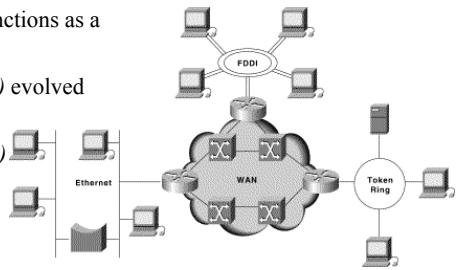
Computer Security

Networks:
Hardware, Protocols, Wireless Networks

LANs, WANs, and Internetworks

- An *internetwork* is a collection of individual networks, connected by intermediate networking devices, that functions as a single large network.
- *Local-area networks (LANs)* evolved around the PC revolution.
- *Wide-area networks (WANs)* interconnect LANs with geographically dispersed users to create connectivity



Networks and Components

- A physical network is a collection of*:
  - Cables
  - Routers
  - Switching equipment
  - and the *transport stacks* that glue it all together
- Transport stacks (TCP/IP, NetBIOS, IPX/SPX, DECnet, AppleTalk, SNA/APPC) provide reliable end-to-end communications across Wide Area Networks (WANs) and Local Area Networks (LANs)

**Client/Server Survival Guide (Third Edition)*, by Orfali, Harkey & Edwards, published by John Wiley & Sons, Inc. ©1999

The Open System Interconnection (OSI) Reference Model

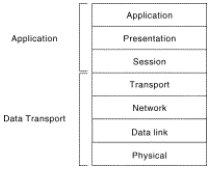
- ***OSI*** is a conceptual framework which breaks down the complexity of networking into seven ***layers***, each of which represents an abstraction:

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Mnemonic: "**A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing"

The OSI Reference Model

- The *upper layers* of the OSI model deal with application issues and generally are implemented only in software.
  - The highest layer, the *application layer* (layer 7), is closest to the end user.
- The *lower layer*s of the OSI model handle data transport issues.
  - The *physical layer* (layer 1) and the *data link layer* (layer 2) are implemented in hardware and software.
  - The lowest layer, the *physical layer* (layer 1), is closest to the physical network medium (the network cabling).

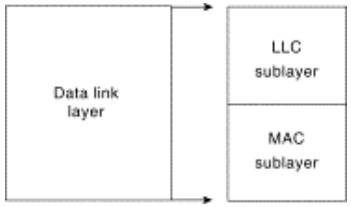


The OSI Data Transport Layers

- ***Physical Layer*** (Layer 1)
  - Concerned with the physical, mechanical and electrical characteristics of the network hardware -- cables, voltages, etc.
  - Examples:
    - IEEE 802.3 Ethernet specification
    - IEEE 802.5 Token Ring specification
- ***Data Link Layer*** (Layer 2)
  - Concerned with the error-free delivery of data
  - Organizes raw bit stream into groupings of bits, called frames
  - Transfers frames between devices on a single network
  - Appends to frame a header, which contains the hardware addresses of the source and destination, etc.

The OSI Data Link Layer (Layer 2)

- The Institute of Electrical and Electronics Engineers (IEEE) has subdivided the data link layer into two sublayers:
  - Logical Link Control (LLC) and
  - Media Access Control (MAC).



The OSI Data Link Layer (Layer 2)

- The *Media Access Control (MAC)* sub-layer defines the relationship at the hardware level between Physical Layer devices, like Network Adapter Cards, and the Data Link Layer
  - The IEEE MAC specification defines MAC addresses, which enable multiple devices to uniquely identify one another at the data link layer.
- The *Logical Link Control (LLC)* sub-layer defines the relationship between the MAC sub-layer and Data Link Layer devices and drivers

The OSI Data Transport Layers

- ***Network Layer*** (Layer 3)
  - Handles routing between networks and timely delivery of data
  - Organizes frames from the Data Link Layer into *packets*
  - Packets include a header which includes network addresses for the source and destination
  - Examples:
    - The Internet Protocol (IP) portion of the TCP/IP protocol
    - The Internet Packet Exchange (IPX) of the Novell IPX/SPX protocol

The OSI Data Transport Layers

- ***Transport Layer*** (Layer 4)
  - Responsible for delivering data reliably
  - Operations:
    - Building up and tearing down connections
    - Packet sequencing
    - Acknowledgements
    - Flow control
  - Examples:
    - The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) portions of the TCP/IP protocol
    - The Sequenced Packet Exchange (SPX) portion of the Novell IPX/SPX protocol

The OSI Application Layers

- ***Session Layer*** (Layer 5)
  - Provides mechanisms to establish and maintain communications between applications.
    - Access authentication (for example, logging into a server)
    - Session Management
    - Verification that adequate disk space is available for a request
    - Notifying a user that a printer is offline
  - Examples:
    - Various Remote Procedure Calls (RPCs) used by network operating systems.

The OSI Application Layers

- ***Presentation Layer*** (Layer 6)
  - Responsible for formatting, representing and translating data
    - ASCII to EBCDIC translation
    - Compression/decompression of data
    - Encryption/decryption of data

- ***Application Layer*** (Layer 7)
  - Provides interface between the network and the application software

The OSI Reference Model and the IEEE

- The OSI Reference Model does not explicitly specify all functions related to the seven layers.
- The Institute of Electrical and Electronic Engineers (IEEE) provides this missing information through their 802 committees:
  - IEEE 802.1 -- Umbrella committee
  - IEEE 802.2 -- Responsible for the LLC sub-layer of the Data Link Layer
  - IEEE 802.3 -- Defines Ethernet and its variations, including 10Base5, 10Base2, 10BaseT and 100BaseT
  - IEEE 802.5 -- Defines Token Ring

Network Hardware: NICs

- Each computer connected to a network needs at least one ***Network Interface Card*** (NIC)
  - Operates at the Physical and Data Link Layers of the ISO Reference Model
    - Physical Layer:
      - Provides the physical and electrical connection required to access the network cabling.
    - Data Link Layer
      - Provides the processing to assemble or disassemble the bit stream on the cable into frames suitable for the Media Access Method* in use
  - Media-dependent (physical connector)
  - Media Access Method-dependent (Ethernet vs Token Ring, etc.)
  - Protocol-independent (i.e. an Ethernet NIC can simultaneously connect to a LAN server running IPX/SPX and to a UNIX host running TCP/IP)

*ARCnet, Token Ring, Ethernet, 100BaseT, etc.

Network Hardware: Repeaters

- A ***repeater***:
  - Amplifies and rebroadcasts a signal
  - Extends the distance a signal may be run reliably over a cable
  - Makes no decisions based on signal content

Network Hardware: Hubs

- A ***hub***:
  - Used as a concentrator to join multiple workstations with a single link to the rest of the LAN
  - Functions as a multi-port repeater
  - Signals received on any port are immediately retransmitted to all other ports on the hub.
  - Increases the number of connectable devices
  - Operates at the OSI Physical Layer (Level 1)

A Personal Hub

A Stackable Hub

Network Hardware: Switches

- A ***switch***:
  - Essentially an intelligent hub.
  - Looks at destination address of a frame and internally establishes a logical connection with the port connected to the destination node.
    - Other ports on the switch have no part in the connection
    - Result: Each port on the switch corresponds to an individual collision domain, and network collision is avoided.
  - Operates at the OSI Data Link Layer (Level 2)

A Desktop Switch

Network Hardware: Switches

- There are actually two main types of switch:
  - Layer-2 (based on bridging technologies)
    - Operate at the Data Link layer
    - Establish logical connections between ports based on MAC addresses
    - Used to segment existing network into small collision domains
  - Layer-3 (based on routing technologies) (aka *routing* or *multilayer switches*)
    - Operate at the Network Layer
    - Establish logical connections between ports based on network addresses
    - Used to connect different networks into an internetwork
    - See http://www.cisco.com/warp/public/cc/so/neso/lnso/cpso/l3c85_wp.htm

A Layer 3 Managed Rack-Mountable Switch

Network Hardware: Bridges

- A ***bridge***:
  - Used to divide a network into mutually isolated segments
  - Operates at the Data Link Layer (layer 2) of the ISO Reference Model
  - Physical media-dependent; usually media access layer dependent
  - Protocol-independent above the Data Link Layer

A Wireless-G Ethernet Bridge

Network Hardware: Bridges

- A ***bridge***:
  - Divides a single network cable into two or more physical and logical segments
  - Listens to all traffic on all segments and examines the destination hardware address of each frame
    - If the source and destination hardware addresses are located on the same segment:
      - discards the frame (since destination can hear source directly)
    - Otherwise:
      - repeats the frame onto the segment where the destination address is located
  - Thus, traffic with both source and destination on the same segment is not transmitted to other segments.

Network Hardware: Routers

- A ***router***:
  - Used to connect one network to another
  - Operates at the Network Layer (layer 3) of the ISO Reference Model
  - Media-independent
  - Protocol-dependent above the Data Link Layer
  - Works with *packets* and their *logical* addresses
  - May have to make a complex decision about how to deliver a packet to a distant network

An Ethernet Cable/DSL Router

Network Hardware: Routers

- A ***router***:
  - Is typically programmable, to control how it relays packets
    - Entire books have been written on how to program just a single router product from a single vendor.
  - Unlike with a hub or a switch, the two networks connected by a router are still separate networks.

Network Hardware: Routers

- ***Routed/Routable protocols***
  - Some protocols (e.g. TCP/IP, IPX/SPX) have packets that include the Network Layer logical addresses needed by routers
  - Others (e.g. NetBEUI) do not, and are *non-routed/non-routable* protocols

Network Hardware: Gateways

- A ***gateway***:
  - Used to translate between incompatible protocols
  - Can function at any one layer of the ISO Reference Model, or at at several layers simultaneously.
  - Most commonly used at Session Layer (layer 5) and above
  - Example:
    - A gateway could be used to allow SMTP (Simple Mail Transport Protocol) email users to exchange email with MHS (Message Handling System) email users

A Cisco Universal Gateway

Proxy Servers

- A ***proxy server*** acts as an intermediary for certain protocol exchanges.
  - Operates at the Application Layer (layer 7)
  - The most common use for a proxy server is as an ***HTTP proxy:***
    - An HTTP proxy server program runs on some machine in the network
    - Users reconfigure their browser to use this HTTP proxy server
    - Subsequently, all HTTP requests from the browser go through the HTTP proxy server, and do not go directly to the Internet.

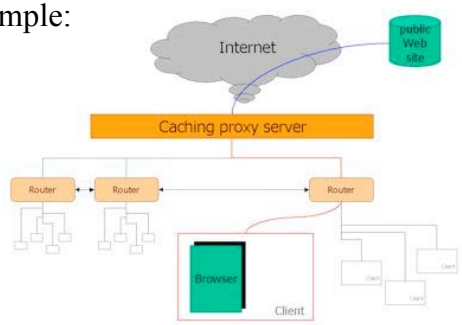
proxy
1 : the agency, function, or office of a deputy who acts as a substitute for another
2 a : authority or power to act for another
b : a document giving such authority
3 : a person authorized to act for another

Proxy Servers

- There are three reasons to employ a proxy server:
  - ***Firewalling and Filtering***
    - Can prevent access to certain web sites, such as pornographic sites, or a company's competitors' sites.
  - ***Connection Sharing***
    - The network can be configured so that the HTTP proxy server is the only machine that is directly connected to the Internet.
    - This can improve network bandwidth, and thus performance.
  - ***Caching***
    - If many users access certain sites often, an HTTP proxy server can cache those web sites' pages/images/etc. in its own local storage, and thus avoid unnecessary Internet access.
    - This can improve network bandwidth, and response times.

Proxy Servers

- For example:



Data Transmission

- Data is transmitted over a network using ***packets.***
  - A packet is a block of user data together with necessary address and administration information attached, to allow the network to deliver the data to the correct destination.
  - A packet consists of:
    - A ***header***, which contains the information needed to get the packet from the source to the destination
    - A ***data area***, which contains the information to be transmitted
  - A packet is like a letter:
    - The header is like the envelope
    - The data area is like the contents of the envelope.

Packets and Datagrams

- Another name for a packet is a ***datagram***
  - Sometimes packet and datagram mean subtly different things
- Strictly speaking, a datagram is a ***self-contained packet,*** which:
  - Contains enough information in the header to allow the network to forward it to the destination, independently of previous or future datagrams.
  - Requires no setup before a computer tries to send datagrams to a computer with which it has not previously communicated

Packets and Datagrams

- Some systems, such as ***ATM (Asynchronous Transfer Mode)***, require a connection setup before any packets may be sent.
  - Here, a distinction is made between packets and datagrams.
- Other systems, like IP (Internet Protocol) do not require prior setup.
  - Here, no distinction is made.

Frames

- A ***frame***, or ***data frame***, is:
  - a packet which has been encoded for transmission over a particular link. (see http://en.wikipedia.org/wiki/Frame_%28telecommunications%29)
- This process involves, at a minimum, adding:
  - ***delimiters*** to distinguish the packet from "dead air"
  - ***address*** and ***control*** fields specific to the link, and
  - ***checksums*** to detect errors.
- The term ***frame*** may also refer to the way a multiplexer divides the underlying communication channel so that it can be used simultaneously for more than one transmission.
  - Conceptually, each frame is a slot which could be filled by a transmitted packet.
  - In these schemes, not all frames are necessarily in use at once.

Message Transmission Methods

- ***Unicast Messages***
  - Messages that are sent from one device to another device
  - Not intended for others
  - A "private conversation" (but eavesdropping is still possible).
- ***Broadcast Messages***
  - Messages sent to every device on a network.
  - "Making an announcement"
- ***Multicast Messages***
  - Messages sent to a group of stations that meet a particular set of criteria
  - These stations are usually related to each other in some way, such as serving a common function, or being set up into a particular *multicast group*
  - A "small discussion group"

Network Protocols

- A ***network protocol*** is:
  - the specification of a set of rules for a particular type of communication.
- Protocols are ***layered***, to divide the protocol design into a number of smaller parts, each of which accomplishes a particular sub-task.
  - This is the principle on which the OSI model, and its specific implementations, are based.
- Common network protocols include:
  - TCP, IP, UDP, ICMP (Internet Control Message Protocol)
  - FTP, Telnet, SMTP, DNS, HTTP, POP3, NNTP, NetBIOS, IRC, SSH.

The Internet Protocol Suite

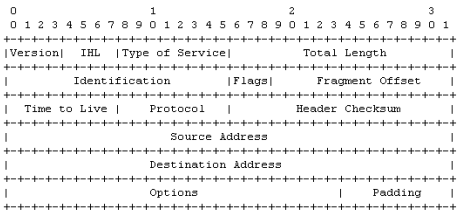
- Application layer
  - HTTP, SMTP, FTP, SSH, IRC, SNMP, SIP ...
- Transport layer:
  - TCP, UDP, ICMP, SCTP, RTP, DCCP ...
- Network layer:
  - IPv4, IPv6, ARP ...
- Data link layer:
  - Ethernet, Wi-Fi, Token ring, FDDI, ...

TCP/IP: The Internet Protocol

- The main protocols on which the Internet is based are:
  - ***IP*** : The ***Internet Protocol*** is a data-oriented protocol used by source and destination hosts for communicating data across a packet-switched internetwork.
    - IP is a Network Layer (Layer 3) protocol
  - ***TCP***: The ***Transmission Control Protocol*** allows programs on networked computers to create *connections* to one another, over which they can send data.
    - A connection involves two ***endpoints***
    - The TCP protocol guarantees that data sent by one endpoint will be received in the same order by the other, and without any pieces missing.
    - TCP is a Transport Layer (level 4) protocol

The IP Header

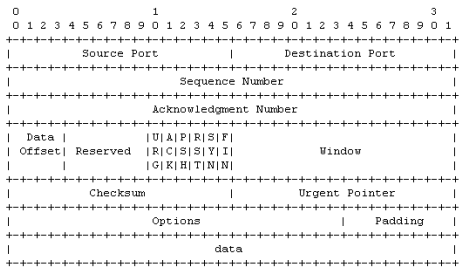
- Here's what the IP header looks like:



(See: http://www.faqs.org/rfcs/rfc791.html)

The TCP Header

- Here's what the TCP header looks like:



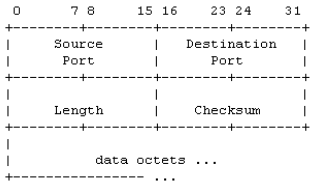
(From: http://www.faqs.org/rfcs/rfc793.html)

UDP

- ***UDP (User Datagram Protocol)***:
  - A ***connectionless protocol***.
  - A minimal message-oriented transport layer protocol
  - Provides a very simple interface between a network layer below and an application layer above.
  - Provides ***no guarantees for message delivery*** and a UDP sender ***retains no state*** on UDP messages once sent onto the network.
  - Examples of applications that often use UDP include:
    - Streaming media
    - Real-time multi-player games
    - Voice over IP (VoIP)
    - DNS (Domain Name System)
    - SNMP (Simple Network Management Protocol)
    - DHCP (Dynamic Host Configuration Protocol)
    - RIP (Routing Information Protocol
    - General message broadcasting or multicasting

The UDP Header

- Here's what the UDP header looks like:



(See: http://www.faqs.org/rfcs/rfc768.html)

ICMP

- ***ICMP (Internet Control Message Protocol)***:
  - An extension of IP; a Network Layer (Layer 3) protocol
  - Supports packets containing error, informational, and control messages
  - Used to deliver many different types of administrative control messages, such as:
    - Network / host / port unreachable
    - Packet lifetime expired
    - To pause incoming traffic in the event of an overload
    - Message redirection / rerouting
    - Determination of whether a host is active on the network
      - Used by **`ping`** command.

IPSec

- ***IPSec (IP Security)*** is a standard for securing IP communications by ***encrypting*** and ***authenticating*** all IP packets. Operates at the Network Layer (layer 3) of the OSI model.
  - Uses three major protocols:
    - The ***Internet Security Association and Key Management Protocol (ISAKMP)*** is used for creating and maintaining ***Security Associations (SAs)***
    - ***Authentication Header (AH)*** adds information to the header of a packet the for purpose of *integrity* and *authentication*.
    - ***Encapsulating Security Payload (ESP)*** adds guarantees of *confidentiality* by means of *encryption.* ESP supports two different modes of operation:
      - ***Transport Mode***
        - » Used mainly for host-to-host communication over a network that may or may not support IPSec
      - ***Tunnel Mode***
        - » Creates virtual circuits between two networking devices, and encrypts all the data passed between them.
        - » Encrypts the packet header, as well as the payload.

Wi-Fi

- ***"Wi-Fi" (Wireless Fidelity)*** is a set of standards for wireless local area networks (WLAN), based on the IEEE 802.11 specifications:
  - ***802.11b*** uses the 2.4 GHz spectrum, and has a maximum raw data rate of 11 Mbit/s (in practice, more like 5.9 Mbit/s over TCP)
  - ***802.11a*** operates in the 5 GHz band, with a maximum raw data rate of 54 Mbit/s (realistically in the mid-20 Mbit/s).
  - ***802.11g*** uses the 2.4 GHz spectrum, and operates at a maximum raw data rate of 54 Mbit/s. It interoperates with 802.11b.
  - ***802.11n*** is not yet standardized (expected end of 2006), but holds the prospect of a data throughput of at least 100 Mbit/s.
    - Some "Pre-n" devices are available now. Their eventual fate is currently unclear.

    (See http://en.wikipedia.org/wiki/802.11a#802.11b)

Ports

- There are two different kinds of ***ports***:
  - Hardware ports (serial port, parallel port, RJ-11, RJ-45, USB, etc.)
  - ***Network ports***, used by TCP & UDP:
    - A ***connection point***
    - A ***numerical designation*** for a pathway of communications
    - A combination of a port and a network address is called a ***socket***.
    - The **Internet Assigned Numbers Authority** (IANA) is an organization that oversees IP address, top level domain and Internet protocol code point allocations.
    - Port numbers range from 0 to 65535:
      - **0 to 1023**: *Well-known ports* (access requires root privileges on UNIX)
      - **1024 to 49151:** *Registered port numbers*
      - **49152-65535** : *private or dynamic ports* (not used by any defined application)

Well-Known Ports

- Here are some well-known ports, and their usage:

13	: Daytime Protocol	110	: POP3
20/21	: FTP	119	: NNTP
22	: SSH	139	: NetBIOS
23	: Telnet	143	: IMAP
25	: SMTP	194	: IRC
53	: DNS	443	: HTTPS
69	: TFTP	445	: Microsoft-DS (Active Directory, Windows Shares)
70	: Gopher	445/udp	: Microsoft-DS SMB file sharing
79	: Finger	591	: FileMaker
80	: HTTP	666	: id Software's Doom game (appropriate, huh?)
88	: Kerberos	993	: IMAP4 over SSL
		995	: POP3 over SSL

IP Addresses

- Originally, every computer on the Internet was assigned a fixed identifier, called an ***IP address***
  - An IP address is, for IP4, a 32-bit, 4-byte, binary number
  - Typically represented by four 3-digit decimal numbers, separated by periods
    - For example:
      - The IP address of `www.rivier.edu` is `66.251.112.2`
      - The IP address of `www.microsoft.com` is `207.46.156.252`

IP Addresses

- Two types of IP Addresses:
  - Public IP addresses:
    - For computers connected to the Internet
    - No two can be the same
  - Private IP addresses:
    - For computers within a private company or organization's network
    - Only have to be unique within that network.
    - Often start with 10. ...

IP Addresses

- Another reason for the dotted quad notation is that IP addresses are split into:
  - a network number, which is contained in the leading octets, and
  - a host number, which is the remainder.
  - The size of the host part depends on the size of the network. To accommodate different needs, several classes of networks, defining different places to split IP addresses, have been defined.

IP Addresses

- The class networks are:
  - Class A (1.0.0.0 through 127.0.0.0)
    - The network number is contained in the first octet.
    - This class provides for a 24-bit host part, allowing roughly 1.6 million hosts per network.
  - Class B (128.0.0.0 through 191.255.0.0)
    - The network number is in the first two octets.
    - This class allows for 16,320 nets with 65,024 hosts each.
  - Class C (192.0.0.0 through 223.255.255.0)
    - The network number contained in the first three octets.
    - This class allows for nearly 2 million networks with up to 254 hosts.
  - Classes D, E, and F (224.0.0.0 through 254.0.0.0)
    - Experimental or reserved for special purpose use and don't specify any network.
    - IP Multicast, which is a service that allows material to be transmitted to many points on an internet at one time, has been assigned addresses from within this range.

IP Addresses

- There are four regional Internet registries that assign Internet addresses from the A, B & C classes:
  - ARIN
  - RIPE NCC,
  - LACNIC
  - APNIC

IP Addresses

- In the host part, not all octets are used:
  - Octets 0 and 255 are used for special purposes:
    - If all host part bits are 0, the address ***refers to the network***
    - If all host part bits are 1, the address is called a ***broadcast address***.
- A number of network addresses are reserved for special purposes:
  - 0.0.0.0 is called the ***default route***, and relates to the way IP routes datagrams
  - 127.0.0.1 is called the ***loopback address***, and is reserved for IP traffic local to your host.
    - Designated for the ***software loopback interface*** of the local machine
    - The loopback interface has no hardware associated with it, and it is not physically connected to a network
    - Used for testing software without having to be connected to the network.

IP Addresses

- The previous description of IP addresses referred to what is known as ***IP V4 addresses***, where there are 4 bytes (octets) in an address.
  - IP V4 gives us about 4.2 billion possible IP addresses
  - However, the number of unassigned addresses is running out. Problem!
- A new addressing system, ***CIDR (Classless Inter-Domain Routing)***, was introduced in 1993.
  - CIDR uses ***variable length subnet masks (VLSM)*** to allocate IP addresses to ***subnets*** according to individual need, rather than some general network-wide rule.
  - Thus the network/host division can occur at any bit boundary in the address
  - The process can be ***recursive***, with a portion of the address space being further divided into even smaller portions, through the use of masks which cover more bits
  - See http://en.wikipedia.org/wiki/Subnetwork

CIDR

- ***CIDR address notation***:
  - Begins with the network address (padded on the right with the appropriate number of zero-valued bits - up to 4 octets for IPv4, and up to 8 16-bit hexadecimal fields for IPv6).
  - Followed by a "/" character and a prefix length, in bits, defining the length of the ***subnet mask***, which determines the size of the network.

CIDR

- For example:
  - 192.168.0.0 /**24** represents the 256 IPv4 addresses 192.168.0.0 through 192.168.0.255 inclusive, with 192.168.0.255 being the broadcast address for the network.
  - 192.168.0.0 /**22** represents the 1024 IPv4 addresses 192.168.0.0 through 192.168.3.255 inclusive, with 192.168.3.255 being the broadcast address for the network.
  - 2002:C0A8::/48 represents the IPv6 addresses 2002:C0A8:0:0:0:0:0:0 through 2002:C0A8:0:FFFF:FFFF:FFFF:FFFF:FFFF, inclusive.

CIDR

- For IPv4, an alternative representation uses the network address followed by the network's ***subnet mask***, written in dotted decimal form:
  - 192.168.0.0 /**24** could be written 192.168.0.0 **255.255.255.0**
  - 192.168.0.0 /**22** could be written 192.168.0.0 **255.255.252.0**

Subnets

- ***Subnetting*** a network allows you to break down a large network into smaller ones
- In order to subnet, every machine must be told its ***subnet mask***, which defines what part of its IP address is allocated for the subnetwork ID, and what part for the host ID on that subnetwork.
- Subnetting was originally introduced before the introduction of classful network numbers in IPv4, to allow a single site to have a number of local area networks
- The fact that all hosts already used masks allowed CIDR to be deployed fairly painlessly.

Subnet Masks

- A ***network mask***, also known as a ***subnet mask***, ***netmask*** or ***address mask***, is a bitmask used to tell how much of an IP address identifies the ***subnetwork*** the host is on and how much identifies the host.
- Subnet masks are usually represented in the same representation used for addresses themselves
  - In IPv4, dotted quad notation (four numbers from zero to 255 separated by periods) or, less commonly, as an eight-digit hexadecimal number.
- A shorter form, which is known as CIDR notation, gives the network number followed by a slash and the number of 'one' bits in the binary notation of the netmask (i.e. the number of relevant bits in the network number).
  - Using this notation, in IPv4 a subnet could be referred to simply as 130.94.122.199/28.

Subnetting

- In subnetting, IPv4 addresses are broken down into three parts:
  - the network part
  - the subnet part and
  - the host part.
- As we said before, there are three classes of IP address:

Class	Start	End	First bits	Mask in dotted decimal
A	1.0.0.0	126.0.0.0	0	255.0.0.0
B	128.0.0.0	191.255.0.0	10	255.255.0.0
C	192.0.0.0	223.255.255.0	110	255.255.255.0

Wi-Fi Security

- Wi-Fi has had a checkered history with regard to security:
  - ***WEP (Wired Equivalent Privacy)***:
    - Part of the original IEEE 802.11 standard (1999)
    - A scheme used to secure wireless networks
    - Uses ***RC4*** cipher for confidentiality and the ***CRC-32*** checksum for integrity.
      - For RC4, WEP uses two key sizes: ***40 bit and 104-bit***; to each is added a ***24-bit initialization vector (IV)*** *which is transmitted in the clear.*
    - Now considered insecure by cryptographers:
      - The use of WEP was optional, resulting in many installations never even activating it
      - WEP did not include a key management protocol, relying instead on a single shared key amongst users.
      - Papers were written documenting successful attacks on WEP.

Wi-Fi Security

- WEP (although still used) was superseded in 2003 by:
  - ***WPA (Wi-Fi Protected Access)***
    - Designed for use with an ***802.1X authentication server***, which distributes different keys to each user
      - Can also be used in a less secure ***pre-shared key (PSK) mode***.
    - ***Data encrypted using RC4 with a 128-bit key and a 48-bit IV***
    - Major improvement over WEP is use of ***Temporal Key Integrity Protocol (TKIP)***, which dynamically changes keys as the system is used.
      - TKIP, when combined with the much larger IV, defeats the well-known key recovery attacks on WEP.
    - Also provides greatly improved ***payload integrity***.
      - WEP's inherently insecure CRC-32 replaced by a message authentication code (MAC)
      - The MAC includes a frame counter, which prevents replay attacks.

Wi-Fi Security

- WPA was an intermediate solution, and was superseded by:
  - ***IEEE 802.11i***, formally known as ***WPA2***, in June 2004
    - Uses the Advanced Encryption Standard (AES) block cipher
    - The IEEE 802.11i architecture also contains the following components:
      - ***802.1X*** for *authentication*, involving the use of:
        - » ***EAP (Extensible Authentication Protocol)***, and
        - » An ***authentication server***
      - ***RSN (Robust Security Network)*** for *keeping track of associations*
      - ***CCMP (Counter-Mode/CBC-Mac Protocol)*** to provide confidentiality, integrity and origin authentication.
    - An important feature of IEEE 802i is the ***Four-Way Handshake***
      - See http://en.wikipedia.org/wiki/WPA2

Bluetooth

- ***Bluetooth*** is a new wireless standard
  - Developed by a group of electronics manufacturers
    - Sony Ericsson, IBM, Intel, Toshiba, & Nokia; joined later by others
  - Aptly named after a Danish king*, known for his unification of previously warring tribes from Denmark, Norway and Sweden.
  - Allows any sort of electronic equipment to interconnect without wires, cables or any direct action by a user
    - Short range radio solution (2.45 GHz; spread-spectrum frequency hopping technology)
    - Inexpensive
  - See http://en.wikipedia.org/wiki/Bluetooth

*__Harald Bluetooth__ was king of Denmark between 940-986 AD, and was the son of Gorm. He brought Christianity to Scandinavia and also united Denmark and Norway. Much of Harald's history was learnt from two runic stones erected to his memory in the town of Jelling in Denmark. He was killed in 986 during a battle with his son, Svend Forkbeard.

Bluetooth

- ***Bluetooth:***
  - Provides a way to connect and exchange information between devices:
    - personal digital assistants (PDAs)
    - mobile phones
    - laptops & PCs
    - printers
    - digital cameras
  - Lets these devices talk to each other, as long as they are within 10m (32ft) of each other.
  - Also includes support for more powerful, longer-range devices suitable for constructing wireless LANs.
  - In the future, may also be used for Voice Over IP (VOIP) telephone support.

Bluetooth

- There are a number of versions of Bluetooth:
  - ***1.0*** & ***1.0B*** -- had significant interoperability problems
  - ***1.1*** -- fixed some errors found in the 1.0B specs; added support for non-encrypted channels
  - ***1.2*** -- added:
    - *Adaptive Frequency Hopping (AFH)*
    - *Higher transmission speeds* in practice
    - *Extended Synchronous Connections (eSCO)*
    - *Received Signal Strength Indicator (RSSI)*
    - *Host Controller Interface (HCI) support*
    - *HCI access to timing information* for Bluetooth applications.
  - ***2.0*** -- added
    - *Non-hopping narrowband channel(s)*
    - *Broadcast/multicast support*.
    - *Enhanced Data Rate (EDR)* of 2.1 Mbit/s.
    - Built-in *quality of service*.
    - *Distributed media-access control protocols*.
    - *Faster response times*.
    - *Halved power consumption* due to shorter duty cycles.

Bluetooth Security

- Bluetooth uses the ***SAFER+*** algorithm for authentication and key generation.
- A number of concerns have been raised about Bluetooth security
  - See http://en.wikipedia.org/wiki/Bluetooth#Security_concerns
  - In particular, it has been shown that, with directional antennas, the range of class 2 Bluetooth radios could be extended to one mile.
    - This enables attackers to access vulnerable Bluetooth-devices from a much greater distance than previously thought.