assignment & auto assignment
- DHCP relay agent exists on each LAN



DHCP OPERATIONS



A NOTE ON LEASES

- DCHP gives out IP addresses
    - How many IPv4 addresses do we have?
- Routers are computers with small amounts of memory
    - 256 connected devices – what does this mean ?
- Am I always connected to my network ?

DHCP EXPERIMENT

- Note: do not do this if you are watching me live on stream!
- Open wireshark and start a capture
- Tell the router you are done with your IP address

```
ipconfig /release
```

- Now refresh your information

```
ipconfig /renew
```

- Refresh again

```
ipconfig /renew
```

- And release again

```
ipconfig /release
```

- Lets check wireshark! (dchp.cap on loop)
- Client lists info required
    - Address of local router
    - Subnet mask
    - Domain name
- Server responds with DHCP OFFER msg
    - Broadcast so that IPless station will read it
    - Contains IP address, local router, subnet mask, domain name & local domain name server
- Client indicated acceptance of address by echoing DHCP REQUEST with same information.

DHCP LEASES

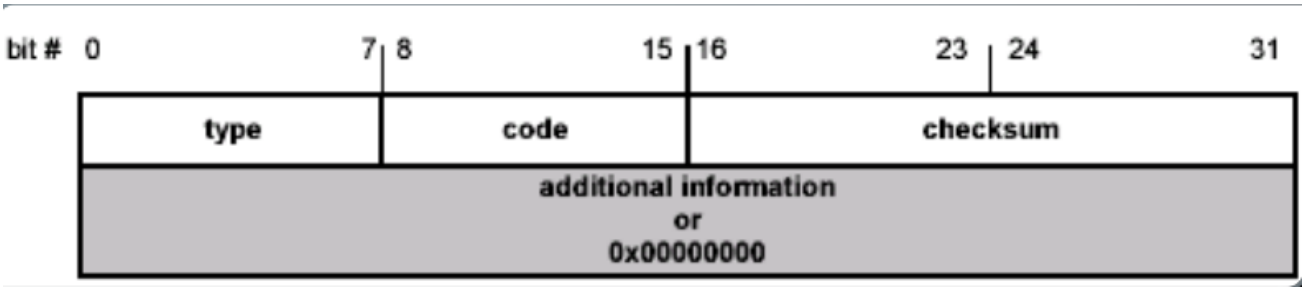
- IP addresses are leased only, not forever.
- Packets 14 & 15 show process of lease renewal.
- They happened because of our second ipconfig /renew command
- DHCP ACK includes duration of lease renewal (one day).
- If a lease expires, DHCP server is free to reallocate that IP address.
- The final ipconfig /release allows DHCP server to reallocate out IP address, thus recycling it.

ICMP

- INTERNET CONTROL MESSAGE PROTOCOL
- The IP (Internet Protocol) relies on several other protocols to perform necessary control and routing functions:
- Control functions (ICMP)
- Multicast signaling (IGMP)
- Setting up routing tables (RIP, OSPF, BGP, PIM, …)
- We will look at one of the simpler functions (e.g. PING)
- Helper protocol
- Supports:
- Error reporting
- Simple Queries
- All messages encapsulated as IP datagrams

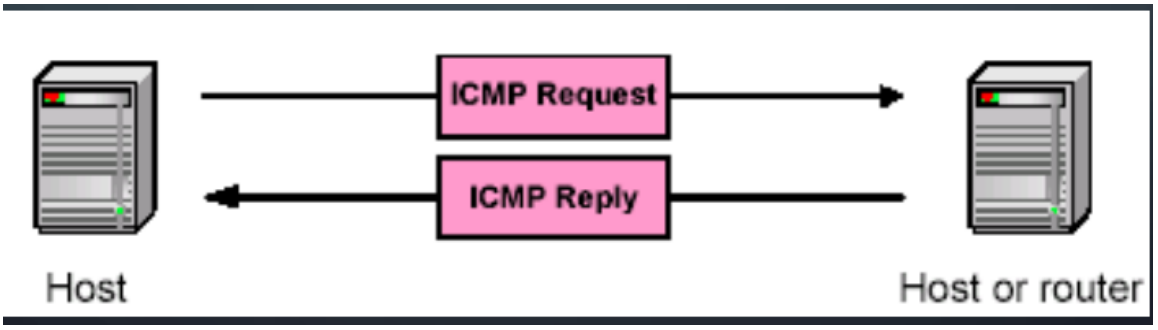
MESSAGE FORMAT

- 4 byte header:
- Type (1 byte): type of ICMP message
- Code (1 byte): subtype of ICMP message
- Checksum (2 bytes): similar to IP header checksum.
- Checksum is calculated over entire ICMP message
- If there is no additional data, there are 4 bytes set to zero.
- Each ICMP messages is at least 8 bytes lon



ICMP QUERY MESSAGE

- Simple request & response
- ICMP Request sent by host to a router or host
- ICMP Reply sent back to querying host



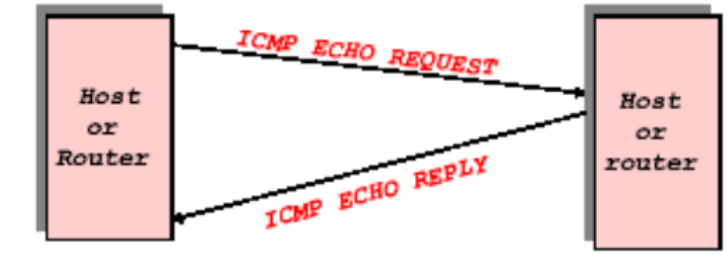
EXAMPLE ICMP QUERIES

- The ping command uses Echo Request/ Echo Reply

Type/Code:	Description
8/0 Echo	Request
0/0 Echo	Reply
13/0	Timestamp Request
14/0	Timestamp Reply
10/0	Router Solicitation
9/0	Router Advertisement

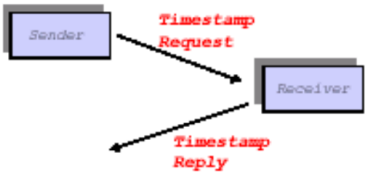
PING ECHO REQUEST AND REPLY

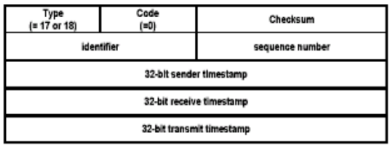
- Pings are handled directly by the kernel
- Each Ping is translated into an ICMP Echo Request
- The Pinged host responds with an ICMP Echo Reply
- The data portion of the request can be padded out to any size and is replicated in the reply
    - Useful for testing MTU and/or fragmentation
    - cf. “Ping of Death” DoS attack



ICMP TIMESTAMP

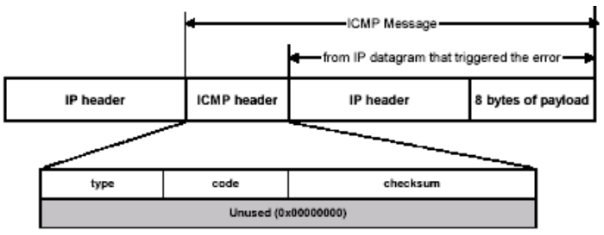
- A system (host or router) asks another system for the current time.
- Time is measured in milliseconds after midnight UTC (Universal Coordinated Time) of the current day
- Sender sends a request, receiver responds with reply

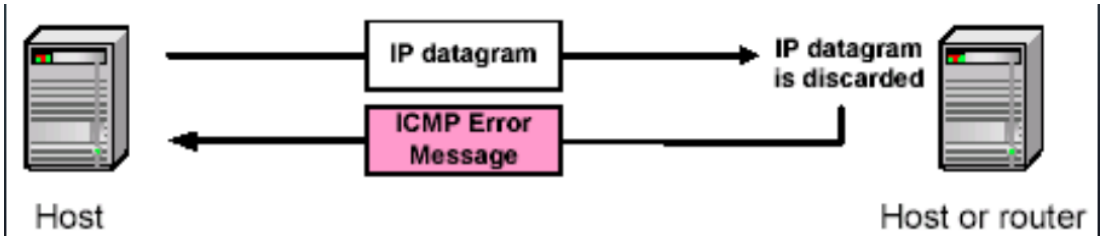




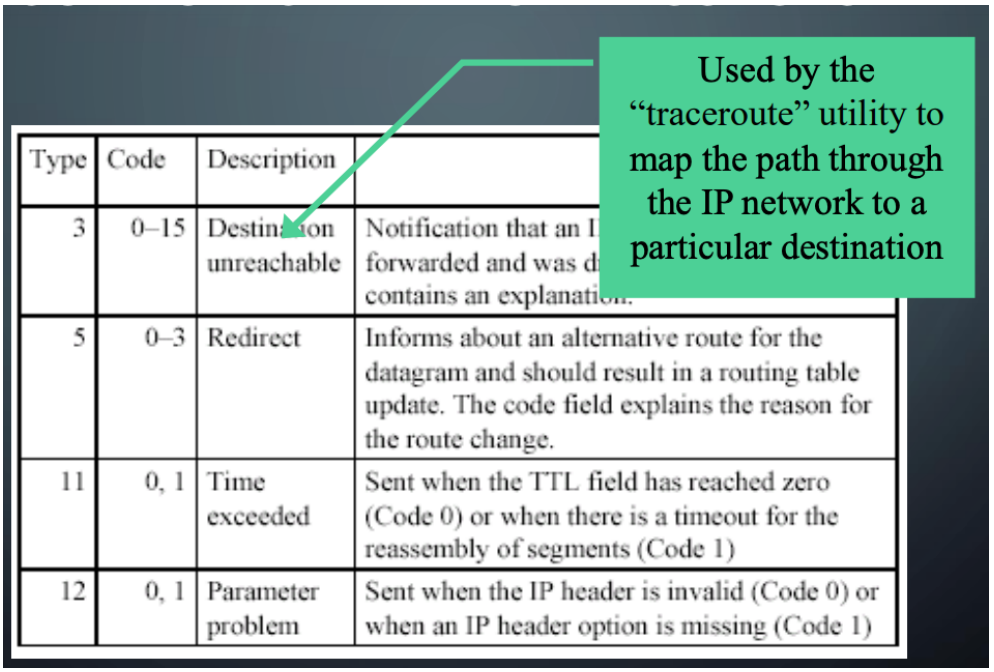
ICMP ERROR MESSAGE

- ICMP error messages report error conditions
- Typically sent when a datagram is discarded
- Error message is often passed from ICMP to the application program
- ICMP error messages include the complete IP header and the first 8 bytes of the payload (typically: UDP, TCP)





COMMON ICMP ERROR MESSAGES



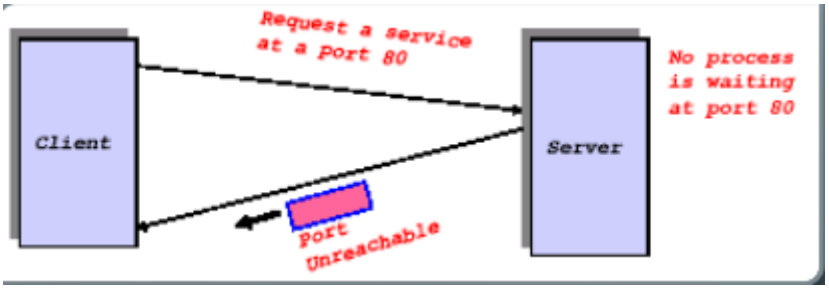
Type	Code	Description	
3	0–15	Destination unreachable	Notification that an I… forwarded and was d… contains an explanation.
5	0–3	Redirect	Informs about an alternative route for the datagram and should result in a routing table update. The code field explains the reason for the route change.
11	0, 1	Time exceeded	Sent when the TTL field has reached zero (Code 0) or when there is a timeout for the reassembly of segments (Code 1)
12	0, 1	Parameter problem	Sent when the IP header is invalid (Code 0) or when an IP header option is missing (Code 1)

DESTINATION UNREACHABLE

Code	Description	Reason for Sending
0	Network Unreachable	No routing table entry is available for the destination network.
1	Host Unreachable	Destination host should be directly reachable, but does not respond to ARP Requests.
2	Protocol Unreachable	The protocol in the protocol field of the IP header is not supported at the destination.
3	Port Unreachable	The transport protocol at the destination host cannot pass the datagram to an application.
4	Fragmentation Needed and DF Bit Set	IP datagram must be fragmented, but the DF bit in the IP header is set.

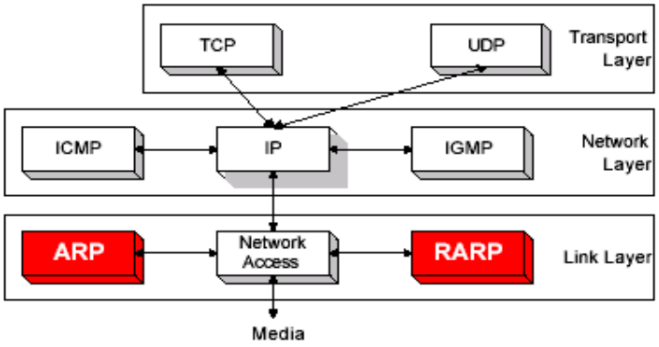
ICMP PORT UNREACHABLE

- From RFC 792: If, in the destination host, the IP module cannot deliver the datagram because the indicated protocol module or process port is not active, the destination host may send a destination unreachable message to the source host.



ARP

- ADDRESS RESOLUTION PROTOCOL
- The Internet is based on IP addresses
- Data link protocols (Ethernet, FDDI, ATM) may have different (MAC) addresses
- The ARP and RARP protocols perform the translation between IP addresses and MAC layer addresses
- ARP performs a lookup service that finds a MAC address for a given IP address.
- A system that needs a MAC address for a given IP address broadcasts a query which contains the IP address to all systems on the network.
- If a system receives the query and the IP address in the message matches its own IP address, it sends its MAC address to the sender of the query.



- IP and MAC addresses are the usual but not the only formats available to ARP

OPERATION OF ARP

- Each host maintains a table, the ARP cache, temporarily stores the results from previous address resolutions.
- ARP Request is broadcast to all systems on the network.
- In Ethernet, a frame is broadcast when the destination MAC address is set to broadcast address ff:ff:ff:ff:ff:ff.
- A broadcast frame is received and processed by all hosts.
- If a system receives the ARP request and the IP address in the message matches its own IP address, it issues an ARP Reply message to the sender of the query.

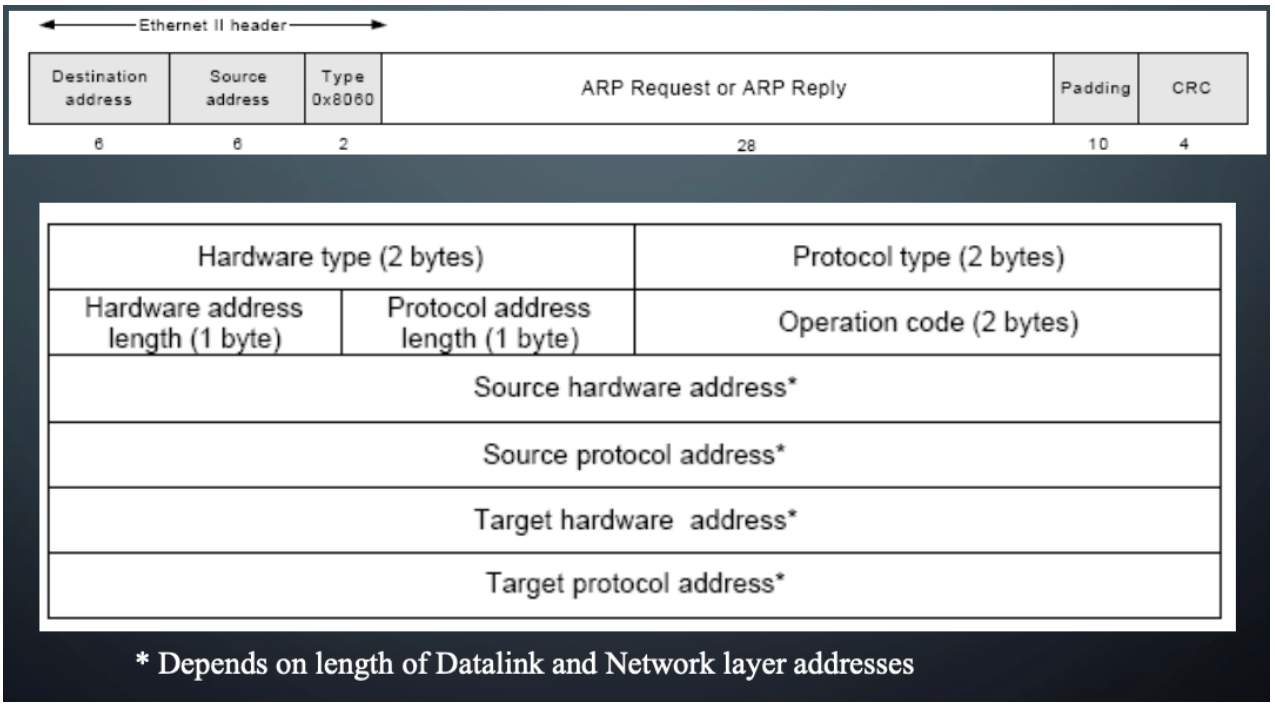
GRATUITOUS ARP

- Every host that sees an ARP Request verifies its ARP cache checking for the sender IP of the ARP Request.
- If such an entry exists, it updates the MAC address with the address in the ARP Request.
- Since ARP Requests are broadcast message, these updates are made by all systems each time an ARP Request is transmitted on the network.
- This feature is exploited in a concept that is called gratuitous ARP.

ARP VULNERABILITIES

- ARP may be used to redirect traffic intended for a certain IP address to another on the NW
- Broadcast ARP replies with invalid MAC addresses insert incorrect entries into ARP caches.
    - Poison ARP attack

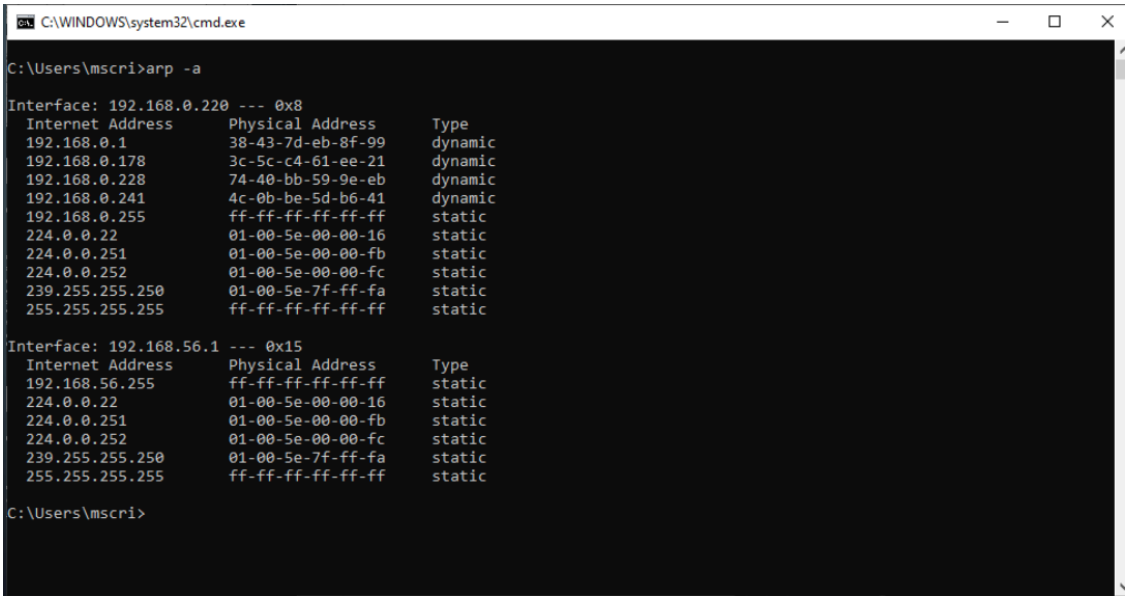
ARP PACKET FORMATS



NOTE: ARP PACKET FORMATS

- Ethernet carries ARP, with type set to 0x8060
- ARP message, in IP and Ethernet scenario is 28 bytes (48 bit MAC + 32 bit IP)
- Hardware type is datalink protocol
    - Ethernet = 0x0001, 802 = 0x0006
- Protocol type field is the network layer used
    - IP = 0x8000
- Operation code is 0x0001 for ARP requests and 0x0002 for ARP replies
- Hardware address length and Protocol address length specify length of addresses (MAC-6, IP-4).
- The next four fields contain the hardware address and the network address of the sender and the intended receiver of the ARP packet.
- The former is referred to as the source and the latter is referred to as the target.

An ARP, the Router, and My PC



arp Tool

- Issue `arp` command
- Tells you how to use it
- Issue `arp –a` it dumps its cache
  >arp –a I
  nterface 192.168.0.105 --- 0x10004

Internet Address	Physical Address	Type
192.168.0.1	00-06-25-8d-be-1d	dynamic
192.168.0.100	00:07:e9:53:87:d9	dynamic

MAKE DATA

- Issue `ping –n 1 192.168.0.1` from A
- Machine A sends a request message to B
- Check out arp.cap for results
- Note the source and destination addresses used in this trace.
- Now delete the arp cache with

  ```
  arp –d 192.168.0.1
  ```
- Do second `ping –n 1 192.168.0.1`
- A issues arp request
- B replies , replenishing arp cache of A and allowing it to issue a ping request
- Finally issue third

  ```
  ping –n 1 192.168.0.1
  ```

ARP EXERCISE

- Replicate the previous experiments
- Use `arp` and `ipconfig` to find out the IP and MAC addresses of the machines, clear the caches etc as done in the experiments. You will need 2 machines to do this.
- Something new:
- Check out the CRC calculations in the frames and account for any discrepancies.
- Use appropriate filters in Wireshark to limit captured traffic to that of interest for the experiment.
- Save your traces in Wireshark to a file.
-

PROXY ARP

- Proxy ARP is a configuration option for IP routers, where an IP router responds to ARP
- Request that arrive from one of its connected networks for a host that is on another of its connected networks.
- Without Proxy ARP enabled, an ARP Request for a host on a different network is unsuccessful, since routers do not forward ARP packets toanother network.

RARP

- Given an Ethernet address, what is the IP?
- RFC 903 – RARP sovves this problem – Broadcasts MAC gets back IP from RARP server.
- Broadcast address stays within 1 domain (router)
- Needs to get further or else have 1 RARP server in each MAC broadcast domain.
- Solution – use BOOTP

BOOTP

- RFCs 951, 1048, 1084
- Use UDP messages, broadcasts forwarded over routers!
- Also provides
    - info on IP of file server with disk image
    - IP address of default router
    - Subnet mask
- Problem: Manual config of IP – MAC, gives rise to errors.

WHY DNS

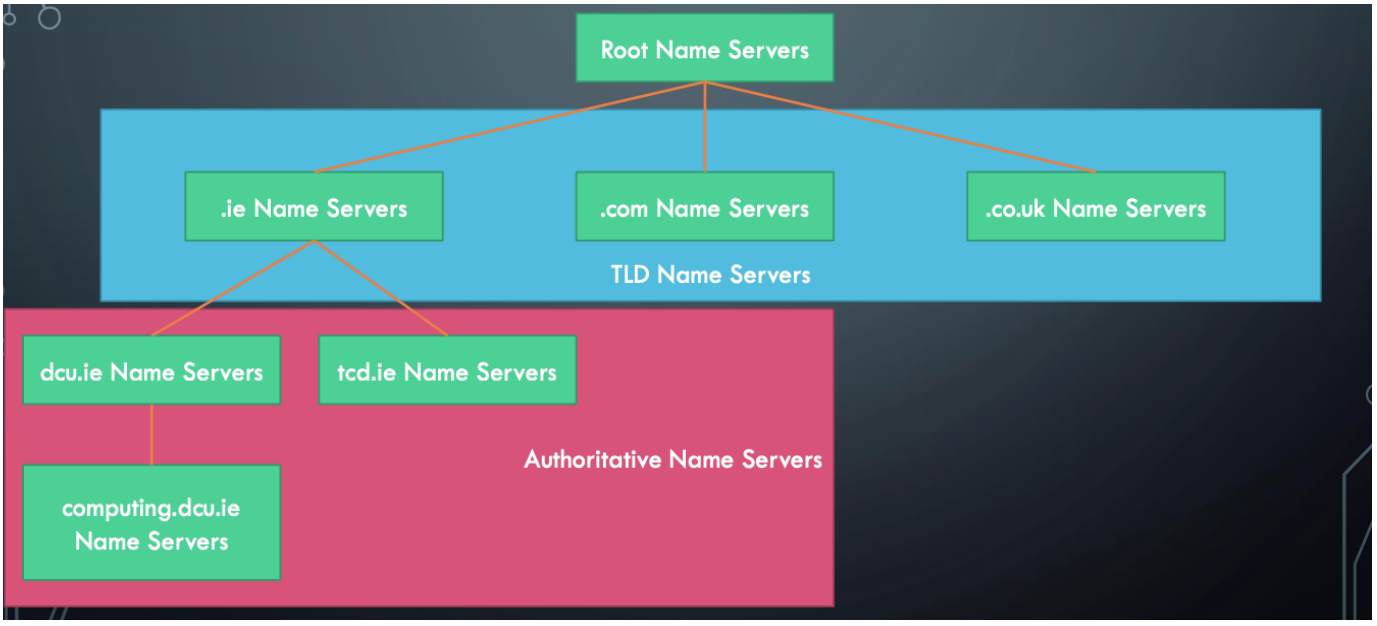
- DOMAIN NAME SYSTEM
- When you make a connection to a remote server you usually supply a domain name (e.g. www.google.com)
- The TCP/IP stack is used to send/receive data from remote computers
- The method for addressing in TCP/IP is an IP address
- How does www.google.com get resolved into an IP address
- Answer: DNS the Domain Name System

WHAT IS DNS

- A phone book mapping domain names to ip addresses
- When the number of domain names was small we used hosts.txt stored on your machine
- E.g. www.google.com 74.125.193.947
- Hosts.txt still exists!!
- C:\Windows\System32\Drivers\etc\hosts
- As the number of domain names grew, this solution became unworkable
- Essentially it's a server (DNS server) with a database of IP addresses
- When you send it a domain name, it returns an IP address
- This process is called a DNS lookup (or DNS resolve)

DNS STRUCTURE

- Think of how many times per second/minute people are visiting domains
    - Browsing
    - Email
    - Social Media
    - Phone apps
    - A single server would not be able to handle this load!
- The DNS system is structured to handle this
- The DNS database is distributed
    - There is no single DNS database
    - It is split into parts and distributed across the world
- The DNS database is structured
    - There are rules guiding what part of the database each server has
- The DNS database is replicated
    - Multiple copies of each database exist
- Root Name Servers
- Top Level Domain Name Servers
- Authoritative Servers
- Local Name Servers



DNS ROOT NAME SERVER

- Contacted first in order to find out the ip address for a domain
- Decides which TLD server to forward the request to
- There are many root name servers spread across the world
- Check: https://root-servers.org/

DNS - TLD NAME SERVERS

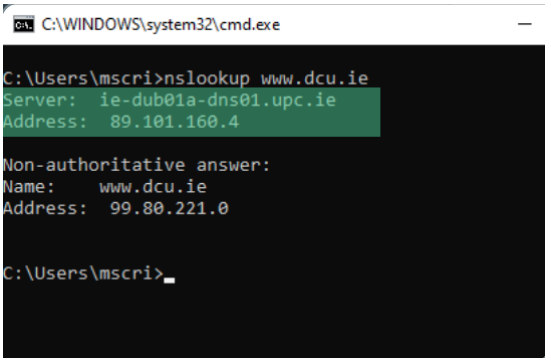
- Manages the DNS mappings for a top level domain
  - .com
  - .ie
  - .org
- ..ie name servers are managed by RIPE NCC
  - https://www.ripe.net/
    - RIPE also assigned us with our Class B address !

DNS - AUTHORITATIVE NAME SERVERS

- DNS mappings provided by an organisation
- E.g. HEANET manage the network infrastructure for third level universities in Ireland
- They contain the DNS mappings for DCU, TCD, UCD etc..
- Authoritative name servers can also be DCU itself
  - Mappings for “computing.dcu.ie”
- Computing.dcu.ie is also an authoritative name server
  - student.computing.dcu.ie

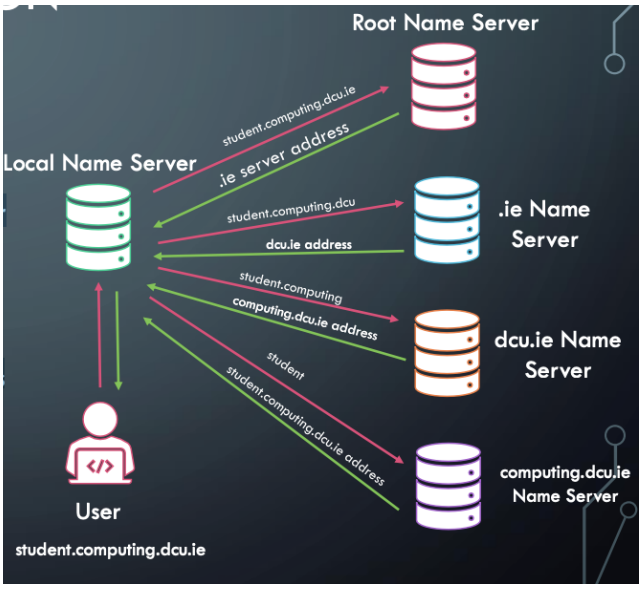
DNS – LOCAL NAME SERVERS

- There are also local name servers
- When you make a request from your home network you will use your network providers name server at first instance
- You can use nslookup to determine which name server is being used
- The local name server caches the addresses of common domains
  - E.g. www.google.com
-



DNS – ADDRESS RESOLUTION

- A user wants to visit student.computing.dcu.ie
- The local name server is first queried
- If it is not in the local name server, ask root server
- Root server returns the address of the TLD server
- The .ie server is then asked
- This returns the authoritative name server address
- We then ask the authoritative name server
- Finally we ask the last server
- Our address is returned
-



CA169: Week 10

HTTP

HTTP – HYPERTEXT TRANSFER PROTOCOL

- Invented in 1989 at CERN by Tim Berners-Lee
- Application layer protocol
- The protocol of the world wide web
- Latest RFC 7230- https://tools.ietf.org/html/rfc7230

HTTP – APPLICATION LAYER

- HTTP lives in the application layer
- Focuses on program to program communication
    - E.g. Web Server -> Google Chrome
- The underlying network architecture and protocols are abstracted

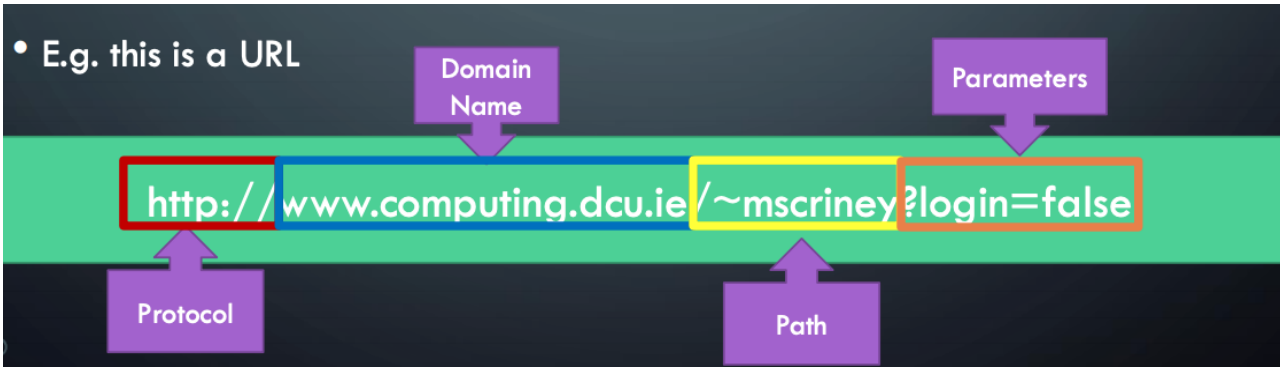
HTTP – RFC 7230

- Standards document for HTTP
- Describes
    - formats for all legal HTTP requests and responses
    - Formats of URLs
    - Controls for caching web pages
    - Persistence of connections
- Allows independent developers to develop their own web servers and clients and have them inter- operable

HTTP – URLS

- HTTP requires a URL (Uniform Resource Locator) to be passed to it
- It is more than just a domain name or IP address
- In addition to these, it specifies a protocol and a path and parameters
- E.g. this is a URL

    http://www.computing.dcu.ie/~mscriney?login=false



HTTP – OTHER URL COMPONENTS

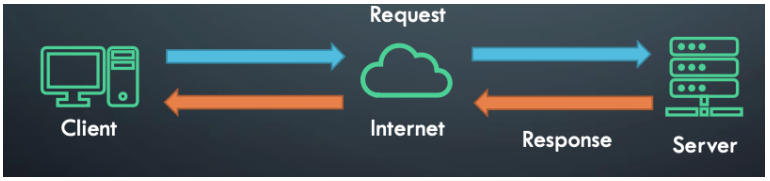
- The port – http://192.168.0.1:8000/hello.html
- User authentication – ssh://myuser:mypassword@192.168.0.1
- HTML Fragments – https://www.computing.dcu.ie/~mscriney/#teaching

HTTP - HTML

- HTTP was developed with HTML
- HTML – Hypertext Markup Language
- Hypertext – text containing links to other text documents
- We are currently on HTML5 RFC 7992 - https://tools.ietf.org/html/rfc7992

HTTP – REQUEST / RESPONSE

- HTTP works on a request/response mechanism
- The client makes a request
- The server provides the response



HTTP – REQUESTS

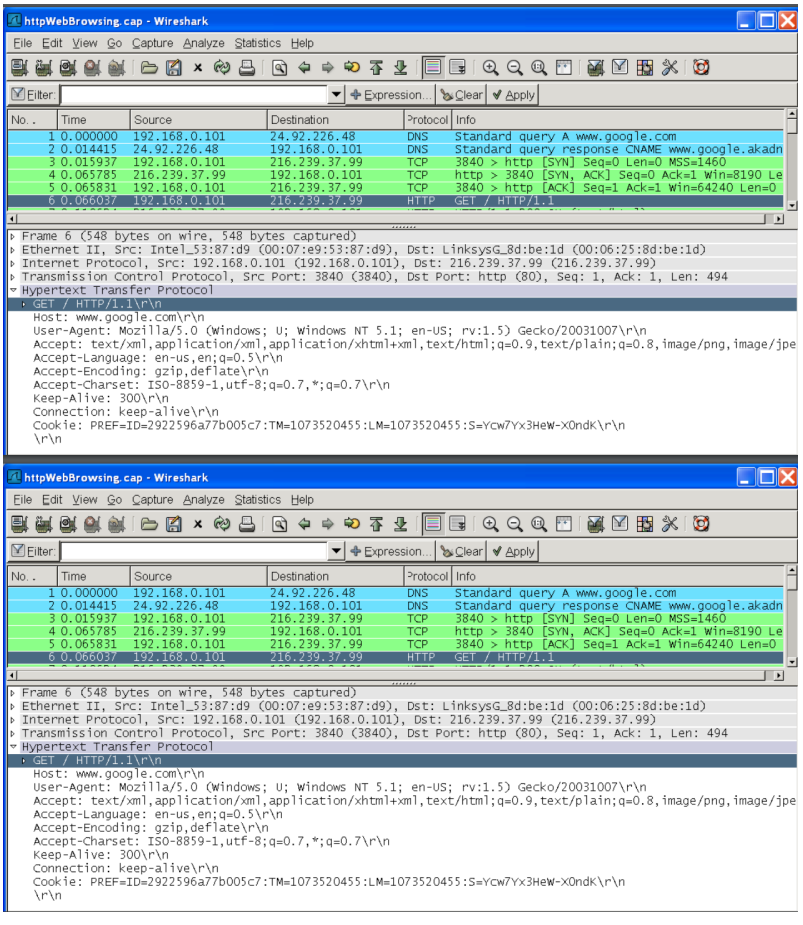
- HTTP Requests are made up of:
- The URL
- HTTP Headers
- Additional Data (e.g. username/password)

HTTP RESPONSE

- A response is made up of
  - Headers
  - Data (whatever you asked for, webpage, picture etc…)
  - A status code

HTTP REQUEST - WIRESHARK

- Open Wireshark and go to www.google.com
- See `http1.cap` on Loop
- The first 2 packets resolve the domain name (A DNS query!)
- Now a TCP connection is established, packets 3-5.
- Packet 6 sends "`GET / HTTP1.1\r\n`"



HTTP – GET REQUEST

- `"GET / HTTP1.1\r\n"`
- GET something, a file called "/" (default)
- \r is carriage return and \n is a line feed
    - Old typewriter terminology, used to separate one header from the next, each successive header has one, check it out.
- GET is one of the HTTP VERBS

HTTP HEADERS

- The name www.google.com\r\n specifies which webserver is being contacted.
- IP addressed machines may support several web-servers
- User-agent describes web browser and client machine making the request (this setup is quite old, a Mozilla browser, forerunner of Firefox and the
- Windows NT operating system

HTTP REQUEST METHODS

- GET – the most common method
    - Request a resource from a server
- POST
    - Submit data to be processed
    - Main use in web forms
- HEAD – Same as get but don't return any data

HTTP METHODS

- PUT – Update a resource with a new version
- PATCH – Update a resource (specify how it should be updated)
- DELETE – Remove a resource

HTTP HEADERS

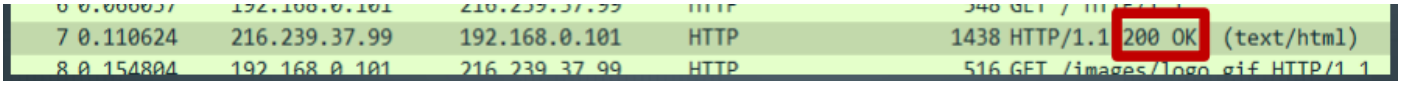
- Accept headers
- Server may support several languages, encodings, character sets, these tell server which is preferred.
- Keep alive and connection headers tell about the TCP connection being used, whether connection should be kept open and for how long.
- Most connections are persistent, allowing multiple requests from same client to server. This improves performance greatly of HTTP 1.1 over HTTP 1.0

HTTP RESPONSE

- Packet 7 the response…
- First HTTP 1.1 is fine with the server
- Headers…
- Cache-control: whether to store copies for future reference. Private here means that this is a specially generated and can be cashed by the user, but not by a group of users on a "shared proxy cache"
- Lists the types of content and encodings it can accept, text/html and gzip (compressed)
- GWS identifies itself as google's own webserver
- Content length is 1216 long and we get the date.

HTTP RESPONSE CODES

- On packet 7 we can see the response code



- A response code of 200 means a successful request
- There are many others
- The first digit specifies the class of the response
- 1xx – Information
  - 101 Switching protocols
- 2xx Success
  - 200 – OK
  - 204 – No content
  - Usually if your code makes a web request you look at the code
  - If code !=200 //Something has gone wrong
- 3xx – Redirection
  - 301 – Moved permanently (used to redirect to a new resource)
  - 304 – Not modified
- 4xx – Client error
  - 404 – not found (because of UCC!)
  - 403 – forbidden (request is ok, but you're not allowed to view the contents)
  - 401 – Unauthorized (username/password incorrect)
  - 410 – Gone – Resource unavailable now and in the future (tell search engines to remove)
- 5xx – Server Error
  - 500 - Internal server error – Generic error , something is wrong on the server
  - 501 – Not implemented – The request cannot be fulfilled
  - 503 – Service unavailable – Web server is overloaded or down for maintenance
- And the weird ones
- 418 – I am a teapot
  - https://tools.ietf.org/html/rfc2324
- 420 – Enhance your calm
  - Sent by twitter if you are being rate limited (similar to real error code 429, too many requests)
  - https://developer.twitter.com/en/docs/basics/response-codes

HTTP – MULTIPLE GET

- Only 1 GET request in packet 8
- Second request generated by the HTML source sent back for processing at the client.
  - `GET /images.logo.gif HTTP/1.1\r\n`
- It asks for the Google logo
- Several requests may be daisy-chained like this
- Multiple requests are very sophisticated now

GNU

- GNU is a famous open source and licensing organisation on the web
- From packet 21 a similar interaction can be seen sorting out where it is
- Packet 26 onwards contains the interactions with it.

WIRESHARK – FOLLOW TCP STREAM

- Wireshark allows us to follow particular interactions.
- Looking at the full interaction for Google
    - Select <Analyze> menu, and <Follow TCP Stream> from the menu. You will see every interaction between your client and the server. Each are coloured differently.
- A filter has been automatically entered for you
    - (tcp.stream eq 0)
    - This is very useful

MULTIPLE TCP STREAMS

- Packets 35, 41 and 42 open second TCP connection, same IP address as the first, same port (80), but local client port is different, 3842 instead of 3841.
- This gives rise to a second, parallel connection which speeds up transfer.

QUESTIONS

- Isolate the requests sent by the browser to the server
- Visit Google.com
    - <View ><Page Source>
    - Copy it into a file called test.html using Notepad application
    - Open a web browser and drag the file into the browser
    - What website do you see and what is missing and why?
    - Write a colour filter to highlight all of the HTTP requests in the trace
    - Write a colour filter to highlight all of the HTTP responses
    - Combine the two above, HTTP requests and responses only
- Visit three websites, one in DCU, another in Ireland and one abroad
    - compute the average response time for each. Describe how you did the calculation
    - What is the IP address of each

CA169: Week 11

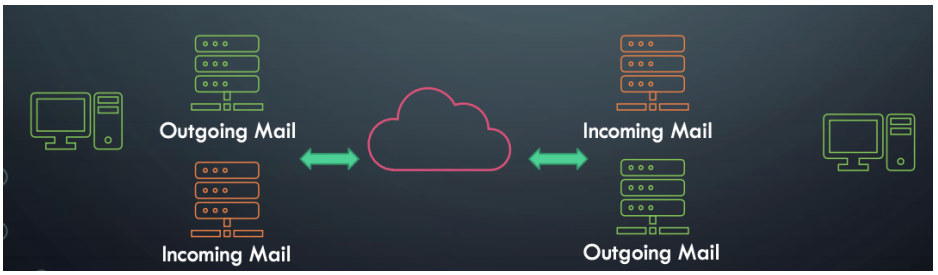
Email - SMTP, POP, IMAP

EMAIL

- One of the killer apps on the Internet – 1965
- Must be connected to the Internet
- Sending and receiving are different
    - SMTP and POP
- Simple Mail Transfer Protocol for outgoing
- Post Office Protocol for retrieving incoming mail
- IMAP is another for retrieving email, some retrieve through file system shared with email server, some proprietary protocols available.

EMAIL & MAIL SERVERS

- Email is managed by mailservers
- You have two
- Incoming mail
- Outgoing mail

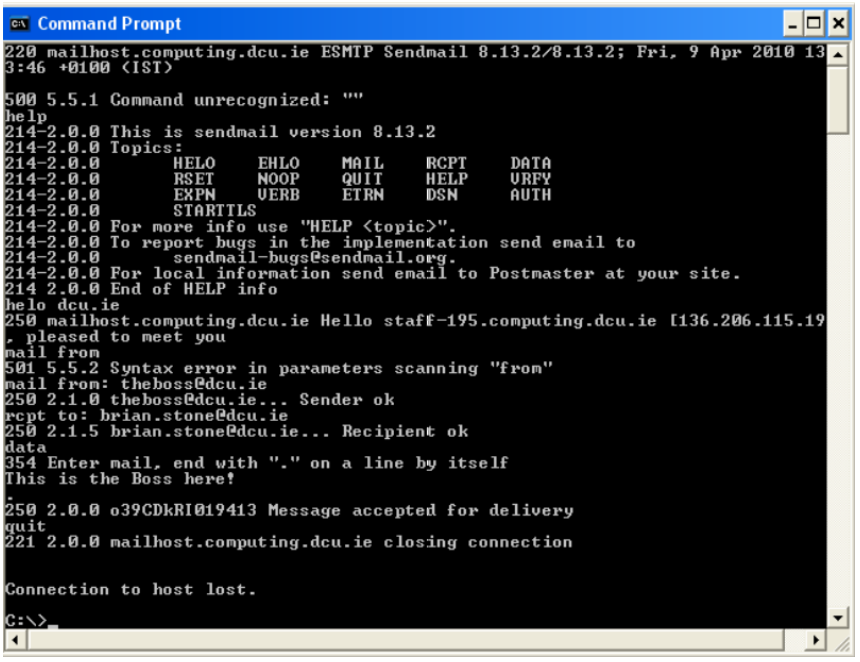


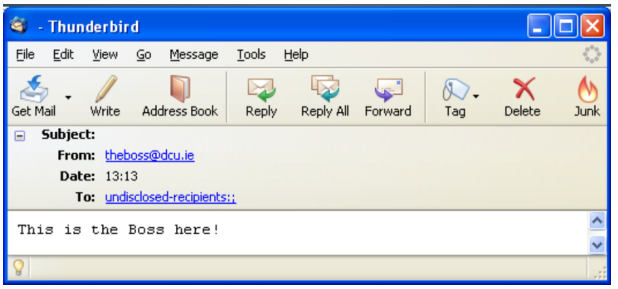
SENDING MAIL (SMTP)

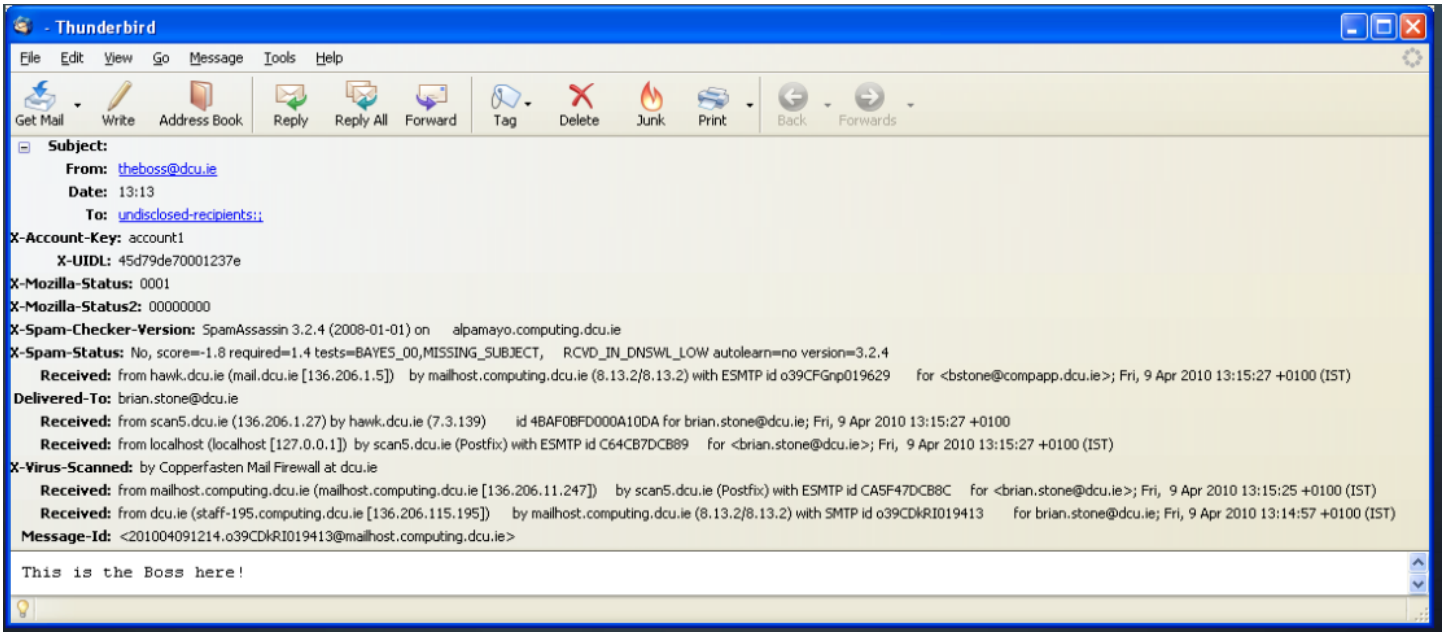
- Sending mail is handled by mailservers
- Your local mail server (gmail) takes responsibility to deliver the mail
- It is sent to the recipients incoming mail server

OLD EXAMPLE (PRE-GMAIL)

- `telnet mailhost.computing.dcu.ie 25`
- Opens an insecure shell to the mailhost on port 25
- When you make the connection on port 25 (the mail port), the mailserver says what it is and awaits commands.





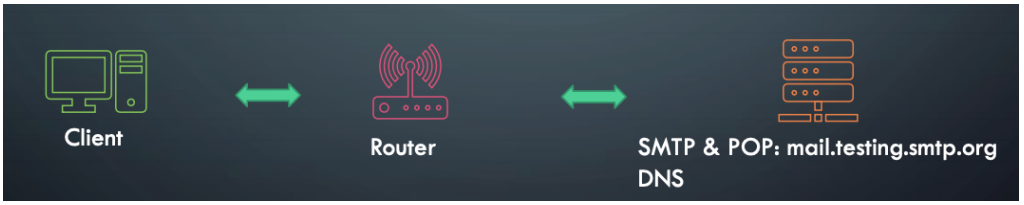


USING EMAIL

- Using an email client to send\receive email
  - Specify your email address
  - A password for the account
  - Name of outgoing mailserver
  - Name of incoming mail server
- User must present a password to retrieve email
- Mail may be sent without a password

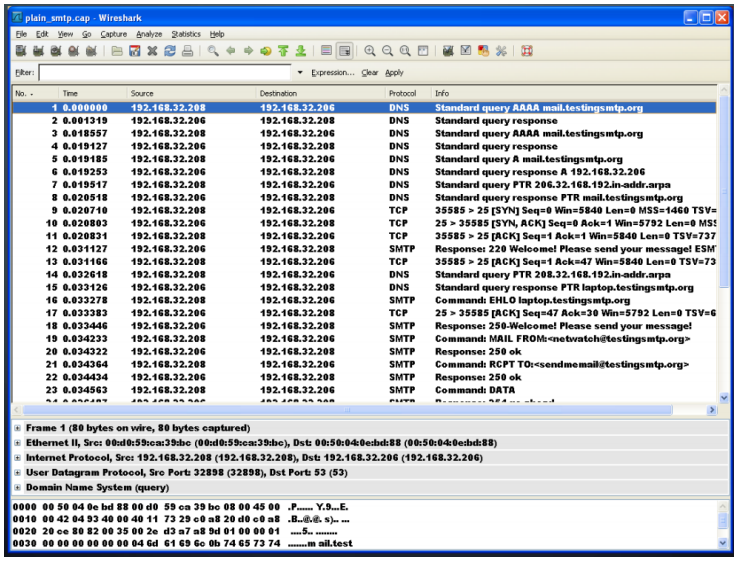
SAMPLE CONFIGURATION

- Here is the sample configuration used for the email capture files



CONFIG NOTES

- The server runs DNS, SMTP and POP3 on the Linux OS
- The client also runs Linux on a laptop
    - The qmail package is running
- The dummy domain for this is testsmtp.org
- Two mail accounts setup on the mail servers
    - `sendmemail@testingsmtp.org`
    - `netwatcher@testingsmtp.org`
- Outgoing mail is directed to
    - `mail.testingsmtp.org`
- Incoming is directed to
    - `pop3.testingsmtp.org`
- Many servers may be configured on a single physical machine, in this case 192.168.32.206
- SMTP listens on port 25
- POP3 listens on port 110
- The machine also runs a DNS so the host name testingsmtp.org can be translated into the IP address of the server



OUTGOING MAIL

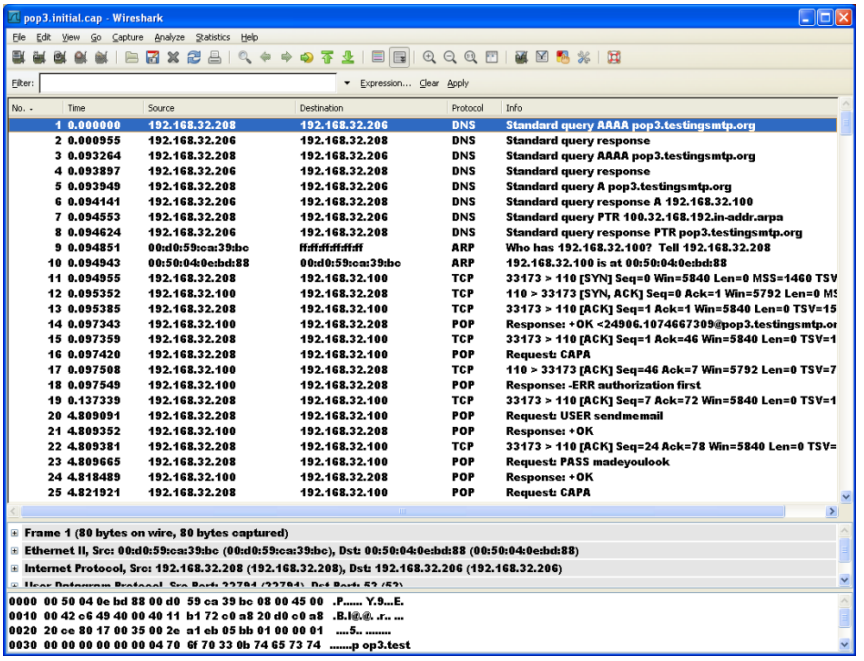
- Look at the Wireshark capture file
- plain.smtp.cap
- `netwatch@testingsmtp.org` sends an email from the laptop
- Things start off with several DNS requests (P1,P3,P5) and ass for the address of the outgoing mail server
    - `mail.testingsmtp.org`
- P1,P3 are AAAA requests for compatibility with IP V6, not really interested in that
    - P5 is a DNS A record, responded to by server with IP 192.168.32.206
    - P7 is a PTR request to translate 192.168.32.206 back to a machine name (to be sure)
    - Server responds with name `mail.testingsmtp.org`
- P9 a TCP connection is initialised to port 25 on 192.168.32.206 (email well known port)
- P12 from server is a greeting
    - 220 Welcome! Please send your message! ESMTP
    - Ready and speaks Extended SMTP
- P16 client responds
    - EHLO `laptop.testingsmtp.org` (EHLO is extended HELO)
    - Thus laptop is identified
- P14,P15 issues DNS requests to validate ID of client
- SMTP servers today are configured to identify the email clients and to allow only those on their LAN to send outgoing email
- This prevents them from being used to send lots of spam or to hide the true source of the email (address spoofing)
- As before with HTTP, you can follow the entire TCP trace by going to the Analyse menu and choosing Follow TCP Stream from the menu

SMTP TRANSFERS

- Commands
- MAIL FROM specifies email address of sender
- RCPT TO specifies address of recipient, may me many
- DATA the body of the email itself, terminated by a single dot “.” on a line by itself (CRLF.CRLF) (carriage return line feed)

DATA SECTION

- Headers
    - subject, from, to, content-type etc. and the message itself
    - Used for display purposes when viewed by recipients
- After the data section, another email could start off again, so emails may be batched together when sending over the SMTP connection
- Terminates with a RSET and QUIT



INCOMING MAIL

- pop3_initial.cap has the retrieved client side email
- P1-P8 contain DNS interactions
- P11 the POP connection starts. POP3 is version 3 of the Post Office Protocol POP
- Server speaks first
    - +OK24906.1074667309@pop3.testingsmtp.org
- CAPA is first command issued by client, requests that server return a list of capabilities including saying which authorisation mechanisms it supports
    - Server does not do this (it is an extension of the basic protocol) and answers –ERR authorisation first
- Client sends username and password in plain text with USER and PASS commands.
- Server responds that both are OK
- Client once again tries CAPA, server responds –ERR unimplemented, so authorisation was required to get anything out of the server
- UIDL 1, LIST and UIDL commands used to gather information about user `sendmemail@testingsmtp.org`
- There are 2 messages
- LIST returns a list of messages with their size in bytes
- UIDL returns a list of messages with an identification number
    - POP does not specify how these numbers are assigned exactly
- LIST and UIDL provide information to client to allow it to decide whether to download the messages
    - May look at identification number to see if it has it already
    - Look at the size to see if it is too big do download over perhaps a slow network.
- RETR 1 requests that message 1 be sent over the channel.
- This is the message sent in plain.smtp.cap

EMAIL HEADERS

- Received emails carry a lot of information in their headers, more than outgoing email
- Email servers add headers as they process the email
- Take the email from the Wireshark file
- Start with header immediately above Subject header
    - First line added is “Received from laptop.testingsmtp.org (192.168.32.208) by mail.testingsmtp.org with SMTP; 21 Jan 2004 06:40:40 -0000”
    - Second line added, “Received (qmail 24897 invoked from network); 21 Jan 2004 06:40:40 -0000” This indicates that as soon as it was received by the SMTP server from the client, it transferred the message to the qmail server.
    - qmail placed it in the user sendmemail@tectingsmtp.org and added the header “Delivered-To: sendmemail.testingsmtp.org”
    - qmail adds a Return-Path header to reflect the contents of the MAIL FROM field used in transferring the message
- Full set of headers sent to recipient, you can see them by turning on full headers in your email client.
- Headers are useful in tracking unwanted email
- Headers can be forged!

POP3

- Simple download and delete (optional)
- Uses well-known port 110
- May be encrypted with TLS or SSL on well-known TCP port 995 (gmail does this)
- RFC 1939 and RFC 2449 and RFC 1734
- No new proposals since 2003
- IMAP is now becoming the more common one to use

IMAP

- Set up your email client to use either POP or IMAP
- Some advantages over POP
- Download only the headers, download full emails one, by one
- Track state of massages, been read, replied to , deleted, state stored on server
- Multiple clients on same mailbox (forbidden in POP)
- Stay connected or not, for users with many or large messages, may result in faster response times.