Networking Tutorial

The CTDP Networking Guide Version 0.6.3 February 3, 2001

Revised to Version 0.6.4 November, 4, 2002

Introduction

This guide is primarily about TCP/IP network protocols and ethernet network architectures, but also briefly describes other protocol suites, network architectures, and other significant areas of networking. This guide is written for all audiences, even those with little or no networking experience. It explains in simple terms the way networks are put together, and how data packages are sent between networks and subnets along with how data is routed to the internet. This document is broken into five main areas which are:

1. Basics - Explains the protocols and how they work together
2. Media - Describes the cabling and various media used to send data between multiple points of a network.
3. Architecture - Describes some popular network architectures. A network architecture refers to the physical layout (topology) of a network along with the physical transmission media (Type of wire, wireless, etc) and the data access method (OSI Layer 2). Includes ethernet, Token Ring, ARCnet, AppleTalk, and FDDI. This main area of the document can and should be skipped by those learning networking and read later.
4. Other Transport Protocols - Describes IPX/SPX, NetBEUI, and more.
5. Functions - Explains some of the functionality of networking such as routing, firewalls and DNS.
6. Further Details - Gives information about some protocols not covered in the "Basics" section. In the future, it will include more information about packet fragmentation and re-assembly along with more details about UDP and especially TCP and TCP connections.
7. More Complex functions - Documents multicasting, dynamic routing, and network management
8. Applications - Documents how some of the applications work such as ping and traceroute. In the future, it will cover telnet, Rlogin, and FTP.
9. Other Concerns - Includes installing drivers, network operating systems, applications, wide area networks, backing up the network and troubleshooting the network.
10. References - Includes a reference list of terms, RFCs and recommended reading.

The reader may read this document in any order, but for beginners, it would be best to read through from the beginning with the exception of sections 2 (media), 3 (architecture), and 4 (other). At some point, however, the reader should be able to break from the basics and read about routing and IP masquerading.

There are no links to various reading material or software packages inside this document, except under the references section. This is because it is more structured, and makes it easier to keep the document current.

This document will first talk about the network basics so the reader can get a good grasp of networking concepts. This should help the reader understand how each network protocol is used to perform networking. The reader will be able to understand why each protocol is needed, how it is used, and what other protocols it relies upon. This document explains the data encapsulation techniques in preparation for transport along with some of the network protocols such as IP, TCP, UDP, ICMP, and IGMP. It explains how ARP and RARP support networking. In functional areas, such as routers, several examples are given so the user can get a grasp on how networking is done in their particular situation. This document covers routing, IP masquerading, and firewalls and gives some explanation of how they work, how they are set up, and how and why they are used. Firewalls and the available packages are described, but how to set them up is left to other documentation specific to the operating system and the package. Application protocols such as FTP and Telnet are also briefly described. Networking terms are also explained and defined.

This document explains the setup of networking functions using Linux Redhat version 6.1 as an operating system (OS) platform. This will apply to server functions such as routing and IP masquerading. For more documentation on setting up packages, read documentation on this web site and other locations specific to the operating system and the package. If you know how to set up other operating servers such as Windows NT, you can apply the information in this document to help you understand how to configure services on that OS platform.

This document was written because I perceived a need for a basic networking document to explain how these networking services work and how to set them up, with examples. It will help a novice to learn networking more quickly by explaining the big picture concerning how the system works together. I have seen much good networking documentation, but little that explains the theory along with practical setup and applications.

Network Topology

A network consists of multiple computers connected using some type of interface, each having one or more interface devices such as a Network Interface Card (NIC) and/or a serial device for PPP networking. Each computer is supported by network software that provides the server or client functionality. The hardware used to transmit data across the network is called the media. It may include copper cable, fiber optic, or wireless transmission. The standard cabling used for the purposes of this document is 10Base-T category 5 ethernet cable. This is twisted copper cabling which appears at the surface to look similar to TV coaxial cable. It is terminated on each end by a connector that looks much like a phone connector. Its maximum segment length is 100 meters.

Network Categories

There are two main types of network categories which are:

- Server based
- Peer-to-peer

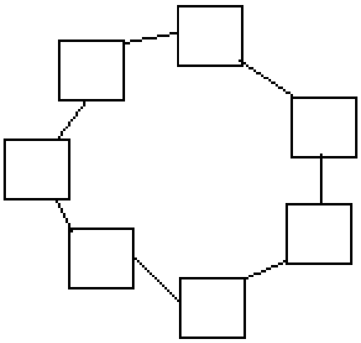
In a server based network, there are computers set up to be primary providers of services such as file service or mail service. The computers providing the service are are called servers and the computers that request and use the service are called client computers.

In a peer-to-peer network, various computers on the network can act both as clients and servers. For instance, many Microsoft Windows based computers will allow file and print sharing. These computers can act both as a client and a server and are also referred to as peers. Many networks are combination peer-to-peer and server based networks. The network operating system uses a network data protocol to communicate on the network to other computers. The network operating system supports the applications on that computer. A Network Operating System (NOS) includes Windows NT, Novell Netware, Linux, Unix and others.

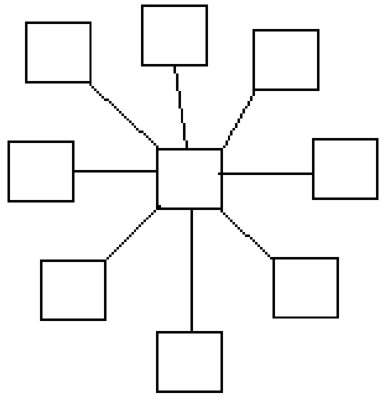
Three Network Topologies

The network topology describes the method used to do the physical wiring of the network. The main ones are bus, star, and ring.

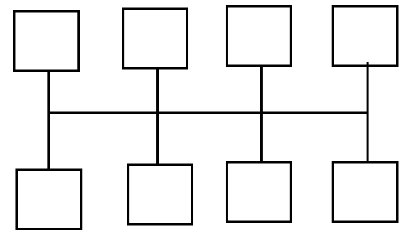
Networking Topologies



Ring



Star



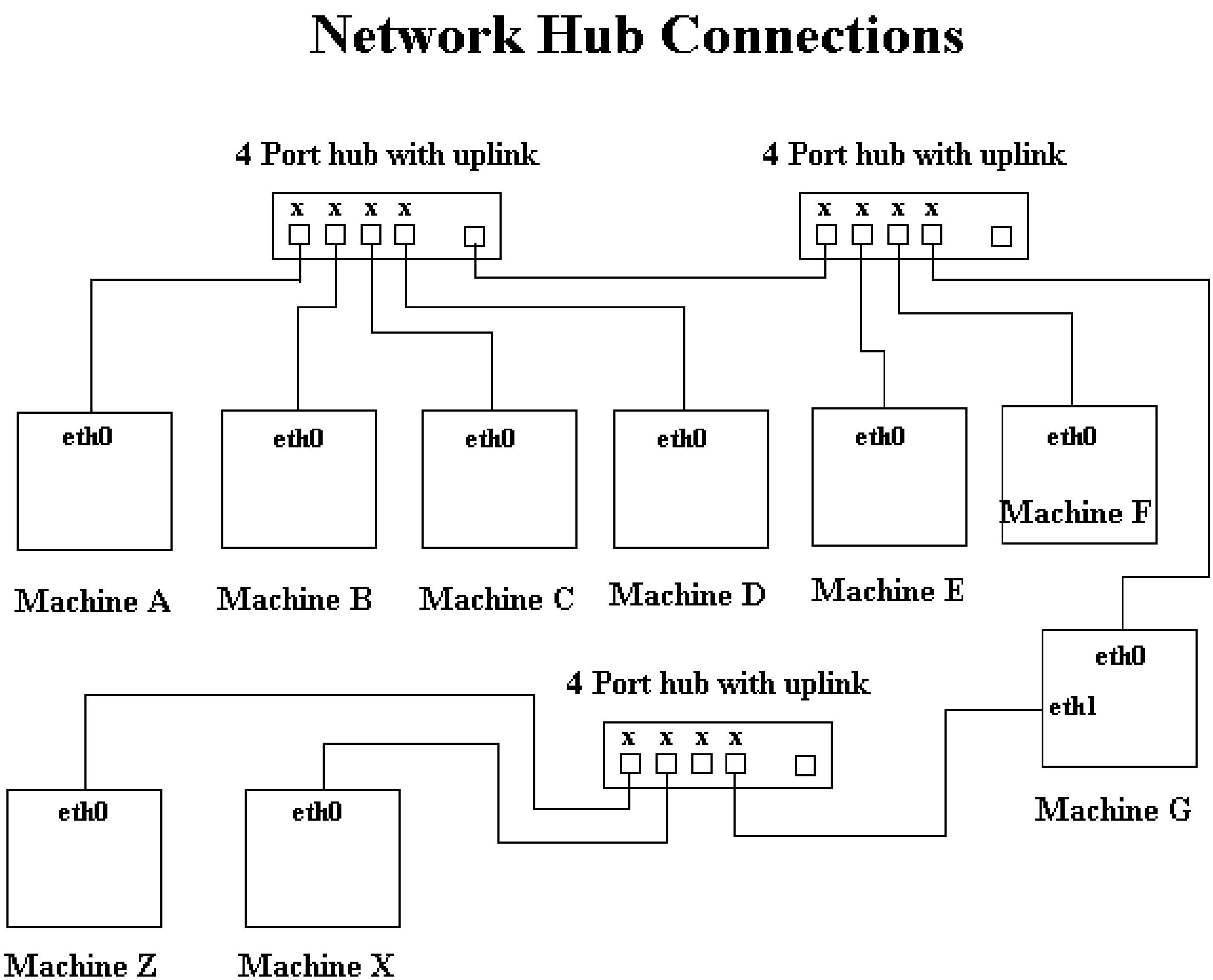
Bus

1. Bus - Both ends of the network must be terminated with a terminator. A barrel connector can be used to extend it.
2. Star - All devices revolve around a central hub, which is what controls the network communications, and can communicate with other hubs. Range limits are about 100 meters from the hub.
3. Ring - Devices are connected from one to another, as in a ring. A data token is used to grant permission for each computer to communicate.

There are also hybrid networks including a star-bus hybrid, star-ring network, and mesh networks with connections between various computers on the network. Mesh networks ideally allow each computer to have a direct connection to each of the other computers. The topology this documentation deals with most is star topology since that is what ethernet networks use.

Network Hardware Connections

Ethernet uses star topology for the physical wiring layout. A diagram of a typical ethernet network layout is shown below.



On a network, a hub is basically a repeater which is used to re-time and amplify the network signals. In this diagram, please examine the hubs closely. On the left are 4 ports close to each other with an x above or below them. This means that these ports are crossover ports. This crossover is similar to the arrangement that was used for serial cables between two computers. Each serial port has a transmitter and receiver. Unless there was a null modem connection between two serial ports, or the cable was wired to cross transmit to receive and vice versa, the connection would not work. This is because the transmit port would be sending to the transmit port on the other side.

Therefore note that you cannot connect two computers together with a straight network jumper cable between their network cards. You must use a special crossover cable that you can buy at most computer stores and some office supply stores for around 10 dollars. Otherwise, you must use a hub as shown here.

The hub on the upper left is full, but it has an uplink port on the right which lets it connect to another hub. The uplink does not have a crossover connection and is designed to fit into a crossover connection on the next hub. This way you can keep linking hubs to put computers on a network. Because each hub introduces some delay onto the network signals, there is a limit to the number of hubs you can sequentially link. Also the computers that are connected to the two hubs are on the same network and can talk to each other. All network traffic including all broadcasts is passed through the hubs.

In the diagram, machine G has two network cards, eth0 and eth1. The cards eth1 and eth0 are on two different networks or subnetworks. Unless machine G is programmed as a router or bridge, traffic will not pass between the two networks. This means that machines X and Z cannot talk to machines A through F and vice versa. Machine X can talk to Z and G, and machines A though F can talk to each other and they can talk to machine G. All machines can talk to machine G. Therefore the machines are dependent on machine G to talk between the two networks or subnets.

Each network card, called a network interface card **(NIC)** has a built in hardware address programmed by its manufacturer. This is a 48 bit address and should be unique for each card. This address is called a media access control **(MAC)** address. The media, in our specific case will be the ethernet. Therefore when you refer to ethernet, you are referring to the type of network card, the cabling, the hubs, and the data packets being sent. You are talking about the hardware that makes it work, along with the data that is physically sent on the wires.

There are three types of networks that are commonly heard about. They are ethernet, token-ring, and ARCnet. Each one is described briefly here, although this document is mainly about ethernet.

Ethernet:

The network interface cards share a common cable. This cable structure does not need to form a structure, but must be essentially common to all cards on the network. Before a card transmits, it listens for a break in traffic. The cards have collision detection, and if the card detects a collision while trying to transmit, it will retry after some random time interval.

Token Ring:

Token ring networks form a complete electrical loop, or ring. Around the ring are computers, called stations. The cards, using their built in serial numbers, negotiate to determine what card will be the master interface card. This card will create what is called a token, that will allow other cards to send data. Essentially, when a card with data to send, receives a token, it sends its data to the next station up the ring to be relayed. The master interface will then create a new token and the process begins again.

ARCnet:

ARCnet networks designate a master card. The master card keeps a table of active cards, polling each one sequentially with transmit permission.

TCP/IP Ports and Addresses

Each machine in the network shown below, has one or more network cards. The part of the network that does the job of transporting and managing the data across the network is called TCP/IP which stands for Transmission Control Protocol (TCP) and Internet Protocol (IP). There are other alternative mechanisms for managing network traffic, but most, such as IPX/SPX for Netware, will not be described here in much detail. The IP layer requires a 4 (IPv4) or 6 (IPv6) byte address to be assigned to each network interface card on each computer. This can be done automatically using network software such as dynamic host configuration protocol (DHCP) or by manually entering static addresses into the computer.

Ports

The TCP layer requires what is called a port number to be assigned to each message. This way it can determine the type of service being provided. Please be aware here, that when we are talking about "ports" we are not talking about ports that are used for serial and parallel devices, or ports used for computer hardware control. These ports are merely reference numbers used to define a service. For instance, port 23 is used for telnet services, and HTTP uses port 80 for providing web browsing service. There is a group called the IANA (Internet Assigned Numbers Authority) that controls the assigning of ports for specific services. There are some ports that are assigned, some reserved and many unassigned which may be utilized by application programs. Port numbers are straight unsigned integer values which range up to a value of 65535.

Addresses

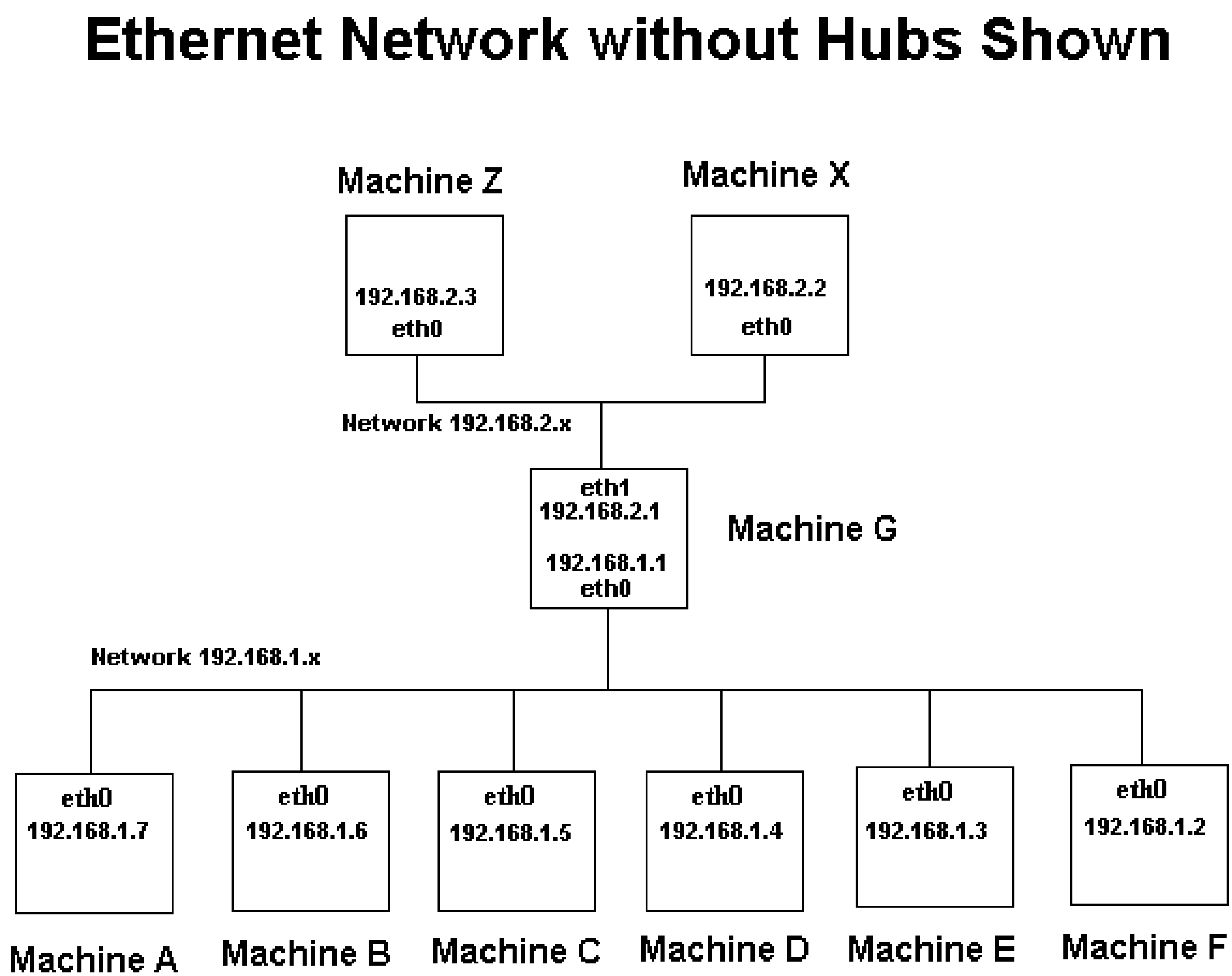
Addresses are used to locate computers. It works almost like a house address. There is a numbering system to help the mailman locate the proper house to deliver customer's mail to. Without an IP numbering system, it would not be possible to determine where network data packets should go.

IPv4, which means internet protocol version 4, is described here. Each IP address is denoted by what is called dotted decimal notation. This means there are four numbers, each separated by a dot. Each number represents a one byte value with a possible mathematical range of 0-255. Briefly, the first one or two bytes, depending on the class of network, generally will indicate the number of the network, the third byte indicates the number of the subnet, and the fourth number indicates the host number. This numbering scheme will vary depending on the network and the numbering method used such as Classless Inter-Domain Routing (CIDR) which is described later. The host number cannot be 0 or 255. None of the numbers can be 255 and the first number cannot be 0. This is because broadcasting is done with all bits set in some bytes. Broadcasting is a form of communication that all hosts on a network can read, and is normally used for performing various network queries. An address of all 0's is not used, because when a machine is booted that does not have a hardware address assigned, it provides 0.0.0.0 as its address until it receives its assignment. This would occur for machines that are remote booted or those that boot using the dynamic host configuration protocol (DHCP). The part of the IP address that defines the network is referred to as the network ID, and the latter part of the IP address that defines the host address is referred to as the host ID.

IPv6 is an enhancement to the IPv4 standard due to the shortage of internet addresses. The dotted notation values are increased to 12 bit values rather than byte (8 bit) values. This increases the effective range of each possible decimal value to 4095. Of course the values of 0 and 4095 (all bits set) are generally reserved the same as with the IPv4 standard.

An Example Network

In the diagram below, the earlier hardware wiring example is modified to show the network without the hubs. It also shows IP addresses assigned to each interface card. As you can see there are two networks which are 192.168.1.x and 192.168.2.x. Machines A through F are on network 192.168.1.x. The machines X and Z are on network 192.168.2.x, and machine G has access to both networks.



NIC	A	B	C	D	E	F	G	X	Z
eth0	192.168.1.7	192.168.1.6	192.168.1.5	192.168.1.4	192.168.1.3	192.168.1.2	192.168.1.1	192.168.2.2	192.168.2.3
eth1	-	-	-	-	-	-	192.168.2.1	-	-

Using this port and addressing scheme, the networking system can pass data, addressing information, and type of service information through the hardware, from one computer to another. The reason, there is an address for the hardware card (ethernet address, also called MAC address), and another assigned address for that same card (IP address), is to keep the parts of the network system that deal with the hardware and the software, independent of each other. This is required in order to be able to configure the IP addressing dynamically. Otherwise, all computers would have a static address and this would be very difficult to manage. Also, if a modification needs to be made to the hardware addressing scheme for any reason, in ethernet, it will be transparent to the rest of the system. Conversely if a change is made to the software addressing scheme in the IP part of the system, the ethernet and TCP protocols will be unaffected.

In the example above, machine F will send a telnet data packet to machine A. Roughly, the following steps occur.

1. The Telnet program in machine F prepares the data packet. This occurs in the application (Telnet), presentation, and session layers of the OSI network model.
2. The TCP software adds a header with the port number, 23, to the packet. This occurs in the transport (TCP) layer.
3. The IP software adds a header with the sender's and recipient's IP address, 192.168.1.2 to the packet. This occurs in the network (IP) layer.
4. The ethernet header is added to the packet with the hardware address of the network card and the packet is transmitted. This occurs in the link (Ethernet) layer.
5. Machine A's network card detects it's address in the packet, retrieves the data, and strips its header data and sends it to the IP layer.
6. The IP layer looks at the IP header, and determines if the sender's IP address is acceptable to provide service to (hosts.allow, hosts.deny, etc), and if so, strips the IP header and sends it to the TCP layer.
7. The TCP Layer reads the port number in it's header, determines if service is provided for that port, and what application program is servicing that port. It strips the TCP header and passes the remainder of the data to the telnet program on machine A.

Please note, that the network layers mentioned here are described in the next section. Also there are many types of support at each of the four TCP/IP network system layers, but that issue is addressed in the next section.

Network Protocol Levels

You should be aware of the fact, that when talking about networking you will hear the word "protocol" all the time. This is because protocols are sets of standards that define all operations within a network. They define how various operations are to be performed. They may even define how devices outside the network can interact with the network. Protocols define everything from basic networking data structures, to higher level application programs. They define various services and utility programs. Protocols operate at many layers of the network models described below. There are protocols considered to be transport protocols such as TCP and UDP. Other protocols work at the network layer of the OSI network model shown below, and some protocols work at several of the network layers.

RFCs

Protocols are outlined in Request for Comments (RFCs). At the end of this document is a list of protocols and associated RFC numbers.Protocols. Although RFCs define protocols not all RFCs define protocols but may define other requirements for the internet such as RFC 1543 which provides information about the preparation of RFCs. The following RFCs are very central to the TCP/IP protocol.

- RFC 1122 - Defines host requirements of the TCP/IP suite of protocols covering the link, network (IP), and transport (TCP, UDP) layers.
- RFC 1123 - The companion RFC to 1122 covering requirements for internet hosts at the application layer
- RFC 1812 - Defines requirements for internet gateways which are IPv4 routers

Network Models

There are several network models which you may hear about but the one you will hear about most is the ISO network model described below. You should realize, however that there are others such as:

- The internet layered protocol
- The TCP/IP 4 layered protocol
- The Microsoft networking protocol

If you don't like any of these models, feel free to invent your own along with your own networking scheme of course, and add it to the list above. You can call it "The MyName Protocol". Ever wonder why networking can be so complex and confusing? Welcome to the world of free enterprise!

The ISO Network Model Standard

The International Standards Organization (ISO) has defined a standard called the Open Systems Interconnection (OSI) reference model. This is a seven layer architecture listed below. Each layer is considered to be responsible for a different part of the communications. This concept was developed to accommodate changes in technology. The layers are arranged here from the lower levels starting with the physical (hardware) to the higher levels.

1. Physical Layer - The actual hardware.
2. Data Link Layer - Data transfer method (802x ethernet). Puts data in frames and ensures error free transmission. Also controls the timing of the network transmission. Adds frame type, address, and error control information. IEEE divided this layer into the two following sublayers.
    1. Logical Link control (LLC) - Maintains the Link between two computers by establishing Service Access Points (SAPs) which are a series of interface points. IEEE 802.2.
    2. Media Access Control (MAC) - Used to coordinate the sending of data between computers. The 802.3, 4, 5, and 12 standards apply to this layer. If you hear someone talking about the MAC address of a network card, they are referring to the hardware address of the card.
3. Network Layer - IP network protocol. Routes messages using the best path available.
4. Transport Layer - TCP, UDP. Ensures properly sequenced and error free transmission.
5. Session Layer - The user's interface to the network. Determines when the session is begun or opened, how long it is used, and when it is closed. Controls the transmission of data during the session. Supports security and name lookup enabling computers to locate each other.
6. Presentation Layer - ASCII or EBCDEC data syntax. Makes the type of data transparent to the layers around it. Used to translate date to computer specific format such as byte ordering. It may include compression. It prepares the data, either for the network or the application depending on the direction it is going.
7. Application Layer - Provides services software applications need. Provides the ability for user applications to interact with the network.

Many protocol stacks overlap the borders of the seven layer model by operating at multiple layers of the model. File Transport Protocol (FTP) and telnet both work at the application, presentation, and the session layers.

The Internet, TCP/IP, DOD Model

This model is sometimes called the DOD model since it was designed for the department of defense It is also called the TCP/IP four layer protocol, or the internet protocol. It has the following layers:

1. Link - Device driver and interface card which maps to the data link and physical layer of the OSI model.
2. Network - Corresponds to the network layer of the OSI model and includes the IP, ICMP, and IGMP protocols.
3. Transport - Corresponds to the transport layer and includes the TCP and UDP protocols.
4. Application - Corresponds to the OSI Session, Presentation and Application layers and includes FTP, Telnet, ping, Rlogin, rsh, TFTP, SMTP, SNMP, DNS, your program, etc.

Please note the four layer TCP/IP protocol. Each layer has a set of data that it generates.

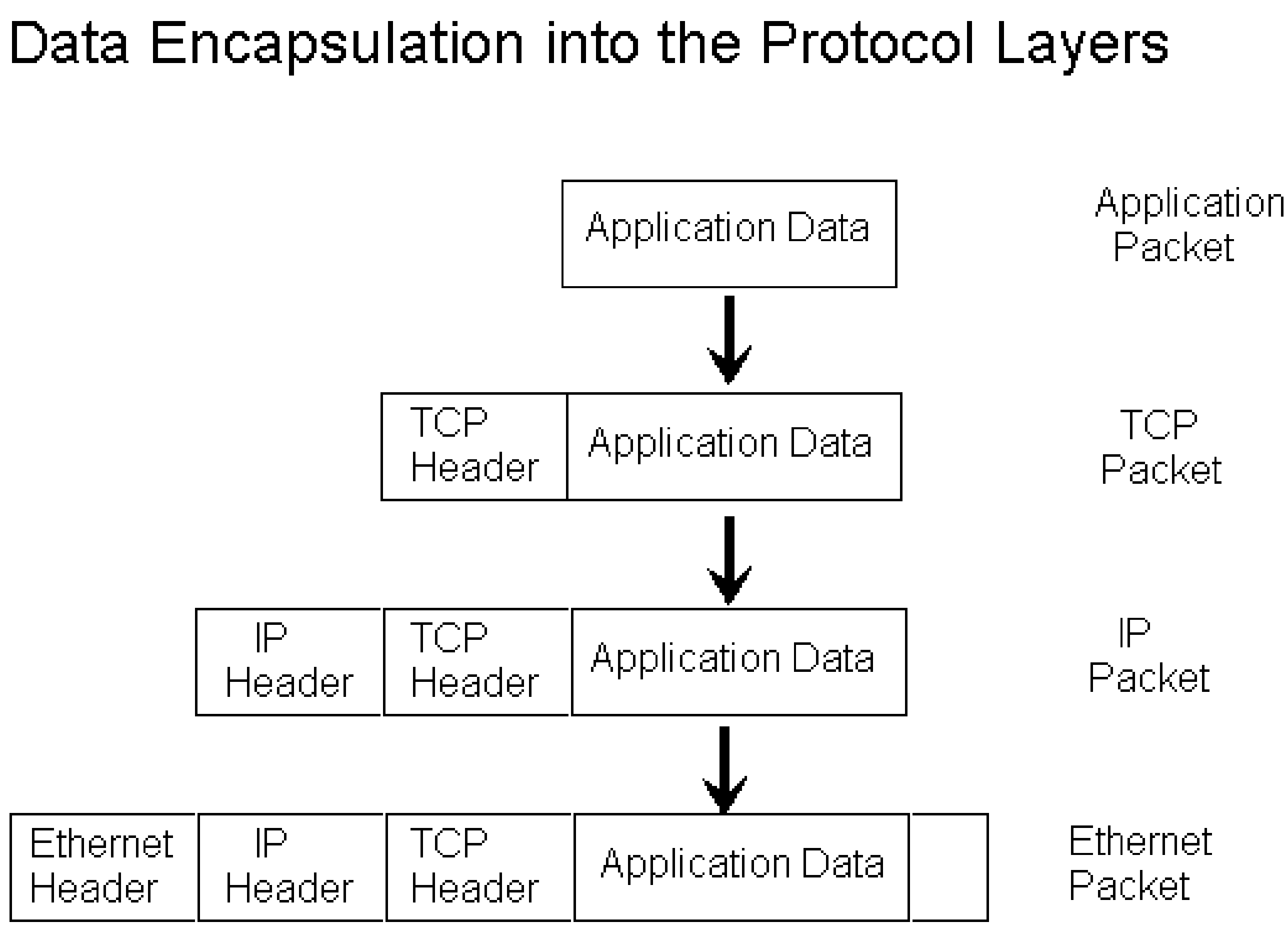
1. The Link layer corresponds to the hardware, including the device driver and interface card. The link layer has data packets associated with it depending on the type of network being used such as ARCnet, Token ring or ethernet. In our case, we will be talking about ethernet.
2. The network layer manages the movement of packets around the network and includes IP, ICMP, and IGMP. It is responsible for making sure that packages reach their destinations, and if they don't, reporting errors.
3. The transport layer is the mechanism used for two computers to exchange data with regards to software. The two types of protocols that are the transport mechanisms are TCP and UDP. There are also other types

of protocols for systems other than TCP/IP but we will talk about TCP and UDP in this document.

4. The application layer refers to networking protocols that are used to support various services such as FTP, Telnet, BOOTP, etc. Note here to avoid confusion, that the application layer is generally referring to protocols such as FTP, telnet, ping, and other programs designed for specific purposes which are governed by a specific set of protocols defined with RFC's (request for comments). However a program that you may write can define its own data structure to send between your client and server program so long as the program you run on both the client and server machine understand your protocol. For example when your program opens a socket to another machine, it is using TCP protocol, but the data you send depends on how you structure it.

Data Encapsulation, a Critical concept to be understood

When starting with protocols that work at the upper layers of the network models, each set of data is wrapped inside the next lower layer protocol, similar to wrapping letters inside an envelope. The **application** creates the data, then the **transport** layer wraps that data inside its format, then the **network** layer wraps the data, and finally the **link** (ethernet) layer encapsulates the data and transmits it.



To continue, you should understand the definition of a client and server with regards to networking. If you are a server, you will provide services to a client, in much the same way as a private investigator would provide services to their clients. A client will contact the server, and ask for service, which the server will then provide. The service may be as simple as sending a single block of data back to the client. Since there are many clients, a server must be constantly ready to receive client requests, even though it may already be working with other clients. Usually the client program will operate on one computer, while the server program will operate on another computer, although programs can be written to be both a client and a server.

Lets say you write a client chat program and a server chat program to be used by two people to send messages between their machines. You run the server program on machine B, and the client program on machine A. Tom is on machine A and George is on machine B. George's machine is always ready to be contacted, but cannot initiate a contact. Therefore if George wants to talk to Tom, he cannot, until Tom contacts him. Tom, of course can initiate contact at any time. Now you decide to solve the problem and merge the functionality of the two programs into one, so both parties may contact the other. This program is now a client/server program which operates both as a client and a server. You write your code so when one side initiates contact, he will get a dialog box, and a dialog box will pop up on the other side. At the time contact is initiated, a socket is opened between the two machines and a virtual connection is established. The program will let the user (Tom) type text into the dialog window, and hit send. When the user hits send, roughly the following will happen.

1. Your program will pass Tom's typed text in a buffer, to the socket. This happens on machine A.
2. The underlying software (Code in a library called by a function your program used to send the data) supporting the socket puts the data inside a TCP data packet. This means that a TCP header will be added to the data. This header contains a source and destination port number along with some other information and a checksum. Deamon programs (Daemon definition at the bottom of this page) may also work at this level to sort packages based on port number (hence the TCP wrapper program in UNIX and Linux).
3. The TCP packet will be placed inside an IP data packet with a source and destination IP address along with some other data for network management. This may be done by a combination of your library function, the operating system and supporting programs.
4. The IP data packet is placed inside an ethernet data packet. This data packet includes the destination and source address of the network interface cards (NIC) on the two computers. The address here is the hardware address of the respective cards and is called the MAC address.
5. The ethernet packet is transmitted over the network line.
6. Assuming there is a direct connection between the two computers, the network interface card on machine B, will recognize its MAC address and grab the data.
7. The IP data packet will be extracted from the ethernet data packet. A combination of deamons and the operating system will perform this operation.
8. The TCP data packet will be extracted from the IP data packet. A combination of deamons, the operating system, and libraries called by your program will perform this function.
9. The data will be extracted from the TCP packet. Your program will then display the retrieved data (text) in the text display window for George to read.

Be aware that for the sake of simplicity, we are excluding details such as error management, routing, and identifying the hardware address of the NIC on the computer intended to receive the data. Also we are not mentioning the possible rejection of service based on a packet's port number or sender's IP address.

A deamon program is a program that runs in the background on a computer operating system. It is used to perform various tasks including server functions. It is usually started when the operating system is booted, but a user or administrator may be able to start or stop a daemon at any time.

IEEE 802 Standard

The Data Link Layer and IEEE

When we talk about Local Area Network (LAN) technology the IEEE 802 standard may be heard. This standard defines networking connections for the interface card and the physical connections, describing how they are done. The 802 standards were published by the Institute of Electrical and Electronics Engineers (IEEE). The 802.3 standard is called ethernet, but **the IEEE standards do not define the exact original true ethernet standard that is common today**. There is a great deal of confusion caused by this. There are several types of common ethernet frames. Many network cards support more than one type.

The ethernet standard data encapsulation method is defined by RFC 894. RFC 1042 defines the IP to link layer data encapsulation for networks using the IEEE 802 standards. The 802 standards define the two lowest levels of the seven layer network model and primarily deal with the control of access to the network media. The network media is the physical means of carrying the data such as network cable. The control of access to the media is called media access control (MAC). The 802 standards are listed below:

- 802.1 - Internetworking
- 802.2 - Logical Link Control *
- 802.3 - Ethernet or CSMA/CD, Carrier-Sense Multiple Access with Collision detection LAN *
- 802.4 - Token-Bus LAN *
- 802.5 - Token Ring LAN *
- 802.6 - Metropolitan Area Network (MAN)
- 802.7 - Broadband Technical Advisory Group
- 802.8 - Fiber-Optic Technical Advisory Group
- 802.9 - Integrated Voice/Data Networks
- 802.10 - Network Security
- 802.11 - Wireless Networks
- 802.12 - Demand Priority Access LAN, 100 Base VG-AnyLAN

*The Ones with stars should be remembered in order for network certification testing.

Network Access Methods

There are various methods of managing access to a network. If all network stations tried to talk at once, the messages would become unintelligible, and no communication could occur. Therefore a method of being sure that stations coordinate the sending of messages must be achieved. There are several methods listed below which have various advantages and disadvantages.

- Contention
  - Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) - Used by Ethernet
  - Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)
- Token Passing - A token is passed from one computer to another, which provides transmission permission.
- Demand Priority - Describes a method where intelligent hubs control data transmission. A computer will send a demand signal to the hub indicating that it wants to transmit. The hub sill respond with an acknowledgement that will allow the computer to transmit. The hub will allow computers to transmit in turn. An example of a demand priority network is 100VG-AnyLAN (IEEE 802.12). It uses a star-bus topology.
- Polling - A central controller, also called the primary device will poll computers, called secondary devices, to find out if they have data to transmit. Of so the central controller will allow them to transmit for a limited time, then the next device is polled.

Token passing performs better when the network has a lot of traffic, while ethernet which uses CSMA/CD is generally faster but loses performance when the network has a lot of traffic. CSMA/CD is basically a method that allows network stations to transmit any time they want. They, however, sense the network line and detect if another station has transmitted at the same time they did. This is called a collision. If a collision happened, the stations involved will retransmit at a later, randomly set time in hopes of avoiding another collision.

IP to link layer encapsulation

The requirements for IP to link layer encapsulation for hosts on a Ethernet network are:

- All hosts must be able to send and receive packets defined by RFC 894.
- All hosts should be able to receive a mix of packets defined by RFC 894 and RFC 1042.
- All hosts may be able to send RDC 1042 defined packets.

Hosts that support both must provide a means to configure the type of packet sent and the default must be packets defined by RFC 894.

Ethernet and IEEE 802 Encapsulation formats

Ethernet (RFC 894) message format consists of:

1. 6 bytes of destination address.
2. 6 bytes of source address.
3. 2 bytes of message type which indicates the type of data being sent.
4. 46 to 1500 bytes of data.
5. 4 bytes of cyclic redundancy check (CRC) information.

IEEE 802 (RFC 1042) Message format consists of 3 sections plus data and CRC as follows:

1. 802.3 Media Access Control section used to coordinate the sending of data between computers.
    1. 6 bytes of destination address.
    2. 6 bytes of source address.
    3. 2 bytes of length - The number of bytes that follow not including the CRC.
2. 802.2 Logical Link control establishes service access points (SAPs) between computers.
    1. 1 byte destination service access point (DSAP).
    2. 1 byte source service access point (SSAP).
    3. 1 byte of control.
3. Sub Network Access Protocol (SNAP).
    1. 3 bytes of org code.
    2. 2 bytes of message type which indicates the type of data being sent.
4. 38 to 1492 bytes of data.
5. 4 bytes of cyclic redundancy check (CRC) information.

Some ethernet message types include:

- 0800 - IP datagram with length of 38 to 1492 bytes.
- 0806 - ARP request or reply with 28 bytes and pad bytes that are used to make the frame long enough for the minimum length.
- 8035 - RARP request or reply of 28 bytes and pad bytes that are used to make the frame long enough for the minimum length.

These message types are the same for both formats above with the exception of the pad bytes. The pad bytes for the RFC 894 and RFC 1042 datagrams are of different lengths between the two message formats because the RFC 894 minimum message length is 46 bytes and the RFC 1042 minimum message length is 38 bytes. Also the two message formats above are distinguishable from each other. This is because the RFC 894 possible length values are exclusive of RFC 1042 possible type values.

Trailor Encapsulation

This is described in RFC 1122 and RFC 892, but this scheme is not used very often today. The trailer protocol [LINK:1] is a link-layer encapsulation method that rearranges the data contents of packets sent on the physical network. It may be used but only after it is verified that both the sending and receiving hosts support trailers. The verification is done for each host that is communicated with.

RFC 1122 states: "Only packets with specific size attributes are encapsulated using trailers, and typically only a small fraction of the packets being exchanged have these attributes. Thus, if a system using trailers exchanges packets with a system that does not, some packets disappear into a black hole while others are delivered successfully."

Trailer negotiation is performed when ARP is used to discover the media access control (MAC) address of the destination host. RFC 1122 states: "a host that wants to speak trailers will send an additional "trailer ARP reply" packet, i.e., an ARP reply that specifies the trailer encapsulation protocol type but otherwise has the format of a normal ARP reply. If a host configured to use trailers receives a trailer ARP reply message from a remote machine, it can add that machine to the list of machines that understand trailers, e.g., by marking the corresponding entry in the ARP cache."

Network Categories

TDP/IP includes a wide range of protocols which are used for a variety of purposes on the network. The set of protocols that are a part of TCP/IP is called the TCP/IP protocol stack or the TCP/IP suite of protocols.

Considering the many protocols, message types, levels, and services that TCP/IP networking supports, I believe it would be very helpful to categorize the various protocols that support TCP/IP networking and define their respective contribution to the operation of networking. Unfortunately I have never seen this done to any real extent, but believe it would be worthwhile to help those learning networking understand it faster and better. I cannot guarantee that experts will agree with the categorizations that will be provided here, but they should help the reader get the big picture on the various protocols, and thus clarify what the reason or need is for each protocol.

As mentioned previously, there are four TCP/IP layers. They are link, network, transport, and application. The link layer is the hardware layer that provides ability to send messages between multiple locations. In the case of this document, ethernet provides this capability. Below I define several categories some of which fit into the 4 layer protocol levels described earlier. I also define a relative fundamental importance to the ability of the network to function at all. Importance includes essential, critical, important, advanced, useful.

1. Essential - Without this all other categories are irrelevant.
2. Critical - The network, as designed, is useless without this ability.
3. Important - The network could function, but would be difficult to use and manage.
4. Advanced - Includes enhancements that make the network easier to use and manage.
5. Useful - Functionality that you would like to be able to use as a network user. Applications or some functionality is supported here. Without this, why build a network?

The categories are:

Name(layer)	Importance	Names of protocols	What it does
Hardware(link)	Essential	ethernet, SLIP, PPP, Token Ring, ARCnet	Allows messages to be packaged and sent between physical locations.
Package management(network)	Essential	IP, ICMP	Manages movement of messages and reports errors. It uses message protocols and software to manage this process. (includes routing)
Inter layer communication	Essential	ARP	Communicates between layers to allow one layer to get information to support another layer. This includes broadcasting
Service control(transport)	Critical	TCP, UDP	Controls the management of service between computers. Based on values in TCP and UDP messages a server knows what service is being requested.
Application and user support	Important	DNS, RPC	DNS provides address to name translation for locations and network cards. RPC allows remote computer to perform functions on other computers.
Network Management	Advanced	RARP, BOOTP, DHCP, IGMP, SNMP,RIP, OSPF, BGP, CIDR	Enhances network management and increases functionality

Utility(Application)	Useful	FTP, TFTP, SMTP, Telnet, NFS, ping, Rlogin	Provides direct services to the user.

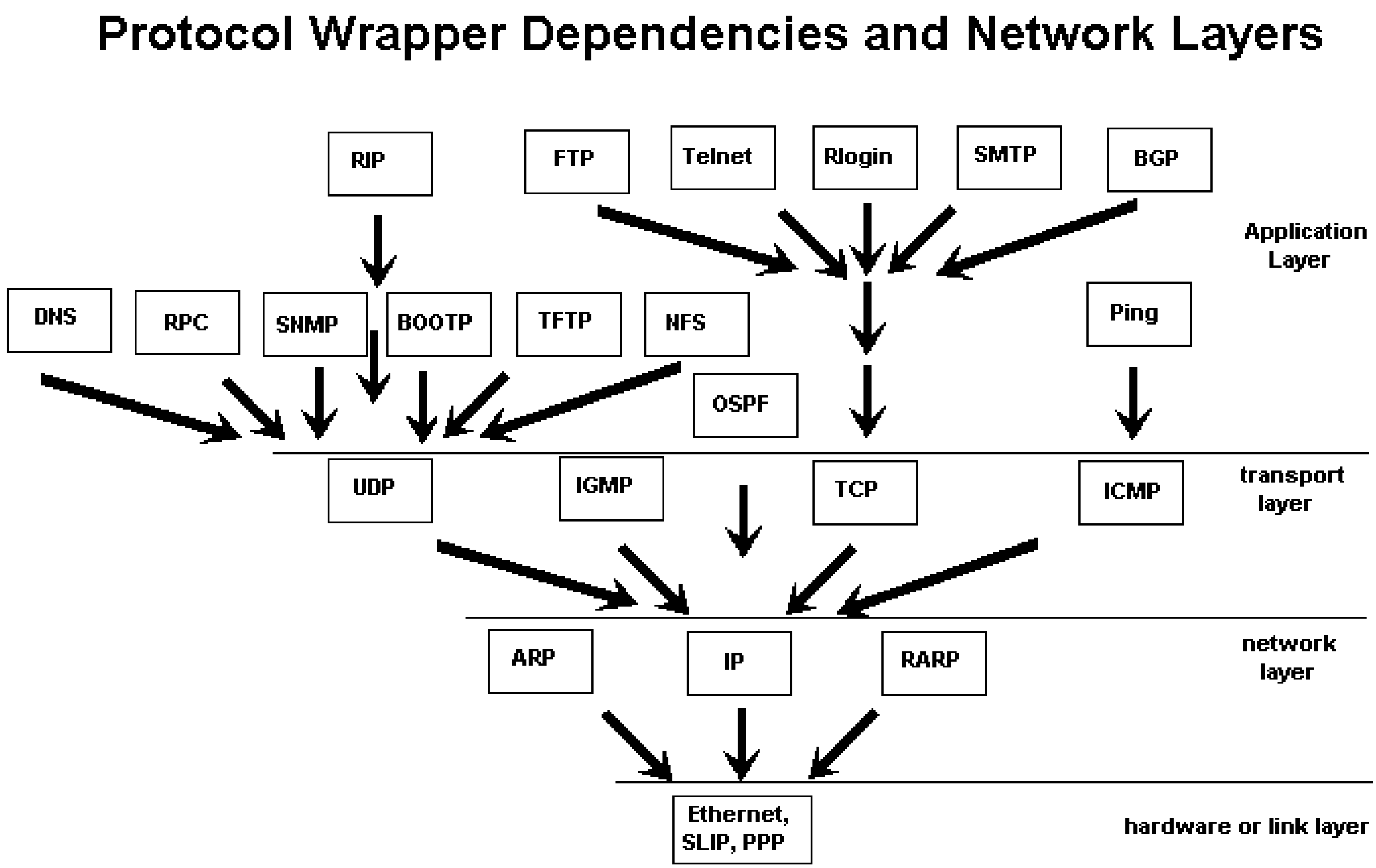
There are exceptions to my categorizations that don't fit into the normal layering scheme, such as IGMP is normally part of the link layer, but I have tried to list these categorizations according to network functions and their relative importance to the operation of the network. Also note that ethernet, which is not really a protocol, but an IEEE standard along with PPP, SLIP, TokenRing, and ArcNet are not TCP/IP protocols but may support TCP/IP at the hardware or link layer, depending on the network topology.

The list below gives a brief description of each protocol

- ethernet - Provides for transport of information between physical locations on ethernet cable. Data is passed in ethernet packets
- SLIP - Serial line IP (SLIP), a form of data encapsulation for serial lines.
- PPP - Point to point protocol (PPP). A form of serial line data encapsulation that is an improvement over SLIP.
- IP - Internet Protocol (IP). Except for ARP and RARP all protocols' data packets will be packaged into an IP data packet. Provides the mechanism to use software to address and manage data packets being sent to computers.
- ICMP - Internet control message protocol (ICMP) provides management and error reporting to help manage the process of sending data between computers.
- ARP - Address resolution protocol (ARP) enables the packaging of IP data into ethernet packages. It is the system and messaging protocol that is used to find the ethernet (hardware) address from a specific IP number. Without this protocol, the ethernet package could not be generated from the IP package, because the ethernet address could not be determined.
- TCP - A reliable connection oriented protocol used to control the management of application level services between computers.
- UDP - An unreliable connection less protocol used to control the management of application level services between computers.
- DNS - Domain Name Service, allows the network to determine IP addresses from names and vice versa.
- RARP - Reverse address resolution protocol (RARP) is used to allow a computer without a local permanent data storage media to determine its IP address from its ethernet address.
- BOOTP - Bootstrap protocol is used to assign an IP address to diskless computers and tell it what server and file to load which will provide it with an operating system.
- DHCP - Dynamic host configuration protocol (DHCP) is a method of assigning and controlling the IP addresses of computers on a given network. It is a server based service that automatically assigns IP numbers when a computer boots. This way the IP address of a computer does not need to be assigned manually. This makes changing networks easier to manage. DHCP can perform all the functions of BOOTP.
- IGMP - Internet Group Management Protocol used to support multicasting.
- SNMP - Simple Network Management Protocol (SNMP). Used to manage all types of network elements based on various data sent and received.
- RIP - Routing Information Protocol (RIP), used to dynamically update router tables on WANs or the internet.
- OSPF - Open Shortest Path First (OSPF) dynamic routing protocol.
- BGP - Border Gateway Protocol (BGP). A dynamic router protocol to communicate between routers on different systems.
- CIDR - Classless Interdomain Routing (CIDR).
- FTP - File Transfer Protocol (FTP). Allows file transfer between two computers with login required.
- TFTP - Trivial File Transfer Protocol (TFTP). Allows file transfer between two computers with no login required. It is limited, and is intended for diskless stations.
- SMTP - Simple Mail Transfer Protocol (SMTP).
- NFS - Network File System (NFS). A protocol that allows UNIX and Linux systems remotely mount each other's file systems.

- Telnet - A method of opening a user session on a remote host.
- Ping - A program that uses ICMP to send diagnostic messages to other computers to tell if they are reachable over the network.
- Rlogin - Remote login between UNIX hosts. This is outdated and is replaced by Telnet.

Each protocol ultimately has it's data packets wrapped in an ethernet, SLIP, or PPP packet (at the link level) in order to be sent over the ethernet cable. Some protocol data packets are wrapped sequentially multiple times before being sent. For example FTP data is wrapped in a TCP packet which is wrapped in a IP packet which is wrapped in a link packet (normally ethernet). The diagram below shows the relationship between the protocols' sequential wrapping of data packets.



Network Devices

Repeaters, Bridges, Routers, and Gateways

Network Repeater

A repeater connects two segments of your network cable. It retimes and regenerates the signals to proper amplitudes and sends them to the other segments. When talking about, ethernet topology, you are probably talking about using a hub as a repeater. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row. Repeaters work only at the physical layer of the OSI network model.

Bridge

A bridge reads the outermost section of data on the data packet, to tell where the message is going. It reduces the traffic on other network segments, since it does not send all packets. Bridges can be programmed to reject packets from particular networks. Bridging occurs at the data link layer of the OSI model, which means the bridge cannot read IP addresses, but only the outermost hardware address of the packet. In our case the bridge can read the ethernet data which gives the hardware address of the destination address, not the IP address. Bridges forward all broadcast messages. Only a special bridge called a translation bridge will allow two networks of different architectures to be connected. Bridges do not normally allow connection of networks with different architectures. The hardware address is also called the MAC (media access control) address. To determine the network segment a MAC address belongs to, bridges use one of:

- Transparent Bridging - They build a table of addresses (bridging table) as they receive packets. If the address is not in the bridging table, the packet is forwarded to all segments other than the one it came from. This type of bridge is used on ethernet networks.
- Source route bridging - The source computer provides path information inside the packet. This is used on Token Ring networks.

Network Router

A router is used to route data packets between two networks. It reads the information in each packet to tell where it is going. If it is destined for an immediate network it has access to, it will strip the outer packet, readdress the packet to the proper ethernet address, and transmit it on that network. If it is destined for another network and must be sent to another router, it will re-package the outer packet to be received by the next router and send it to the next router. The section on routing explains the theory behind this and how routing tables are used to help determine packet destinations. Routing occurs at the network layer of the OSI model. They can connect networks with different architectures such as Token Ring and Ethernet. Although they can transform information at the data link level, routers cannot transform information from one data format such as TCP/IP to another such as IPX/SPX. Routers do not send broadcast packets or corrupted packets. If the routing table does not indicate the proper address of a packet, the packet is discarded.

Brouter

There is a device called a brouter which will function similar to a bridge for network transport protocols that are not routable, and will function as a router for routable protocols. It functions at the network and data link layers of the OSI network model.

Gateway

A gateway can translate information between different network data formats or network architectures. It can translate TCP/IP to AppleTalk so computers supporting TCP/IP can communicate with Apple brand computers. Most gateways operate at the application layer, but can operate at the network or session layer of the OSI model. Gateways will start at the lower level and strip information until it gets to the required level and repackage the information and work its way back toward the hardware layer of the OSI model. To confuse issues, when talking about a router that is used to interface to another network, the word gateway is often used. This does not mean the routing machine is a gateway as defined here, although it could be.

Address Resolution Protocol

ARP and RARP Address Translation

Address Resolution Protocol (ARP) provides a completely different function to the network than Reverse Address Resolution Protocol (RARP). ARP is used to resolve the ethernet address of a NIC from an IP address in order to construct an ethernet packet around an IP data packet. This must happen in order to send any data across the network. Reverse address resolution protocol (RARP) is used for diskless computers to determine their IP address using the network.

Address Resolution Protocol (ARP)

In an earlier section, there was an example where a chat program was written to communicate between two servers. To send data, the user (Tom) would type text into a dialog box, hit send and the following happened:

1. The program passed Tom's typed text in a buffer, to the socket.
2. The data was put inside a TCP data packet with a TCP header added to the data. This header contained a source and destination port number along with some other information and a checksum.
3. The TCP packet was be placed inside an IP data packet with a source and destination IP address along with some other data for network management.
4. The IP data packet was placed inside an ethernet data packet. This data packet includes the destination and source address of the network interface cards (NIC) on the two computers. The address here is the hardware address of the respective cards and is called the MAC address.
5. The ethernet packet was transmitted over the network line.
6. With a direct connection between the two computers, the network interface card on the intended machine, recognized its address and grabbed the data.
7. The IP data packet was extracted from the ethernet data packet.
8. The TCP data packet was extracted from the IP data packet.
9. The data was extracted from the TCP packet and the program displayed the retrieved data (text) in the text display window for the intended recipient to read.

In step 4 above, the IP data was going to be placed inside an ethernet data packet, but the computer constructing the packet does not have the ethernet address of the recipient's computer. The computer that is sending the data, in order to create the ethernet part of the packet, must get the ethernet hardware (MAC) address of the computer with the intended IP address. This must be accomplished before the ethernet packet can be constructed. The ethernet device driver software on the receiving computer is not programmed to look at IP addresses encased in the ethernet packet. If it did, the protocols could not be independent and changes to one would affect the other. This is where address resolution protocol (ARP) is used. Tom's computer sends a network broadcast asking the computer that has the recipient's IP address to send it's ethernet address. This is done by broadcasting. The ethernet destination is set with all bits on so all ethernet cards on the network will receive the data packet. The ARP message consists of an ethernet header and ARP packet. The ethernet header contains:

1. A 6 byte ethernet destination address.
2. A 6 byte ethernet source address.
3. A 2 byte frame type. The frame type is 0806 hexadecimal for ARP and 8035 for RARP

The encapsulated ARP data packet contains the following:

1. Type of hardware address (2 bytes). 1=ethernet.
2. Type of protocol address being mapped(2 bytes). 0800H (hexadecimal) = IP address.
3. Byte size of the hardware address (1 byte). 6
4. Byte size of the protocol address (1 byte). 4
5. Type of operation. 1 = ARP request, 2=ARP reply, 3=RARP request, 4=RARP reply.
6. The sender's ethernet address (6 bytes)
7. The sender's IP address (4 bytes)
8. The recipient's ethernet address (6 bytes)
9. The recipient's IP address (4 bytes)

When the ARP reply is sent, the recipient's ethernet address is left blank.

In order to increase the efficiency of the network and not tie up bandwidth doing ARP broadcasting, each computer keeps a table of IP addresses and matching ethernet addresses in memory. This is called ARP cache. Before sending a broadcast, the sending computer will check to see if the information is in it's ARP cache. If it is it will complete the ethernet data packet without an ARP broadcast. Each entry normally lasts 20 minutes after it is created. RFC 1122 specifies that it should be possible to configure the ARP cache timeout value on the host. To examine the cache on a Windows, UNIX, or Linux computer type "arp -a".

If the receiving host is on another network, the sending computer will go through its route table and determine the correct router (A router should be between two or more networks) to send to, and it will substitute the ethernet address of the router in the ethernet message. The encased IP address will still have the intended IP address. When the router gets the message, it looks at the IP data to tell where to send the data next. If the recipient is on a network the router is connected to, it will do the ARP resolution either using it's ARP buffer cache or broadcasting.

Reverse Address Resolution Protocol (RARP)

As mentioned earlier, reverse address resolution protocol (RARP) is used for diskless computers to determine their IP address using the network. The RARP message format is very similar to the ARP format. When the booting computer sends the broadcast ARP request, it places its own hardware address in both the sending and receiving fields in the encapsulated ARP data packet. The RARP server will fill in the correct sending and receiving IP addresses in its response to the message. This way the booting computer will know its IP address when it gets the message from the RARP server.

Network Addressing

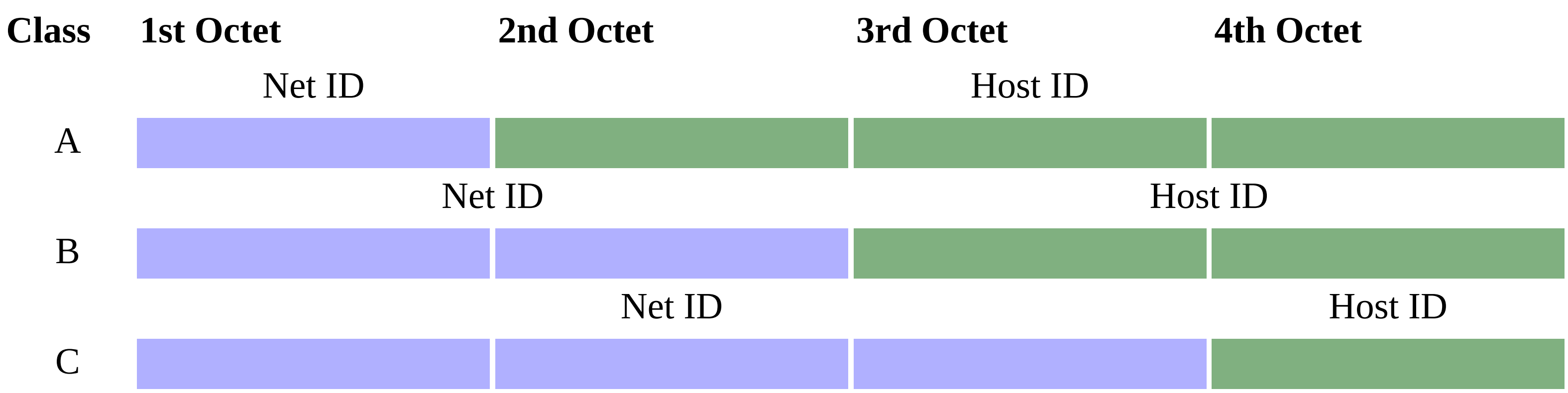
IP addresses are broken into 4 octets (IPv4) separated by dots called dotted decimal notation. An octet is a byte consisting of 8 bits. The IPv4 addresses are in the following form:

192.168.10.1

There are two parts of an IP address:

- Network ID
- Host ID

The various classes of networks specify additional or fewer octets to designate the network ID versus the host ID.



When a network is set up, a **netmask** is also specified. The netmask determines the class of the network as shown below, except for CIDR. When the netmask is setup, it specifies some number of most significant bits with a 1's value and the rest have values of 0. The most significant part of the netmask with bits set to 1's specifies the network address, and the lower part of the address will specify the host address. When setting addresses on a network, remember there can be no host address of 0 (no host address bits set), and there can be no host address with all bits set.

Class A-E networks

The addressing scheme for class A through E networks is shown below. Note: We use the 'x' character here to denote don't care situations which includes all possible numbers at the location. It is many times used to denote networks.

Network Type	Address Range	Normal Netmask	Comments

Class A	001.x.x.x to 126.x.x.x	255.0.0.0	For very large networks
Class B	128.1.x.x to 191.254.x.x	255.255.0.0	For medium size networks
Class C	192.0.1.x to 223.255.254.x	255.255.255.0	For small networks
Class D	224.x.x.x to 239.255.255.255		Used to support multicasting
Class E	240.x.x.x to 247.255.255.255		

RFCs 1518 and 1519 define a system called Classless Inter-Domain Routing (CIDR) which is used to allocate IP addresses more efficiently. This may be used with subnet masks to establish networks rather than the class system shown above. A class C subnet may be 8 bits but using CIDR, it may be 12 bits.

There are some network addresses reserved for private use by the Internet Assigned Numbers Authority (IANA) which can be hidden behind a computer which uses IP masquerading to connect the private network to the internet. There are three sets of addresses reserved. These address are shown below:

- 10.x.x.x
- 172.16.x.x - 172.31.x.x
- 192.168.x.x

Other reserved or commonly used addresses:

- 127.0.0.1 - The loopback interface address. All 127.x.x.x addresses are used by the loopback interface which copies data from the transmit buffer to the receive buffer of the NIC when used.
- 0.0.0.0 - This is reserved for hosts that don't know their address and use BOOTP or DHCP protocols to determine their addresses.
- 255 - The value of 255 is never used as an address for any part of the IP address. It is reserved for broadcast addressing. Please remember, this is exclusive of CIDR. When using CIDR, all bits of the address can never be all ones.

To further illustrate, a few examples of valid and invalid addresses are listed below:

1. Valid addresses:
   - 10.1.0.1 through 10.1.0.254
   - 10.0.0.1 through 10.0.0.254
   - 10.0.1.1 through 10.0.1.254
2. Invalid addresses:
   - 10.1.0.0 - Host IP can't be 0.
   - 10.1.0.255 - Host IP can't be 255.
   - 10.123.255.4 - No network or subnet can have a value of 255.
   - 0.12.16.89 - No Class A network can have an address of 0.
   - 255.9.56.45 - No network address can be 255.
   - 10.34.255.1 - No network address can be 255.

Network/Netmask specification

Sometimes you may see a network interface card (NIC) IP address specified in the following manner:

> 192.168.1.1/24

The first part indicates the IP address of the NIC which is "192.168.1.1" in this case. The second part "/24" indicates the netmask value meaning in this case that the first 24 bits of the netmask are set. This makes the netmask value 255.255.255.0. If the last part of the line above were "/16", the netmask would be 255.255.0.0.

Subnet masks

Subnetting is the process of breaking down a main class A, B, or C network into subnets for routing purposes. A subnet mask is the same basic thing as a netmask with the only real difference being that you are breaking a larger organizational network into smaller parts, and each smaller section will use a different set of address numbers. This will allow network packets to be routed between subnetworks. When doing subnetting, the number of bits in the subnet mask determine the number of available subnets. Two to the power of the number of bits minus two is the number of available subnets. When setting up subnets the following must be determined:

- Number of segments
- Hosts per segment

Subnetting provides the following advantages:

- Network traffic isolation - There is less network traffic on each subnet.
- Simplified Administration - Networks may be managed independently.
- Improved security - Subnets can isolate internal networks so they are not visible from external networks.

A 14 bit subnet mask on a class B network only allows 2 node addresses for WAN links. A routing algorithm like OSPF or EIGRP must be used for this approach. These protocols allow the variable length subnet masks (VLSM). RIP and IGRP don't support this. Subnet mask information must be transmitted on the update packets for dynamic routing protocols for this to work. The router subnet mask is different than the WAN interface subnet mask.

One network ID is required by each of:

- Subnet

- WAN connection

One host ID is required by each of:

- Each NIC on each host.
- Each router interface.

Types of subnet masks:

- Default - Fits into a Class A, B, or C network category
- Custom - Used to break a default network such as a Class A, B, or C network into subnets.

IPv6

IPv6 is 128 bits. It has eight octet pairs, each with 16 bits and written in hexadecimal as follows:

> 2b63:1478:1ac5:37ef:4e8c:75df:14cd:93f2

Extension headers can be added to IPv6 for new features.

Supernetting

Supernetting is used to help make up for some of the shortage if IP addresses for the internet. It uses Classless Inter-Domain Routing (CIDR). If a business needs a specific number of IP addresses such as 1500, rather than allocating a class B set of addresses with the subnet mask of 255.255.0.0, a subnet mask of 255.255.248.0 may be allocated. Therefore the equivalent of eight class C addresses have been allocated. With supernetting, the value of 2 is not subtracted from the possible number of subnets since the router knows that these are contiguous networks. 8 times 254 = 2032.

What section of this document to read next

At this point the reader should have enough fundamental knowledge to grasp routing, so the reader may continue on or skip to the section entitled, "simple routing". The reader may at this time read all the sections in the "Functions" group of sections, then continue back at the section after this one where you left off.

Internet Protocol

Internet Protocol (IP) provides support at the network layer of the OSI model. All transport protocol data packets such as UDP or TCP are encapsulated in IP data packets to be carried from one host to another. IP is a connection-less unreliable service meaning there is no guarantee that the data will reach the intended host. The datagrams may be damaged upon arrival, out of order, or not arrive at all (Sounds like some mail services, doesn't it?). Therefore the layers above IP such as TCP are responsible for being sure correct data is delivered. IP provides for:

- Addressing.
- Type of service specification.
- Fragmentation and re-assembly.
- Security.

IP Message Format

IP is defined by RFC 791.

1. Version (4 bits) - The IP protocol version, currently 4 or 6.
2. Header length (4 bits) - The number of 32 bit words in the header
3. Type of service (TOS) (8 bits) - Only 4 bits are used which are minimize delay, maximize throughput, maximize reliability, and minimize monetary cost. Only one of these bits can be on. If all bits are off, the service is normal. Some networks allow a set precedences to control priority of messages the bits are as follows:
    - Bits 0-2 - Precedence.
        - 111 - Network Control
        - 110 - Internetwork Control
        - 101 - CRITIC/ECP
        - 100 - Flash Override
        - 011 - Flash
        - 010 - Immediate
        - 001 - Priority
        - 000 - Routine
    - Bit 3 - A value of 0 means normal delay. A value of 1 means low delay.
    - Bit 4 - Sets throughput. A value of 0 means normal and a 1 means high throughput.
    - Bit 5 - A value of 0 means normal reliability and a 1 means high reliability.
    - Bit 6-7 are reserved for future use.
4. Total length of the IP data message in bytes (16 bits)
5. Identification (16 bits) - Uniquely identifies each datagram. This is used to re-assemble the datagram. Each fragment of the datagram contains this same unique number.
6. flags (3 bits) - One bit is the more fragments bit

   1. Bit 0 - reserved.
   2. Bit 1 - The fragment bit. A value of 0 means the packet may be fragmented while a 1 means it cannot be fragmented. If this value is set and the packet needs further fragmentation, an ICMP error message is generated.
   3. Bit 2 - This value is set on all fragments except the last one since a value of 0 means this is the last fragment.
7. Fragment offset (13 bits) - The offset in 8 byte units of this fragment from the beginning of the original datagram.
8. Time to live (TTL) (8 bits) - Limits the number of routers the datagram can pass through. Usually set to 32 or 64. Every time the datagram passes through a router this value is decremented by a value of one or more. This is to keep the datagram from circulating in an infinite loop forever.
9. Protocol (8 bits) - It identifies which protocol is encapsulated in the next data area. This is may be one or more of TCP(6), UDP(17), ICMP(1), IGMP(2), or OSPF(89). A list of these protocols and their associated numbers may be found in the /etc/protocols file on Unix or Linux systems.
10. Header checksum (16 bits) - For the IP header, not including the options and data.
11. Source IP address (32 bits) - The IP address of the card sending the data.
12. Destination IP address (32 bits) - The IP address of the network card the data is intended for.
13. Options - Options are:
    - Security and handling restrictions
    - Record route - Each router records its IP address
    - Time stamp - Each router records its IP address and time
    - Loose source routing - Specifies a set of IP addresses the datagram must go through.
    - Strict source routing - The datagram can go through only the IP addresses specified.
14. Data - Encapsulated hardware data such as ethernet data.

The message order of bits transmitted is 0-7, then 8-15, in network byte order. Fragmentation is handled at the IP network layer and the messages are reassembled when they reach their final destination. If one fragment of a datagram is lost, the entire datagram must be retransmitted. This is why fragmentation is avoided by TCP. The data on the last line, item 14, is ethernet data, or data depending on the type of physical network.

Transmission Control Protocol

Transmission Control Protocol (TCP) supports the network at the transport layer. Transmission Control Protocol (TCP) provides a reliable connection oriented service. Connection oriented means both the client and server must open the connection before data is sent. TCP is defined by RFC 793 and 1122. TCP provides:

- End to end reliability.
- Data packet re sequencing.
- Flow control.

TCP relies on the IP service at the network layer to deliver data to the host. Since IP is not reliable with regard to message quality or delivery, TCP must make provisions to be sure messages are delivered on time and correctly (Federal Express?).

TCP Message Format

The format of the TCP header is as follows:

1. Source port number (16 bits)
2. Destination port number (16 bits)
3. Sequence number (32 bits) - The byte in the data stream that the first byte of this packet represents.
4. Acknowledgement number (32 bits) - Contains the next sequence number that the sender of the acknowledgement expects to receive which is the sequence number plus 1 (plus the number of bytes received in the last message?). This number is used only if the ACK flag is on.
5. Header length (4 bits) - The length of the header in 32 bit words, required since the options field is variable in length.
6. Reserved (6 bits)
7. URG (1 bit) - The urgent pointer is valid.
8. ACK (1 bit) - Makes the acknowledgement number valid.
9. PSH (1 bit) - High priority data for the application.
10. RST (1 bit) - Reset the connection.
11. SYN (1 bit) - Turned on when a connection is being established and the sequence number field will contain the initial sequence number chosen by this host for this connection.
12. FIN (1 bit) - The sender is done sending data.
13. Window size (16 bits) - The maximum number of bytes that the receiver will to accept.
14. TCP checksum (16 bits) - Calculated over the TCP header, data, and TCP pseudo header.
15. Urgent pointer (16 bits) - It is only valid if the URG bit is set. The urgent mode is a way to transmit emergency data to the other side of the connection. It must be added to the sequence number field of the segment to generate the sequence number of the last byte of urgent data.

16. Options (variable length)

The header is followed by data. TCP data is full duplex.

User Datagram Protocol

User Datagram Protocol (UDP) supports the network at the transport layer. User Datagram Protocol (UDP) is an unreliable connection-less protocol and is defined by RFC 768 and 1122. It is a datagram service. There is no guarantee that the data will reach its destination. UDP is meant to provide serivce with very little transmission overhead. It adds very little to IP datapackets except for some error checking and port direction (Remember, UDP encapsulates IP packets). The following protocols or services use UDP:

- DNS
- SNMP
- BOOTP
- TFTP
- NFS
- RPC
- RIP

UDP Message Format

The UDP header includes:

1. Source port number (16 bits) - An optional field
2. Destination port number (16 bits)
3. UDP length (16 bits)
4. UDP checksum (16 bits)

This is followed by data. The UDP checksum includes UDP data, not just the header as with IP message formats. For UDP and TCP checksum calculation a 12 byte pseudo header is included which contains some fields form the IP message header. This header is not transmitted as part of UDP or TCP, but is only used to help compute the checksum as a means of being sure that the data has arrived at the correct IP address. This is the TCP/UDP pseudo header:

1. Source IP address (32 bits)
2. Destination IP address (32 bits)
3. blank filler(0) (8 bits)
4. Protocol (8 bits)
5. UDP length (16 bits)

Internet Control Message Protocol

Internet Control Message Protocol (ICMP) defined by RFC 792 and RFC 1122 is used for network error reporting and generating messages that require attention. The errors reported by ICMP are generally related to datagram processing. ICMP only reports errors involving fragment 0 of any fragmented datagrams. The IP, UDP or TCP layer will usually take action based on ICMP messages. ICMP generally belongs to the IP layer of TCP/IP but relies on IP for support at the network layer. ICMP messages are encapsulated inside IP datagrams.

ICMP will report the following network information:

- Timeouts
- Network congestion
- Network errors such as an unreachable host or network.

The ping command is also supported by ICMP, and this can be used to debug network problems.

ICMP Messages:

The ICMP message consists of an 8 bit type, an 8 bit code, an 8 bit checksum, and contents which vary depending on code and type. The below table is a list of ICMP messages showing the type and code of the messages and their meanings.

Type	Codes	Description	Purpose
0	0	Echo reply	Query
3	0	Network Unreachable	Error
3	1	Host Unreachable	Error
3	2	Protocol Unreachable	Error
3	3	Protocol Unreachable	Error
3	4	Fragmentation needed with don't fragment bit set	Error
3	5	Source route failed	Error
3	6	Destination network unknown	Error
3	7	Destination host unknown	Error
3	8	Source host isolated	Error
3	9	Destination network administratively prohibited	Error
3	10	Destination host administratively prohibited	Error
3	11	Network Unreachable for TOS	Error

3	12	Host Unreachable for TOS	Error
3	13	Communication administratively prohibited by filtering	Error
3	14	Host precedence violation	Error
3	15	Precedence cutoff in effect	Error
4	0	Source quench	Error
5	0	Redirect for network	Error
5	1	Redirect for host	Error
5	2	Redirect for type of service and network	Error
5	3	Redirect for type of service and host	Error
8	0	Echo request	Query
9	0	Normal router advertisement	Query
9	16	Router does not route common traffic	Query
10	0	Router Solicitation	Query
11	0	Time to live is zero during transit	Error
11	1	Time to live is zero during reassembly	Error
12	0	IP header bad	Error
12	1	Required option missing	Error
12	2	Bad length	Error
13	0	Timestamp request	Query
14	0	Timestamp reply	Query
15	0	Information request	Query
16	0	Information reply	Query
17	0	Address mask request	Query
18	0	Address mask request	Query

ICMP is used for many different functions, the most important of which is error reporting. Some of these are "port unreachable", "host unreachable", "network unreachable", "destination network unknown", and "destination host unknown". Some not related to errors are:

- Timestamp request and reply allows one system to ask another one for the current time.
- Address mask and reply is used by a diskless workstation to get its subnet mask at boot time.
- Echo request and echo reply is used by the ping program to test to see if another unit will respond.

Network Cabling

This section may be skipped by those more interested on the software aspects of networking or those learning networking, but all readers should at some time be aware of the terminology used in this section since they are used with regard to cabling. If this section is skipped by those learning networking, it should be read later. This section should be read by those who plan to physically install their own network.

Types of Transmission

1. Baseband - Data bits are defined by discrete signal changes.
2. Broadband - Uses analog signals to divide the cable into several channels with each channel at its own frequency. Each channel can only transmit one direction.

Physical media

1. Twisted pair - Wire is twisted to minimize crosstalk interference. It may be shielded or unshielded.
    - UTP-Unshielded Twisted Pair. Normally UTP contains 8 wires or 4 pair. 100 meter maximum length. 4-100 Mbps speed.
    - STP-Shielded twisted pair. 100 meter maximum length. 16-155 Mbps speed. Lower electrical interference than UTP.
2. Coaxial - Two conductors separated by insulation such as TV 75 ohm cable. Maximum length of 185 to 500 meters.
    1. Thinnet - Thinnet uses a British Naval Connector (BNC) on each end. Thinnet is part of the RG-58 family of cable*. Maximum cable length is 185 meters. Transmission speed is 10Mbps. Thinnet cable should have 50 ohms impedance and its terminator has 50 ohms impedance. A T or barrel connector has no impedance.
    2. Thicknet - Half inch rigid cable. Maximum cable length is 500 meters. Transmission speed is 10Mbps. Expensive and is not commonly used. (RG-11 or RG-8). A vampire tap or piercing tap is used with a transceiver attached to connect computers to the cable. 100 connections may be made. The computer has an attachment unit interface (AUI) on its network card which is a 15 pin DB-15 connector. The computer is connected to the transceiver at the cable from its AUI on its network card using a drop cable.

    Coax cable types:
    - RG-58 /U - 50 ohm, with a solid copper wire core.
    - RG-58 A/U* - 50 ohm, with a stranded wire core.
    - RG-58 C/U* - Military version of RG-58 A/U.
    - RG-59 - 75 ohm, for broadband transmission such as cable TV.
    - RG-62 - 93 ohm, primarily used for ArcNet.
    - RG-6 - Used for satellite cable (if you want to run a cable to a satellite!).

*Only these are part of the IEEE specification for ethernet networks.

3. Fiber-optic - Data is transmitted using light rather than electrons. Usually there are two fibers, one for each direction. Cable length of 2 Kilometers. Speed from 100Mbps to 2Gbps. This is the most expensive and most difficult to install, but is not subject to interference. Two types of cables are:
    1. Single mode cables for use with lasers.
    2. Multimode cables for use with Light Emitting Diode (LED) drivers.

Cable Standards

The Electronic Industries Association and Telecommunications Industries Association (EIA/TIA) defined a standard called EIA/TIA 568 which is a commercial building wiring standard for UTP cable. It defines transmission speed and twists per foot.

Category	Speed	Notes
1	None	Used for old telephone systems
2	4Mps	
3	10Mps	The minimum category for data networks
4	16Mps	
5	100Mps	Cat 5 network cable, used by most networks today
6		Data patch, Two pair with foil and braided shield
7		Undefined
8		Flat cable for under carpets with two twisted pair
9		Plenum cable with two twisted pair. It is safe if you're having a fire.

The maximum transmission length is 100 meters. This cable is susceptible to interference.

STP

Shielded twisted pair has a maximum cable length of 100 meters (328 feet). Data rate from 16 to 155 Mbps. Cables require special connectors for grounding but this cabling method resists electrical interference and is less susceptible to eavesdropping. Costs more than UTP or Thinnet, but not as much as Thicknet or Fiber-optic.

Terms

- Attenuation - Signal loss due to impedance.
- Bandwidth - Indicates the amount of data that can be sent in a time period. Measured in Mbps which is one million bits per second.
- Impedance - The amount of resistance to the transmission device.

- Interference - Electromagnetic Interference (EMI). Crosstalk - When wires pick up electromagnetic signals from nearby wires also carrying signals.
- Plenum - Space above a false ceiling in an office area where heat ducts and cables may be run. Plenum cabling is special fire resistant cabling required for use in these areas due to fire hazards.
- Shielding - Used to minimize interference.

Wireless Networking

This section may be skipped by all readers and used by those interested in wireless network technology. Transmission of waves take place in the electromagnetic (EM) spectrum. The carrier frequency of the data is expressed in cycles per second called hertz(Hz). Low frequency signals can travel for long distances through many obstacles but can not carry a high bandwidth of data. High frequency signals can travel for shorter distances through few obstacles and carry a narrow bandwidth. Also the effect of noise on the signal is inversely proportional to the power of the radio transmitter, which is normal for all FM transmissions. The three broad categories of wireless media are:

1. Radio - 10 Khz to 1 Ghz. It is broken into many bands including AM, FM, and VHF bands. The Federal communications Commission (FCC) regulates the assignment of these frequencies. Frequencies for unregulated use are:
   - 902-928Mhz - Cordless phones, remote controls.
   - 2.4 Ghz
   - 5.72-5.85 Ghz
2. Microwave
   - Terrestrial - Used to link networks over long distances but the two microwave towers must have a line of sight between them. The frequency is usually 4-6GHz or 21-23GHz. Speed is often 1-10Mbps. The signal is normally encrypted for privacy.
   - Satellite - A satellite orbits at 22,300 miles above the earth which is an altitude that will cause it to stay in a fixed position relative to the rotation of the earth. This is called a geosynchronous orbit. A station on the ground will send and receive signals from the satellite. The signal can have propagation delays between 0.5 and 5 seconds due to the distances involved. The transmission frequency is normally 11-14GHz with a transmission speed in the range of 1-10Mbps.
3. Infared - Infared is just below the visible range of light between 100Ghz and 1000Thz. A light emitting diode (LED) or laser is used to transmit the signal. The signal cannot travel through objects. Light may interfere with the signal. The types of infared are
   - Point to point - Transmission frequencies are 100GHz-1,000THz . Transmission is between two points and is limited to line of sight range. It is difficult to eavesdrop on the transmission.
   - broadcast - The signal is dispersed so several units may receive the signal. The unit used to disperse the signal may be reflective material or a transmitter that amplifies and retransmits the signal. Normally the speed is limited to 1Mbps. The transmission frequency is normally 100GHz-1,000THz with transmission distance in 10's of meters. Installation is easy and cost is relatively inexpensive for wireless.

Terms:

- AMPS - Advanced Mobile Phone Service is analog cellular phone service.

- CDMA - Code division multiple access allows transmission of voice and data over a shared part of radio frequencies. This is also called spread spectrum.
- CDPD - Cellular Digital Packet Data will allow network connections for mobile users using satellites.
- cellular - An 800 Mhz band for mobile phone service.
- D-AMPS - Digital AMPS using TDMA to divide the channels into three channels.
- FDMA - Frequency Division Multiple Access divides the cellular network into 30Khz channels.
- GSM - Global System for Mobile Communications.
- HDML - Handheld Device Markup Language is a version of HTML only allowing text to be displayed.
- MDBS - Mobile Data Base Station reviews all cellular channels at cellular sites.
- PCS - Personal communications Service is a 1.9 Ghz band.
- TDMA - Time Division Multiple Access uses time division multiplexing to divide each cellular channel into three sub channels to service three users at a time.
- wireless bridge - Microwave or infared is used between two line of site points where it is difficult to run wire.
- WML - Wireless markup language is another name for HDML.

Categories of LAN Radio Communications

- Low power, single frequency - Distance in 10s of meters. Speed in 1-10Mbps. Susceptible to interference and eavesdropping.
- High power, single frequency - Require FCC licensing and high power transmitter. Speed in 1-10Mbps. Susceptible to interference and eavesdropping.
- Spread spectrum - It uses several frequencies at the same time. The frequency is normally 902-928MHz with some networks at 2.4GHz. The speed of 902MHz systems is between 2 and 6Mbps. If frequency-hopping is used, the speed is normally lower than 2Mbps. Two types are:
  1. Direct sequence modulation - The data is broken into parts and transmitted simultaneously on multiple frequencies. Decoy data may be transmitted for better security. The speed is normally 2 to 6 Mbps.
  2. Frequency hopping - The transmitter and receiver change predetermined frequencies at the same time (in a synchronized manner). The speed is normally 1Gbps.

Network WAN Connections

Three options for connecting over a telephone service:

- Dial-up connections.
- Integrated Services Digital Network(ISDN) - A method of sending voice and data information on a digital phone line.
    - Basic ISDN - Two 64Kbps B-channels with one 16Kbps D channel is provided. The D-channel is used for call control and setup. Basic ISDN can provide 128Kbps speed capability.
    - Primary ISDN - 23 B-channels and one D channel is provided.
- Leased Lines - This involves the leasing of a permanent telephone line between two locations.

Remote Communication Protocols

- Serial Line Internet Protocol (SLIP) - Allows computers to connect to the internet with a modem. No error checking or data compression is supported. Only the TCP/IP protocols are supported.
- Point to Point Protocol (PPP) - Provides error checking and data compression. Also supports multiple network protocols such IPX/SPX and NetBEUI in addition to TCP/IP. Supports dynamic allocation of IP addresses.

Remote Access Service

Remote Access Service (RAS) with Windows NT allows users connecting to the network using a modem to use network resources. RAS may be called dial up networking (DUN) depending on the version of Windows you are using. The NT RAS server can handle 256 connections. Windows NT RAS servers provide the following security features:

1. User account security
2. Encryption between the DUN (dial up networking) client and the server
3. Callback capability

The client software is called Dial up networking (DUN) in windows NT4 and Windows95. For NT 3.51 and Windows 3.1 it is called a RAS client. These clients may be used to connect to the internet through an internet service provider (ISP).

Ethernet

The IEEE 802.3 standard defines ethernet at the physical and data link layers of the OSI network model. Most ethernet systems use the following:

- Carrier-sense multiple-access with collision detection (CSMA/CD) for controlling access to the network media.
- Use baseband broadcasts
- A method for packing data into data packets called frames
- Transmit at 10Mbps, 100Mbps, and 1Gbps.

Types of Ethernet

- 10Base5 - Uses Thicknet coaxial cable which requires a transceiver with a vampire tap to connect each computer. There is a drop cable from the transceiver to the Attachment Unit Interface (AIU). The AIU may be a DIX port on the network card. There is a transceiver for each network card on the network. This type of ethernet is subject to the 5-4-3 rule meaning there can be 5 network segments with 4 repeaters, and three of the segments can be connected to computers. It uses bus topology. Maximum segment length is 500 Meters with the maximum overall length at 2500 meters. Minimum length between nodes is 2.5 meters. Maximum nodes per segment is 100.
- 10Base2 - Uses Thinnet coaxial cable. Uses a BNC connector and bus topology requiring a terminator at each end of the cable. The cable used is RG-58A/U or RG-58C/U with an impedance of 50 ohms. RG-58U is not acceptable. Uses the 5-4-3 rule meaning there can be 5 network segments with 4 repeaters, and three of the segments can be connected to computers. The maximum length of one segment is 185 meters. Barrel connectors can be used to link smaller pieces of cable on each segment, but each barrel connector reduces signal quality. Minimum length between nodes is 0.5 meters.
- 10BaseT - Uses Unshielded twisted pair (UTP) cable. Uses star topology. Shielded twisted pair (STP) is not part of the 10BaseT specification. Not subject to the 5-4-3 rule. They can use category 3, 4, or 5 cable, but perform best with category 5 cable. Category 3 is the minimum. Require only 2 pairs of wire. Cables in ceilings and walls must be plenum rated. Maximum segment length is 100 meters. Minimum length between nodes is 2.5 meters. Maximum number of connected segments is 1024. Maximum number of nodes per segment is 1 (star topology). Uses RJ-45 connectors.
- 10BaseF - Uses Fiber Optic cable. Can have up to 1024 network nodes. Maximum segment length is 2000 meters. Uses specialized connectors for fiber optic. Includes three categories:
  - 10BaseFL - Used to link computers in a LAN environment, which is not commonly done due to high cost.
  - 10BaseFP - Used to link computers with passive hubs to get cable distances up to 500 meters.
  - 10BaseFB - Used as a backbone between hubs.
- 100BaseT - Also known as fast ethernet. Uses RJ-45 connectors. Topology is star. Uses CSMA/CD media access. Minimum length between nodes is 2.5 meters. Maximum number of connected segments is 1024. Maximum number of nodes per segment is 1 (star topology). IEEE802.3 specification.
  - 100BaseTX - Requires category 5 two pair cable. Maximum distance is 100 meters.
  - 100BaseT4 - Requires category 3 cable with 4 pair. Maximum distance is 100 meters.
  - 100BaseFX - Can use fiber optic to transmit up to 2000 meters. Requires two strands of fiber optic cable.

- 100VG-AnyLAN - Requires category 3 cable with 4 pair. Maximum distance is 100 meters with cat 3 or 4 cable. Can reach 150 meters with cat 5 cable. Can use fiber optic to transmit up to 2000 meters. This ethernet type supports transmission of Token-Ring network packets in addition to ethernet packets. IEEE 802.12 specification. Uses demand-priority media access control. The topology is star. It uses a series of interlinked cascading hubs. Uses RJ-45 connectors.

The IEEE naming convention is as follows:

1. The transmission speed in Mbps
2. Baseband (base) or Broadband data transmission
3. The maximum distance a network segment could cover in hundreds of meters.

Comparisons of some ethernet types. distances are in meters.

Ethernet Type	Cable	Min length between nodes	Max Segment length	Max overall length
10Base2	Thinnet	0.5	185	925
10Base5	Thicknet	2.5	500	2500
10BaseF	Fiber		2000	
10BaseT	UTP	2.5	100	

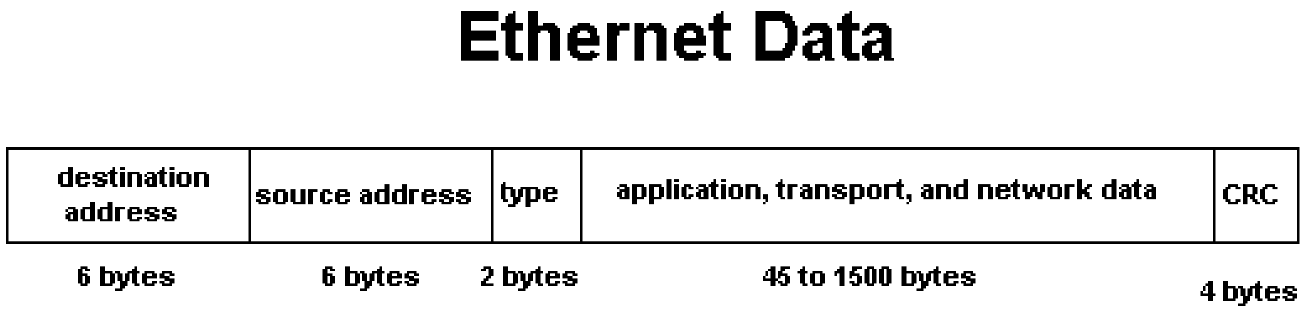
Types of ethernet frames

- Ethernet 802.2 - These frames contain fields similar to the ethernet 802.3 frames with the addition of three Logical Link Control (LLC) fields. Novell NetWare 4.x networks use it.
- Ethernet 802.3 - It is mainly used in Novell NetWare 2.x and 3.x networks. The frame type was developed prior to completion of the IEEE 802.3 specification and may not work in all ethernet environments.
- Ethernet II - This frame type combines the 802.3 preamble and SFD fields and include a protocol type field where the 802.3 frame contained a length field. TCP/IP networks and networks that use multiple protocols normally use this type of frames.
- Ethernet SNAP - This frame type builds on the 802.2 frame type by adding a type field indicating what network protocol is being used to send data. This frame type is mainly used in AppleTalk networks.

The packet size of all the above frame types is between 64 and 1,518 bytes.

Ethernet Message Formats

The ethernet data format is defined by RFC 894 and 1042. The addresses specified in the ethernet protocol are 48 bit addresses.



The types of data passed in the type field are as follows:

1. 0800 IP Datagram
2. 0806 ARP request/reply
3. 8035 RARP request/reply

There is a maximum size of each data packet for the ethernet protocol. This size is called the maximum transmission unit **(MTU)**. What this means is that sometimes packets may be broken up as they are passed through networks with MTUs of various sizes. SLIP and PPP protocols will normally have a smaller MTU value than ethernet. This document does not describe serial line interface protocol (SLIP) or point to point protocol (PPP) encapsulation.

Token Ring

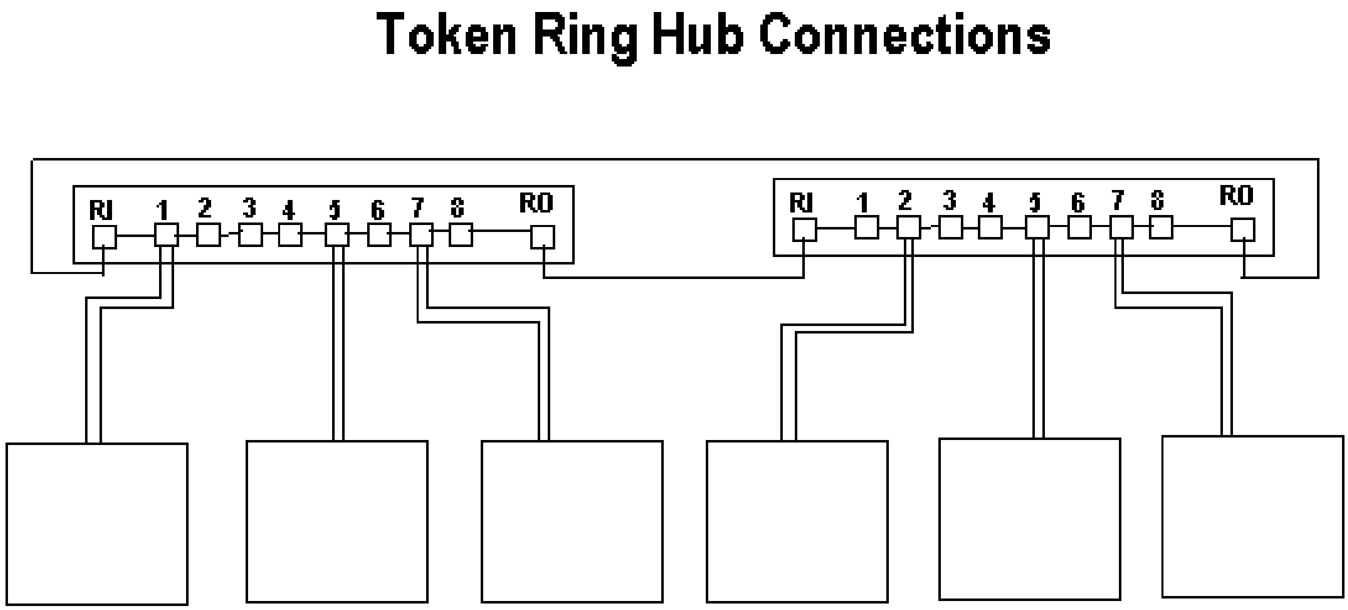
Developed by IBM is standardized to IEEE 802.5. It uses a star topology, but it is wired so the signal will travel from hub to hub in a logical ring. These networks use a data token passed from computer to computer around the ring to allow each computer to have network access. The token comes from the nearest active upstream neighbor (NAUN). When a computer receives a token, if it has no attached data and the computer has data for transmission, it attaches its data to the token then sends it to its nearest active downstream neighbor (NADN). Each computer downstream will pass the data on since the token is being used until the data reaches its recipient. The recipient will set two bits to indicate it received the data and transmit the token and data. When the computer that sent the data receives the package, it can verify that the data was received correctly. It will remove the data from the token and pass the token to its NADN.

Characteristics

Maximum cable length is 45 meters when UTP cable is used and 101 meters when STP is used. Topology is star-wired ring. It uses type 1 STP and type 3 UTP. Connectors are RJ-45 or IBM type A. Minimum length between nodes is 2.5 meters. Maximum number of hubs or segments is 33. Maximum nodes per network is 72 nodes with UTP and 260 nodes with STP. Speed is 4 or 16 Mps. Data frames may be 4,000 to 17,800 bytes long.

Hubs

A token ring network uses a **multistation access unit (MAU)** as a hub. It may also be known as a Smart Multistation Access Unit (SMAU). A MAU normally has ten ports. Two ports are Ring In (RI) and Ring Out (RO) which allow multiple MAUs to be linked to each other. The other 8 ports are used to connect to computers.



Cables

UTP or STP cabling is used as a media for token ring networks. Token Ring uses an IBM cabling system based on American Wire Gauge (AWG) standards that specify wire diameters. The larger the AWG number, the small diameter the cable has.

Token ring networks normally use type 1, type 3 or regular UTP like cable used on ethernet installations. If electrical interference is a problem, the type 1 cable is a better choice. Cable types:

Type	Description
1	Two 22 AWG solid core pair of STP cable with a braided shield. This cable is normally used between MAUs and computers.
2	Two 22 AWG solid core pair with four 26 AWG solid core of STP cable.
3	Four 22 or 24 AWG UTP cable. This is voice-grade cable and cannot transmit at a rate above 4Mbps.
4	Undefined.

5	Fiber-optic cable. Usually used to link MAUs.
6	Two 26 AWG stranded core pair of STP cable with a braided shield. The stranded-core allows more flexibility but limits the transmission distance to two-thirds that of type 1.
7	Undefined.
8	Type 6 cable with a flat casing to be used under carpets.
9	Type 6 cable with plenum-rating for safety.

Beaconing

The first computer turned on on a token ring will be the active monitor. Every seven seconds it sends a frame to its nearest active downstream neighbor. The data gives the address of the active monitor and advertised the fact that the upstream neighbor is the active monitor. That station changes the packets upstream address and sends it to its nearest active downstream neighbor. When the packet has traveled around the ring, all stations know the address of their upstream neighbor and the active monitor knows the state of the network. If a computer has not heard from its upstream neighbor after seven seconds, it will send a packet that announces its own address, and the NAUN that is not responding. This packet will cause all computers to check their configuration. The ring can thereby route around the problem area giving some fault tolerance to the network.

ARCnet Network

ARCnet (Attached Resource Computer Network) (CR)

Topology is star and bus or a mixture. Cable type is RG-62 A/U coaxial (93 ohm), UTP or fiber-optic. A network can use any combination of this media. Connectors used include BNC, RJ-45, and others. It passes tokens passing for media access. Maximum segment length is 600 meters with RG-62 A/U, 121 meters with UTP, 3485 meters with fiber-optic, and 30 meters from a passive hub. The specification is ANSI 878.1. It can have up to 255 nodes per network. The speed is 2.5 Mbps. ARCnet Plus has operating speeds approaching 20Mbps.

Signals are broadcast across the entire network with computers processing only signals addressed to them. ARCnet tokens travel based on a station identifier (SID) which each computer has. Each network card has a DIP switch used to set the SID with an address between 1 and 255. Signals are generally sent from the lowest numbered station to the next until they wrap around back to SID of 1. To determine non-existent stations, the station with the lowest ID indicates it has the token and begins querying IDs of higher value until it gets a response. Then the next computer does the same until the original station is queried. This procedure is done when a station is added or removed from the network or when the network is originally started. How does the network know when a station has been added or removed? How is the lowest numbered SID identified? Addresses assignment is based on proximity, which helps the network operate more efficiently.

The acronym SID is used for a station identifier with regard to ARCnet, but as used in the Windows NT and Windows 95 operating systems, it refers to the security identification number of a user or group.

AppleTalk Network

Topology is bus. Cable type is STP. The connectors are specialized. The media access method is CSMA/CA . Maximum segment and network length is 300 meters. The maximum number of connected segments is 8. There are 32 maximum nodes per segment with 254 maximum number of nodes per network. Speed is 230.4Kbps. The cabling system used with AppleTalk is called LocalTalk.

Addressing

Addressing is dynamic with each computer, when powered on, choosing its last used address or a random address. The computer broadcasts that address to determine if the address is used. If it is used, it will broadcast another random address until it finds an unused address.

EtherTalk and TokenTalk provide for use of AppleTalk network protocols on top of ethernet and token ring architectures respectively.

LocalTalk

LocalTalk uses STP cable and bus topology. Using CSMA/CA for media access, computers will first determine if any other computers are transmitting, before they transmit. A packet is transmitted prior to transmitting that alerts other computers that a transmission will be sent. Usually LocalTalk is only used in small environments.