COMP3203 Final Exam Notes

William Findlay
et al.

December 14, 2018

Contents

1 Test 1 Stuff (Brief and Important Only)

1.1 Units

prefix	base 10 conversion	base 2 conversion
pico	10^{-12}	2^{-40}
nano	10^{-9}	2^{-30}
micro	10^{-6}	2^{-20}
milli	10^{-3}	2^{-10}
—	10^{0}	2^{0}
kilo	10^{3}	2^{10}
mega	10^{6}	2^{20}
giga	10^{9}	2^{30}
tera	10^{12}	2^{40}
peta	10^{15}	2^{50}

- $Hz \implies$ cycles per second
  - $GHz \implies 10^9$ cycles per second
  - etc.

1.2 Equations

1.2.1 Frequency and Period

- $T = \frac{1}{f}$
- $f = \frac{1}{T}$

1.2.2 Wavelength

- $\lambda = vT$
- $f = \frac{v}{\lambda}$, since $f = \frac{1}{T} \implies \lambda = \frac{v}{f}$
  - for electromagnetic waves in a vacuum, $v = c$

1.2.3 Bandwidth

- $B =$ lowest frequency $-$ highest frequency
  - Hz
  - bps
  - or any scalar of the above two

1.2.4 Delay

- propagation delay $= \frac{\text{distance}}{\text{speed of light in medium}}$
- transmit delay $= \frac{\text{packet size}}{\text{bandwidth}}$
- queue delay = buffering and switching delays at nodes
- **total delay** = propagation + transmit + queue
- **RTT** or round-trip-time $= 2 \times$ delay

1.2.5 Delay Bandwidth Product

- # of bits $= B \times D$
  - e.g., # of bits $= 10bps \times 10s = 100b$
- this is the number of bits of data that can be sent before the first bit arrives
- we can send $2(B \times D)$ bits before we receive the first reply bit

1.2.6 Shannon Capacity

- maximum theoretical capacity
- $C = B\log_2\left(1 + \frac{S}{N}\right)$, where $\frac{S}{N}$ is the signal/noise ratio
  - high $\frac{S}{N} \implies$ good capacity
  - low $\frac{S}{N} \implies$ poor capacity $\because \log_2(1+0) = 0$
- $\frac{S}{N}$ should be in Db

1.2.7 Redundancy

- redundancy $= \frac{n+r}{n}$
- r redundancy bits must cover $n + r$ bits for errors
  - in other words, 2^r must be able to express $n + r$ bits
  - this means $2^r > n + r$
  - or, $n < 2^r - r$

1.3 Error Checking

- VRC
- LRC
- **CRC**
  - *this is usually used before ARQ*
- checksum

2 ARQs

- **(A)**utomatic **(R)**epeat Re**(Q)**uests
- strategy to handle errors detected by the CRC
  - or whatever other detection method
- main types
  - **stop and wait**
  - sliding window
    - **go back N**
    - **selective reject**

2.1 Sliding Window

2.1.1 Go Back N

- most commonly used sliding window
- sequential frames numbered $n \mod N$
- send up to $N - 1$ frames **before an ACK is received**
- **unbounded sequence numbers** is a hurdle for sliding window in **non-FIFO** channels

ACKs and NAKs

- if no error
  - send RR (ACK) for frame[n]
- if error
  - send REJ (NAK) for frame[n]
- if frame lost, send a NAK
- if no ACK or NAK received before *timeout*, **assume lost**

When Sender Receives a NAK[n]

- resend frame[n] and all frames sent since

When a Sender Receives No ACK or NAK

- go back to the previous ACK and resend all frames sent since

2.1.2 Selective Reject

- similar to go back N
- **BUT** we only resend the **lost frame**
  - out of order!
  - receiver needs *sorting logic* to store frames after a NAK
- in general, smaller window size

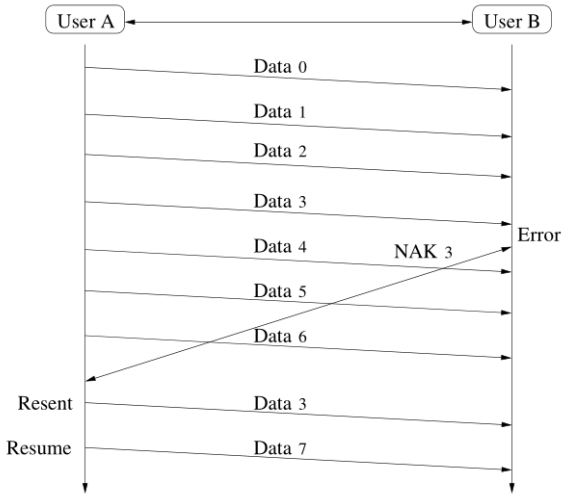


Figure 1: An example of the Selective Reject protocol.

2.2 Stop and Wait

- also called an **ABP**
  - *alternating bit protocol*
  - because the label bits alternate between `0` and `1`
- you can think of it as sliding "window" with a **window size of 1**
- works only in **FIFO queues**
  - suitable for **data link layer**

2.2.1 Errors in Stop and Wait

- two main types
- **frame** errors
  - damaged frame
- **ACK** errors
  - damaged acknowledgement

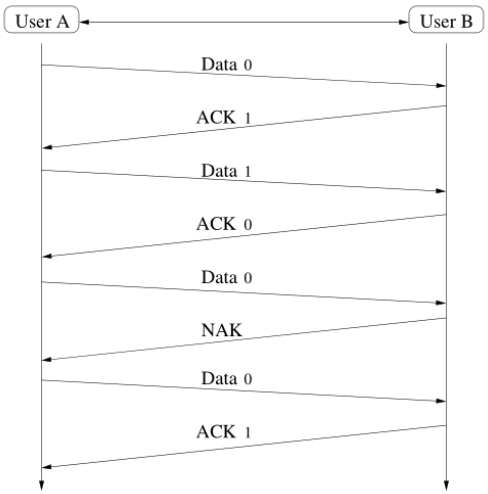


Figure 2: A diagram of the Stop and Wait ARQ protocol.

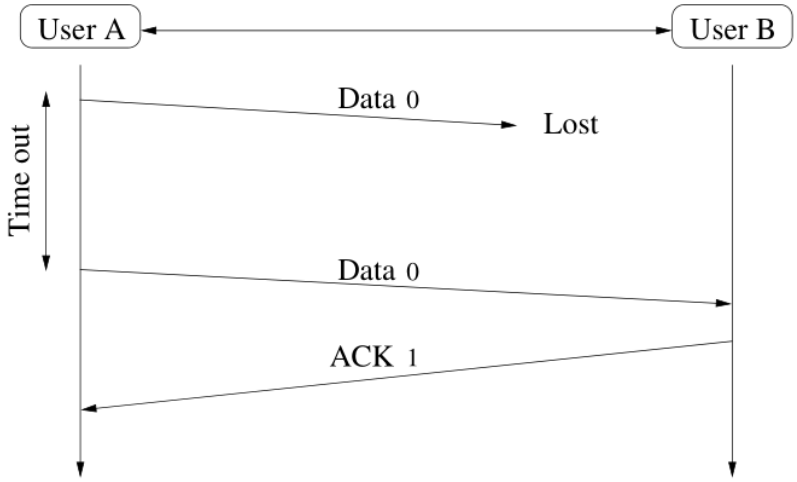


Figure 3: A lost frame error in the Stop and Wait ARQ protocol.

Frame Errors

- frame is damaged
  - one or more bits have been altered
- discard the frame
- source waits for ACK
  - if it doesn't receive one, it will resend

ACK Errors

- frame is received but ACK is damaged
- sender will resend message
- receiver will accept the same message twice
  - so we need to label frames
  - and label ACKs

- use a bit for this
  - ACK[b] acknowledges frame[$b+1 \mod 2$]
  - says receiver is ready for frame[b]

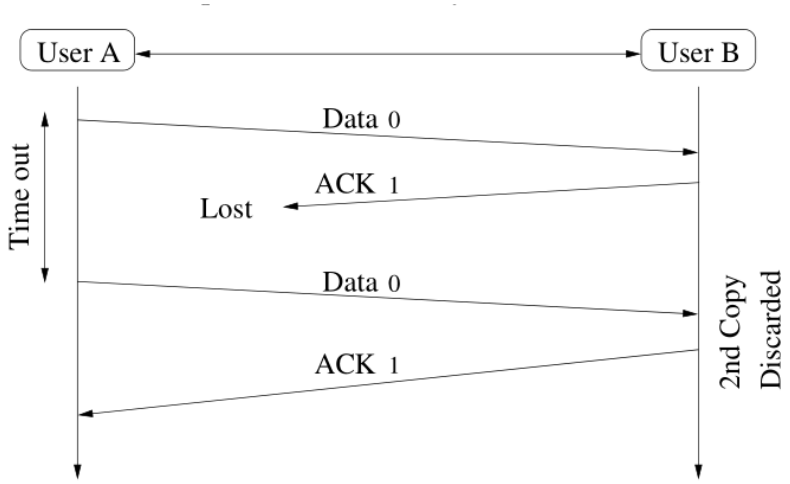


Figure 4: An ACK error in the Stop and Wait ARQ protocol.

2.2.2 Correctness

- satisfies:
  - safety
    - algorithm never gives an incorrect result
    - always results in a "corrected" error
  - liveness
    - never enters a deadlock condition

3 Multiaccess

3.1 LANs

- two types
  - *switched*: interconnection by means of transmission
    - lines, multiplexes, switches
    - hierarchical addressing scheme
    - routing tables
  - *broadcast*: information received by all users
    - no routing
    - flat addressing scheme
    - **(M)**)edium **(A)**)ccess **(C)**)ontrol to coordinate transmissions
    - *preferred over switched* due to *simplicity*

3.2 The Problem with Shared Channels

- in point-to-point networks, received signal is a function of one transmitted signal
- In broadcast networks a single transmission medium is shared. Received signal is a function of possibly more than one transmitted signal

- How do we mediate access to shared channels? -Medium Access Control (MAC) sublayer between Physical and DLC (Data Link Control) is used to solve this problem

3.3 MAC Protocol

- *Centralized*: A distinguished node (master) makes access decisions for the remaining nodes (slaves).
  - Centralized schemes are too dependent on master failure and generally less efficient.
- *Distributed*: All nodes are equivalent and the access decision is derived together in a distributed fashion.

3.4 How do you share a medium?

- *Static Partitioning Schemes*: Partition transmission medium into separate dedicated channels.
- *MAC Schemes*: Dynamic and on-demand. However, must minimize collisions.

3.5 Some examples: Types of Networks

- Satellite channels (wireless) Iridium network
- Multitapped bus (wired): Ethernet
- Star topology with hub (wired) Fast Ethernet
- Packet radio networks (wireless) Ad Hoc, Bluetooth, Piconets, Wireless networks
- Cellular networks (wireless) Cell phones, Wireless LANs

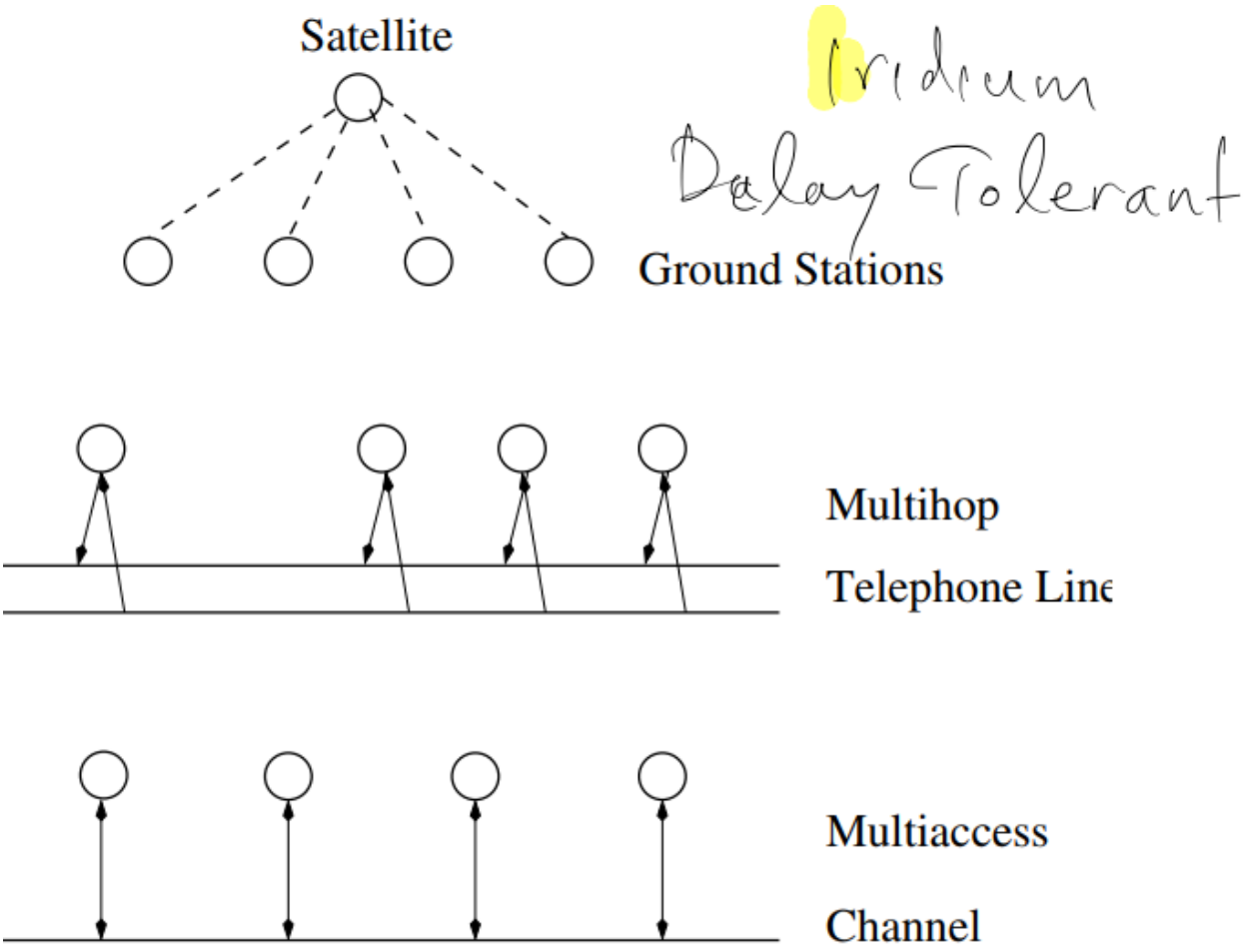


Figure 5: Some example of network topologies.

3.6 How Do You Mediate Access?

- Given that there are many users, several issues must be taken into account.
  1. Give access to each user that wants to communicate.
  2. Decide who talks first.
  3. Be fair to all.
- Let's work with the case of 2 hosts
  - We need to address the following
    1. Measure the Propagation Time
    2. Coordinate access.
    3. Select a winner.

3.7 Measuring the Propagation Time(2 hosts)

- Let T_{prop} be the bit-propagation time of a channel.
- Let d = "distance between the two stations" and v = "the speed of the medium"

Then we have:

$$T_{prop} = \frac{d}{v}$$

- Both stations can measure T_{prop}, can use ping
- So we can assume they both have the same value for T_{prop}.
- T_{prop} is also

$$\frac{RTT}{2}$$

3.8 Access Coordination Algorithm(2 hosts)

```
A (B) listens to channel
if channel not busy:
  A (B) transmits packet
  A (B) continues to listen to channel
  if B (A) has not began transmission "by time T_prop":
    A (B) is certain packet will reach B (A)
  else:
    A (B) detects collision and retransmits.
```

- If user A is to be able to detect a collision it must occupy the channel for a time period of $2T_{prop}$ time units.
- Note: Since both stations can measure T_{prop} , at the latest, by time $2T_{prop}$, A will know if a collision occurred
- Stations measure time T_A (T_B) from the beginning of (their own) packet transmission to the time a collision occurs.

3.8.1 Conditions for the winner

- Stations A and B can compare T_A and T_B with T_{prop}. $T_A < T_B \iff T_A < T_{prop}$
  1. A wins $\iff T_A < T_B$.
  2. Losing station remains quiet until winner completes transmission.
  3. For the sake of fairness, after completing transmission, the winner remains quiet for $2T_{prop}$ time units to allow the loser to capture channel.

3.9 Efficiency

- For each packet sent, $2T_{prop}$ time is required to coordinate access.
- If bit rate is R and packet length is L then channel efficiency is

$$\begin{aligned} & \frac{L}{L + 2T_{prop}} \\ = & \frac{1}{1 + \frac{2T_{prop}}{L}} \\ = & \frac{1}{1 + 2a} \end{aligned} \qquad \text{where } a = \frac{T_{prop}}{L}$$

- small $a \implies$ more efficient channel

Note The prof also gave us that overhead:

$$\frac{L + 2T_{prop}}{L}$$

$$a = \frac{dR}{vL}$$

Comparing Performance of Some Networks

Use transmission speed $v = 3 \cdot 10^8\ m/s$, and packet length $L = 1,500B = 12,000b$. Vary distance d and transmission rates R.

d Network	Rate $R =$ 10 Mbps	Rate $R =$ 100 Mbps	Rate $R =$ 1 Gbps	
100 m	$3.33 \cdot 10^0$	$3.33 \cdot 10^1$	$3.33 \cdot 10^2$	$= T_{prop}R$
LAN	$2.77 \cdot 10^{-4}$	$2.77 \cdot 10^{-3}$	$2.77 \cdot 10^{-2}$	$= a$
10 km	$3.33 \cdot 10^2$	$3.33 \cdot 10^3$	$3.33 \cdot 10^4$	$= T_{prop}R$
MAN	$2.77 \cdot 10^{-2}$	$2.77 \cdot 10^{-1}$	$2.77 \cdot 10^0$	$= a$
1000 km	$3.33 \cdot 10^4$	$3.33 \cdot 10^5$	$3.33 \cdot 10^6$	$= T_{prop}R$
WAN	$2.77 \cdot 10^0$	$2.77 \cdot 10^1$	$2.77 \cdot 10^2$	$= a$

For each d and R we compute $T_{prop}R$ and $a = \frac{T_{prop}R}{L} = \frac{dR}{vL}$.

Figure 6: Comparing performance speeds of networks.

3.10 Scaling Ethernet

- In Ethernet, where there is broadcasting type of message passing, every node is always listening to the network and may initiate transmission only when the network is silent.
- The network is a broadcast media in which every node can hear every other node.
- In order for two nodes not to send data simultaneously in a quiet network, nodes must listen to their transmissions, and if the data a node reads from the Ethernet does not match the data it is placing on the Ethernet, it knows that a collision has occurred.
- Whenever a collision occurs, a node stops sending and waits a random time before attempting to retransmit.

3.11 Limitations of Ethernet: Distance Factor

- In a 10 Mb Ethernet, the minimum packet size is 64 bytes for a 5 km cable.
- In a 1 Gb Ethernet, the minimum packet size is about 6400 bytes.
- From an architectural perspective 6400 bytes is too large a number for the minimum packet size.

3.12 Other Issues

- Medium access protocol is very technology dependent!
- Can we be sure that measurements are accurate?
- Even "Echo" measurements may differ for two hosts!

Nevertheless, resulting protocols are realistic and efficient because they are on-line

- Peer-to-Peer concern communication between two users as opposed to MAC protocols that concern many.
- A rough comparison of tradeoffs is given in the following table.

	Peer-to-Peer	MAC
# Nodes	Two	Many
Concern	Loss/Delay	Interference
Method	Sequencing	Randomization
Mechanism	ACK	Coordination
Performance	Delay × Bandwidth	Delay × Bandwidth
Node-Status	Independent	Coordinated

Figure 7: Comparison of peer-to-peer and MAC protocols.

Some LAN Devices: Host, network bridge, network hub, network transceiver

4 Wireless

4.1 Dynamic

- Wireless networks is a group of nodes in range of each other
- BBS (Basic Service set) is a group of nodes
- BSA (Basic service area) is the geographic area covered by a BSS
- Each BSA has an AP (access point)
- ESS (Extended service set) is used to extend a set of BSS
- For a node to join an ESS it must associate with an AP

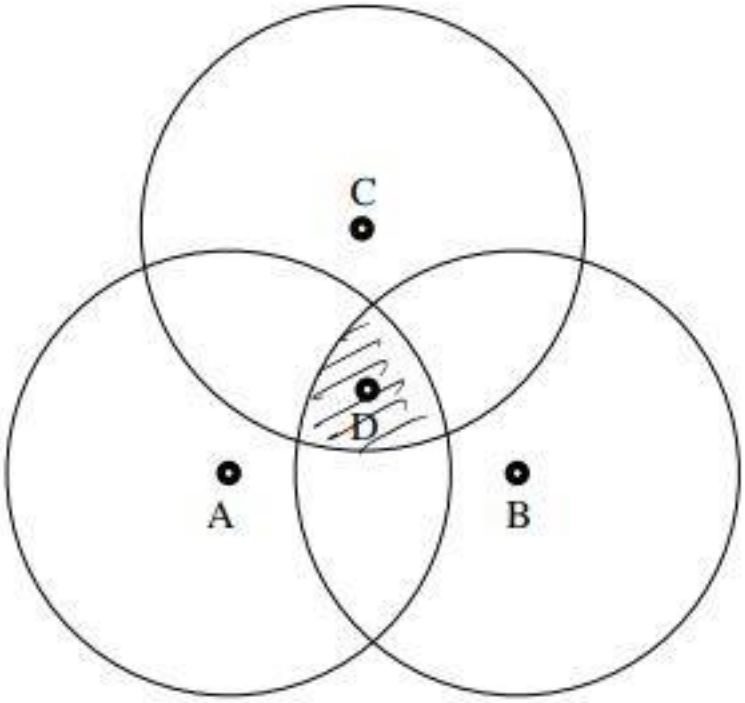


Figure 8: Let A, B, C be a unit distant graph and D be in the intersection of the three unidirectional coverage. How do we avoid collisions in this circumstance?

4.2 Spread Spectrum

- Spread information over wider bandwidth to make jamming or interception harder
- Two types of spread techniques
  - Direct Sequencing
  - Frequency Hopping
- We do this to hide / encrypt signal avoid noise and use independent same bandwidth (CDMA) DSSS (Direct Sequence Spread Spectrum)
- Let n be the number of bits we transmit at a time
- Sender randomly generates b bits, $b_1, b_2, \ldots, b_n$. Each bit gets XOR by b the original bit
- Implemented in physical layer
- Not a multi access method
- XOR bit data by chip

4.3 FHSS (Frequency Hopping Spread Spectrum)

- Let B be the number of bits and n being the number of channels to hop
- Hops frequency sending B/n bits on each frequency (loop once all n channels visited)
- Time user stays in a band in called dwell time

4.4 CDMA: Code Division Multiple Access

- Multiplexing (Allowing multiple users to communicate over the same time on the same channel)
- Break each bit into k chips according to a fixed pattern called the user's code
- New channel has chip data rate (k * R) chips per second.

4.5 Sharing Methods Over a Channel With CDMA

- Exclusive FDMA or TDMA
- Simultaneous use of FDMA and TDMA
- Calls are distinguished along the "code" dimension
- All calls may share the same frequency since each transmission s assigned a unique code
- Analogy is a cocktail party which people talk in different languages at the same time. Now the issue is controlling volume.
- Example if chip code is (1, -1, -1, 1, -1, 1)
  - Send 1 bit send the chip code
  - Send 0 bit send the compliment of the chip code which is (-1, 1, 1, -1, 1, -1)
- Each user in U owns a specific bit pattern consisting of n bits (b1,. . . ,bn)

4.6 Selecting Patterns for CDMA

- Let $\vec{U}$ be assigned a vector which is either -1 or 1 for an n generated bit sequence.
- Let $\bar{u} = (-u_1, \ldots, -u_n) becomponentsof \vec{U}$
- Let $\vec{u} = (u_1, \ldots, u_n)$
- Let the inner product of $\langle u, \rangle >= 1$ and $\langle u, \bar{u} \rangle = -1$
- Transmission: Transmit bit 1 user U send its vector u, transmit 0 send compliment u
- Example to send 1011 given A has code 00011011 we send a(compliment a)aa etc.

4.7 Decoding CDMA

- Compute $\langle u, \sum_{v \in S}(Bv) \rangle$

4.8 Collision Avoidance

- B and C will collide if they transmit at the same time
- A can reach B but is unaware of C
- C can reach B but is unaware of A

4.9 Exposed Node

- Nodes can transmit but other nodes in the range of that given node can hear that node

4.10 Communication Paths in Wireless

- Each node can propagate a message to the next for instance given A,B,C,D,E,F,G and each node is in range of the next we can form a path from A to G even if A is not in range of G.
- Asymmetry in networks are when we have to nodes which one node can reach the other but not vice versa.

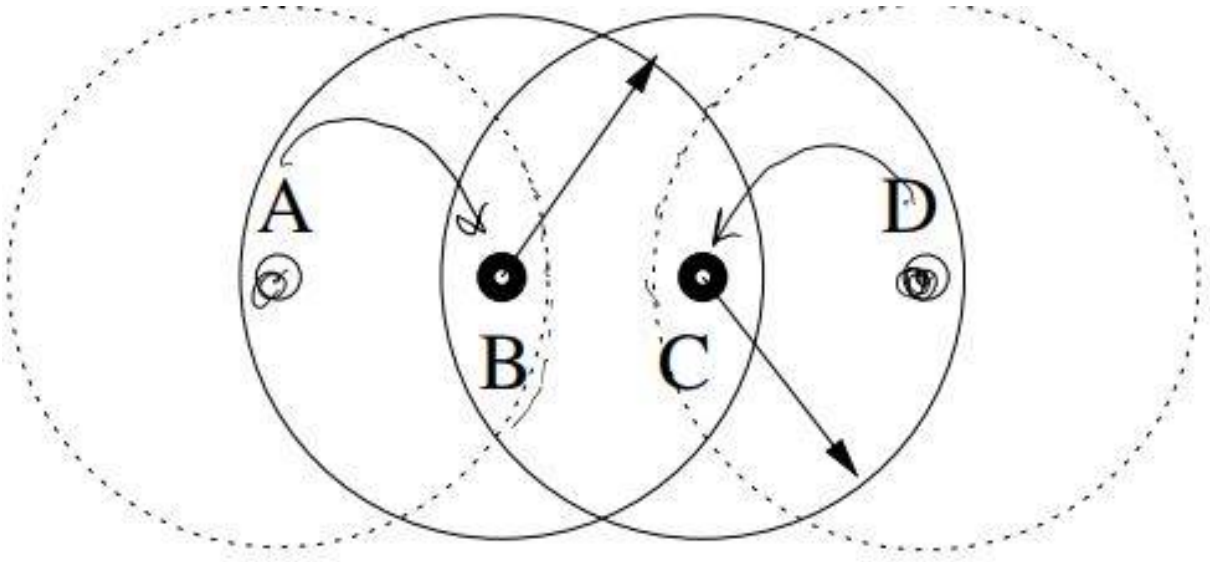


Figure 9: Collision avoidance in action.

4.11 Attenuation

- The farther away a device is from a base station the more objects in its way

4.12 Power Levels

- TPC (Transmission Power Control) Algorithm
- Attempts to equalize power transmitted to received signal powers

4.13 Interference

- When two signals over lap transmissions will be coupled

4.14 Signal to Interference Ratio (SIR)

- Device tells base station to lower or increase power of transmission

4.15 MACA (Multiple Access Collision Avoidance) Algorithm

- Sender sends (RTS) request to send which includes how long it wants to use the medium.
- Receiver replies with CTS (Clear to send)
- If CTS not received after a timeout then Back off algorithm is executed
- Receiver sends ACK after receiving
- All other nodes must wait for ACK before transmitting

4.16 Nodes are NOT All Equal

- In a distributed system node transmit over access points
  - Scanning for Access Points
  - Station sends Probe frame
  - If AP is in range respond with Probe response frame
  - Station selects AP and responds with Association Request frame
  - Access Point responds with Association Response frame

4.17 IEEE 802.11: Framers

- Three types of frames
  - MF (Management Frames): association, disassociation, timing, synchronization, authentication and de authentication
  - CF (Control Frames): Used for Handshaking and positive ACKs during an exchange
  - DF (Data Frames): Used for data for data transmission

4.18 Bluetooth

- Piconets
- Star network
- Master is the central node slave nodes connect to master
- Communication is strictly Master -> Slave or Slave to Master
- All masters have at least 1 and at most 7 slaves
- Piconets can be enlarged to form scatter nets
- Master and slave can switch by using different frequencies
- Scatter nets care multiple Pico nets connected by bridges

4.19 Scatter Net

- Network of Pico nets
- Consists of Masters and Slaves (Bridge or Pure)
- Two Masters can share only a single slave (Bridge)
- Piconet can only have at most 7 slaves
- Each bridge may only connect two Pico nets

4.20 Bluetooth establishing links

- Start
- Synchronization
- Discovery
- Paging
- Connection established

4.21 Discovery Delay Procedure

- To support spontaneous connectivity inquiry is used and connection are established based on information exchange
- Application sets Bluetooth into inquiry mode then sends inquiry msg to probe for other nodes
- Other Bluetooth devices will only listen unless set to inquiryScan
- Collision Avoidance which is the method used to avoid collision which uses some randomness

4.22 Connection Establishment

- Takes several seconds
- Follows uniform distribution between inquiry and inquiryScan

4.23 Bluetooth frames

- 72 Access Code 54 Header 0-2744 Data
- Header broken down is 3 Addr 4 Type 1 F 1 A 1 S 8 Checksum

4.24 Broadband Wireless

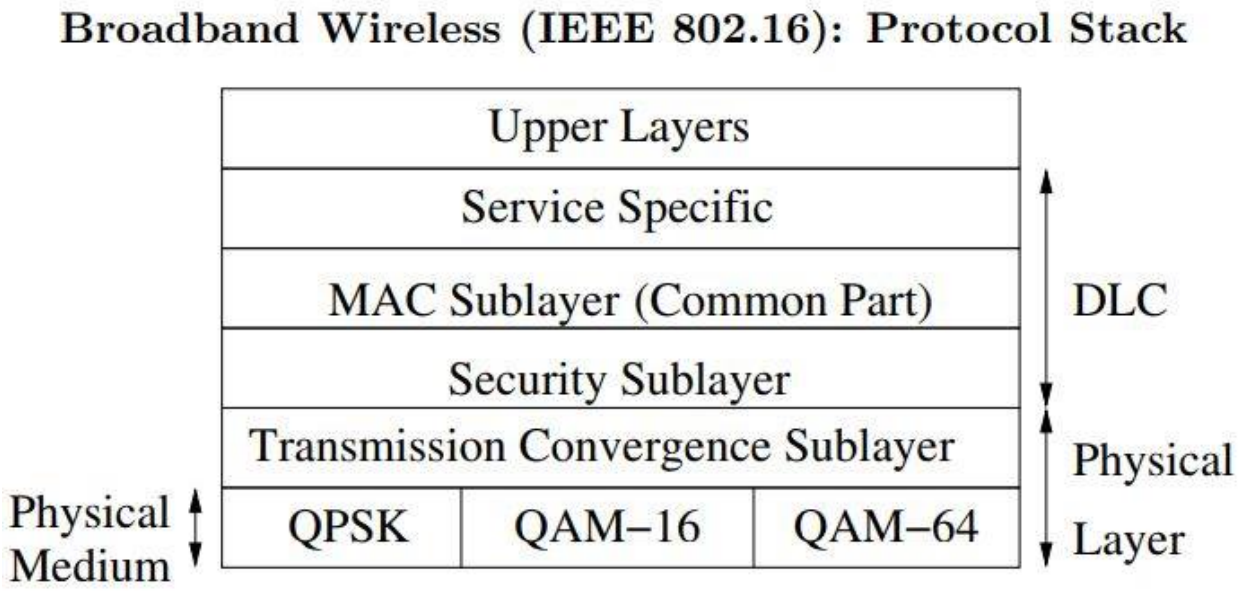


Figure 10: The broadband wireless IEEE protocol stack.

5 GPS

5.1 Three Techniques

5.2 Satellites

6 Routing

6.1 Distance Vector (RIP)

6.2 Link State Protocol (LSP)

6.3 MSTs

6.4 Dijkstra

7 IP

7.1 8.1 IP Networks

- Most widely deployed network layer protocol worldwide. Emerged as a project made by the US and has grown exponentially.
- Defined in RFC (Request for Comments) 760 and 791.
  - RFC 791 is based on editions of the ARPA Internet Protocol referred to as IPv4
    - 791 States that the IP performs tow basic functions: addressing and fragmentation
      - **addressing**: assures unique addressability of hosts
      - **fragmentation**: splitting the messages into a number of IP packets to combat packet size constraints, and reassembly of packets at destination in order

7.2 8.1.1 IP Addressing/classes

- In addition to physical addresses nodes have 32 bit IP Addresses

- Has a two level hierarchy consisting of the net ID and the Host ID which identifies the network the host is connected to.
- There are five classes of addresses: A, B, C, D, E.

Class	Net ID	Host ID
A	7 bits	24 bits
B	14 bits	16 bits
C	21 bits	8 bits

Figure 11: Division of bits in class A, B, and C IP classes.

- D is used for multicasting and E for experiments.
- To reach a host on the internet, there are two levels.
  - First level: We reach the network using the first portion of our address
  - Second level: We reach the host itself using the last portion of the address.
- Addresses are broken into four bytes

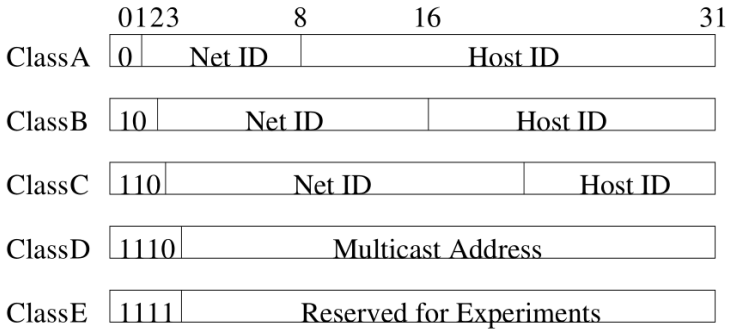


Figure 12: Breakdown of the five IP classes.

7.3 8.1.2 Subnetting

- Is the solution to the two level hierarchy where addresses cannot be grouped into a "less flat" scheme
- Only the router should be aware of the subnetting.
- from subnetting, we have three levels in the hierarchy
  - Net-id (`135.17`)
  - Subnet-id (`12.22.23`)
  - Host-id
- Subnetting provides routing boundaries for communications and routing protocol updates.
- Subnetting is facilitated by specifying a network mask along with the network address.
- Subnetting takes the single IP network address and allocates it to several physical networks referred to subnets.
  - Subnets should be near each other physically.

7.4 8.1.3 Subnet Masks

- The mechanism to allow a network number to shared by numerous networks is subnet masking.
- A subnet number is where all hosts on the same network have the same subnet number.
- Subnet masks introduce another level hierarchy into IP-addressing, where the Address now has three parts: network part, subnet part, and host part.
- A subnet mask is used "hide" addresses.

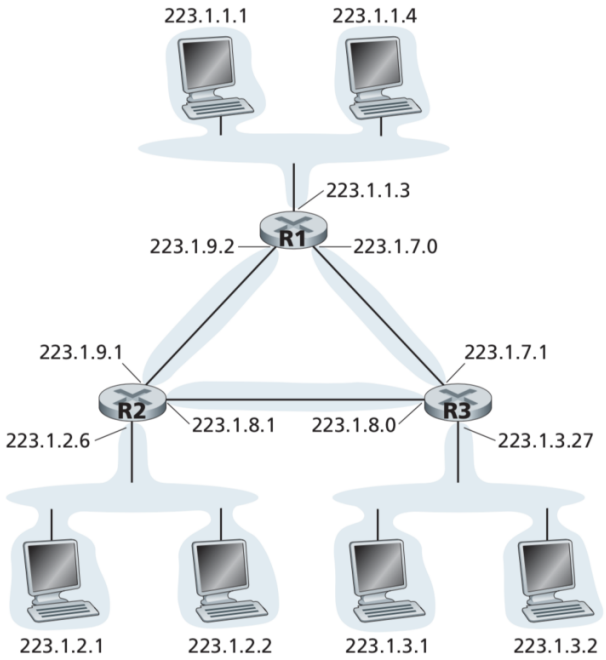


Figure 13: An example of subnetting.

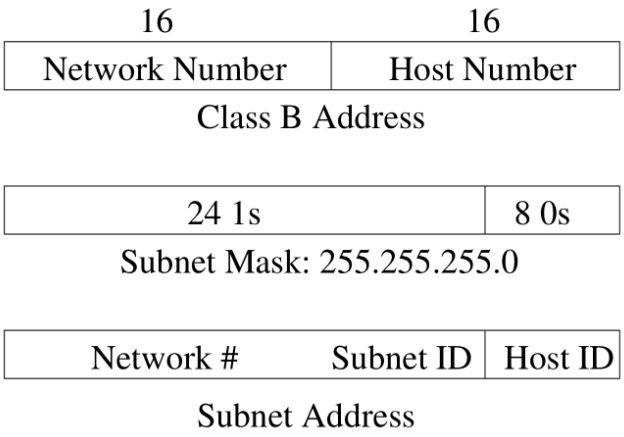


Figure 14: Subnet masks.

- A subnet mask separates the IP address into network and host addresses
  - (`<network><host>`)
- Subnetting further would divide the host part of an IP address into a subnet and host address.
  - (`<network><subnet><host>`)
- Masking extracts the address of the physical network from an IP address.
- If there is no subnet masking, it'll extract the networks address from the IP address. If there is a subnet division, it will extract the subnet address from the IP address.
- Hosts are configured with an address and the subnet mask.
- The bitwise And of these two numbers defines the subnet number of the given host.

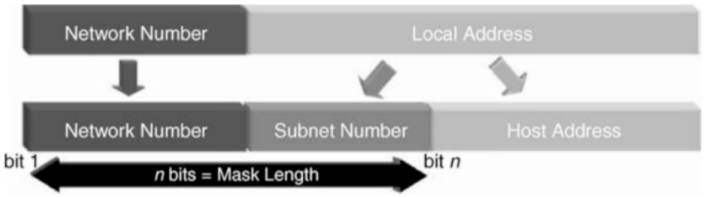


Figure 15: Subnet masks.

Host	H1	H2
Subnet Number	128.96.34.15	128.96.34.139
Subnet Mask	255.255.255.128	255.255.255.128
BIT-WISE AND	128.96.34.0	128.96.34.128

Figure 16: Subnet masks.

1. H1 forwards to H2
2. H1 calculates AND of H2's subnet address (`128.96.34.139`) with subnet mask (`255.255.255.128`)
   i) If result is equal to H1's Subnet Number (`128.96.34.128`)
      - then it is delivered to NextHop for H2 of its forwarding table
   ii) If it is not equal to H1's Subnet Number
      - then packet is forwarded to H1's default router.

7.5 8.2 IPv4

- A connectionless protocol for use on packet-switched Link Layer networks
- Operates on best effort delivery model, no guarantee of IP packets, no assurance of proper sequencing, and avoidance of duplicate delivery.
- All of the above is addressed by an upper layer transport protocol, such as TCP (Transmission Control Protocol)
- IP is the vehicle for traffic management, based on IP based internets were designed to support delay insensitive applications
  - Control congestion
  - Provide low delay
  - Provide high throughput
  - Support QoS
  - Provide fair service

7.5.1 IPv4 Header

- IP's with no options are 20 Bytes, **IHL** (Header Length) is in 32-bit words
- TOS (Type of Service): Guidance on selecting next hops and relative allocation of router resources.
- TOS Subfields: provide route selection, subnetwork service, queuing discipline.
- Procedence Subfield: indicates the degree of urgency from highest level to lowest level
- IPv4 options: Security, Timestamping, Source routing, Route Recording.

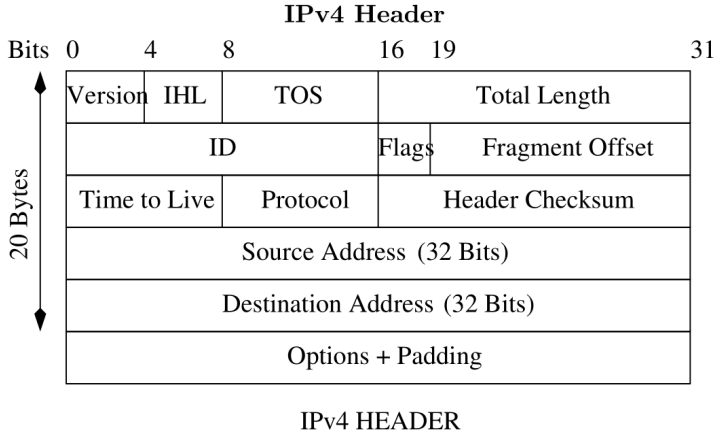


Figure 17: A diagram of the IPv4 header.

7.6 8.3 ARP (Address Resolution Protocol)

- enables hosts to build tables which can be managed either by an administrator or dynamically by the host.
  - performs updates approximately every 15 minutes
  - performs queries that take advantage of broadcasting capabilities of local networks.

7.7 8.3.1 RARP (Reverse Address Resolution Protocol)

- an obsolete computer protocol where a client computer is used to request its internet protocol (IPv4) address from a computer network.
- All the protocol will have is the link layer or hardware address
- The client will broadcast the request and does not have prior knowledge of the network.

7.8 8.4 DHCP (Dynamic Host Configuration Protocol)

- DHCP Is a protocol that automates the process where before the host can send packets, they'll need to know the address of a default router. This would be alot of work if done directly or manually by hosts.
- Saves administrators from having to walk to each host and the information from this protocol is stored in a table.

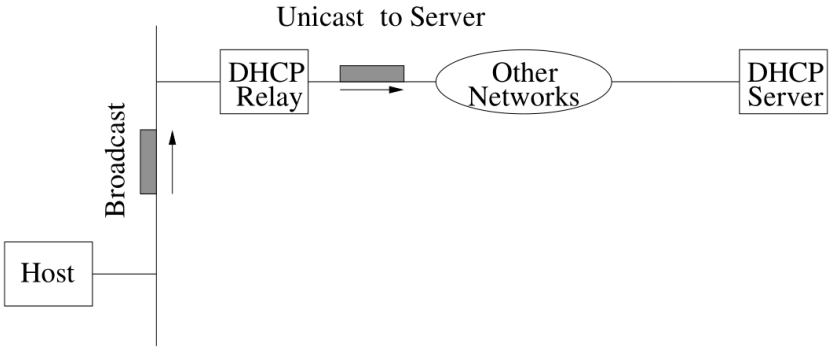
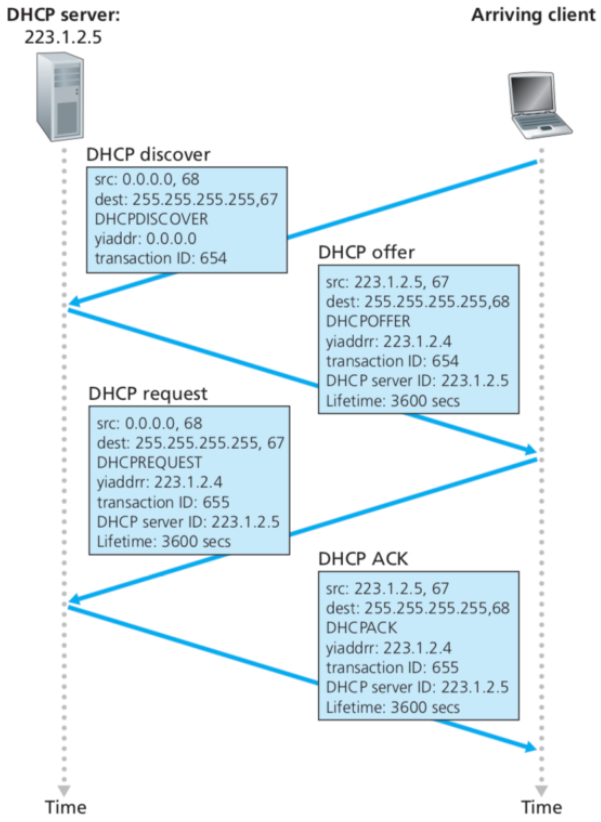


Figure 18: DHCP protocol application.



DHCP Packet Format

Operation	HType	HLen	Hops
Xid			
Secs		Flags	
ciaddr (client IP address)			
yiaddr (your IP address)			
siaddr			
giaddr			
chaddr (client hardware address)			
sname (server name)			
file			
options (defaults, etc)			

- How does DHCP work?
  - The host broadcasts a Discover Message in its network
  - The network servers respond with a Offer message
  - The host then selects one of the offers and broadcasts a request message.
  - The network servers then acknowledges the message with a DHCP ACK and assigns IP addresses for a period of time with two thresholds. $T1, T2$ (usually, $T1 = T/2 and T2 = 7T/8$).
  - When $T1$ expires host attempts to extend lease by sending DHCP Request to same server. If accepted host also gets new values T, $T0 = 1$, $T0 = 2$ If host does not receive DHCP ACK by time $T2$ then it broadcasts to any server in the network. If no ACK is received by time T then host must relinquish old IP address and begin anew.
  - If a router or host is unable to sent a message, the IP will report an error/errors
  - IP has a companion protocol, called Internet Control Message Protocol (ICMP) that defines error messages

7.9 8.5 IPv6

- built to provide more addressing capacity to meet current and future address requirements.
  - main issues with IPv4
    - support for real time services
    - security support
    - autoconfiguration
    - enhanced routing functionality

7.9.1 8.5.1 IPv6 Header

- Designed to accommodate higher speeds with 128 bit addresses.
  - IPv4 can address up to 232 (= 4 billion) nodes. IPv6 can address up to 2128 = (232) 4 hosts.

- IPv6 Format: An IPv6 packet has the form: IPv6-header, extension field, · · · , extension header, format level PDU (Protocol Data Unit).
- Priority Field: defines types of traffic
- Flow Labels: e.g. multimedia traffic consists of audio flow, video flow, data flow.

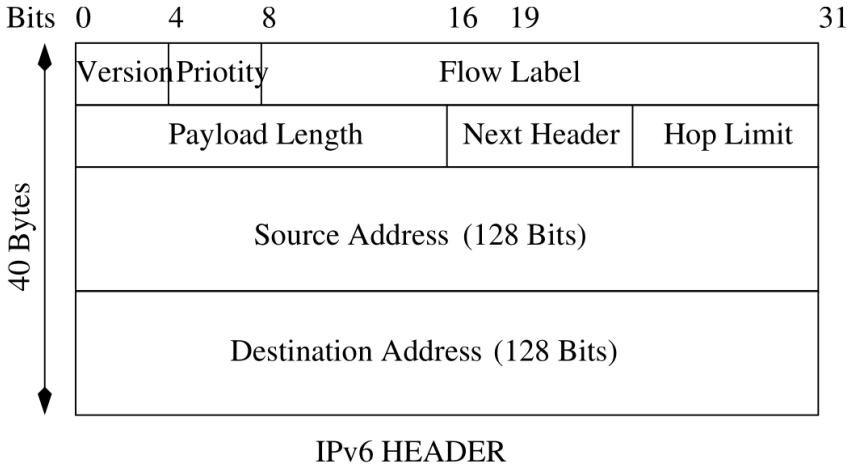


Figure 19: IPv6 header.

- No classes are being used, which leaves large addresses chunks unaddressed which allow for future growth.
  - NSAP used for ISO
  - IPX for Novell
  - Link local and Site local enable address construction without concern for global addresses (useful for autoconfigurations)
  - Multicast is for multicast addresses, by zero extending with a byte of 0s one assigns IPv4-compatible and IPv4-mapped IPv6 addresses.

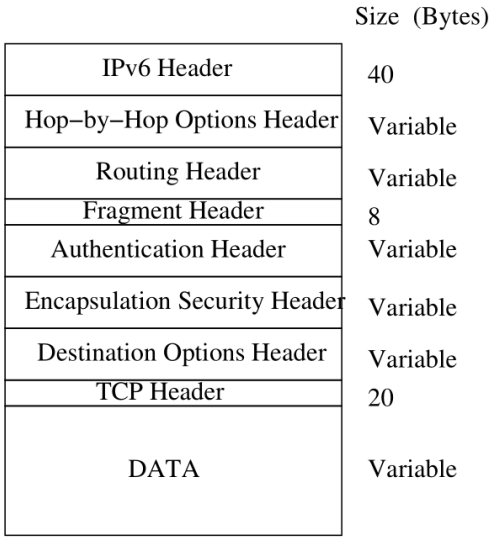


Figure 20: IPv6 header.

7.9.2 8.5.2 Assigning Addresses

- Three types of addresses:
  - Unicast
  - Anycast (different interfaces)
  - Multicast (different nodes)
- Hop-by-Hop Options Header: carries optional information that must be examined (like next header, header extension length, options)
- Fragment Header: only done by source nodes and not by routers. These nodes perform a path discovery algorithm to determine smaller max transmission unit.
- Routing Header: contains a list of one or more intermediate nodes to be visited along the way. Intermediate nodes that should be visited like Next Header, Header Extension Length, Routing Type,
- Destinations Options Header: carries optional information.

7.9.3 8.5.3 Notation

- hexadecmial digits are used, represented in eight 16-bit blocks.
- One set of contiguous 0s can be omitted: `block1::block7:block8`
- An IPv4-mapped address, like `128.33.87.51` is now written as: `00FF:128.33.87.51`
- 001 prefix used for global unicast addressing.
- 010 prefix used for IPv6 provider based address. Here, registry IDs are provided as common identifiers.
- IPv6 and DHCP provides s IPv4 autoconfiguration.
  1. obtain correct subnet address prefix (through a router)
  2. IPv6 provides for anycast addresses: selects one of a set of any. Also multicast and security provided.

7.9.4 8.5.4 Neighbour Discovery

- Allows a node to discover subnet addresses on which the IPv6 node is connected with.
- Automatically identifies routers on the subnet
- This process allows each router to periodically send advertisements on each of its configured subnets, showing their IP address, ability to provide default gateway functionality, link layer address, networks served on the link and valid address lifetime.

7.9.5 8.5.6 IPv6 Deployment / Classless Inter-Domain Routing (CIDR)

- Only 3% domain names and 12% of networks have IPv6 protocol support.
- Implemented on all major operation systems in use in commercial, business, and home consumer environments.
- IoT (Internet of Things) is giving a significant boost to IPv6.
- First major use in 2008 summer Olympics
- China and the Federal U.S. Government are also starting to require support for IPv6 on their equipment.
- Modern cellular telephones also mandate IPv6 operation and deprecate IPv4 as an optional capability
- As of 2018
  - Over 25% of all Internet-connected networks advertise IPv6 connectivity.
  - 49 countries deliver more than 5% of traffic over IPv6, with new countries joining all the time.
  - In 24 countries IPv6 traffic exceeds 15%

8 TCP

- based on the end-to-end connectivity paradigm
  - functions should **not** be implemented at **lower system levels** unless they can be **correctly implemented** at that level
- main features:
  - sliding window

  - variable RTTs
  - packets can be out of order
  - connections learn about each other's resources
  - monitor congestion
  - control resource allocation

8.1 How it Works (Sliding Window)

8.1.1 Connecting

- A sets SYN bit and register a SEQ#
- B sets SYN bit and registers a SEQ#
  - acknowledges with A's SEQ# + 1
- A acknowledges with B's SEQ# + 1

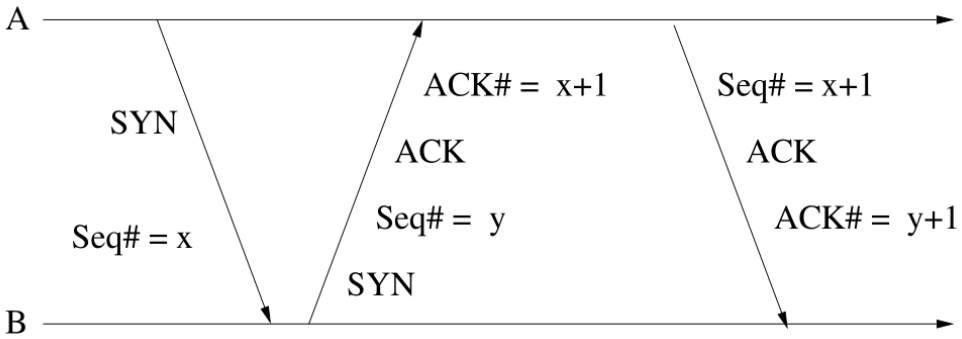


Figure 21: The three-way handshake of a TCP connection.

- this is important because
  - A informs B of its starting number
  - B acknowledges and informs A of its own starting number
  - A acknowledges B's starting number
- in this way, they can anticipate what the other will do
- a timer makes sure that if an expected response is not received, they will retry

8.1.2 Disconnecting

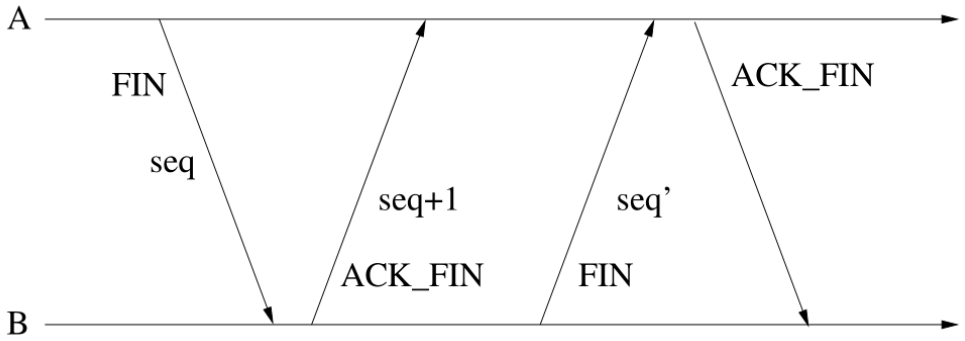


Figure 22: Closing a TCP connection.

- A sets FIN bit with SEQ#
- B responds with its own FIN bit

- A acknowledges

8.2 How it Builds Statistics

8.3 Equilibrium Model

9 Sample Test

1

A system has an n-layer protocol hierarchy. Applications generate messages of length M Bytes. At each level of the layers, an h-Byte header is added.

1.1

[3 pts] What fraction of the network bandwidth is filled with headers? (Give the formula.)

$$\text{overhead} = \frac{nh}{nh + M}$$

1.2

[3 pts] Now assume $M = 20h$. What should the max number n of layers be so that the fraction in previous Question 1 does not exceed 10 % of the total?

$$\begin{aligned}
\text{overhead} &= \frac{nh}{nh + M} \\
10\% &\geq \frac{nh}{nh + 20h} \\
\frac{1}{10} &\geq \frac{n}{n + 20} \\
(n + 20)\frac{1}{10} &\geq n \\
(n + 20)\frac{1}{10} &\geq n \\
\frac{n}{10} + 2 &\geq n \\
n + 20 &\geq 10n \\
20 &\geq 9n \\
n &\leq \frac{20}{9}
\end{aligned}$$

1.3

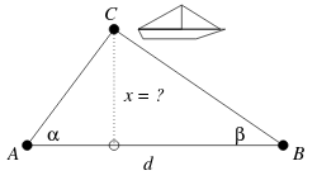
Two CDMA users are assigned the 9-bit vectors $A = 110011011, B = 100101111$, respectively. Are they orthogonal? (Prove or disprove!) **Hint:** Recall $0 \to -1$ and $1 \to +1$.

Take inner product of vectors in $\mod 2$.

$$\begin{aligned}
\langle \vec{A}, \vec{B} \rangle \mod 2 &= 1 + 0 + 0 + 0 + 1 + 0 + 0 + 1 + 1 \mod 2 \\
&= 0 \qquad \iff \text{orthogonal}
\end{aligned}$$

2

You are observing a ship from two base stations A, B. Assume that at this time of observation $\alpha = \pi/3, \beta = \pi/4$ and $d = 1000\ m$.

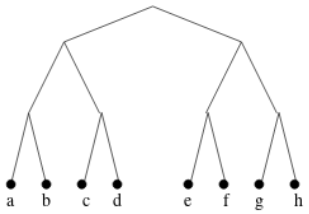


Derive a formula for the unknown distance x (You are not required to evaluate the trigonometric functions of $\pi/3$ and $\pi/4$).

$$x = d\frac{\tan\alpha\tan\beta}{\tan\alpha + \tan\beta}$$
$$x = 1000\,\mathrm{m}\frac{\tan\frac{\pi}{3}\tan\frac{\pi}{4}}{\tan\frac{\pi}{3} + \tan\frac{\pi}{4}}$$

3

Ethernet stations a, b, c, d, e, f, g, h contend for a channel. Assume a, e, f, g, h become ready at once and that they use the tree resolution protocol to resolve contentions.

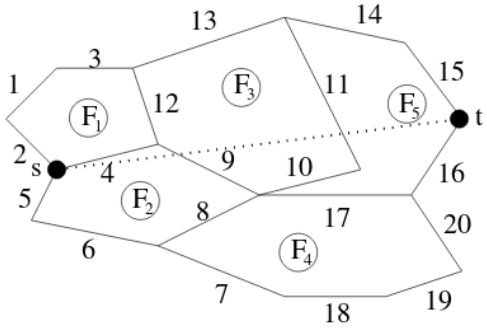


for each contention slot give in the table below the winning stations.

Slot	Station
1	a e f g h
2	a
3	e f g h
4	e f
5	e
6	f
7	g h
8	g
9	h

4

The links and faces of a planar wireless network are labeled as depicted in the Figure below. Moreover there is a source node s and a destination node t.



4.1

Apply the face routing algorithm with the left-hand rule (on a face) to give a path from s to t. In the table below name the face and the edges of that face being traversed. **Your answers must list all the links traversed and the paths formed must arise from the corresponding routing algorithm!**

Face	List of Edges Being Traversed
F_1	2, 1, 3
F_3	13
F_5	14, 15

4.2

Apply the compass routing algorithm to give a path from s to t.

5

6

7