COSC244 Contents

[Data Security 2](#_Toc23448752)

[Caesar Ciphers 2](#_Toc23448753)

[Polyalphabetic Cipher 2](#_Toc23448754)

[Transposition Cipher 2](#_Toc23448755)

[Bit Level Cipher 2](#_Toc23448756)

[Data Encryption Standard (DES) 3](#_Toc23448757)

[Private Key Encryption 3](#_Toc23448758)

[Public Key Encryption 3](#_Toc23448759)

[RSA Algorithm 3](#_Toc23448760)

[Authentication 3](#_Toc23448761)

[Pretty Good Privacy (PGP) 3](#_Toc23448762)

[Networks 4](#_Toc23448763)

[Topologies 4](#_Toc23448764)

[ISO’s OSI Model 4](#_Toc23448765)

[Protocols 4](#_Toc23448766)

[Layers 4](#_Toc23448767)

[Media Access Control 6](#_Toc23448768)

[Random-access Protocols 6](#_Toc23448769)

[Pure Aloha Protocol 6](#_Toc23448770)

[Slotted Aloha Protocol 6](#_Toc23448771)

[Carrier Sense Multiple Access (CSMA) 6](#_Toc23448772)

[Medium Sensing Methods 6](#_Toc23448773)

[p-Persistent CSMA 6](#_Toc23448774)

[CSMA/CD (with Collision Detection) 7](#_Toc23448775)

[Binary Exponential Backoff Algorithm 7](#_Toc23448776)

[Controlled-access Protocols 7](#_Toc23448777)

[Token Passing 7](#_Toc23448778)

[Slotted Ring 7](#_Toc23448779)

[Ring Problems 7](#_Toc23448780)

[Channelization Protocols 7](#_Toc23448781)

[FDMA 7](#_Toc23448782)

[TDMA 7](#_Toc23448783)

[CDMA 7](#_Toc23448784)

[Flow and Error Control 8](#_Toc23448785)

[Flow Control 8](#_Toc23448786)

[Frame Format 8](#_Toc23448787)

[Flow Control Protocols 8](#_Toc23448788)

[Unrestricted Protocol 8](#_Toc23448789)

[Stop and Wait Protocol 8](#_Toc23448790)

[Measures of Protocol Efficiency 8](#_Toc23448791)

[Sliding Window Protocol 8](#_Toc23448792)

[Go-back-N Protocol 9](#_Toc23448793)

[Selective Repeat Protocol 9](#_Toc23448794)

[Sliding Window Size 9](#_Toc23448795)

[Local Area Networking 10](#_Toc23448796)

[LAN Standards 10](#_Toc23448797)

[Ethernet 10](#_Toc23448798)

[IEEE Standard 802.3 10](#_Toc23448799)

[Hardware Components 10](#_Toc23448800)

[Ethernet Frame Format 10](#_Toc23448801)

[Advanced Ethernet Techniques 10](#_Toc23448802)

[Token Ring 11](#_Toc23448803)

[IEEE Standard 802.5 11](#_Toc23448804)

[Token Frame 11](#_Toc23448805)

[Data Frame 11](#_Toc23448806)

[Ring Maintenance 11](#_Toc23448807)

[Fiber Distributed Data Interface (FDDI) 11](#_Toc23448808)

[Wide Area Networking 12](#_Toc23448809)

[Network Connecting Devices 12](#_Toc23448810)

[Repeater/Hub 12](#_Toc23448811)

[Bridge 12](#_Toc23448812)

[Router 12](#_Toc23448813)

[Gateways 12](#_Toc23448814)

[Connection Concepts 12](#_Toc23448815)

[Connection-Oriented Service 12](#_Toc23448816)

[Connectionless Service 12](#_Toc23448817)

[Switching 12](#_Toc23448818)

[Circuit Switching 12](#_Toc23448819)

[Message Switching 12](#_Toc23448820)

[Packet Switching 12](#_Toc23448821)

[LANs vs WANs 13](#_Toc23448822)

[Routing 13](#_Toc23448823)

[Centralised Routing 13](#_Toc23448824)

[Distributed Routing 13](#_Toc23448825)

[Static Routing 13](#_Toc23448826)

[Dynamic Routing 13](#_Toc23448827)

[Routing Comparisons 13](#_Toc23448828)

[Routing Algorithms 14](#_Toc23448829)

[Shortest Path Routing 14](#_Toc23448830)

[Distance Vector Routing 14](#_Toc23448831)

[Link Stating Routing 14](#_Toc23448832)

[Hierarchical Routing 14](#_Toc23448833)

[Routing in Internet 14](#_Toc23448834)

[Internet Protocol 15](#_Toc23448835)

[History of the Internet 15](#_Toc23448836)

[Who Controls It 15](#_Toc23448837)

[Internet Activites Board 15](#_Toc23448838)

[IPv4 15](#_Toc23448839)

[Packet Fields 15](#_Toc23448840)

[Address Classes 15](#_Toc23448841)

[Problems 15](#_Toc23448842)

[IP Routing 16](#_Toc23448843)

[Router’s Actions 16](#_Toc23448844)

[Address Resolution Protocol (ARP) 16](#_Toc23448845)

[Packet Fragmentation 16](#_Toc23448846)

[IPv6 16](#_Toc23448847)

[Purpose 16](#_Toc23448848)

[Packet Header 16](#_Toc23448849)

[Extension Header 16](#_Toc23448850)

[IPv4 and IPv6 Differences 16](#_Toc23448851)

[Domain Name System (DNS) 17](#_Toc23448852)

[Internet Control Message Protocol (ICMP) 17](#_Toc23448853)

[Transport Control Protocol 18](#_Toc23448854)

[Overview 18](#_Toc23448855)

[Types of Data Deliveries 18](#_Toc23448856)

[Transport Layer 18](#_Toc23448857)

[Functions 18](#_Toc23448858)

[Address 18](#_Toc23448859)

[Internet 18](#_Toc23448860)

[TCP Segment 18](#_Toc23448861)

[TCP Connection 18](#_Toc23448862)

[Connection Establishment 18](#_Toc23448863)

[Connection Termination 19](#_Toc23448864)

[Error Control 19](#_Toc23448865)

[Checksum 19](#_Toc23448866)

[Acknowledgement 19](#_Toc23448867)

[Retransmission 19](#_Toc23448868)

[Duplicate Segments 19](#_Toc23448869)

[Out-of-order Segments 19](#_Toc23448870)

[Lost/corrupted Segments 20](#_Toc23448871)

[Flow Control 20](#_Toc23448872)

[Congestion Control 20](#_Toc23448873)

[Slow Start 20](#_Toc23448874)

[Congestion avoidance 20](#_Toc23448875)

[Congestion detection 20](#_Toc23448876)

[User Datagram Protocol (UDP) 20](#_Toc23448877)

[User Datagram Format 20](#_Toc23448878)

[Socket Programming 20](#_Toc23448879)

[Internet Applications 21](#_Toc23448880)

[Client/Server Model 21](#_Toc23448881)

[Telnet 21](#_Toc23448882)

[Secure Shell (SSH) 21](#_Toc23448883)

[Automatically generated key pairs 21](#_Toc23448884)

[Manually generated key pairs 21](#_Toc23448885)

[File Transfer Protocol (FTP) and Secure FTP 21](#_Toc23448886)

[Electronic Mail 21](#_Toc23448887)

[Simple Mail Transport Protocol (SMTP) 21](#_Toc23448888)

[Post Office Protocol (POP) 21](#_Toc23448889)

[IMAP and MIME 22](#_Toc23448890)

[World-Wide Web 22](#_Toc23448891)

[Web Server 22](#_Toc23448892)

[Web Browser 22](#_Toc23448893)

[HyperText Transfer Protocol (HTTP) 22](#_Toc23448894)

[Peer-to-Peer Model 22](#_Toc23448895)

[Firewalls 22](#_Toc23448896)

[ADSL, ATM 23](#_Toc23448897)

[Modems 23](#_Toc23448898)

[Digital Subscriber Line (DSL)/ Asymmetric DSL (ADSL) 23](#_Toc23448899)

[Asynchronous Transfer Mode (ATM) 23](#_Toc23448900)

[Small Fixed-Size Cells 23](#_Toc23448901)

[Switching 23](#_Toc23448902)

[ATM Reference Model 23](#_Toc23448903)

[IP Security (IPSec) 23](#_Toc23448904)

[Transport Mode 23](#_Toc23448905)

[Tunnel Mode 23](#_Toc23448906)

[Security Protocols 24](#_Toc23448907)

[Wireless Technologies 25](#_Toc23448908)

[IEEE 802.11 25](#_Toc23448909)

[Architectures 25](#_Toc23448910)

[Physical Layer 25](#_Toc23448911)

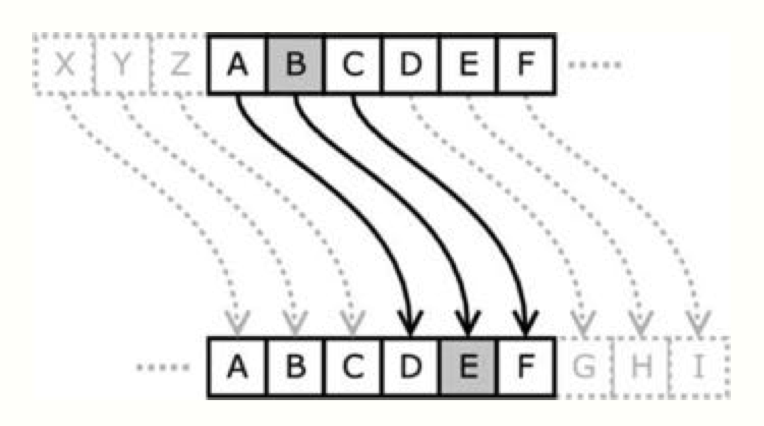
[Advanced Networks 25](#_Toc23448912)

# Data Security

## Caesar Ciphers

An example of a substitution cipher wherein each plaintext letter is substituted for another letter according to some rule set. All letters are shifted by a constant amount (e.g +3).

This is easily broken by frequency analysis as the frequency of each plaintext letter is the same. This allows you to make much more accurate guesses about what the plaintext character is, by looking for more common letters like a space, ‘a’s and ‘e’s.



## Polyalphabetic Cipher

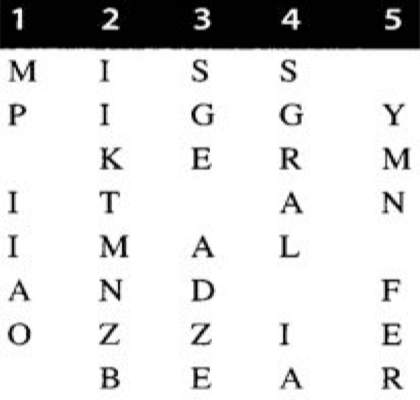
An example of a substitution cipher which uses a matrix to change the letter frequency so the plaintext character is not always replaced by the same ciphertext. If *i* is the position of the plaintext character in the message, and *j* is the position of *i* in the alphabet, the ciphertext character is found at M[*i* % 26, *j*].

It can be broken by looking for clues such as TIG being alphabetical successors to SHF. Why does this help?



## Transposition Cipher

The idea is to rearrange the plaintext of a message, by ordering the characters in a 2d array, and sending the columns out of order.



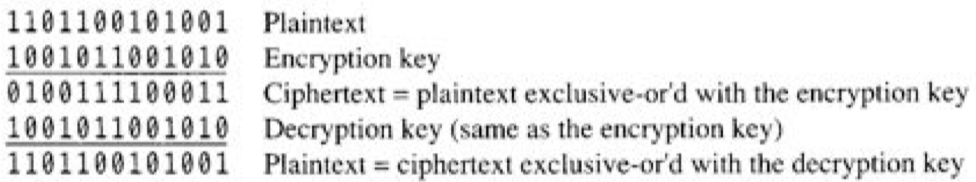
If you sent the columns in the order 2,4,3,1,5, the encrypted message would be: IIKTMNZB SGRAL IA SGE ADZE MP IIAO YMN FER

Letter frequencies will be what is expected, which implies a transposition cipher was used, not a substitution cipher. Hackers will try arrange the columns in order so it makes common substrings such as ING, THE, IS etc.

## Bit Level Cipher

Uses the idea that not all data are characters. This cipher performs an XOR operation between the data and key, and sends the result. To decrypt, perform the same operation.

With this cipher, short keys may result in repeated substrings, which would help break patterns.



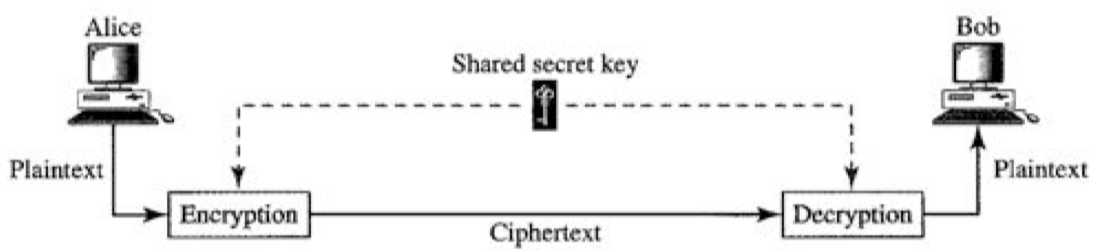
## Data Encryption Standard (DES)

A complex combination of transpositions, substitutions, XOR operations to produce 64 bits of encrypted data. It is divided into 64-bit blocks and uses a 56-bit key (256 possible keys).

It is not sufficiently secure and can broken in a few hours on a massively parallel computer.

## Private Key Encryption

Sender and receiver uses a shared symmetric-key, (e.g Caesar, transposition, DES). Secrecy of the key is vital – cannot stay encrypted if the key is not secret.



## Public Key Encryption

Encryption and decryption is separate and uses asymmetric keys, and the encryption key cannot be used to decipher the ciphertext. The receiver gives the sender a public key to encrypt the plaintext, and uses their decryption (private) key to decrypt the ciphertext.

### RSA Algorithm

Choose 2 prime numbers, *p* and *q*

*n* = *p* \* *q*

*m* = (*p*-1) \* (*q*-1)

*e* = number where greatest common divider of *e* and *m* is 1

*d* = (*e* \* *d* – 1) % *m* = 0

Public key = {*e*} (*e* = 7 and *n* = 77)

Private key = {*d*} (*d* = 43 and *m* = 60) (SECRET)

Encryption: *C* = *Pe*% *n*

Decrpytion: *P* = *Cd*% *n*

You cannot decrypt the message by a reverse operation, you would need to find *p* and *q* and *d*. If *n* is very large (over 100), finding prime numbers (factors of *n*) is very time consuming.

RSA is slow if the message is long. Good for short messages.

### Authentication

A digital signature is when the sender signs the message using their private and public key, and only they can decrypt the signature, proving they sent the message.

A message digest is a ‘summary’ of the message, using hashing algorithms. It is encrypted using the sender’s private key (this makes a digital signature), and is sent to the receiver. The receiver uses the sender’s public key to decrypt the signature and then uses the same hashing algorithms to generate a message digest of the received message. The receiver compares both message digests (the one sent, and the one they generated themselves) and if they are not the same, the message has been tampered with.

### Pretty Good Privacy (PGP)

A combination of hashing, data compression, symmetric-key cryptography and public-key cryptography.

The message is encrypted using a symmetric-key encryption algorithm, which requires a symmetric key (each key is a session key and only used once). The session key is encrypted using public-key encryption. The encrypted message along with the encrypted session key is sent to the receiver.

Using the strengths of an algorithm to compensate for weaknesses in others, it is one of the strongest and fastest encrypting algorithms.

# Networks

Computer Network: “an interconnection collection of autonomous computers which are able to exchange information online”

## Topologies

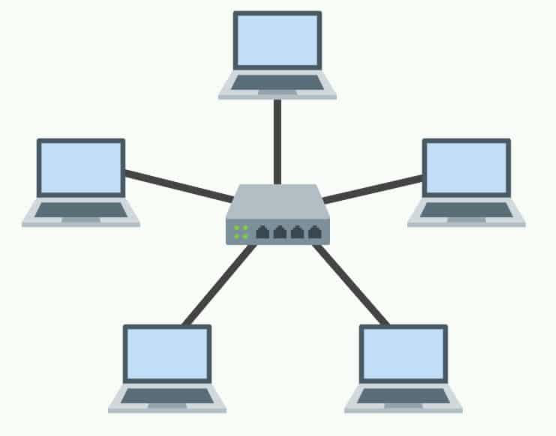
Actual networks combine these 3 types.

#### Star

Control is centralised – if a device wants to communicate it has to go through the central computer.

This means there is a focal point of responsibility and everything can be monitored through this point.

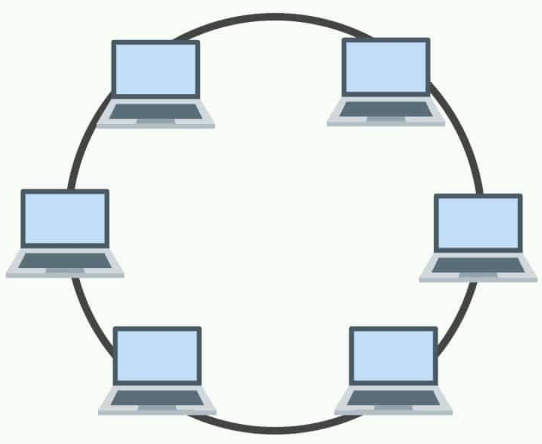
However if the central device fails, it brings down the whole network.



#### Ring

Devices are connected circularly, unidirectionally or bi-directionally.

This means there is no focal point, but failure of a device will cause a break. It takes longer to send information through this network type.

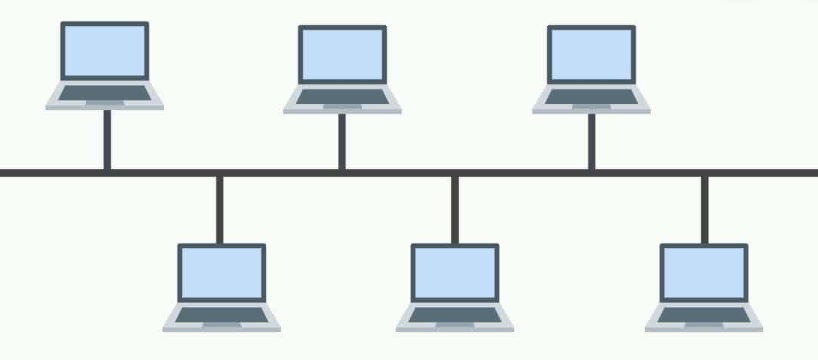


#### Bus

Devices communicate through a single bus, and only the communicating devices are involved.

It is easy to add/remove devices from this network type.

However there is a high collision rate and will slow down the data rate.



## ISO’s OSI Model

### Protocols

“set of rules governing the exchange or transmission of data electronically through devices”

They enable computers and software built by different developers to be able to communicate.

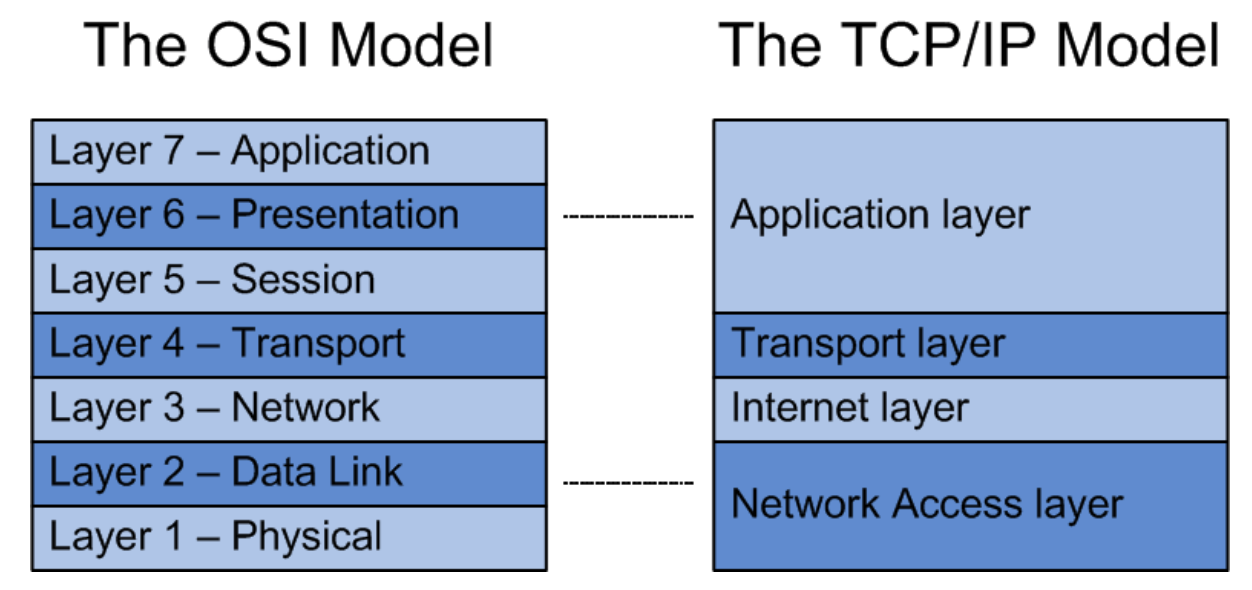
### Layers

A, P, S, T, N, DL, Ph

The OSI Model is a guideline for protocol design, not actual protocols.

Not all layers are used – Internet only uses 4 (Application, Transport, Internet, Network Access)

Some layers may get combined (often the top 3)



By using a layered protocol, it reduces complexity, provides compatibility, accelerates evolution of technology, simplifies learning

#### Application Layer

Responsible for providing services to the user and allows for communication between application and user. Provides services and protocols for electronic mail, fail transfers, virtual terminals.

#### Presentation Layer

Responsible for translation, compression and encryption. It presents data in a legible, human-readable format (e.g translating ASCII, EBCDIC). It is concerned with the syntax and semantics of the information transmitted.

#### Session Layer

Responsible for dialog control and synchronization. It allows for applications on different computers to establish and maintain connections. May coordinate the process by determining when each end is to send or listen (synchronization)

#### Transport Layer

Responsible for the delivery of a message from one process to another. Accepts data from the session layer, splits it into smaller units, and passes information to the network layer. Also ensures pieces all arrive correctly at receiver and reassemble them into the original order. It may establish multiple connections for a high throughput application.

Example protocols are TCP and UDP.

#### Network Layer

Responsible for the delivery of individual packets from the source to the destination. It determines routes, controls data congestion, and does address mapping.

Example protocols are IP, ARP, ICMP

#### Data Link Layer

Responsible for moving frames from one node to the next. It sends and receives frames. The sender accepts messages from the higher layer, breaks them into frames and hands them to the physical layer. The receiver assembles them from the physical layer into messages and hands them to the next higher layer. Detects and corrects errors (CRC, Hamming Codes). Deals with damaged, lost and duplicate frames.

Sub layers: Medium Access Control (MAC) and Logical Link Control (LLC).

#### Physical Layer

Responsible for movements of individual bits from one node to the next. Defines how signals are sent by a media and the singals and encoding used. Concerned with the physical and electrical and electrical aspects, and those interfaces between user equipment and network equipment.

Example protocols are: RS-242, RS-449, RJ-45.

# Media Access Control

MAC creates a shared communication medium that multiple stations/devices can access.

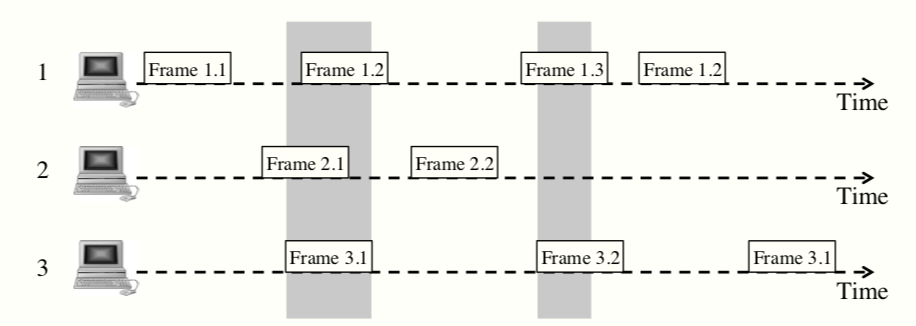
## Random-access Protocols

There is no scheduled time for a station to transmit, and they compete with each other to access the medium.

A collision occurs when 2 or more stations access the medium with an overlap, and all frames involved will either be destroyed or modified.

### Pure Aloha Protocol

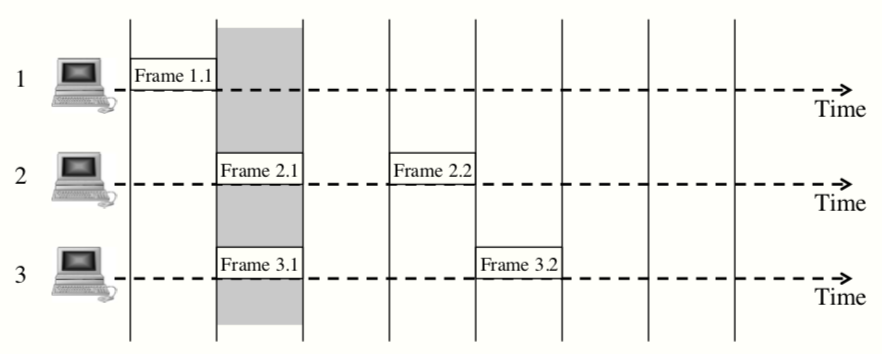
Each station transmits when it has a frame to transmit. When the receiver receives a frame, it sends an acknowledgement to the sender. When the sender receives that acknowledgement, it knows data has been received. Otherwise the sender assumes a collision and retransmits. If a collision occurs, each collided sender waits a random time before retransmission.



The randomness helps avoid more collisions. This protocol works best when there is minimal traffic. A collision wastes up to 2T time.

### Slotted Aloha Protocol

Divide time into internal slots of T units each, and each station only sends at the beginning of a slot.



Wasted time due to collision is reduced to T. Higher success rate than PAP.

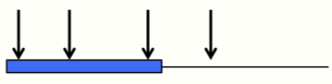
### Carrier Sense Multiple Access (CSMA)

If a station has a frame to send, it first checks the status of the medium, and transmits if there is not activity, otherwise it waits.

### Medium Sensing Methods

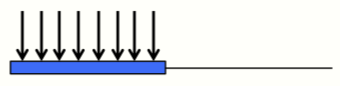
#### Non Persisent Method

If the medium is busy, wait a random amount of time and then sense again. This reduces collisions but reduces network efficiency.



#### Persistent Method

If the medium is busy, continuously sense the medium. This is the p-Persistent method.



### p-Persistent CSMA

If the medium is busy, continue to monitor the medium and when it becomes free, transmit with a probability *p*, otherwise wait for the next time slot (probability 1-*p*) and repeat.

* If *p* = 1, it is 1-persistent CSMA, and will always transmit when the medium is free
* If *p* = 0, it is 0-persistent CSMA, and will always wait 1 time slot

Collisions will still occur. If *p* = 0.5 and there are 2 stations, 4 possibilities exist when the medium becomes idle:

* Both transmit immediately
* Both wait
* Station A sends and station B waits
* Station A waits and station B sends

Result:

* 0.5 probability one will transmit successfully
* 0.25 probability medium won’t be used
* 0.25 probability of collision

### CSMA/CD (with Collision Detection)

If the medium is busy, it waits per the persistent CSMA, and when it is free, it listens to the medium for collision while transmitting the frame. If it detects a collision, it stops the transmission and sends a short jamming signal. If it receives a jamming signal, it stops the transmission. After a collision occurs, it waits a random amount of time according to the Binary Exponential Backoff algorithm and then repeats the above steps.

### Binary Exponential Backoff Algorithm

If a station’s frame collides for the first time, wait 0 or 1 time slot

After *n* collisions, wait from 0 to 2n-1 slots if n <= 10.

If n > 10, wait from 0 to 1024 (210) slots

After 16 collisions, give up and report an error

## Controlled-access Protocols

### Token Passing

Stations are organized into a logical ring, and has a token (a special frame) that circulates the ring. A station can only transmit data when it has the token frame.

When it receives the frame and wants to transmit data, it inserts the data into the token frame (making it a data frame) and passes it to the next neighbour.

When a station receives a data frame and is the destination station, it copies the data from the frame to its memory and passes the frame to the next neighbour. If it is the sender of the frame, it removes the data from the frame (making it a token frame again) and passes the token to the next neighbour.

### Slotted Ring

The same as token passing except it contains several rotating tokens. A station cannot send any other frames until the previous data frame it sent returns back to the sender.

### Ring Problems

A break in any two stations can bring the network down (like a ring network topology)

A faulty interface card can result in a “lost” token or an improperly formatted token

If a station sends a data frame and fails before removing its data, the frame circulates forever

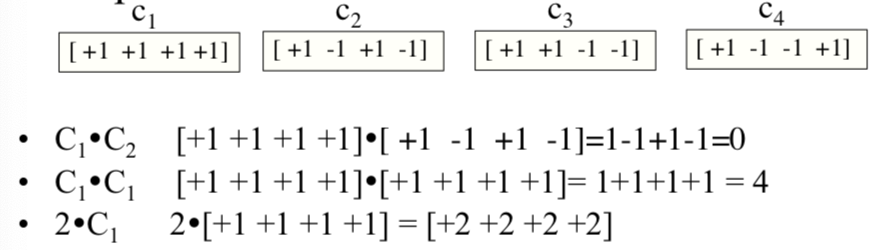
## Channelization Protocols

### FDMA

### TDMA

### CDMA

Code-Division Multiple Access, using only one channel occupies the entire bandwidth, and all stations can send simultaneously. Each station is assigned a code, and two properties on the codes. If you multiply a code by another you get 0, but if you multiply each code by itself, the value you get is equal to the number of stations.



# Flow and Error Control

Flow Control defines the way multiple frames are sent and tracked, and when to send/stop sending frames.

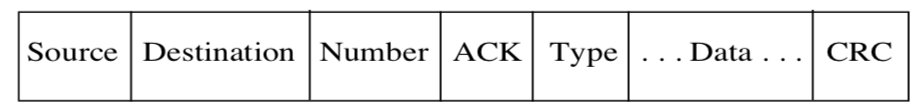
Error control defines how to check frames for errors and what to do if errors occur. It ensures all frames arrive at their destination without errors. All protocols for F&E Control belong to the Data Link OSI model layer.

## Flow Control

A frame is a group of bytes organized according to a specified format (e.g Ethernet frame), and can be carefully formatted for flow and error control. Data is transmitted in frames at the data link layer

### Frame Format

Typical frame format:



Source: address of the sending station

Destination: address of the receiving station

Number: each frame is numbered, starting from 0

ACK: an integer value designating the frame being acknowledged

Type: data, ACK, NAK

Data: the information being transmitted

CRC: error checking bits

## Flow Control Protocols

### Unrestricted Protocol

This protocol assumes the receiver has unlimited capacity/memory and doesn’t consider any problems in transmission. Keeps sending data.

### Stop and Wait Protocol

The sender transmits a data frame and then waits to receive an ACK frame before it transmits the next frame. The receiver simply needs to just send an acknowledgement for each frame it gets.

The ACK frame tells the sender that the data frame has arrived at the destination uncorrupted and in full. The sender sets a timer for the frame sent, and if no ACK frame is received by the time expires, it will resend the frame.

### Measures of Protocol Efficiency

Unrestricted uses as much buffer space as it requires.

Stop and Wait only need 1 frame buffer.

Unrestricted is transmitting data frame 95% of the time (7.6Mbps), whereas Stop and Wait only transmits 75% of the time (5.7Mbps).

## Sliding Window Protocol

Compromise between Unrestricted and Stop and Wait.

A window is defined as a subset of consecutive frames.

The window contains *i* frames numbered starting with *w*:

* Every frame numbered less than *w* has been sent and acknowledged
* No frame numbered >= w+I is sent
* Every frame in the window has been sent, but not all acknowledged. These un-acknowledged are called outstanding frames.
* If frame *j* is acknowledged, the window moves down to *j*+1, so more frames can be sent

#### Analysis

It allows multiple frames to be sent without needing to wait for them to be acknowledged.

If the maximum window size is 1, it is the stop and wait protocol, but if the window size is unrestricted, it is the unrestricted protocol.

Adjusting the window size can help control the traffic on a network.

### Go-back-N Protocol

Frames must be received in the same order as they were sent, and the sender buffers the frames in the window in case it has to resend them.

When the receiver gets a frame, if it is out of order it will send a NAK. If the frame is the expected one, it will send an ACK. The receiver uses the piggyback approach for acknowledgements whenever possible.

When the sender gets a NAK, it will resend all frames in the window. If it receives an ACK for frame *j*, it knows all frames before *j* were received and can move the window to *j*+1, so more frames can be sent.

A frame timer is used, and the sender will resend all outstanding frames if it does not receive an ACK. An ACK timer is also used, and the receiver will send a separate ACK frame if the timer expires.

### Selective Repeat Protocol

This protocol allows the receiver to receive the frames out of order and sort them before delivery to the user. The receiver uses a window to buffer out-of-order frames.

The receiving station’s window buffers all the frames into the correct order once all the frames have arrived successfully. When an out-of-order frame arrives, it sends a NAK for the expected frame, and sends an ACK when the expected frame arrives correctly.

The sending station resends just the frame it received a NAK for, and resends the timed-out frame if a frame timer expires.

### Sliding Window Size

The sending window size of Go-back-N must be less than 2k, and the receiving window size is always 1.

Both the sending and receiving windows of Selective Repeat must be at most ½ of 2k.

## 

# Local Area Networking

## LAN Standards

#### IEEE Standard 802.3

* Ethernet
* Bus topology

#### IEEE Standard 802.5

* Token Ring
* Ring topology

#### IEEE Standard 802.4 (obsolete)

* Token Bus
* Bus topology

## Ethernet

### IEEE Standard 802.3

The standard for Ethernet, using a bus topology. Originally used coax. Can be extended by repeats. CSMA/CD protocol.

In the physical layer of the OSI model, 803.2 uses coax, twisted pair, or fibre optics cables. It uses Manchester digital encoding. Two or more segments of an Ethernet coax cable can be connected by repeaters, a device that receives a singal, regenerates it, and transmits it.

### Hardware Components

#### Network Interface Card (NIC)

* Receives packets from PC software
* Formats frames
* Executes Binary Exponential Backoff algorithm if required
* Performs CRC error checking

#### Ethernet Hardware Address

Six octets: XX XX XX XX XX XX, where X is a hexadecimal number

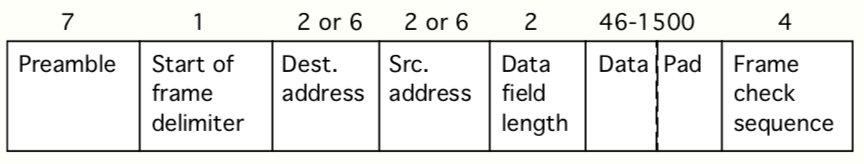
Number of addresses: 281,474,976,710,656 (248) (56,000 MAC addresses for each person on the planet)

#### Transceiver

* Interface between the PC and the cable
* Listens for collisions
* Puts bits on cable from interface card
* Passes received bits to interface card
* The cable has 5 twist pair, 2 pair for sending data and control, 2 for receiving data and control, 1 for power

### Ethernet Frame Format

Typical Ethernet Frame Format:



Preamble: 7-octet pattern of alternating 0’s and 1’s

Start of frame delimiter: 1010 1011 pattern indicating the start of a frame

Destination address/Source address

Data length field: number of octets in the combined data and pad fields

Data field: maximum is 1500 octets

Pad field: decided by the minimum size of a frame (512 bits or 64 octets)

Frame check sequence: 32-bit CRC

### Advanced Ethernet Techniques

Fast Ethernet – 100Mbps

* Mainly differ at physical layer

Gigabit Ethernet

* Burst frame for sending multiple frames
* Full-duplex mode without CSMA/CD

10 Gigabit Ethernet

* For backbone network
* Use the same MAC frames
* No CSMA/CD

## Token Ring

### IEEE Standard 802.5

The standard for Token Ring LAN, consisting of point-to-point links. It can be connected by coax, twisted pair or fibre optic cables. The token means there willi be no collisions, but a failure in any station can bring down the network. It uses Differential Manchester encoding.

Most 802.5 LANs use wire centres to improve reliability – wire centres can bypass a failed station.

### Token Frame

A typical Token Frame format:



Starting delimiter (SD) – JK0JK000

* J and K are special signals. No transition in the middle compared with differential Manchester encoding

Ending delimiter (ED) – JK1JK1IE

* I, intermediate frame bit; E, error bit

Access Control (AC) – ppptmrrr

* T, token bit – determine the frame type; 0, token frame; 1, data frame
* ppp, priority bits – token’s priority
* rrr, reservation bits – priority of the host who makes a reservation
  + a host can reserve the token by setting the reservation bits
* m, monitor bit – for removing orphan frames

### Data Frame

DA: destination address

SA: source address

FCS: frame check sequence (CRC)

FC: frame control: ffzzzzzz

FS: frame status: acxxacxx

### Ring Maintenance

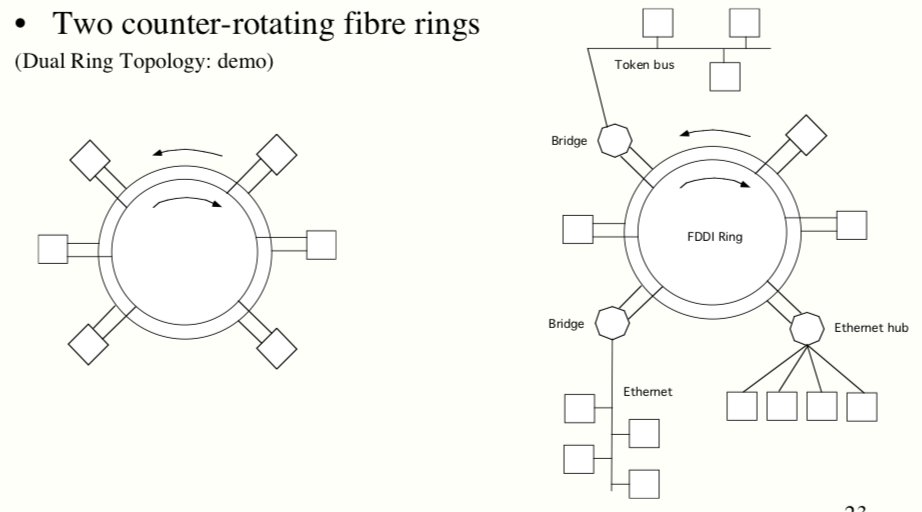
Designate a monitor host to oversee the ring.

An orphan frame is a data frame that cannot be used because the sender is no longer available. When a frame is created, the monitor bit in the AC (Access Control segment of a Token Frame) octet is set to 0. The monitor host sets it to 1. If the monitor host sees it again, the frame is emptied.

To make sure a token is always circulating, the monitor sets a timer whenever it sends a frame or token. If the time expires before a frame or token is received by the monitor, a new token is sent.

## Fiber Distributed Data Interface (FDDI)

Modelled on token ring, mainly used for large span distance up to 200km or for very high data rates. Up to 1000 hosts can connect.



# Wide Area Networking

Wide Area Network: “a computer network that spans a broad area, often a country or a continent”

## Network Connecting Devices

### Repeater/Hub

A repeater reconstructs the signal and sends it on.



### Bridge

A bridge is used to connect different LANs or a router and the internet, and it filters traffic using MAC address.



### Router

A router connects different types of LAN’s and maintains routing tables. Sends routing packets using logical addresses (IP addresses).



### Gateways

Uses character codes, encryption, compression. Has different rules for establishing connects and being secure.

## Connection Concepts

### Connection-Oriented Service

This type of service is modelled after the telephone system.

Establish a connection, use the connection, then release the connection.

The receiver takes out the information in the same order it was sent.

### Connectionless Service

This type of service is similar to the postal system.

Each message is routed through the network independent of others.

The order of information received is not guaranteed.

An independent packet is called a datagram.

## Switching

### Circuit Switching

A physical connection is established before the start of communications, an example is the telephone system. It is suitable for voice/video communication as that has a constant bit rate. It is a type of connection-oriented service: the connection is used solely by the communicating devices.

### Message Switching

At each station, the whole message is stored and then forwarded to the next switch when the route is available. It is a type of a connectionless service, as the message may travel over different routes. A disadvantage is that a long message may occupy the route for a long time.

### Packet Switching

Each message is broken into smaller packets and sent independently. Packets are received and stored until they are forwarded to the next node in the route. This type of switching supports both connection-oriented and connectionless services.

## LANs vs WANs

#### Protocol Conversion

Protocol conversion is simple and happens in LAN’s bridges.

Converts between different LAN protocols in WAN’s routers, using many different protocols and equipment.

#### Routing

Simple routing in LAN’s bridges according to LAN address (e.g Ethernet addresses)

Complex routing in WAN’s routers according to WAN addresses (e.g IP addresses). It requires much more complex strategies and paths can experience failures and congestions.

## Routing

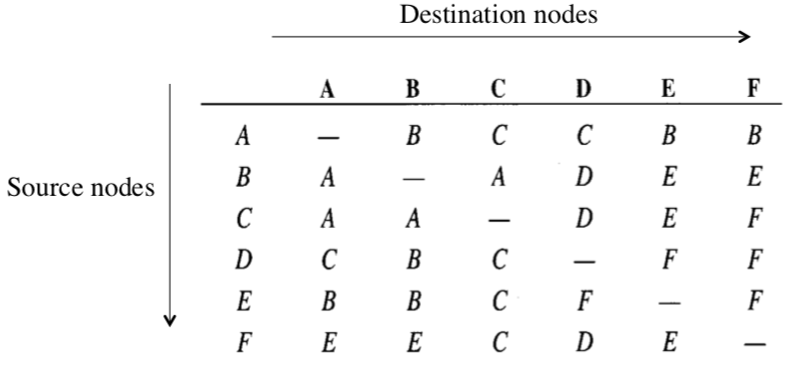
The routing metric is the major factor considered when routing. This includes: length of path, number of hops, transport time, in-route delays.

In routing tables, specify the next-hop node and the cost to get there.

### Centralised Routing

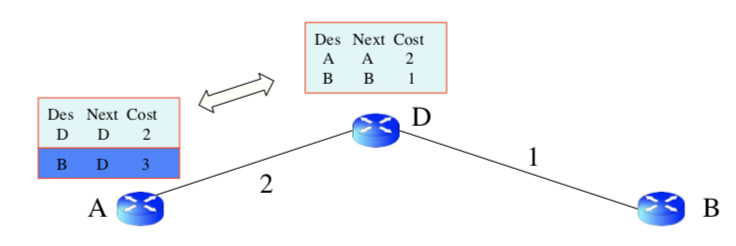
Global routing table is created and maintained by a central device, and is broadcast to all network nodes so that they can set up their own routing tables.

An example routing matrix:



### Distributed Routing

There is no central control, and each node must determine and maintain its own routing table. They need to know its neighbours and cost of getting to them, and share their routing table with neighbours.



### Static Routing

Each routing table is creating once and assumes conditions never change, so it has to be updated manually. In reality, nodes are added and removed constantly, and costs will change.

### Dynamic Routing

Routing table will update in response to changes, and allows a routing node to respond to changes. In reality, this is difficult to implement efficiently, and will increase network traffic due to routing table updates.

### Routing Comparisons

*Centralized* – simple – failure of a central location has sever effect.

*Distributed* – failure of a node has little effect – exchange of information is more complex and takes longer for a node to learn neighbour conditions

*Static* – simple, don’t have to repeatedly execute routing algorithms – insensitive to change conditions

*Dynamic* – always updating – high overhead and network traffic

## Routing Algorithms

“the process of selecting paths in a network along which to send network traffic”. Determines the best route, creates routing tables

### Shortest Path Routing

Dijkstra’s algorithm is a centralized algorithm, and finds the shortest path from a source node to any other node in the graph.

### Distance Vector Routing

The basic idea is to backwards search to learn the cost of each of its neighbours. Each router sends each neighbour a list of estimated costs to all destination its knows about. And then each router updates its tables with the best cost to each destination according to the ones received from its neighbours.

### Link Stating Routing

Each node gathers information on the status of each link to each neighbour, and builds a link state packet for each link. This identifies the two nodes connection by the link and information about the link. A node receiving link state packets forwards them to all its neighbours, except the one it received the packet from. Each node can execute a cheapest route algorithm (e.g Dijkstra’s) to determine its routing table,

### Hierarchical Routing

There may be too many nodes for each to have a complete routing table, so nodes are divided into groups called domains (these are separate and independent networks). Routes between two nodes in a common domain are determined using the domain’s protocols. Each domain has at least one specially designation nodes called routers which determine routes between domains. Domains may consist of subdomains.

### Routing in Internet

Autonomous System (AS): a group of networks and routers controlled by a single administrative authority

Intra-AS routing: Routing Information Protocol (RIP): distance-vector

Open Shortest Path First (OSPF): link-state routing

Inter-AS routing: Border Gateway Protocol (BGP): path-vector routing

# Internet Protocol

An unreliable connectionless protocol that uses packet-switching. Provide a datagram service between stations, delivering packets, making routing decisions. Packets are not guaranteed to arrive in order or via the same route.

## History of the Internet

Started in the 60’s, by the US Department of Defence, as a packet-switching network used to connect research universities and military.

## Who Controls It

### Internet Activites Board

#### Internet Engineering Task Force (IETF)

Ongoing evolution of the TCP/IP protocols

#### Internet Research Task Force

Works on advancing network technology and long-term research

#### Network Information Center

Assigns network IP addresses

## IPv4

### Packet Fields

Version (4 bits): IPv4, may be replaced by IPv6 eventually

Header length (4 bits): Number of 32-bit words in the packet header, min 5 and max 15

Type of service (8 bits): what kind of service it desires (reliability, speed)

Packet length (16 bits): length of the entire packet, max 64KB

Identification (16 bits), flags (3 bits), fragment offset (13 bits): these fields are used for breaking down a packet if it’s too big and reassembling them at the destination

Time to live (8 bits): controls the maximum number of hops visited by the packet. Packet gets discarded if its reaches 0

Protocol (8 bits): specifies the next higher layer protocol. Used at dest.

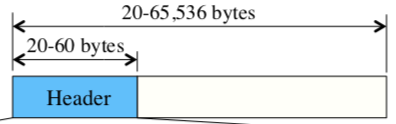
Header checksum (16 bits): error detection for the header

Source and destination IP addresses (32 bit fields)

Options: record route, source route, timestamp

Padding: makes header end at a 32 bit boundary

Data: provided by higher layer



### Address Classes

The structure is split into two main components, Network ID and Host ID.

Addresses are split into 5 classes (A-E):

* A: 8-bit network address, 24-bit node ID address, 126 networks of 16 million hosts
* B: 16-bit network address, 16-bit node ID address, 16,384 networks of 64K hosts
* C: 24-bit network address, 8-bit node ID address, 2 million network of 254 hosts
* D: multicast address
* E: reserved for future use

### Problems

Only 232 (4.3 billion) addresses, so many organizations got a class B network because all the class A addresses were used. IPv4 cannot meet the requirements of multimedia applications, as there is no constant bit rate guarantee. It’s not very secure and does not have good support for host mobility.

## IP Routing

An IP router keeps track of other networks and all local hosts by using routing tables

### Router’s Actions

Verifies the checksum, decrements the time-to-live field, recomputes checksum. Then it extracts the IP address of the packet, and routes the packet according to the route. If there is no allocated route, it checks if the network ID matches any network the router is connection to, and sends it there. If there is no match, it will find the network ID in the routing table and forward the packet to the specified router. If the network is not in the routing table, it forwards the packet to a default router.

## Address Resolution Protocol (ARP)

When the IP layer receives a frame with an IP address on its own LAN, it determines the hardware address of the destination. It does this by the router broadcasting a frame onto the network asking who owns the IP address, and the host with the specified IP will respond with its hardware address, and the router sends the IP to the correct destination.

## Packet Fragmentation

Different networks allow different maximum packet sizes called maximum transfer units (MTUs). If an IPv4 router receives a packet larger than the MTU of the network, it breaks it up into fragments. The identification, flags and fragment offset fields are used in this process.

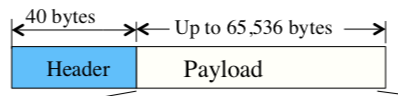
## IPv6

### Purpose

IPv6 was developed to overcome IPv4’s problems, and it can co-exist with IPv4. IPv6 makes it possible for a host to roam without needing to change its address, and the protocol will evolve in the future.

IPv6 addresses are 128 bits long.

### Packet Header



Version field (4 bits): value 4 for IPv4, 6 for IPv6

Priority field (4 bits): used in congestion control, values above 7 are for real-time/multimedia, lower values will have longer delay.

Flow label field (24 bits): allows a source and destination to set up a pseudo-connection with particular properties and requirements (essentially combining the flexibility of a datagram and virtual circuit)

Payload length field (16 bits): how many bytes follow the 40-byte header (max 64k bytes)

Next header field (8 bits): tells which of the six extension headers (if any) follow. If it’s the last IP header, the next header tells which transport protocol handler (TCP/UDP) to pass the packet to

Hop limit field (8 bits): is the same as the time-to-live field

Source/Destination address fields (128 bits)

### Extension Header

IPv6 implements several extension headers to allow more options, like authentication, destination options, fragmentation header, hop-by-hop header, routing header, security header

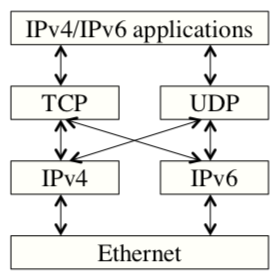
## IPv4 and IPv6 Differences

IPv4 addresses are 32 bits, IPv6 are 128 bits.

IPv4 headers contains 13 fields, IPv6 only 8 (with no checksum and TTL is replaced by hop limit)

Fragmentation is not allowed at routers in IPv6.

IPv6 has better support for options, supports more security (authentication and privacy), pays more attention to type of service (flow label)



## Domain Name System (DNS)

Converts IP names (ASCII strings) into IP addresses, using a hierarchical scheme implemented using a distributed database system. The DNS name space is divided into non-overlapping zones, each zone containing some part of the tree and name servers holding information about that zone.

DNS database is distributed among the name servers, and each zone contains at least one name server which maintains a file containing all IP names and addresses. There being 13 root level name servers that know all the top level name servers.

If a host has a query about an IP name, it passes the query to one of the local name servers. If the IP name is remote and no info is available, sends a query to its parent (keep repeating until something is found, and return that to the host).

## Internet Control Message Protocol (ICMP)

ICMP is used by the routers to report errors and unexpected events, test the state of the network, perform congestion and router updates. Some typical control messages sent by ICMP are: destination unreachable, time exceeded, parameter problem, source quench, redirect, echo request, echo reply, timestamp request, timestamp reply.

# Transport Control Protocol

## Overview

TCP connection is virtual, not physical

TCP is a connection-oriented protocol

* Connections are full duplex and end-to-end
* Does not support multicasting or broadcasting

TCP is a stream-oriented protocol

* Provides a reliable end-to-end byte stream over an unreliable network such as IP
* Each byte of data has a position in the stream

## Types of Data Deliveries

Transport: process-to-process

Internet: host-to-host

Host-to-network: node-to-node

## Transport Layer

### Functions

This is the first layer to define end-to-end communication, and it is responsible for ensuring the message arrives intact and in order. It oversees error and flow control at the source-to-destination level. Sets up and releases connections. Provides Quality-of-Service (QoS): reliability, delay, throughput.

### Address

Otherwise known as a port number, and is a 16-bit integer between 0 and 65535. It is used to choose among multiple processes on the same host.

Examples of numbers: SSH – 22, HTTP – 80, DNS – 53, SMTP – 25.

### Internet

IP/ICMP are on the network layer, above is TCP/ UDP on the transport layer, above that is SMTP/FTP/TELNET/DNS on the application layer.

## TCP Segment

Its size is limited by 65,536 (64K) bytes of the IP payload, and the MTU of the network. A TCP packet/segment consists of a fixed 20- to 60-byte-header, followed by data bytes:

Source port address (16 bits): specifies the application sending it

Destination port address (16 bits): identifies the application its sent to

Sequence number (32 bits): each byte to be transmitted is numbered. Defines the number of the first byte of data

Acknowledgement number (32 bits): contains the byte number the receiving TCP entity expects to receive next

Header length (4 bits): size of TCP header

Flags (6 bits): urgent pointer, acknowledgement, request for push, reset the connection, synchronize sequence numbers, terminate the connection.



Window size (16 bits): tells the receiving TCP entity how many data bytes the sending TCP entity can accept

Checksum (16 bits): transport layer error detection

Urgent pointer (16 bits): signal the receiver to deliver the data to the higher layer as quickly as possible

Options/padding

## TCP Connection

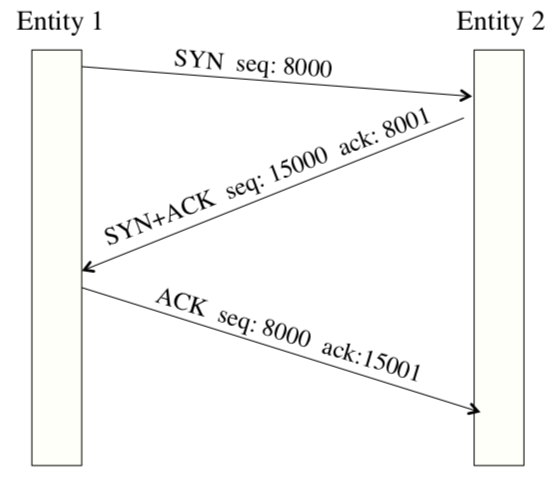
### Connection Establishment

#### Two-Way Handshaking

An entity requests a connection, and the receiving entity accepts the request, and the connection is established. Problems occur with this when the network loses, store and duplicate packets. This type would be very bad for a bank, if someone requests the bank to send the money to some untrustworthy person and then the connection is released.

#### Three-Way Handshaking

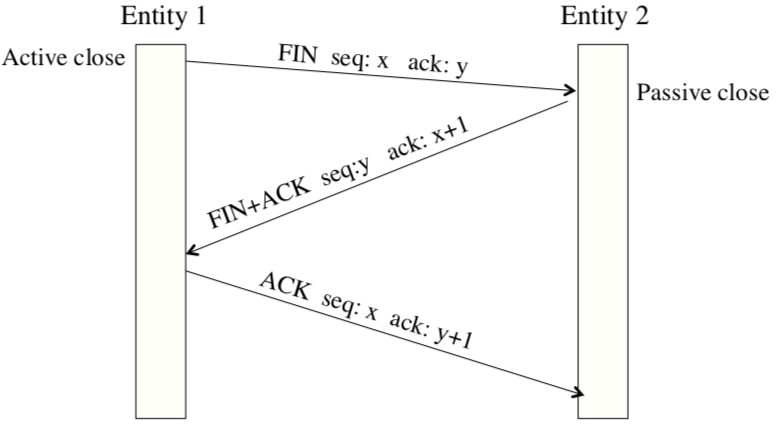
Entity 1 sends a SYN segment, which can’t carry data. Entity 2 sends back a SYN+ACK segment, which also cannot carry data. Then Entity 1 sends back an ACK segment, and the connection is established.



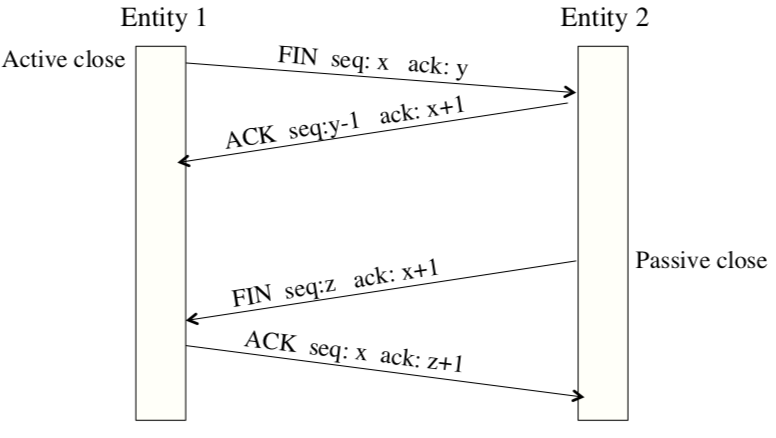
### Connection Termination

#### Three-Way Handshaking

If Entity 1 wants to terminate the connection, they send a FIN segment (this can also include the last chunk of data being sent). Entity 2 sends back a FIN+ACK segment (this can also include data). Entity 1 sends back an ACK segment to acknowledge the receipt of the FIN+ACK segment (cannot include data)



This approach can result in data loss, so the half-close protocol approach is used, where the connection in each direction is released independently of the other.



#### Three-Way Handshake Disconnect with a Timer

A timer is used, and if there is no segment from the other entity for some time, the connection is terminated. The protocol can fail if all transmissions except the initial are all lost. The sender will give up and delete the connection, but the other side does not know and is still fully active.

This is called a half-open connection.

## Error Control

### Checksum

Each segment includes a checksum fields that checks for a corrupted segment. If one is found, it is discarded and considered as lost.

### Acknowledgement

Each segment except any ACK segment is acknowledged on receipt (an ACK is sent back to the sender)

### Retransmission

A retransmission time-out (RTO) timer is running, and when it expires the message is retransmitted. Timer is set based on the round-trip time (RTT).

Three-duplicate-ACK’s rule: retransmit after receiving three duplicate ACK segments. This happens when the receives many out-of-order segments and cannot be buffered. This feature is referred to as fast retransmission.

### Duplicate Segments

Duplicate segments are detected from their sequence number, they are discarded if they occur.

### Out-of-order Segments

Out-of-order segments are also detected using their sequence number, but they are not discarded. They are maintained in the sliding window that temporarily buffers all out-of-order segments until the missing segment arrives.

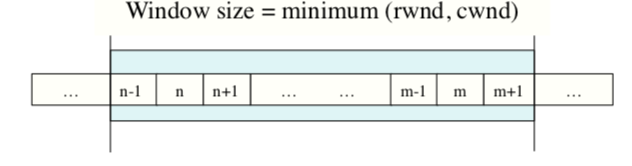
### Lost/corrupted Segments

A lost/corrupted segment are both treated as lost by the receiver. If the sender does not receive an ACK segment in time and the RTO timer expires, the segment is retransmitted.

## Flow Control

Flow control schemes are not used at the data link layer, because a router usually only has a few links to others, while a transport entity may have numerous connections. ????? doesn’t rly explain

TCP sliding window is byte-oriented, not frame-oriented, and it has a variable size. The size of the window is determined by the receiver window (rwnd) and congestion window (cwnd)



The sender requests a certain number of buffers (credit), based on its perceived needs. The receiver grants as many of these as it can afford. The credits will be decremented each time it receives a TPDU (segment), stopping when it reaches 0. The receiver sends both acknowledgements and buffer allocations (credit) that can be piggybacked with data.

## Congestion Control

### Slow Start

The cwnd starts with one maximum segment size (MASS) and increases one MSS each time an ACK is received. It starts slowly but grows exponentially.

### Congestion avoidance

Uses additive increase instead of exponential, and when the size of the congestion window reaches the slow-start threshold, the slow-start phase stops and the additive phase begins.

### Congestion detection

Multiplicative decrease: the size of the cwnd is dropped to ½.

## User Datagram Protocol (UDP)

This is a simple interface between IP and higher layer protocols that adds nothing to the services, but provides process to process communication. It is useful in applications that require simple request-response communication with little concern for flow and error control.

### User Datagram Format

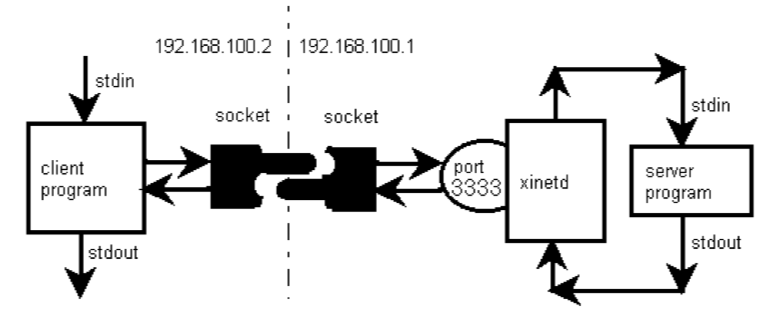
In the data section (after the header section) it has:

Source port address (16 bits), destination port address(16 bits), total length (16 bits) and checksum (16 bits). It provides no flow or error control.

## Socket Programming

A socket is a software component characterized by a unique combination of a local socket address (local IP address and port number), remote socket address (only for TCP sockets) and it uses TCP / UDP.

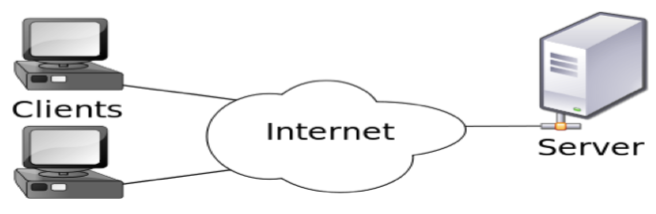
A socket address example: 192.168.100.2:65313.



# Internet Applications

## Client/Server Model

The client requests services from a service, by sending a request message and waiting for a response. The server provides services when it receives a request message, by processing a request and sending a response to the client.



## Telnet

Developed in 1969, Telnet clients use “telnet <host-name>” to send a request to connect to the Telnet server in the remote host. The server will reply asking for a user/pass, and if accepted, the client has access to the remote server from your local virtual terminal.

Telnet does not encrypt any data sent over the connection (including user/pass), and no Telnet implementations can ensure communication can be carried out without a threat of it being intercepted in the middle.

## Secure Shell (SSH)

SSH is a cryptographic network protocol for secure data communication, remote command-line login between two networked computers.

### Automatically generated key pairs

Every host/user has a key, and when a client connects, the remote daemon respons with its public host key. The client compares the key against its database to verify that it has not changed. The client then generates a 256 bit random number and encrypts this number with the host key and sends it to the server. Both sides then use this number as a session key to encrypt data.

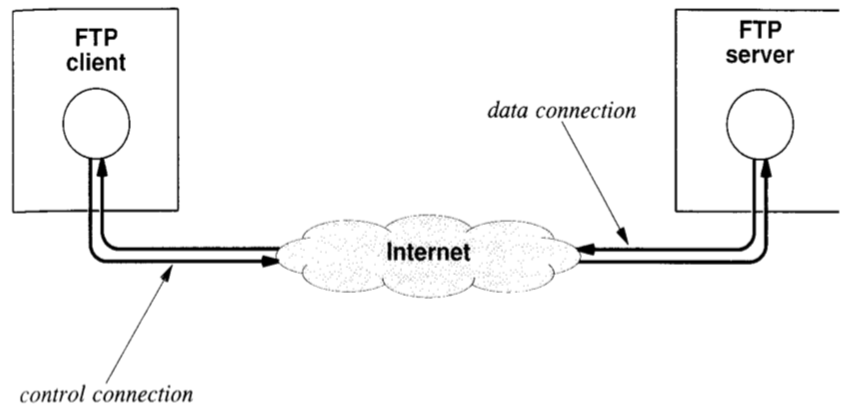
### Manually generated key pairs

Key generation example: ssh-keygen -b 1024 -t dsda

Public key is copied to the server and only the user knows the private key (which is encrypted with passphrase). The server sends the user an encrypted message with the public key. The user will be required to use the private key to decrypt the message and send it back to the server. This authentication procedure is completed automatically by the ssh client.

## File Transfer Protocol (FTP) and Secure FTP

FTP is the oldest application protocol used in Internet, and is now replaced by SFTP. It requires exchanging commands as well as data. SFTP uses encryption for authentication and transfer (SSH).



## Electronic Mail

### Simple Mail Transport Protocol (SMTP)

This is a simple ASCII protocol listening on port 25. It’s secure for authentication. SMTP retrieves mail and establishes a remote connection via TCP and then delivers it according to its protocol.

### Post Office Protocol (POP)

Servers hold emails for machines which are not regular mail servers. POP3 is used to fetch mail from a remote mail server and store it locally. Both POP3 and SMTP manipulate the mail, so the two servers must coordinate access to mailbox.

The client sends a user/pass to authenticate the session, then the client retrieves a message and transfers it, then logs out the client.

### IMAP and MIME

An Internet Message Access Protocol server can be accessed by multiple clients, that has the master copy.

Multipurpose Internet Mail Extensions are used to encode binary data and they specify the schemes used in the body.

## World-Wide Web

Created in 1989, it was originally called Arpanet.

Hypertext Transfer Protocol (HTTP) is used for communication between servers and browsers. HTTPS is a secure version of it, that uses Transport Layer Security (TLS).

Uniform Resource Locations (URL) are used to locate a document (web page) using the format: protocol://machine/path-to-file

HyperText Markup Language (HTML) is the language used to write web pages.

### Web Server

They use TCP for communication, usually on port 80. It’s task is to wait for a browser to open a connection and request a specific page, and then send a copy of the requested item and close the connection. A new connection is opened for each request.

### Web Browser

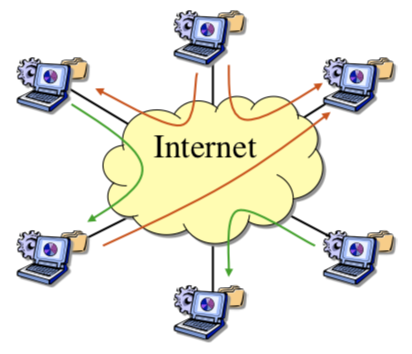
These have a complex structure, of several large software components that work together to provide a seamless service. It consists of a set of clients, a set of interpreters and a controller managing them. It interprets the web page to display it on the users display device.

## HyperText Transfer Protocol (HTTP)

This is an ASCII protocol, and each interaction consists of one ASCII request, followed by one MIME-like response. A new TCP connection is established for each HTTP interaction. Protocol methods like: GET, HEAD, POST, PUT, DELETE, LINK, UNLINK.

## Peer-to-Peer Model

This is a distributed system architecture, with no centralized control, and self-organization. They take advantage of distributed, shared resources (bandwith, CPU, storage) on peer nodes. Applications like BitTorrent, Bitcoin, distributed storage and search are examples of this.



## Firewalls

Everyone try to enter or leave the network has to be checked by a firewall.

This is to stop sensitive data from getting stolen, and stop bad things from getting in.

# ADSL, ATM

## Modems

Enable the communication between a computer and the telephone system by converting between the computer’s digital signal and the telephone’s analog signal.

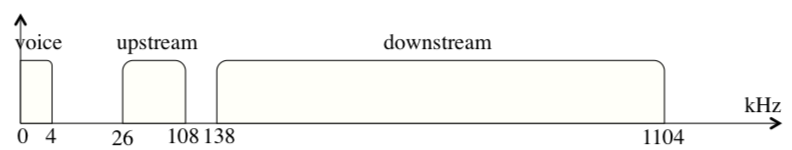
There are phone-line dialup modems, cable modems, broadband modems, mobile modems.

These are very slow and reach their speed limits. Because they use the telephone’s bandwidth, the telephone and the internet cannot be used at the same time. You have to dial an ISP each time you want to connect.

## Digital Subscriber Line (DSL)/ Asymmetric DSL (ADSL)

These are fast and always connected, but still use the existing telephone lines. It does not require any special wiring. ADSL is a faster version.

ADSL is based on a technique called Discrete Multitone (DMT). Divide the frequency range from 0Hz to 1.104MHz into 256 separate channels, each with a bandwidth of 4.3124kHz. The five lowest channels are for the telephone. The remaining channels are for upstream and downstream transmissions.



## Asynchronous Transfer Mode (ATM)

It is a connection oriented service, designed for real-time video and voice applications, using fixed-size cells. The cells arrive is order, at high-speed and low-delay transmission.

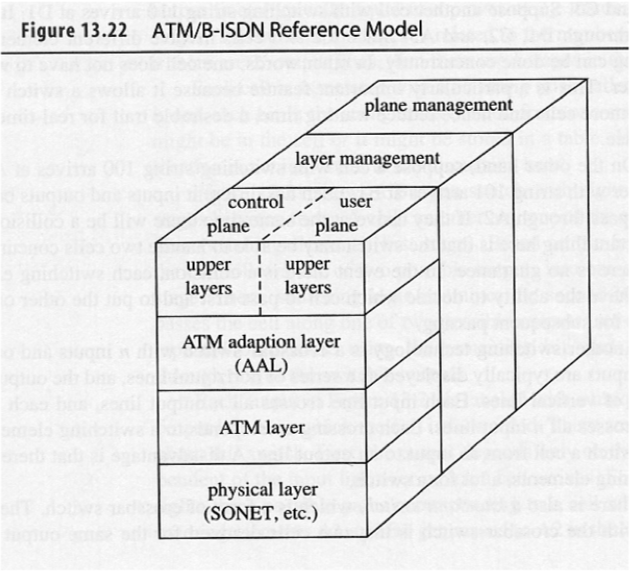
### Small Fixed-Size Cells

They are 53-bytes each. 5 bytes for the header, 48 bytes of data. They are simpler to manipulate/use because of their fixed size. It makes the outgoing queues smaller, and the bytes arrive at a more consistent rate.

### Switching

To set up the connection, a virtual circuit is established. Data cells contain virtual path/channel ID in header. The switch maintains a table of input/output port, virtual path, virtual channel. When it switches, it looks up table entry using the port and virtual path ID, and the cell is sent through that port.

### ATM Reference Model



Write out layers

## IP Security (IPSec)

Network layer security applied between two hosts, two routers, or a host and a router. Its to protect the applications that use the network layer directly.

### Transport Mode

Protects only the data from the transport layer, not protecting the IP header. Sending host uses IPSec to authenticate/encrypt the payload. Receiving host uses IPSec to check authenticate/decrypt the payload.

### Tunnel Mode

Protects the entire IP packet. Normally used between two routers, or a host and a router. The flow is from the network layer to IPSec layer and then back to the network layer.

### Security Protocols

#### Authentican Header (AH) Protocol

Authenticates the source host and ensures data integrity. Does not provide confidentiality. Uses a hash function and a symmetric key to generate a digest.

#### Encapsulating Security Payload (ESP) Protocol

Provides source authentication, integrity and confidentiality. Can replace the AH protocol.

# Wireless Technologies

## IEEE 802.11

### Architectures

Basic Service Set (BSS) is a stationary or mobile wireless stations with an optional access point (AP). It’s configured that without an AP, cannot send data to other BSS’s.

### Physical Layer

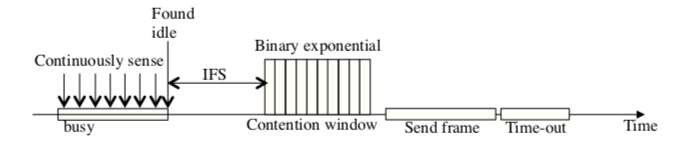
It spreads the signal’s spectral energy over a wide range of frequencies, giving it larger bandwidth. Its less prone to interference, and more secure.

### MAC Sublayer

Uses CSMA/CD. Tries to avoid collision instead of detecting it. To reduce collsions:

#### Interface Space (IFS)

A period of time waited after a free channel is found, to give time for any frames being transmitted to reach their destination.



#### Contention Window

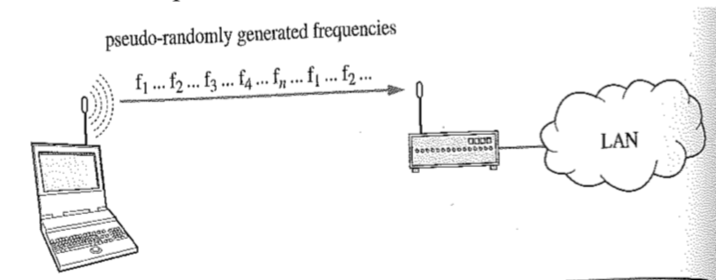
An amount of time divided into slots, so that a station that is ready to send choose a random number of lots as its wait time. Double the window size each time the station cannot detect a free channel after the IFS time (binary exponential back-off algorithm)

#### Acknowledgement

Frame may still get collided. Guarantees the receiver got the frame

## FHSS

Developed in the early 1940s, it operates on a set of frequencies that all lie in the broadcast range. Transmits using one frequency for a fixed period of time then switch to the next frequency. It uses a pseudo-random number generator to generate the frequency sequence so that both the transmitter and the receiver have the same sequence.

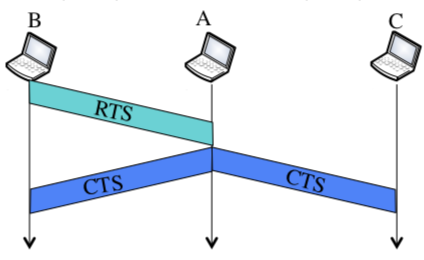


## DSSS

This expands a single data bit into *n* bits. The transmitter starts with a string of data bits, and for each bit, generates a pseudorandom bit string, called a chipping sequence, containing *n* bits. Each data bit is combined with the chipping sequence to create a chip code and transmit the chip code.

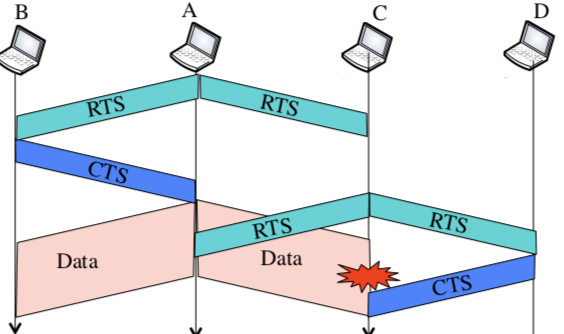
## Hidden Station Problem

Different stations may have different transmission range. So the solution is handshaking, with requests to send (RTS) and clear to sends (CTS)



## Exposed Station Problem

The reverse of the hidden station problem. Handshaking cannot help.



## Bluetooth

Technology in which a microchip containing a radio transceiver is embedded in electronic devices and allows the devices to communicate without wires or cables (eg mouse, keyboard with the computer)

Bluetooth LAN is an ad-hoc network that formed spontaneously by BT devices

Wireless Personal-area Network (PAN) uses IEEE802.15

### Architecture

Uses piconets, up to eight stations, one primary and the rest secondaries.

Uses scatternet, consisting of two or more piconets, a secondary station in one piconet can be the primary in another piconet.

### Radio Layer

Roughly equivalent to the physical layer in the Internet model. Uses minimal power and has a transmission range of 10m. FHSS hops 1600 times/second, uses each frequency for only 1/1600 of a second.

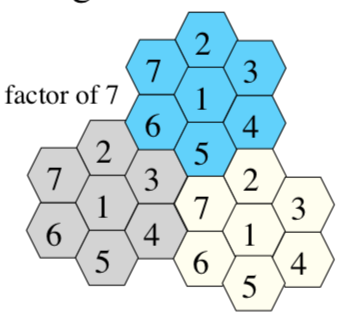
### Baseband Layer

Roughly equivalent to the MAC layer in LANs. Uses TDD-TMDA (time-division duplex TDMA). It’s half-duplex and the time slot is 1/625 of a second. Single-secondary communication – primary uses even-numbered slots (0, 2, 4, etc), secondary uses odd-numbered slots (1, 3, 5,etc). Uses multiple-secondary communication – primary uses even, a secondary sends in the next available odd-numbered slot.

## Cellular Technology

### Frequency-Reuse Principle

Neighbouring cells cannot use the same set of frequencies for communication, the set of frequencies available is limited so frequencies need to be reused. Configuration of N cells where N is the reuse factor.



### Handoff

During a conversation, a mobile station moves from one cell to another. The MSC monitors the signal strength every few seconds and if the signal is bad, it seeks a new base station.

#### Hard handoff

During handoff the communication link must be broken before it can connect to the new base

#### Soft handoff

Can simultaneously communicate with two base stations, and start to communicate with one while breaking off with the other

### Roaming

Traditional roaming is when a service provider allows extended coverage where they don’t have bases

C

### 1G

Used analog signals for voice communication, using FDMA and two separate analog channels

### 2G

Designed for digital voice communication, by using TDMA and FDMA and digital signals.

# Advanced Networks