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

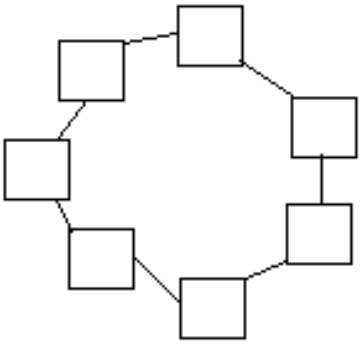
In a server based network, there are computers set up to be primary providers of services such as file service or mail service. The computers providing the service are are called servers and the computers that request and use the service are called client computers.

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.

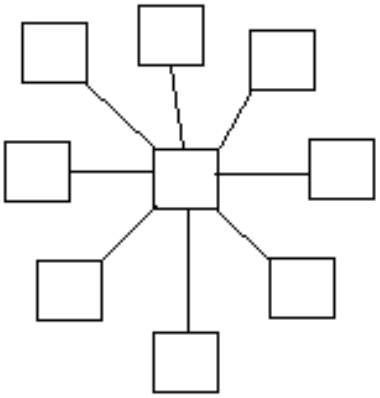
Three Network Topologies

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

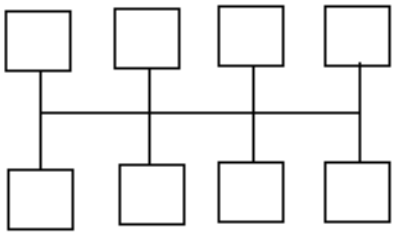
Networking Topologies



Ring



Star



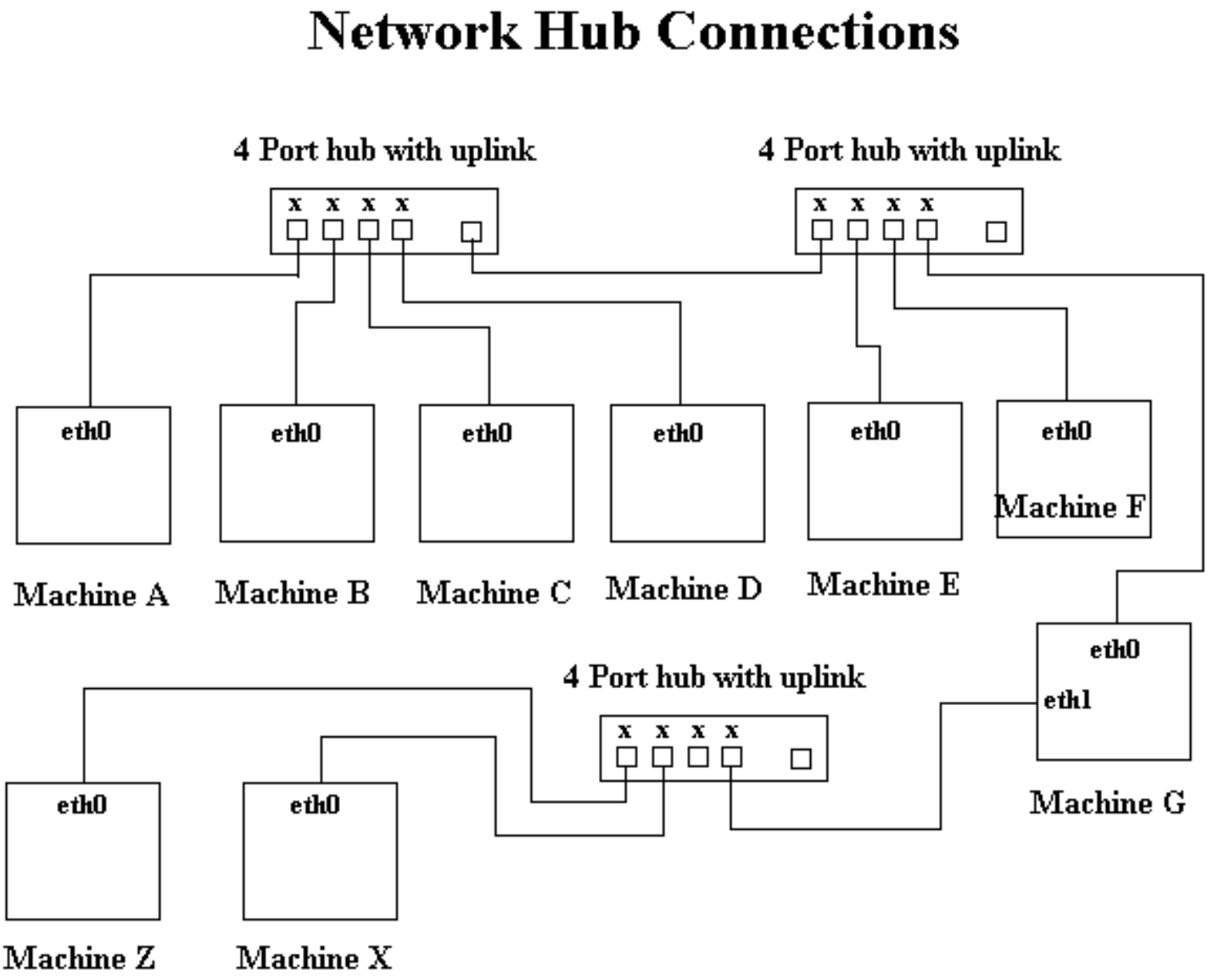
Bus

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

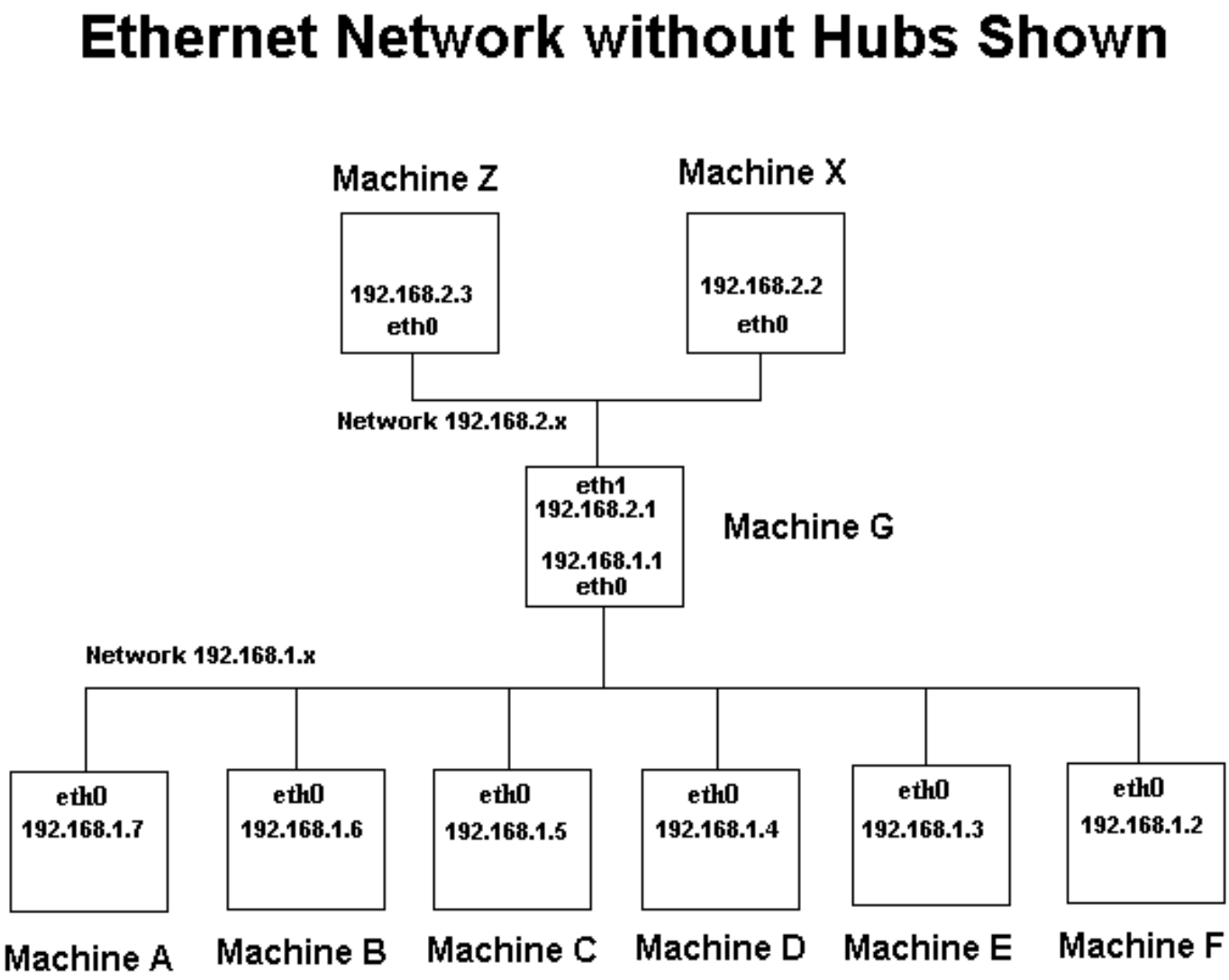
Addresses are used to locate computers. It works almost like a house address. There is a numbering system to help the mailman locate the proper house to deliver customer's mail to. Without an IP numbering system, it would not be possible to determine where network data packets should go.

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.

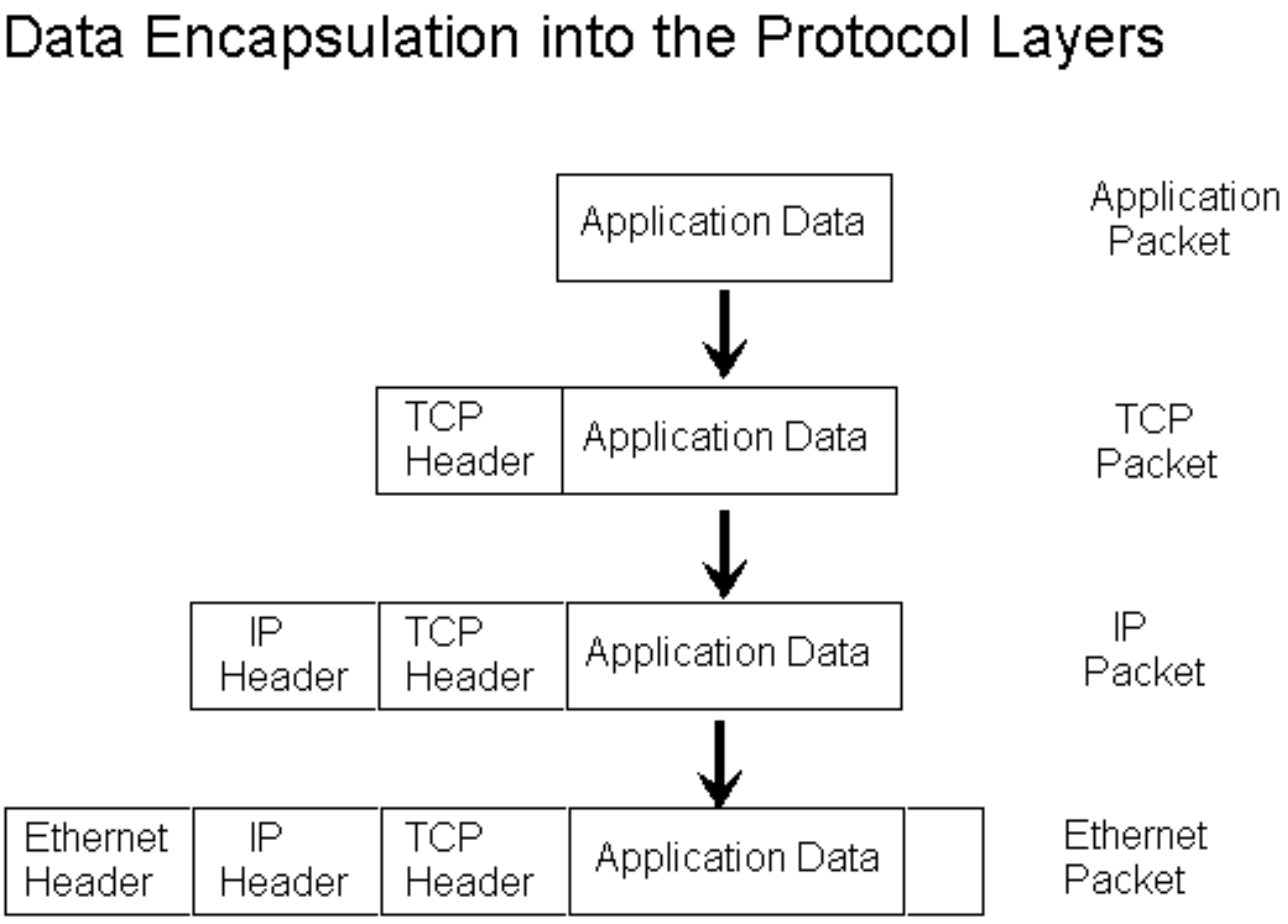
1. The Link layer corresponds to the hardware, including the device driver and interface card. The link layer has data packets associated with it depending on the type of network being used such as ARCnet, Token ring or ethernet. In our case, we will be talking about ethernet.
2. The network layer manages 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.

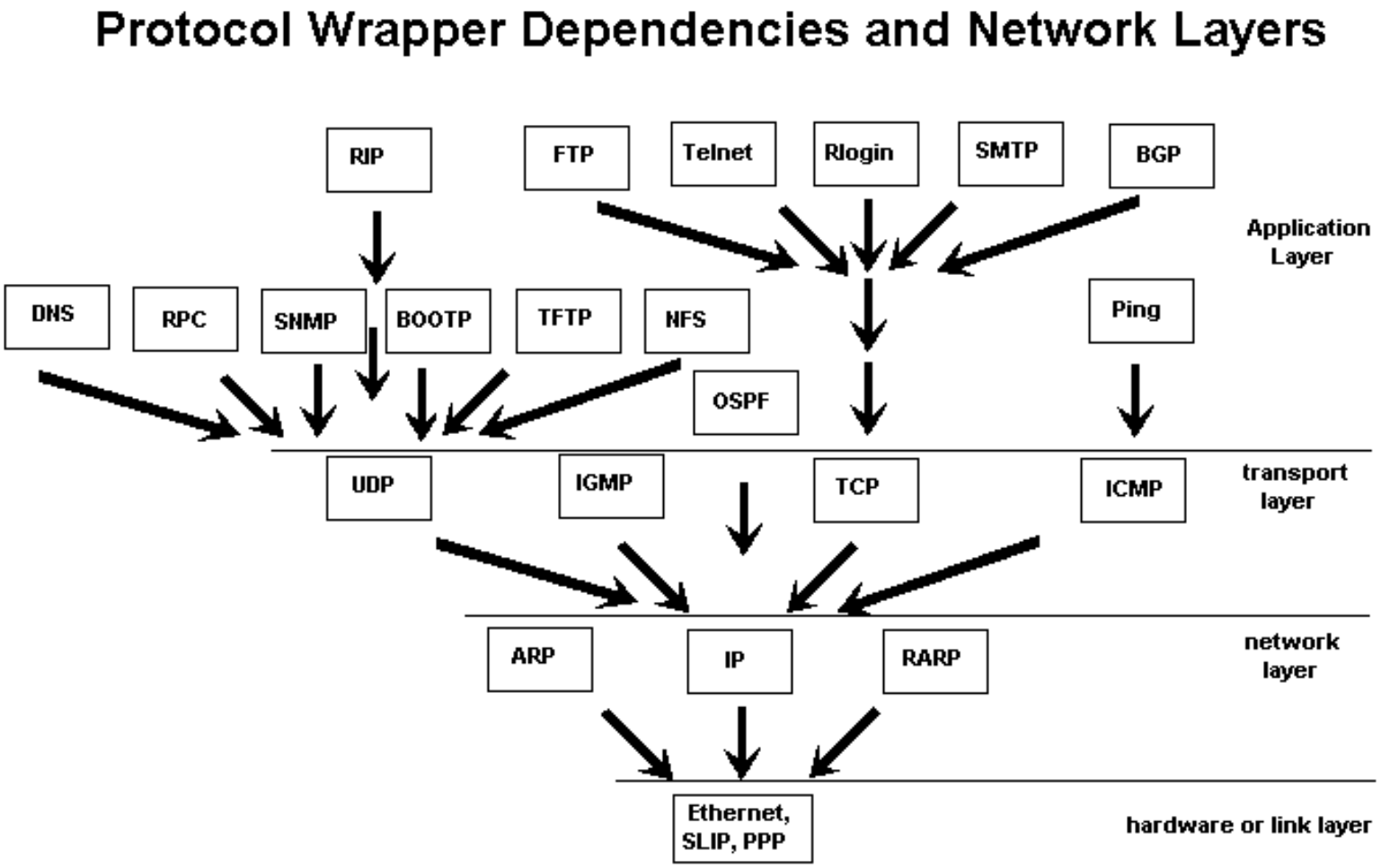
There are exceptions to my categorizations that don't fit into the normal layering scheme, such as IGMP is normally part of the link layer, but I have tried to list these categorizations according to network functions and their relative importance to the operation of the network. Also note that ethernet, 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

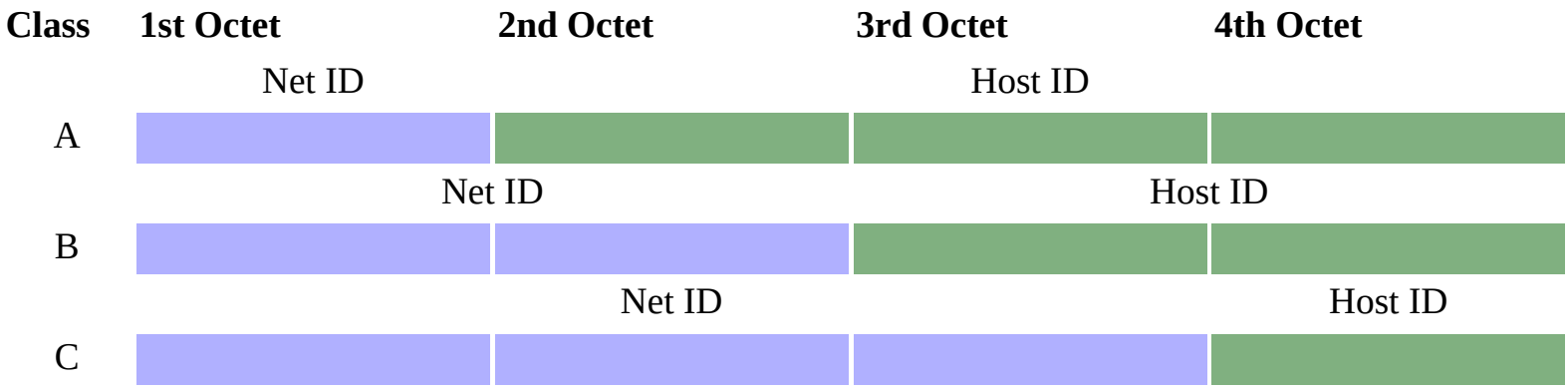
IP addresses are broken into 4 octets (IPv4) separated by dots called dotted decimal notation. An octet is a byte consisting of 8 bits. The IPv4 addresses are in the following form:

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

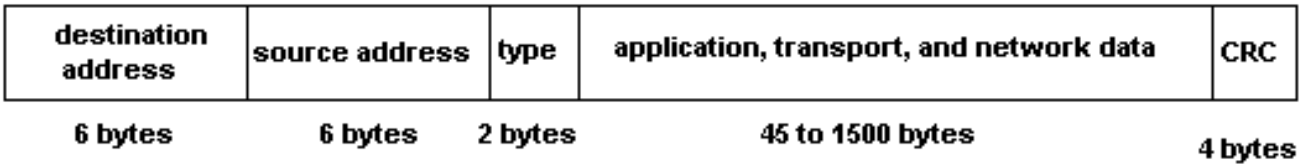
- Ethernet 802.2 - These frames contain fields similar to the ethernet 802.3 frames with the addition of three Logical Link Control (LLC) fields. Novell NetWare 4.x networks use it.
- Ethernet 802.3 - It is mainly used in Novell NetWare 2.x and 3.x networks. The frame type was developed prior to completion 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.

Ethernet Data



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

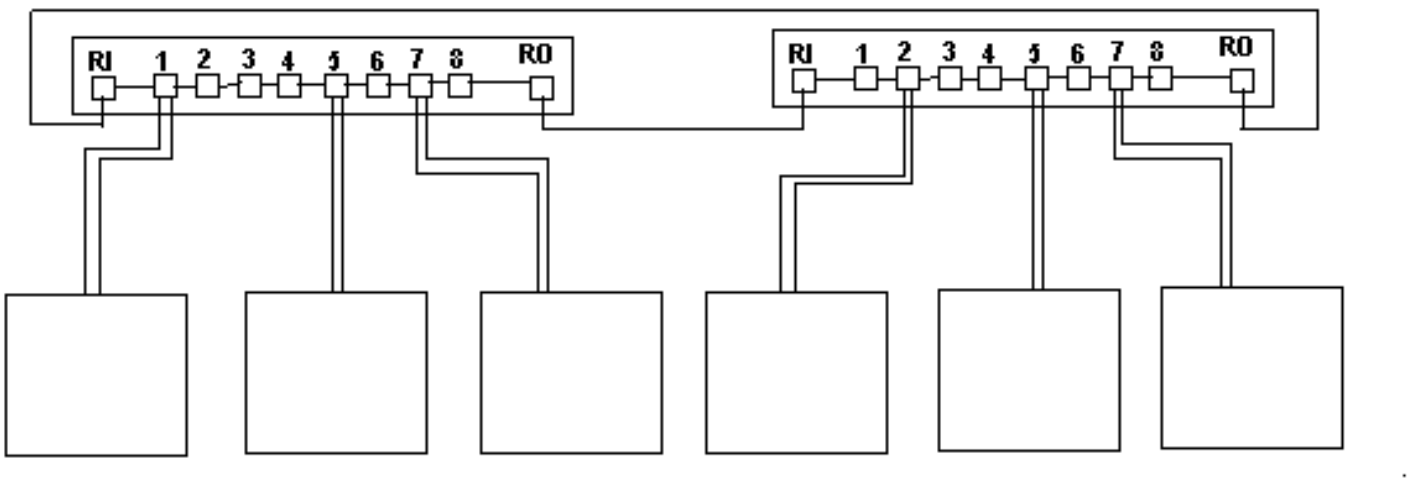
Developed by IBM is standardized to IEEE 802.5. It uses a star topology, but it is wired so the signal will travel from hub to hub in a logical ring. These networks use a data token passed from computer to computer around the ring to allow each computer to have network access. The token comes from the 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.

FDDI

Fiber Distributed Data Interface (FDDI)

Standard is ANSI X3T9.5 . Topology is **ring with two counter rotating rings for reliability** with no hubs. Cable type is fiber-optic. Connectors are specialized. The media access method is token passing. The maximum length is 100 kilometers. The maximum number of nodes on the network is 500. **Speed is 100 Mbps.** FDDI is normally used as a backbone to link other networks. **A typical FDDI network can include servers, concentrators, and links to other networks.**

Devices called concentrators provide functions similar to hubs. Most concentrators use dual attachment station network cards but single attachment concentrators may be used to attach more workstations to the network.

FDDI token passing allows multiple frames to circulate around the ring at the same time. Priority levels of a data frame and token can be set to allow servers to send more data frames. Time sensitive data may also be given higher priority. The second ring in a FDDI network is a method of adjusting when there are breaks in the cable. The primary ring is normally used, but if the nearest downstream neighbor stops responding the data is sent on the secondary ring in attempt to reach the computer. Therefore **a break in the cable will result in the secondary ring being used.** There are two network cards which are:

1. Dual attachment stations (DAS) used for servers and concentrators are attached to both rings.
2. Single Attachment stations (SAS) attached to one ring and used to attach workstations to concentrators.

A router or switch can link an FDDI network to a local area network (LAN). Normally FDDI is used to link LANs together since it covers long distances.

IPX/SPX

IPX/SPX is a routable protocol and can be used for small and large networks. The following protocols are part of the IPX/SPX suite:

- SAP - Service Advertising Protocol packets are used by file and print servers to periodically advertise the address of the server and the services available. It works at the application, presentation, and session levels.
- NCP - NetWare Core Protocol provides for client/server interactions such as file and print sharing. It works at the application, presentation, and session levels.
- SPX - Sequenced Packet Exchange operates at the transport layer providing connection oriented communication on top of IPX.
- IPX - Internetwork Packet Exchange supports the transport and network layers of the OSI network model. Provides for network addressing and routing. It provides fast, unreliable, communication with network nodes using a connection less datagram service.
- RIP - Routing Information Protocol is the default routing protocol for IPX/SPX networks which operates at the network layer. A distance-vector algorithm is used to calculate the best route for a packet.
- ODI - Open Data-link Interface operates at the data link layer allowing IPX to work with any network interface card.

NetWare frame types

Novell NetWare 2.x and 3.x use Ethernet 802.3 as their default frame type. Novell NetWare 4.x networks use Ethernet 802.2 as their default frame type. If communication does not occur between two NetWare computers it is a good idea to check the netware versions of the two computers to be sure their frame types match. If the frame types do not match on an ethernet network, the computers cannot communicate.

NetBEUI

In order to properly describe NetBEUI, the transport protocol sometimes used for Microsoft networking, it is necessary to describe Microsoft networking in some detail and the various protocols used and what network layers they support.

NetBIOS, NetBEUI, and SMB are Microsoft Protocols used to support Microsoft Networking. The NetBIOS stack includes SMB, NetBIOS, and NetBEUI which are described in the table below. The following are parts of the Microsoft networking stack:

Name	Network Layer	Description
Redirector	Application	Directs requests for network resources to the appropriate server and makes network resources seem to be local resources.
SMB	Presentation	Server Message Block provides redirector client to server communication
NetBIOS	Session	Controls the sessions between computers and maintains connections.
NetBEUI	Transport, Network	Provides data transportation. It is not a routable transport protocol which is why NBT exists on large networks to use routable TCP protocol on large networks. This protocol may sometimes be called the NetBIOS frame (NBF) protocol.
NDIS and NIC driver	Data Link	NDIS allows several adapter drivers to use any number of transport protocols. The NIC driver is the driver software for the network card.

NetBIOS Extended User Interface (NetBEUI)

This is a separate protocol from NetBIOS. It supports small to medium networks providing transport and network layer support. It is fast and small and works well for the DOS operating system but NetBEUI **is not a routable protocol**.

Name Resolution

There are three methods of mapping NetBIOS names to IP addresses on small networks that don't perform routing:

1. IP broadcasting - A data packet with the NetBIOS computer name is broadcast when an associated address is not in the local cache. The host who has that name returns its address.

2. The lmhosts file - This is a file that maps IP addresses and NetBIOS computer names.
3. NBNS - NetBIOS Name Server. A server that maps NetBIOS names to IP addresses. This service is provided by the nmbd daemon on Linux.

System wide methods of resolving NetBIOS names to IP addresses are:

1. b-node - Broadcast node
2. p-node - Point-to-point node queries an NBNS name server to resolve addresses.
3. m-node - First uses broadcasts, then falls back to querying an NBNS name server.
4. h-node - The system first attempts to query an NBNS name server, then falls back to broadcasts if the nameserver fails. As a last resort, it will look for the lmhosts file locally.

NetBIOS name services use port 137 and NetBIOS session services use port 139. NetBIOS datagram service uses port 138.

To resolve addresses from names, a computer on a Microsoft network will check its cache to see if the address of the computer it wants to connect to is listed there. If not it sends a NetBIOS broadcast requesting the computer with the name to respond with its hardware address. When the address is received, NetBIOS will start a session between the computers. On larger networks that use routers, this is a problem since routers do not forward broadcasts, nor is NetBEUI a routable protocol. Therefore Microsoft implemented another method of resolving names with the Windows Internet Name Service (WINS). The following steps are taken to resolve NetBIOS names to IP addresses for H-node resolution on larger networks using TCP/IP (NBT):

1. NetBIOS name cache
2. WINS Server
3. NetBIOS broadcast
4. lmhosts file
5. hosts file
6. DNS server

For a more complete explanation of NetBIOS name resolution, WINS, and Windows networking in general, see the manuals in the Windows operating system section such as the "Windows TCP/IP Reference." Also a Windows Networking manual will be written for this section.

NetBIOS over TCP/IP (NBT)

Since NetBEUI is not a routable protocol, Microsoft implemented NBT for larger networks. NetBIOS messages are normally encapsulated in NetBEUI datagrams, but when using NBT, they are encapsulated in TCP/IP datagrams. The NBT protocol is defined by RFC 1001 and RFC 1002.

NWLink

NWLink is Microsoft's implementation of IPX/SPX. NWLink will act as a transport mechanism for NetBIOS similar to the use of TCP/IP described in the NBT section above. NWLink is normally used to support medium networks and may be used where NetWare servers are present.

Windows Internet Name Service (WINS)

WINS is the Microsoft implementation of NetBIOS name service. Samba on Linux can be used as a WINS server.

Computers configured to use WINS, when booted, contact the WINS name server and give the server their NetBIOS name and IP address. The WINS server adds the information to its database and it may send the information to other WINS servers on your network. When a computer that is configured to use WINS needs to get an address of another computer, it will contact the WINS server for the information. Without the use of a WINS server, NetBIOS will only be able to see computers on the unrouted sections of the local network. Does this mean a WINS server must exist in each routed section of the network? The answer is no. This is because WINS uses TCP/IP which is routable. Only one WINS server needs to exist on the network.

The Windows Networking Environment

A domain in a Microsoft networking environment refers to a collection of computers using user level security. It is not the same as the term domain used with regard to the domain name system (DNS). Domain related terms are:

- BDC - Backup Domain Controller is a backup for a PDC
- TLD - Top Level domain
- PDC - Primary Domain Controller is an NT server providing central control of user access permissions and accounts on a network.

AppleTalk Protocols

AppleTalk is the architecture used on with Apple brand computers and is a suite of protocols for networking Apple computers. Some of the protocols are:

- AppleShare - Works at the application layer to provide services.
- AFP - AppleTalk Filing protocol - Makes network files appear local by managing file sharing at the presentation layer.
- ATP - AppleTalk Transaction Protocol provides a Transport Layer connection between computers. Three transaction layers:
    - transaction requires (TREQ)
    - transaction response (TRESP)
    - transaction release (TREL)
- DDP - Datagram Delivery Protocol is a routable protocol that provides for data packet transportation. It operates at the network layer at the same level of the IP protocol.

The AppleTalk networking scheme puts computers into groups called zones. This is similar to workgroups on a Windows network.

Four Session layer protocols

- ASP - AppleTalk session protocol controls the starting and ending of sessions between computers called nodes. It works at the session level. The NBP, described below is used to get addresses from computer names. ATP is used at the transport level.
- ADSP - AppleTalk data stream protocol manages the flow of data between two established socket connections.
- ZIP - Zone information protocol used with RTMP to map zones. Routers use zone information tables (ZITs) to define network addresses and zone names.
- PAP - Printer access protocol manages information between workstations and printers.

Other Protocols

- NBP - Name-binding protocol translates addresses into names.
- AEP - AppleTalk echo protocol uses echoes to tell if a computer, or node, is available.
- RTMP - Routing table maintenance protocol is used to update routers with information about network status and address tables. The whole address table is sent across the network.
- ARUP - AppleTalk update routing is a newer version of RTMP.

System Network Architecture

System Network Architecture (SNA) by IBM is a suite of protocols mainly used with IBM mainframe and AS/400 computers. Two SNA protocols are:

- APPC - Advanced Peer-to-Peer Communications provides peer to peer services at the transport and session layer.
- APPN - Advanced Peer-to-Peer Networking supports the computer connections at the network and transport layers.

Microsoft produced the SNA Server so PC networks could connect with SNA networks.

SNA Layers

SNA has its own network model which is:

- Physical
- Data link - Uses protocols such as token-ring or Synchronous Data Link Control (SDLC).
- Path Control - Performs routing, division, and re-assembly of data packets.
- Transmission - Connection software
- Data flow - Prevents data overflows by monitoring and handling traffic
- Presentation - Handles interfaces to applications
- Transaction - Provides an interface for applications to use network services

SNA Network Devices

- host systems
- terminals
- Output devices
- Communications controllers
- Cluster controllers - Allow many devices to connect through them. They connect ot a host or communications controller.

SNA Network Categories

- Nodes
    - Type 2 - PCs, terminals and printers
    - Type 4 - Communications controllers
    - type 5 - Host computers used to manage the network
- Data links - Connection between combinations of hosts, cluster controllers, or nodes.

Possible SNA communications architectures

- SDLS - Synchronous Data Link Control
- BSC - Binary Synchronous Communication sends bits in frames which are timed sequences of data.
- Token-ring
- X.25
- Ethernet
- FDDI

SNA units

NAU - Network Addressable Units

- LU - Logical Units are ports that users use to access network resources
    - Type 1 - An interactive batch session
    - Type 2 - An IBM 3270 terminal
    - Type 3 - An IBM 3270 printer
    - Type 6.2 - A program to program session
    - Type 7 - An IBM 5250 family session
- PU - Physical Units are a network device used to communicate with hosts.
    - Type 2 - Cluster controllers
    - Type 3 - Front end process
    - Type 5 - Host communications software

SNA software components

- SSCP - Systems Services Control Point manages all resources in the host's domain.
- NCP - Network Control Program performs routing, session management tasks. It runs in the communications controller.

Other Transport Protocols

DECnet

DECnet from Digital Equipment Corporation is a suite of protocols which may be used on large networks that integrate mainframe and minicomputer systems. It is a routable protocol. DNA - Digital Network Architecture.

Data Link Control (DLC)

This protocol operates at the data link layer and is designed for communications between Hewlett-Packard network printers and IBM mainframe computers. This protocol is not routable.

Open Systems Interconnect (OSI)

A suite of protocols developed by the International Standards Organization (ISO) which corresponds with the layers of the OSI model. These protocols provide a number of application protocols for various functions. The OSI protocol stack may be used to connect large systems. OSI is a routable transport protocol.

Network Routing

Simple Networking Routing and Routers

This section will explain routing in simple terms with some simple standard rules. There may be exceptions to these rules, but for introductory purposes we will keep the first example simple. Please be aware, that the examples in this section are working examples, but more complexity may be added when a larger network is considered, and multiple data routes become available.

Each network interface card (NIC) has a specific address which is an IP address or number. When data is sent between two computers, the data must be sent in a package that has the address of the intended receiver (IP) on it. It is like an envelope (ethernet) with the sender's and recipient's address on it. There is somewhat of a difference, however. When the computer intends to send a packet, it first checks its routing table to see if the intended data must be sent through a gateway. Many computers only have a simple routing table, which is built from the network mask and the gateway information entered, when you set your computer up to do networking. The computer, when set up for networking, must be assigned an IP address, netmask, and default gateway. This may be done manually or done automatically using Dynamic Host Configuration Protocol (DHCP) to assign this information to the computer when it boots. DCHP is described in another section. If the computer determines that the packet must be sent to a gateway, it puts it in a special packet (ethernet) for that gateway, with the actual recipient's address wrapped inside.

In the above paragraph, data packets are equated to a letter with an envelope. For this type of thinking, the envelope would be similar to the ethernet, SLIP, or PPP packet which encapsulates the IP packet. The IP packet and its encapsulated data would similar to a letter. Here's generally what happens when a package is sent:

> The sending computer checks the IP part of the package to see the sender's IP address, and based on the address and instructions in its routing table will do one of the following:

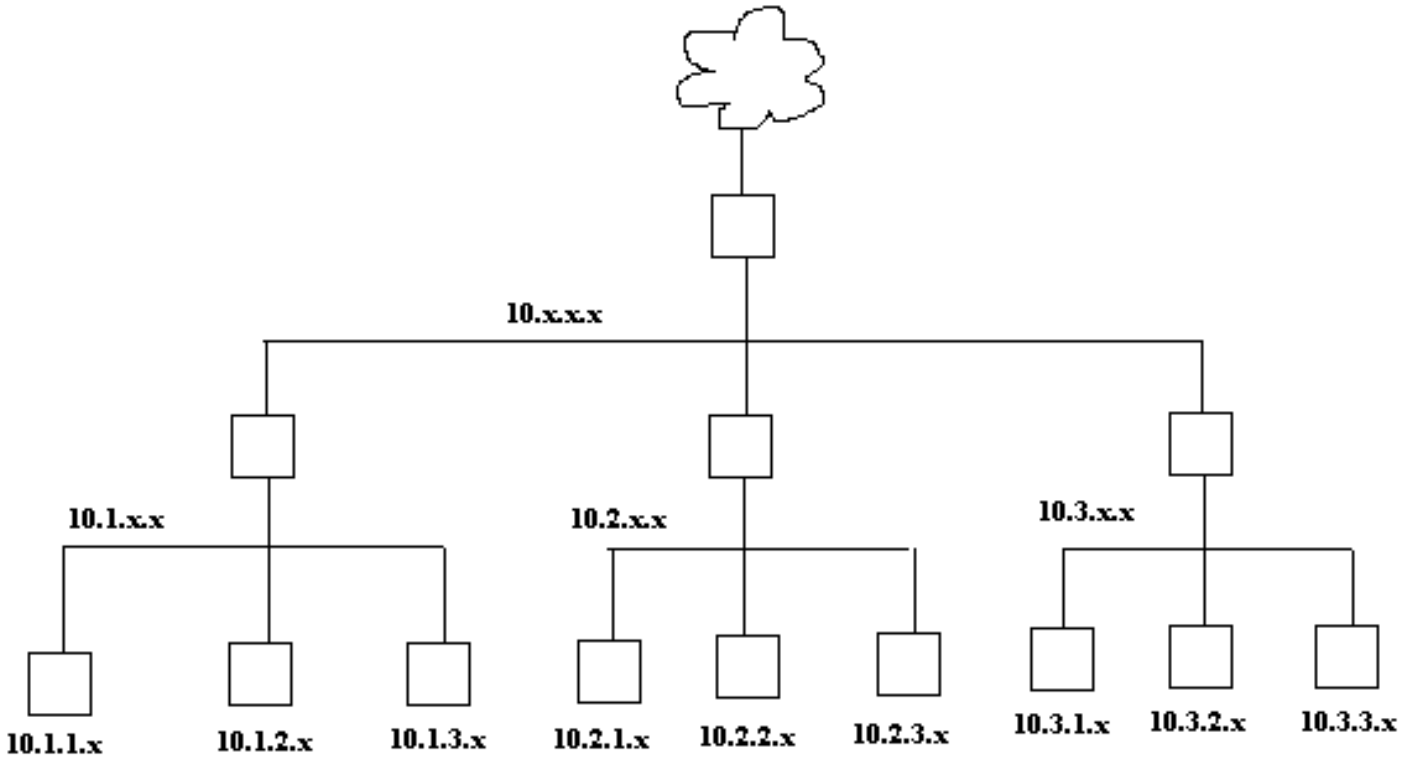
1. Send the packet to the ethernet address of the intended recipient. The following will happen:
    1. The ethernet card on the receiving computer will accept the packet.
    2. The other network levels (IP, TCP) will open the packet and use it according to filtering and other programming instructions.
2. Send the packet to the ethernet address of a router, depending on the instructions in the routing table.
    1. The ethernet card on the router will accept the packet.
    2. The IP level of the router will look at the packet's IP address and determine according to its routing table where to send the packet next. It should send it to another router or to the actual recipient.
    3. The router will encapsulate the IP packet in another ethernet packet with the ethernet address of the next router or the intended recipient.
    4. Router hops will continue until the packet is sent on a network where the intended recipient is physically located unless the packet expires.
    5. The ethernet card on the receiving computer will accept the packet.
    6. The other network levels (IP, TCP) will open the packet and use it according to filtering and other programming instructions.

Lets say you enter an IP address of 10.1.20.45 and a netmask of 255.255.0.0. This means you are on the network 10.1.0.0 (I show it as 10.1.x.x, the X's mean don't care conditions). The machine's IP address and netmask, together define the network, that it's NIC is on. Therefore any machine that fits in the address range provided under 10.1.x.x can be accessed directly from your NIC, and any that are not in this number range, such as 10.3.34.67 cannot be accessed directly and must be sent to a gateway machine since it is on another network. Typically most machines will use their netmask to make this determination which means if the address does not match their known network, the package will be sent to that machine's default gateway in a special package meant for a router. It works similar to a post office. When you send a letter in your town, you put it in the local slot. It can be delivered to someone else in your town (network), but if you are sending to another town (network), you put the letter in the out of town slot (default gateway), then the mail personnel put it in a special container or box and send it to a main town (gateway), which then decides where to send it based on its address. Although this simple network and default gateway may be common, specific computers or gateways can have much more complex rules for routing that allow exceptions to this example.

Please be aware that in order to be forwarded, data packets must be addressed to a router. They cannot just be sent to the recipient's address out to a network. The router does not pick packets off the network and forward them. If a packet is sent on a network and a valid recipient is not on that network, there will be no response. This will be demonstrated in the next section where a subnetwork will be described.

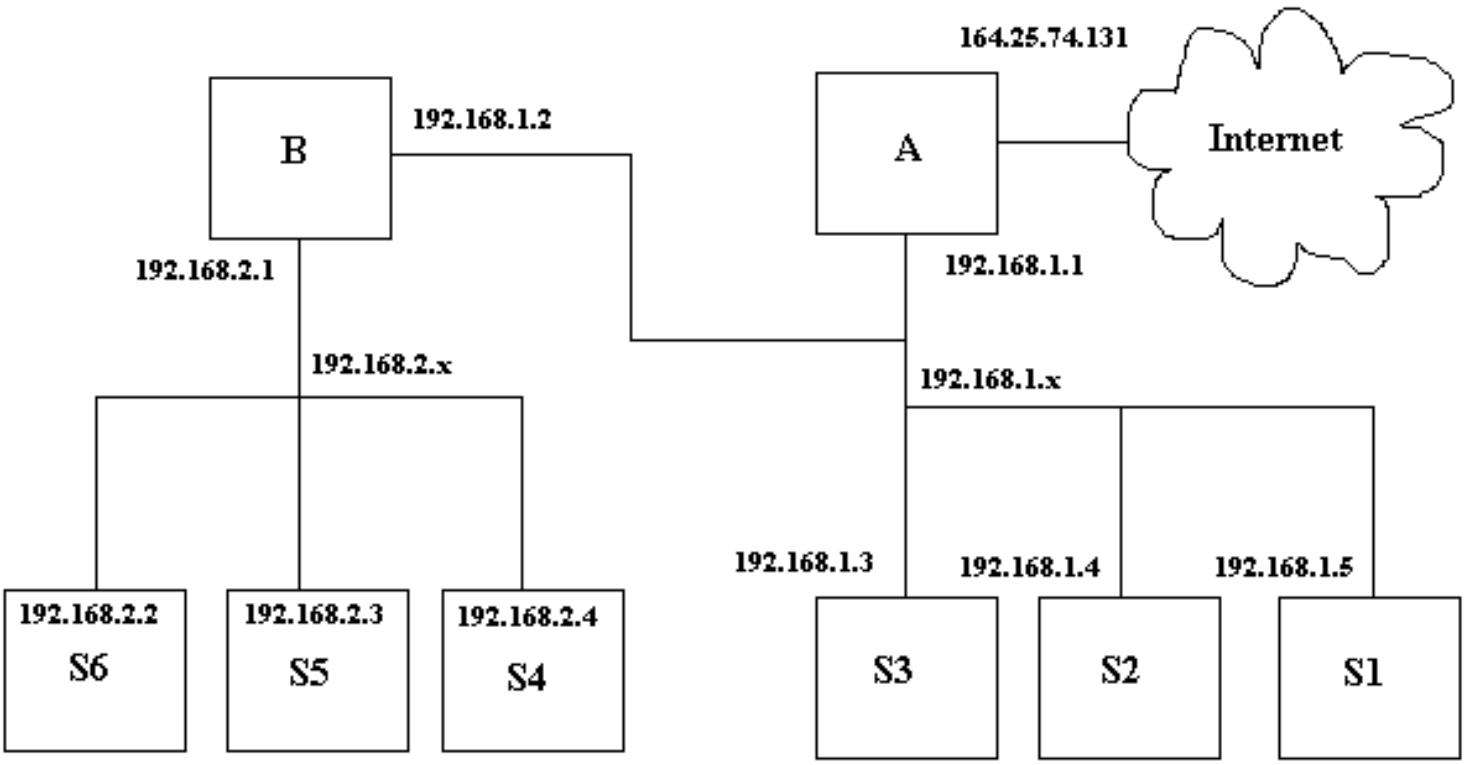
To keep routing simple, most networks are structured as shown below. Generally, the higher networks are 10.x.x.x, then the next are 10.0-254.x.x, then 10.0-254.0-254.x. The number 10 is used as an example Class A network. This numbering scheme keeps routing simple and is the least confusing but networks can be set up in other ways. In the diagram below, only gateways and their networks are shown.

Typical Network Structured Addressing Scheme



In my simple network example below I vary from convention and make network 192.168.2.x be below network 192.168.1.x. causing traffic between the internet and 192.168.2.x to go through the network 192.168.1.x. Normally the network 192.168.1.x would be 192.168.x.x, but this will show you that there can be many variants that will work as long as you have thought your layout through well, and set your routing tables up in your gateways correctly.

A Small Network with Two Gateways



The boxes labeled A and B must be gateways or routers in order for anyone on networks 192.168.2.x or 192.168.1.x to talk to any other network or internet. The boxes labeled S1 through S6 are stations which could be workstations or servers providing services like BOOTP, DHCP, DNS, HTTP, and/or file sharing such as NFS or Samba. The gateways may also provide these services. These stations may combine any combination of server or workstation function. The reasons for putting the various services on separate machines is because of security concerns and the ability of a given machine to handle specific demand. Typically, the computer that is connected directly to the internet, would be a firewall and provide no other services for security reasons. For example, it is not a good idea to provide TFTP services on a machine that you want to have high security. This is why, depending on the security needs of the company or individual along with the relative amount of each service to be provided, various servers are set up with limited functionality.

The machine S6 in the diagram above has the following characteristics:

```
IP Address:   192.168.2.2
Network:      192.168.2.0
Netmask:      255.255.255.0
Gateway:      192.168.2.1
```

In Linux, the "ifconfig" command is used to configure the NIC and the command "route" is used to set up routing tables for that machine. Please note that in Redhat Linux, the GUI interface programs "netconf" and "linuxconf" may be used to set this up also. These GUI interface programs will set these changes up to be permanent by

writing them to files that are used to configure network information. Changes made with "route" without adding the changes to permanent files will no longer be valid when you reboot the machine. The command "ifconfig eth0 192.168.2.2 netmask 255.255.255.0" will set the NIC card up with its address and network number. You can type "netconfig", then select "basic host information" and do the same thing. The command "route add -net default gw 192.168.2.1 dev eth0" will add the route required for this computer for its gateway. This can be done using "ifconf" by selecting "routing and gateways" and "defaults", then setting the address of the default gateway, and enabling routing. Please be aware that various versions of Linux have different means of storing and retrieving network and routing information and you must use the tools that come with your system or learn it well enough to determine what files to modify. On Redhat 6.1 the file "/etc/sysconfig/static-routes" can be modified to make your route changes permanent, but this does not apply to your default route. Other files are "/etc/sysconfig/routed" and "/etc/sysconfig/network". Other files include "/etc/gateways", "/etc/networks", "/proc/net/route", "/proc/net/rt_cache", and "/proc/net/ipv6_route". The file "/etc/sysconfig/network-scripts" is a script file that controls the network setup when the system is booted.

If you type "route" for this machine, the routing table below will be displayed:

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.2.2	*	255.255.255.255	UH	0	0	0	eth0
192.168.2.0	*	255.255.255.0	U	0	0	0	eth0
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	192.168.2.1	0.0.0.0	UG	0	0	0	eth0

Here is a simple explanation of routing tables and their purpose. All computers that are networked have a routing table in one form or another. A routing table is a simple set of rules that tell what will be done with network packets. In programming language it is easiest to think of it as a set of instructions, very similar to a case statement which has a "default" at its end. If can also be thought of as a series of if..then..elseif..then..else statements. If the lines above are labeled A through C and a default (the last line), an appropriate case statement is: (Don't count the header line)

```
switch(address){
    case A: send to me;break;
    case B: send to my network;break;
    case C: send to my local interface;break;
    default: send to gateway 192.168.2.1
```

An appropriate if statement is:

```
if (address=me) then send to me;
elseif (address=my network) then send to my network;
elseif (address=my local) then send to my local interface;
else send to my gateway 192.168.2.1;
```

In everyday terms this is similar to a basic decision process. Imagine you are holding a letter. If it is addressed to

you, you keep it, if it is addressed to someone in your town, you drop it in the local slot at the post office, but if it is addressed to someone out of town, you would drop it in the out of town slot.

Note how the routing table is arranged. It is arranged from the most specific to the least specific. Therefore as you go down the table, more possibilities are covered. You will notice the first Genmask is 255.255.255.255 and the last is 0.0.0.0. There can be no doubt that the last line is the default. The genmasks between the start and the end have a decreasing number of least significant bits set.

The above default routing table may be added manually with the command:

```
route add -net default gw 192.168.2.1 dev eth0
```

The routing table for machine B, the gateway for the network 192.168.2.0 is as follows.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.2.1	*	255.255.255.255	UH	0	0	0	eth0
192.168.1.2	*	255.255.255.255	UH	0	0	0	eth1
192.168.2.0	192.168.2.1	255.255.255.0	UG	0	0	0	eth0
192.168.2.0	*	255.255.255.0	U	0	0	0	eth0
192.168.1.0	192.168.1.2	255.255.255.0	UG	0	0	0	eth1
192.168.1.0	*	255.255.255.0	U	0	0	0	eth1
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	192.168.1.1	0.0.0.0	UG	0	0	0	eth0

The Iface specifies the card where packets for this route will be sent. The address of eth1 is 192.168.1.2 and eth0 is 192.168.2.1. The NIC card addresses could have easily been switched. Line 1 (above) provides for the eth0 address, while line 2 provides for the address of eth1. Lines 3 and 4 are the rules for traffic going from network 192.168.1.0 to network 192.168.2.0 which will be sent out on NIC eth0. Lines 5 and 6 are the rules for traffic going from network 192.168.2.0 to network 192.168.1.0 which will be sent out NIC eth1. This may seem confusing, but please note the first value on lines 3 and 4 is 192.168.2.0 which the header indicates as the destination of the packet. Don't think of it as source! The last line is the default line which specifies that any packet not on one of the networks 192.168.1.0 or 192.168.2.0 will be sent to the gateway 192.168.1.1. This is how the internet access can be attained, though IP masquerading will probably be used. The flags above mean the following:

- U - Route is up
- H - Target is a host
- G - Use gateway

There are other flags, you can look up by typing "man route". Also the metric value above, indicating the distance to the target, is not used by current Linux kernels but may be needed by some routing daemons. Please note that if route knows the name of the gateway machine, it may list its name rather than the IP address. The same is true for defined networks. Networks may be defined in the file "/etc/networks" as in the example:

```
net1 192.168.1.0
net2 192.168.2.0
```

The routing table above can be set up with the following commands.

```
route add -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.2.1 dev eth0
route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.2 dev eth1
```

Again be aware that you are specifying destination networks here and the ethernet device and address the data is to be sent on.
In Redhat Linux this can be specified using "netconf" by selecting "routing and gateways" and "other routes to networks" and entering the following:

Network	Netmask	Gateway
192.168.2.0	255.255.255.0	192.168.2.1
192.168.1.0	255.255.255.0	192.168.1.2

Alternatively in Redhat Linux, you can add the following two lines to the file "/etc/sysconfig/static-routes":

```
eth0 net 192.168.2.0 netmask 255.255.255.0 gw 192.168.2.1
eth1 net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.2
```

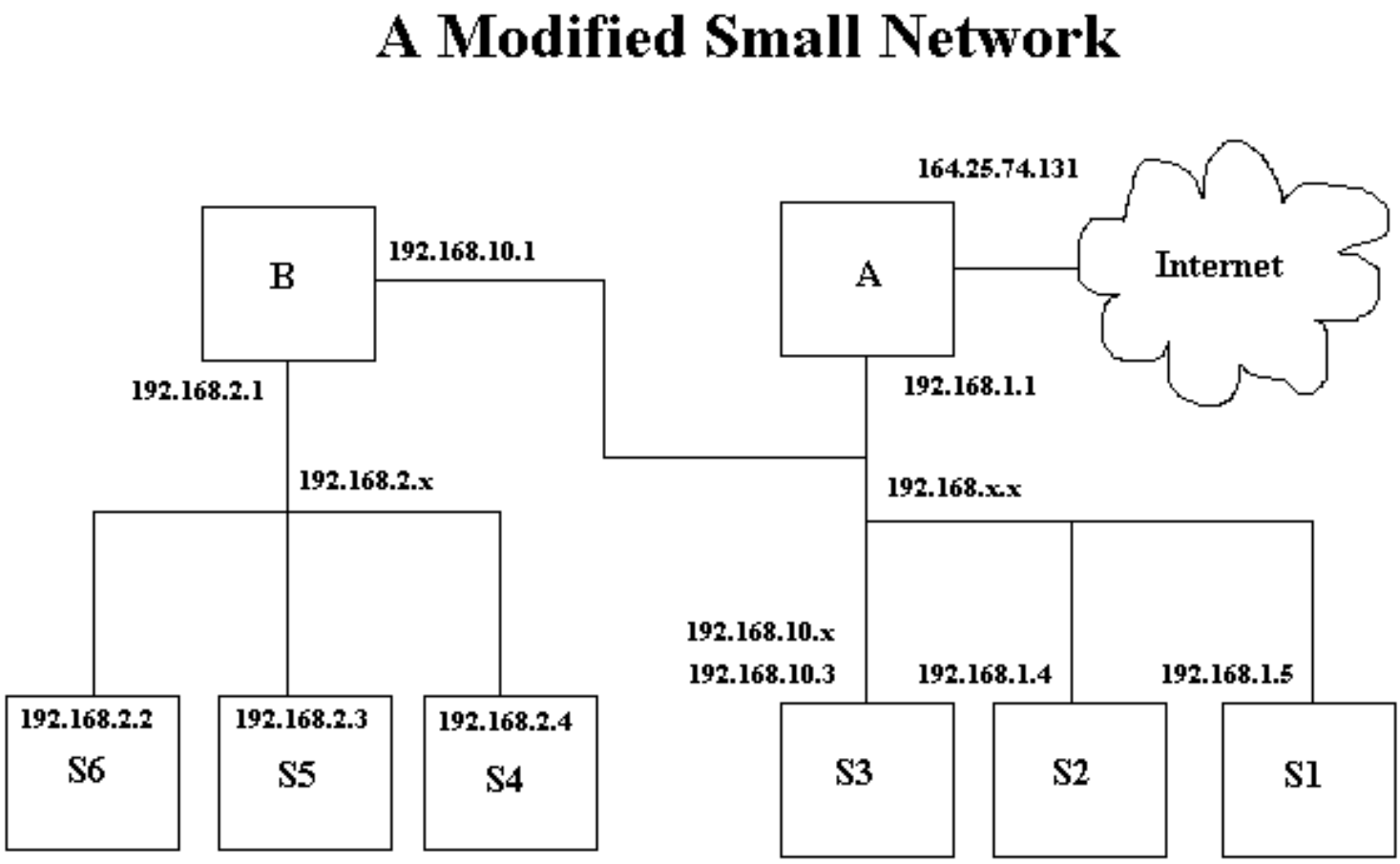
The commands to delete the above routes with route are:

```
route del -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.2.1 dev eth0 route del -net 192.168.1.0
netmask 255.255.255.0 gw 192.168.1.2 dev eth1
```

Be aware, the program route is very particular on how the commands are entered. Even though it may seem that you entered them as the man page specifies, it will not always accept the commands. I don't know if this is a bug or not, but if you enter them as described here with the network, netmask, gateway, and device specified, it should work. The slightest misnomer in network name, netmask, gateway, device, or command syntax and the effort will fail.

More Complex Networking Routing

Now let's modify the small network in the example in the previous section. The 192.168.1.x network is changed to 192.168.x.x and gateway B's address is changed to 192.168.10.1. All the netmasks on the computers on the 192.168.x.x network are modified to 255.255.0.0 to accommodate the change, except machine S3 which keeps the netmask 255.255.255.0 and changes its address to 192.168.10.3. This effectively puts S3 on a different network than S2 and S1, it no longer believes it can talk directly to them and must talk to gateway B to talk to them. It can't even talk to gateway A anymore since it can't address it directly. Machines S1, S2, and A are not on network 192.168.10.0, their addresses are 192.168.1.*. S1 and S2 can talk to S3, but S3 will not be able to respond unless it utilizes gateway B.



Please be aware, in the example in the previous section, that gateway A was aware of gateway B. If it were not, no messages could have been transmitted from the internet to the 192.168.2.0 network. In this example, gateway A knows nothing about gateway B, and as far as it's concerned, the network 192,168.2.0 is part of 192.168.0.0 and there is no gateway between them. Gateway B, does know about gateway A and is using that gateway as its default gateway. Therefore if S1 and S2 use gateway A for their default gateway, they will not be able to talk to S4, 5, or 6 unless their routing table is modified. S1 and S2 will be able to talk to S3, however, assuming S3 is using gateway B.

Here is a listing of machine S1's routing table, using gateway A as default and no other routes.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.1.5	*	255.255.255.255	UH	0	0	0	eth0
192.168.0.0	*	255.255.0.0	U	0	0	0	eth0
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	192.168.1.1	0.0.0.0	UG	0	0	0	eth0

Here it is modified to let it use network 192.168.2.0.

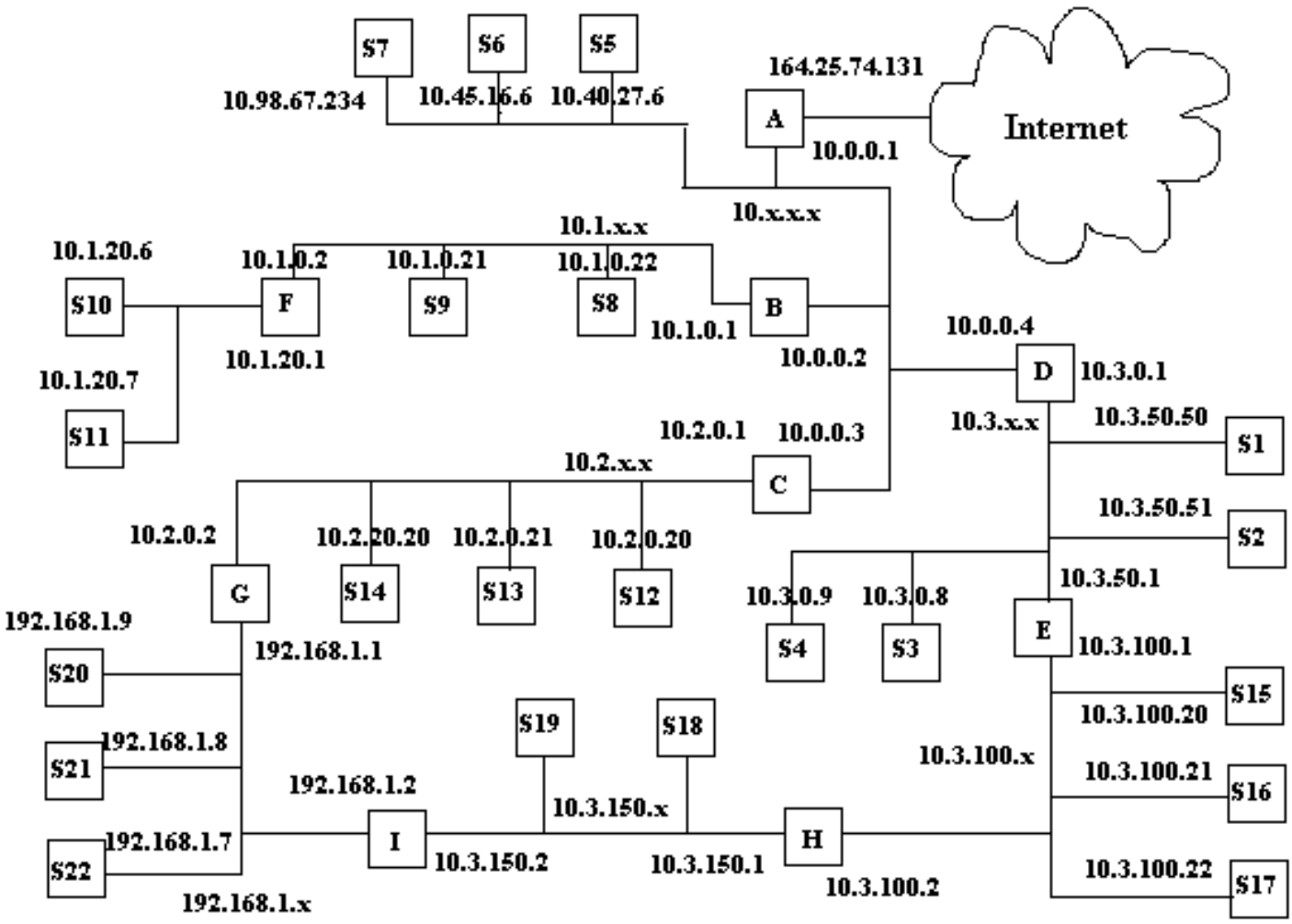
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.1.5	*	255.255.255.255	UH	0	0	0	eth0
192.168.0.0	*	255.255.0.0	U	0	0	0	eth0
192.168.2.0	192.168.10.1	255.255.255.0	UG	0	0	0	eth0
192.168.2.0	*	255.255.255.0	U	0	0	0	eth0
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	192.168.1.1	0.0.0.0	UG	0	0	0	eth0

It specifies the gateway B, 192,168.10.1 to be used if the destination is 192.168.2.x.

The figure below shows an ethernet network with bus topology excluding the hubs. It is a large Class A network with many subnetworks. The machines labeled A through D are routers or potential routers and each have two network interface cards(NIC). These machines may be called gateways since their function is to be a gate to another location. Each card has a valid address on its own network or subnetwork. The table below lists each gateway, and each NIC address and associated network.

Gateway	eth0	eth0 network	eth1	eth1 network
A	10.0.0.1	10.x.x.x	164.25.74.131	Internet
B	10.0.0.2	10.x.x.x	10.1.0.1	10.1.x.x.
C	10.0.0.3	10.x.x.x	10.2.0.1	10.2.x.x.
D	10.0.0.4	10.x.x.x	10.3.0.1	10.3.x.x.
E	10.3.50.1	10.3.x.x	10.3.100.1	10.3.100.x.
F	10.1.0.2	10.1.x.x	10.1.20.1	10.1.20.x.
G	10.2.0.2	10.2.x.x	192.168.1.1	192.168.1.x.
H	10.3.100.2	10.3.100.x	10.3.150.1	10.3.150.x.
I	10.3.150.2	10.3.150.x	192.168.1.2	192.168.1.x.

Large Class A Network



In this figure, there are 9 gateways. which are labeled A through I. There are multiple paths between several networks. The possible paths between networks 10.1.100.x and 192.168.1.x can be through gateways E, D, C, then G (E-D-C-G) or through gateways H-I. The path from 10.3.100.x ot 10.1.20.x can be E-D-B-F or H-I-G-C-B-F. Obviously there are ways to set the routing paths up that may not be fully efficient. In this type of network, the administrator must give careful thought to the setup of the routing tables in their gateways. It would be easy to set up an infinite packet route loop in this network where some packets may go in circles from router to router. Here's how I would route for this network.

The below table lists each network and their default router.

Network	Default Router
10.3.100.x	E
10.3.150.x	H
192.168.1.x	G
10.1.20.x	F

10.1.x.x	B
10.2.x.x	C
10.3.x.x	D
10.x.x.x	A

The router, I, is not used as a default router for any network.

The table below lists an abbreviated route table for each gateway.

Router	Destination	Gateway
A	192.168.1.x	C
	10.1.x.x	B
	10.2.x.x	C
	10.3.x.x	D
	10.x.x.x	10.0.0.1
	default	internet
B	10.1.20.x	F
	10.1.x.x	10.1.0.1
	default	A
C	192.168.1.x	G
	10.2.x.x	10.2.0.1
	default	A
D	10.3.150.x	E
	10.3.100.x	E
	10.3.x.x	10.3.0.1
	default	A
E	192.168.1.x *	H
	10.3.150.x	H
	10.3.100.x	10.3.100.1
	default	D
F	10.1.20.x	10.1.20.1
	default	B
G	10.3.100.x *	I
	192.168.1.x	192.168.1.1
	10.3.150.x *	I
	default	C
H	192.168.1.x	I
	10.3.100.x	10.3.100.2

	10.3.150.x	10.3.150.1
	default	E
I	10.3.100.x	H
	192.168.1.x	192.168.1.2
	10.3.150.x	10.3.150.2
	default	G

The destinations with '*' indicate destinations that shorten the normal route path through network 10.3.150.x.

Also in this network since there are multiple possible paths, dynamic routing can be used to provide alternate routing, if one router goes down.

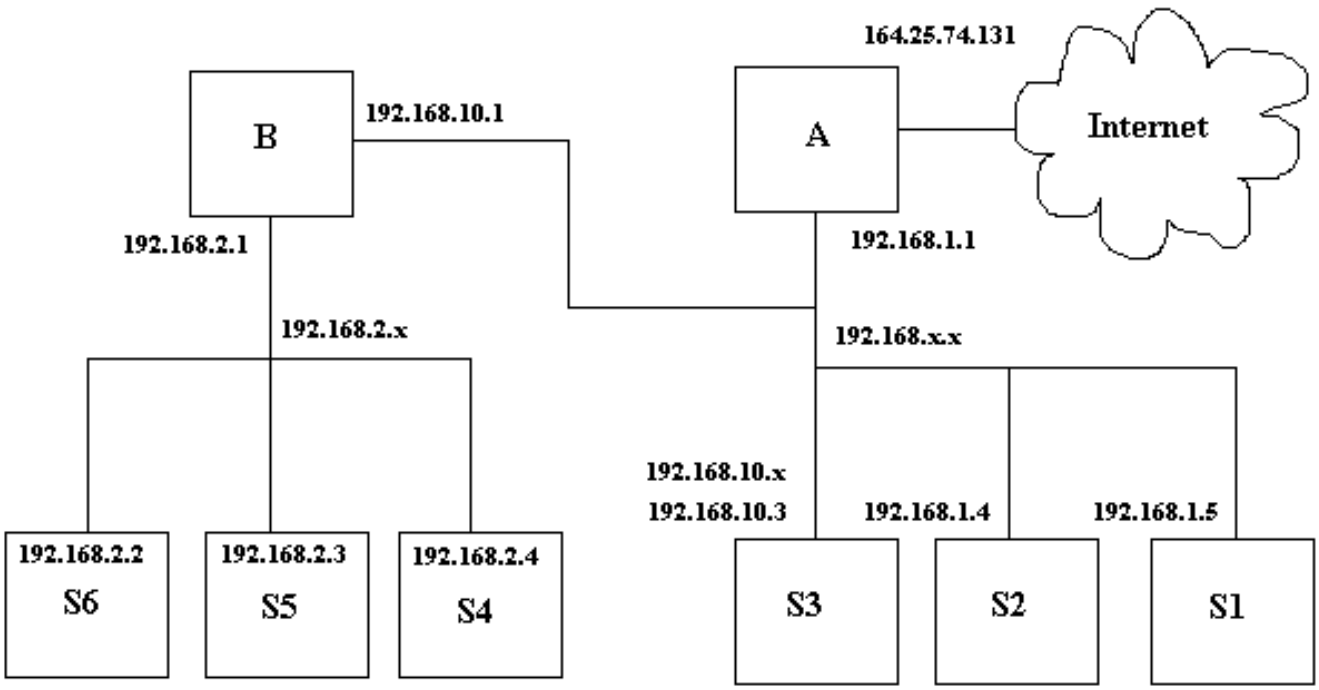
IP Masquerading

IP masquerading is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines. It's similar to someone buying stocks through a broker (without considering the monetary transaction). The person buying stocks, tells the broker to buy the stocks, the broker gets the stocks and passes them to the person who made the purchase. The broker acts on behalf of the stock purchaser as though he was the one buying the stock. No one who sold the stock knew or cared about whether the broker was buying for himself or someone else.

Please DO NOT confuse routers with firewalls and the performance of IP masquerading. The commands that allow IP masquerading are a simple form of a firewall, however routing is a completely different function, as described previously. Setting a computer up to act as a router is completely different than setting up a computer to act as a firewall. Although the two functions are similar in that the router or firewall will act as a communication mechanism between two networks or subnets, the similarity ends there. A computer can be either a router or a firewall, but not both. If you set up a computer to act as both a router and a firewall, you have defeated the purpose of your firewall!

If you refer to the diagram below, the machines on network 192.168.2.x will obtain services through gateway B using IP masquerading, when gateway B is setup properly. What basically happens when IP masquerading is set up on gateway B is described in the following example. If machine S6 tries to ping S2, its ping packages will be wrapped in a package for its default gateway, gateway B, because S6 knows by its netmask that S2 in on another network. When gateway B receives the packages from S6, it converts them to ping packages as though they were sent from itself and sends them to S2. As far as S2 can tell, gateway B has pinged it. S2 receives the packages and responds to gateway B. Gateway B then converts the packages to be addressed to S6 and sends them. This is why it is called IP masquerading, since gateway B masquerades for machines S4, S5, and S6. Machines S1 through S3 and gateway A cannot initiate any communication with S4 through S6. In fact they have no way to know that those machines even exist!

A Modified Small Network



IP masquerading allows internal machines that don't have an officially assigned IP addresses to communicate to other networks and especially the internet. In Linux, IP masquerading support is provided by the kernel. To get it to work you must do essentially three things:

1. Be sure the kernel has support for IP masquerading.
2. Be sure modules needed for support are loaded into the kernel.
3. Set up the firewall rules.

For complete information on the setup of IP masquerading, see the following Linux how-tos:

- IPCHAINS-HOWTO
- Firewall-HOWTO
- IP-Masquerade-HOWTO

Some of the information in this section is based on these how-tos. This section summarizes and puts in simple steps some of the items you will be required to perform to set up IP masquerading. It is not a replacement for the Linux how to documents, but a complement to them by giving an overview of what must be done. You may access the howtos from one of the websites listed in the Linux websites section. The Linux Documentation Project or Metalab's Index of Linux publications will have copies if these howtos.

To set up IP masquerading in Linux you must first be sure your kernel supports IP masquerading with the following options set (This is for a 2.2.x kernel or higher):
Prompt for development and/or incomplete code/drivers (CONFIG_EXPERIMENTAL) [Y/n/?]- YES
Enable loadable module support (CONFIG_MODULES) [Y/n/?] - YES
Networking support (CONFIG_NET) [Y/n/?] - YES
Packet socket (CONFIG_PACKET) [Y/m/n/?] - YES
Kernel/User netlink socket (CONFIG_NETLINK) [Y/n/?] - YES
Routing messages (CONFIG_RTNETLINK) [Y/n/?] - NO
Network firewalls (CONFIG_FIREWALL) [Y/n/?] - YES
TCP/IP networking (CONFIG_INET) - YES
IP: advanced router (CONFIG_IP_ADVANCED_ROUTER) [Y/n/?] - NO
IP: verbose route monitoring (CONFIG_IP_ROUTE_VERBOSE) [Y/n/?] - YES
IP: firewalling (CONFIG_IP_FIREWALL) [Y/n/?] - YES
IP: firewall packet netlink device (CONFIG_IP_FIREWALL_NETLINK) [Y/n/?] - YES
IP: always defragment (required for masquerading) (CONFIG_IP_ALWAYS_DEFRAG) [Y/n/?] - YES
IP: masquerading (CONFIG_IP_MASQUERADE [Y/n/?] - YES
IP: ICMP masquerading (CONFIG_IP_MASQUERADE_ICMP) [Y/n/?] - YES
IP: masquerading special modules support (CONFIG_IP_MASQUERADE_MOD) [Y/n/?] - YES
IP: ipautofw masquerade support (EXPERIMENTAL) (CONFIG_IP_MASQUERADE_IPAUTOFW) [Y/n/?] - NO
IP: ipportfw masq support (EXPERIMENTAL) (CONFIG_IP_MASQUERADE_IPPORTFW) [Y/n/?] - YES
IP: ip fwmark masq-forwarding support (EXPERIMENTAL) (CONFIG_IP_MASQUERADE_MFW) [Y/m/n/?] - NO
IP: optimize as router not host (CONFIG_IP_ROUTER) [Y/n/?] - YES
IP: GRE tunnels over IP (CONFIG_NET_IPGRE) [N/y/m/?] - NO
IP: TCP syncookie support (not enabled per default) (CONFIG_SYN_COOKIES) [Y/n/?] - YES
Network device support (CONFIG_NETDEVICES) [Y/n/?] - YES
Dummy net driver support (CONFIG_DUMMY) [M/n/y/?] - YES
/proc filesystem support (CONFIG_PROC_FS) [Y/n/?] - YES

These are the kernel options you need for IP Masquerade. You will need to select other options for your specific hardware and network setup. Read the IP masquerade and kernel howtos for more information. You may also want the section about how to compile the Linux kernel on the Linux User's Guide in the Linux section of this documentation.

Create the following text and place it in a file "/etc/rc.d/rc.firewall". This will load your needed modules into your kernel and set up your basic firewall rules. If you copy the file from this page, be sure to remove carriage returns when you get it into Linux or it may not work properly.

```
# rc.firewall - Initial SIMPLE IP Masquerade setup for 2.0.x kernels using IPFWADM
#
# Load all required IP MASQ modules
#
#   NOTE:  Only load the IP MASQ modules you need.  All current available IP MASQ
modules
#          are shown below but are commented out from loading.

# Needed to initially load modules
#
/sbin/depmod -a

# Supports the proper masquerading of FTP file transfers using the PORT method
#
/sbin/modprobe ip_masq_ftp

# Supports the masquerading of RealAudio over UDP.  Without this module,
#  RealAudio WILL function but in TCP mode.  This can cause a reduction
#  in sound quality
#
#/sbin/modprobe ip_masq_raudio

# Supports the masquerading of IRC DCC file transfers
#
/sbin/modprobe ip_masq_irc

# Supports the masquerading of Quake and QuakeWorld by default.  This modules is
#   for for multiple users behind the Linux MASQ server.  If you are going to play
#   Quake I, II, and III, use the second example.
#
#Quake I / QuakeWorld (ports 26000 and 27000)
#/sbin/modprobe ip_masq_quake
#
#Quake I/II/III / QuakeWorld (ports 26000, 27000, 27910, 27960)
# /sbin/modprobe ip_masq_quake ports=26000,27000,27910,27960

# Supports the masquerading of the CuSeeme video conferencing software
#
#/sbin/modprobe ip_masq_cuseeme

#Supports the masquerading of the VDO-live video conferencing software
#
#/sbin/modprobe ip_masq_vdolive

#CRITICAL:  Enable IP forwarding since it is disabled by default since
#
#          Redhat Users:  you may try changing the options in /etc/sysconfig/network
from:
```

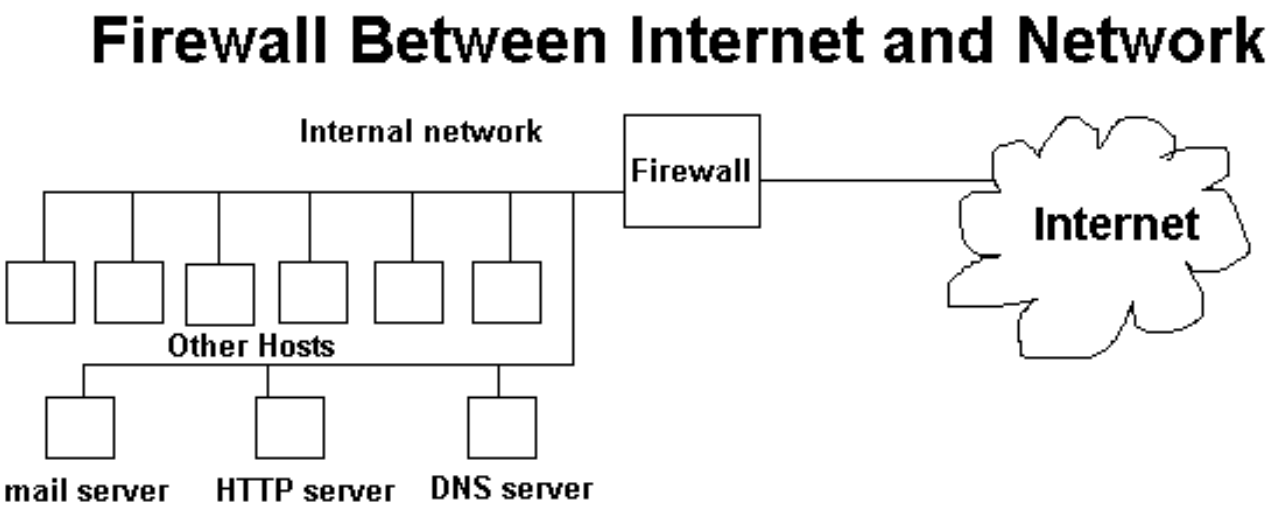
```
#
#                       FORWARD_IPV4=false
#                             to
#                       FORWARD_IPV4=true
#
echo "1" > /proc/sys/net/ipv4/ip_forward

# Dynamic IP users:
#
#   If you get your Internet IP address dynamically from SLIP, PPP, or DHCP, enable
this following
#       option.  This enables dynamic-ip address hacking in IP MASQ, making the life
#       with DialD, PPPd, and similar programs much easier.
#
echo "1" > /proc/sys/net/ipv4/ip_dynaddr

# MASQ timeouts
#
#   2 hrs timeout for TCP session timeouts
#  10 sec timeout for traffic after the TCP/IP "FIN" packet is received
#  160 sec timeout for UDP traffic (Important for MASQ'ed ICQ users)
#
/sbin/ipchains -M -S 7200 10 160

# DHCP:  For people who receive their external IP address from either DHCP or BOOTP
#        such as ADSL or Cablemodem users, it is necessary to use the following
#        before the deny command.  The "bootp_client_net_if_name" should be replaced
#        the name of the link that the DHCP/BOOTP server will put an address on to?
#        This will be something like "eth0", "eth1", etc.
#
#        This example is currently commented out.
#
#
/sbin/ipchains -A input -j ACCEPT -i eth1 -s 0/0 67 -d 0/0 68 -p udp

# Enable simple IP forwarding and Masquerading
#
#  NOTE:  The following is an example for an internal LAN address in the 192.168.0.x
#         network with a 255.255.255.0 or a "24" bit subnet mask.
#
#         Please change this network number and subnet mask to match your internal
LAN setup
#
/sbin/ipchains -P forward DENY
/sbin/ipchains -A forward -s 10.1.199.0/24 -j MASQ
```

Add the following line to the "/etc/rc.d/rc.local" file:
/etc/rc.d/rc.firewall

Of course the machines that you are configuring to be behind the machine providing the masquerading service should be configured to use that as their gateway. In this case S4 through S6 should use gateway B as their default gateway.

Firewalls

Firewalls are mainly used as a means to protect an organization's internal network from those on the outside (internet). It is used to keep outsiders from gaining information to secrets or from doing damage to internal computer systems. Firewalls are also used to limit the access of individuals on the internal network to services on the internet along with keeping track of what is done through the firewall. Please note the difference between firewalls and routers as described in the second paragraph in the IP Masquerading section.



Types of Firewalls

1. Packet Filtering - Blocks selected network packets.
2. Circuit Level Relay - SOCKS is an example of this type of firewall. This type of proxy is not aware of applications but just cross links your connects to another outside connection. It can log activity, but not as detailed as an application proxy. It only works with TCP connections, and doesn't provide for user authentication.
3. Application Proxy Gateway - The users connect to the outside using the proxy. The proxy gets the information and returns it to the user. The proxy can record everything that is done. This type of proxy may require a user login to use it. Rules may be set to allow some functions of an application to be done and other functions denied. The "get" function may be allowed in the FTP application, but the "put" function may not.

Proxy Servers can be used to perform the following functions.

- Control outbound connections and data.
- Monitor outbound connections and data.
- Cache requested data which can increase system bandwidth performance and decrease the time it takes for other users to read the same data.

Application proxy servers can perform the following additional functions:

- Provide for user authentication.
- Allow and deny application specific functions.
- Apply stronger authentication mechanisms to some applications.

Packet Filtering Firewalls

In a packet filtering firewall, data is forwarded based on a set of firewall rules. This firewall works at the network level. Packets are filtered by type, source address, destination address, and port information. These rules are similar to the routing rules explained in an earlier section and may be thought of as a set of instructions similar to a case statement or if statement. This type of firewall is fast, but cannot allow access to a particular user since there is no way to identify the user except by using the IP address of the user's computer, which may be an unreliable method. Also the user does not need to configure any software to use a packet filtering firewall such as setting a web browser to use a proxy for access to the web. The user may be unaware of the firewall. This means the firewall is transparent to the client.

Circuit Level Relay Firewall

A circuit level relay firewall is also transparent to the client. It listens on a port such as port 80 for http requests and redirect the request to a proxy server running on the machine. Basically, the redirect function is set up using ipchains then the proxy will filter the package at the port that received the redirect.

Configuring a Proxy Server

The following packages are available in Linux:

- Ipchains soon to be replaced by netfilter (Packet filtering supported by the Linux kernel). It comes with Linux and is used to modify the kernel packet routing tables.
- SOCKS - Circuit Switching firewall. Normally doesn't come with Linux, but is free.
- Squid - A circuit switching proxy. Normally comes with Linux.
- Juniper Firewall Toolkit - A firewall toolkit product used to build a firewall. It uses transparent filtering, and is circuit switching. It is available as open source.
- The TIS Firewall Toolkit (FWTK). A toolkit that comes with application level proxies. The applications include Telnet, Rlogin, SMTP mail, FTP, http, and X windows. it can also perform as a transparent proxy for other services.

Ipchains and Linux Packet filtering

For complete information on the use of IP chains and setting up a firewall, see the following Linux how-tos:

- IPCHAINS-HOWTO
- Firewall-HOWTO
- IP-Masquerade-HOWTO

Some of the information in this section is based on these how-tos. This section summarizes and puts in simple steps some of the items you will be required to perform to set up a firewall. It is not meant as a replacement for the Linux how to documents, but a complement to them by giving an overview of what must be done. You may access the howtos from one of the websites listed in the Linux websites section. The Linux Documentation Project or Metalab's Index of Linux publications will have copies if these howtos.

The administration of data packet management is controlled by the kernel. Therefore to provide support for things like IP masquerading, packet forwarding, and port redirects, the support must be compiled into the kernel. The kernel contains a series of tables that each contain 0 or more rules. Each table is called a chain. A chain is a sequence of rules. Each rule

contains two items.

1. Characteristics - Characteristics such as source address, destination address, protocol type (UDP, TCP, ICMP), and port numbers.
2. Instructions - Instructions are carried out if the rule characteristics match the data packet.

The kernel filters each data packet for a specific chain. For instance when a data packet is received, the "input" chain rules are checked to determine the acceptance policy for the data packet. The rules are checked starting with the first rule (rule 1). If the rule characteristics match the data packet, the associated rule instruction is carried out. If they don't match, the next rule is checked. The rules are sequentially checked, and if the end of the chain is reached, the default policy for the chain is returned.

Chains are specified by name. There are three chains that are available and can't be deleted. They are:

1. Input - Regulates acceptance of incoming data packets.
2. Forward - Defines permissions to forward packets that have another host as a destination.
3. Output - Permissions for sending packets.

Each rule has a branch name or policy. Policies are listed below:

- ACCEPT - Accept the data packet.
- REJECT - Drop and the packet but send a ICMP message indicating the packet was refused.
- DENY - Drop and ignore the packet.
- REDIRECT - Redirect to a local socket with input rules only even if the packet is for a remote host. This applies to TCP or UDP packets.
- MASQ - Sets up IP masquerading. Works on TCP or UDP packets.
- RETURN - The next rule in the previous calling chain is examined.

You can create more chains then add rules to them. The commands used to modify chains are as follows:

- -N Create a new chain
- -X Delete an empty chain
- -L List the rules in the chain
- -P Change the policy for a chain
- -F Flush=Delete all the rules in a chain
- -Z Zero the packet and byte counters in all chains

Commands to manipulate rules inside the chain are:

- -A Append a new rule to a chain.
- -I Insert a new rule at some position in a chain.
- -R Replace a rule at some position in a chain.
- -D Delete a rule at some position in a chain.
- Options for masquerading:
    - -M with -L to list the currently masqueraded connection.
    - -M with -S to set the masquerading timeout values.

IPchains Options for setting rule specifications:

- -s Source
- -d Destination
- -p Protocol=tcp, upd, icmp, all or a name from /etc/protocols
- -j Jump target, Specifies the target of the rule. The target can be a user defined chain, but not the one this rule is in.
- -i Interface=Name of the interface the packet is received on or the interface where the packet will be sent
- -t Mask used to modify the type of service (TOS) field in the IP header. This option is followed by two values, the first one is and'ed with the TOS field, and the second is exclusive or'ed. The masks are eight bit hexadecimal values. An example of use is "ipchains -A output -p tcp -d 0.0.0.0/0 telnet -t 0x01 0x10" These bits are used to set priority. See the section on IP message formats.
- -f Fragment

When making changes to firewall rules, it is a good idea to deny all packages prior to making changes with the following three commands:

```
ipchains -I input 1 -j DENY
ipchains -I output 1 -j DENY
ipchains -I forward 1 -j DENY
```

These commands inserts a rule at location 1 that denies all packages for input, output, or forwarding. This is done so no unauthorized packets are not let through while doing the changes. When your changes have been completed, you need to remove the rules at position 1 with the following commands:

```
ipchains -D input 1
ipchains -D output 1
ipchains -D forward 1
```

Examples of the use of ipchains to allow various services

Create a new chain:

```
ipchains -N chainame
```

The option "-N" creates the chain.

Add the chain to the input chain:

```
ipchains -A input -j chainame
```

Allow connections to outside http servers from inside our network:

```
ipchains -A chainame -s 10.1.0.0/16 1024: -d 0.0.0.0/0 www -j ACCEPT
```

The "-A chainame" adds a rule to the chain called "chainame". The "-s 10.1.0.0/16 1024:" specifies any traffic on network 10.1.0.0 at port 1024 or above. The "-d 0.0.0.0/0 www" specifies any destination for www service (in the /etc/services file) and the "-j ACCEPT" sets the rule to accept the traffic.

Allow connections from the internet to connect with your http server:

```
ipchains -A chainame -s 0.0.0.0/0 www -d 10.1.1.36 1024: -j ACCEPT
```

The "-A chainame" adds a rule to the chain called "chainame". The "-s 0.0.0.0/0 www" specifies traffic from any source for www service. The "-d 10.1.1.36 1024:" specifies the http server at IP address 10.1.1.36 at ports above 1024 and the "-j ACCEPT" sets the rule to accept the traffic.

Allow DNS to go through the firewall:

```
ipchains -A chainame -p UDP -s 0/0 dns -d 10.1.0.0/16 -j ACCEPT
```

The "-A chainame" adds a rule to the chain called "chainame". The "-p UDP" specifies UDP protocol. The "-s 0/0 dns" specifies any dns traffic from any location. The "-d 10.1.0.0/16" specifies our network and the "-j ACCEPT" sets the rule to accept the traffic. This allows DNS queries from computers inside our network to be received.

Allow e-mail to go from our internal mail server to mailservers outside the network.

```
ipchains -A chainame -s 10.1.1.24 -d 0/0 smtp -j ACCEPT
```

The "-A chainame" adds a rule to the chain called "chainame". The "-s 10.1.1.24" specifies any traffic from 10.1.1.24 IP address. The "-d 0/0 smtp" specifies any smtp type of service going anywhere and the "-j ACCEPT" sets the rule to accept the traffic.

Allow e-mail to come from any location to our mail server:

```
ipchains -A chainame -s 0/0 smtp -d 10.1.1.24 smtp -j ACCEPT
```

The "-A chainame" adds a rule to the chain called "chainame". The "-s 0/0 smtp" specifies mail traffic from anywhere. The "-d 10.1.1.24 smtp" specifies mail traffic going to our mail server and the "-j ACCEPT" sets the rule to accept the traffic.

Perform a HTTP port redirect for a transparent proxy server:

```
ipchains -A input -p tcp -s 10.1.0.0/16 -d 0/0 80 -j REDIRECT 8080
```

The "-A input" adds a rule to the input chain. The "-p tcp" specifies the protocol TCP. The "-s 10.1.0.0/16" specifies the source as a network with netmask 255.255.0.0. The "-d 0/0" specifies a destination of anywhere. The number 80 is the HTTP port number, and the command "-j REDIRECT 8080" redirects the traffic to port 8080.

Give telnet transmissions a higher priority

```
ipchains -A output -p tcp -d 0.0.0.0/0 telnet -t 0x01 0x10"
```

The bits at the end of the line specified in hexadecimal format are used to set the priority of the IP message on the network. The first value is and'ed with the TOS field in the IP message header, and the second value is exclusive or'ed. See the section on IP message formats for more information.

Using ipchains-save and ipchains-restore to make rules permanent

When you are done setting your ipchains rules, use the following procedure while logged on as root to make them permanent:

1. Type the command "ipchains-save > /etc/iprules.save".
2. Create the following script named "packetfw":

```
#! /bin/sh
# Packet filtering firewall script to be used turn the firewall on or off

if [ -f /etc/iprules.save ]
then
   case "$1" in
      start)
          echo -n "Turning on packet filtering firewall:"
          /sbin/ipchains-restore < /etc/iprules.save
          echo 1 > /proc/sys/net/ipv4/ip_forward
          echo "."
          ;;
       stop)
          echo -n "Turning off packet filtering:"
          echo 0 > /proc/sys/net/ipv4/ip_forward
          /sbin/ipchains -X
          /sbin/ipchains -F
          /sbin/ipchains -P input ACCEPT
          /sbin/ipchains -P output ACCEPT
          /sbin/ipchains -P forward ACCEPT
          echo "."
          ;;
       *)
          echo "Usage: /etc/init.d/packetfw {start|stop}"
          exit 1
          ;;
   esac
   exit 0
else
   echo the /etc/iprules.save file does not exist.
   exit 1
fi
```

3. Save the file in the /etc/rc.d/init.d directory.
4. In the /etc/rc.d/rc3.d and the /etc/rc.d/rc5.d directories make a symbolic link called S07packetfw to the /etc/rc.d/init.d/packetfw file with the command "ln -s /etc/rc.d/rc3/S07packetfw /etc/rc.d/init.d/packetfw". This applies to runlevel 3. Do the same for the runlevel 5 initialization directory. Note: You may need to use a different number than the "S07" string to number your link file. Look in your /etc/rc.d/rc3.d and /etc/rc.d/rc5.d directories to determine what number is available to give this file. Try to give it a number just below your network number file. On my system the S10network file is used to start my network.

Domain Name Service

Host Names

Domain Name Service (DNS) is the service used to convert human readable names of hosts to IP addresses. Host names are not case sensitive and can contain alphabetic or numeric letters or the hyphen. Avoid the underscore. A fully qualified domain name (FQDN) consists of the host name plus domain name as in the following example:

computername.domain.com

The part of the system sending the queries is called the resolver and is the client side of the configuration. The nameserver answers the queries. Read RFCs 1034 and 1035. These contain the bulk of the DNS information and are superceded by RFCs 1535-1537. Naming is in RFC 1591. The main function of DNS is the mapping of IP addresses to human readable names.

Three main components of DNS

1. resolver
2. name server
3. database of resource records(RRs)

Domain Name System

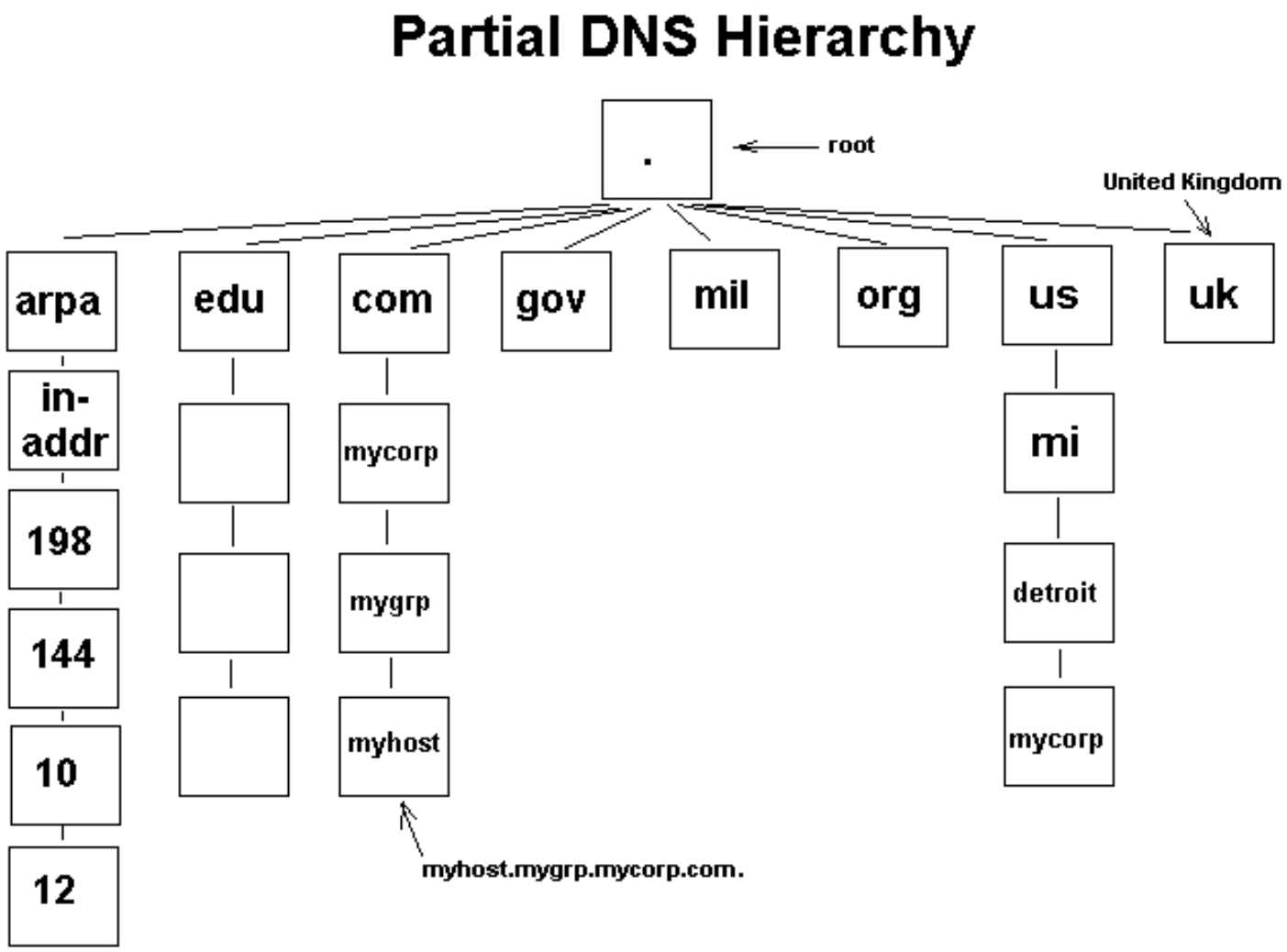
The Domain Name System (DNS) is basically a large database which resides on various computers and it contains the names and IP addresses of various hosts on the internet and various domains. The Domain Name System is used to provide information to the Domain Name Service to use when queries are made. The service is the act of querying the database, and the system is the data structure and data itself. The Domain Name System is similar to a file system in Unix or DOS starting with a root. Branches attach to the root to create a huge set of paths. Each branch in the DNS is called a label. Each label can be 63 characters long, but most are less. Each text word between the dots can be 63 characters in length, with the total domain name (all the labels) limited to 255 bytes in overall length. The domain name system database is divided into sections called **zones**. The name servers in their respective zones are responsible for answering queries for their zones. A zone is a subtree of DNS and is administered separately. There are multiple name servers for a zone. There is usually one primary nameserver and one or more secondary name servers. A name server may be authoritative for more than one zone.

DNS names are assigned through the Internet Registries by the Internet Assigned Number Authority (IANA). The domain name is a name assigned to an internet domain. For example, mycollege.edu represents the domain name of an educational institution. The names microsoft.com and 3Com.com represent the domain names at those commercial companies. Naming hosts within the domain is up to individuals administer their domain.

Access to the Domain name database is through a resolver which may be a program or part of an operating system that resides on users workstations. In Unix the resolver is accessed by using the library functions "gethostbyname" and "gethostbyaddr". The resolver will send requests to the name servers to return information requested by the user. The requesting computer tries to connect to the name server using its IP address rather than the name.

Structure and message format

The drawing below shows a partial DNS hierarchy. At the top is what is called the root and it is the start of all other branches in the DNS tree. It is designated with a period. Each branch moves down from level to level. When referring to DNS addresses, they are referred to from the bottom up with the root designator (period) at the far right. Example: "myhost.mycompany.com.".



DNS is hierarchical in structure. A domain is a subtree of the domain name space. From the root, the assigned top-level domains in the U.S. are:

- GOV - Government body.
- EDU - Educational body.
- INT - International organization
- NET - Networks
- COM - Commercial entity.
- MIL - U. S. Military.
- ORG - Any other organization not previously listed.

Outside this list are top level domains for various countries.

Each node on the domain name system is separated by a ".". Example: "mymachine.mycompany.com.". Note that any name ending in a "." is an absolute domain name since it goes back to root.

DNS Message format:

Bits	Name	Description

0-15	Identification	Used to match responses to requests. Set by client and returned by server.
16-31	Flags	Tells if query or response, type of query, if authoritative answer, if truncated, if recursion desired, and if recursion is available.
32-47	Number of questions	
48-63	Number of answer RRs	
64-79	Number of authority RRs	
80-95	Number of additional RRs	
96-??	Questions - variable lengths	There can be variable numbers of questions sent.
??-??	Answers - variable lengths	Answers are variable numbers of resource records.
??-??	Authority - variable lengths	
??-??	Additional Information - variable lengths	

Question format includes query name, query type and query class. The query name is the name being looked up. The query class is normally 1 for internet address. The query types are listed in the table below. They include NS, CNAME, A, etc.

The answers, authority and additional information are in resource record (RR) format which contains the following.

1. Domain name
2. Type - One of the RR codes listed below.
3. Class - Normally indicates internet data which is a 1.
4. Time to live field - The number of seconds the RR is saved by the client.
5. Resource data length specifies the amount of data. The data is dependent on its type such as CNAME, A, NS or others as shown in the table below. If the type is "A" the data is a 4 byte IP address.

The table below shows resource record types:

Type	RR value	Description
A	1	Host's IP address
NS	2	Host's or domain's name server(s)
CNAME	5	Host's canonical name, host identified by an alias domain name
PTR	12	Host's domain name, host identified by its IP address
HINFO	13	Host information
MX	15	Host's or domain's mail exchanger
AXFR	252	Request for zone transfer
ANY	255	Request for all records

Usage and file formats

If a domain name is not found when a query is made, the server may search for the name elsewhere and return the information to the requesting workstation, or return the address of a name server that the workstation can query to get more information. There are special servers on the Internet that provide guidance to all name servers. These are known as root name servers. They do not contain all information about every host on the Internet, but they do provide direction as to where domains are located (the IP address of the name server for the uppermost domain a server is requesting). The root name server is the starting point to find any domain on the Internet.

Name Server Types

There are three types of name servers:

1. The primary master builds its database from files that were preconfigured on its hosts, called zone or database files. The name server reads these files and builds a database for the zone it is authoritative for.
2. Secondary masters can provide information to resolvers just like the primary masters, but they get their information from the primary. Any updates to the database are provided by the primary.
3. Caching name server - It gets all its answers to queries from other name servers and saves (caches) the answers. It is a non-authoritative server.

The caching only name server generates no zone transfer traffic. A DNS Server that can communicate outside of the private network to resolve a DNS name query is referred to as **forwarder**.

DNS Query Types

There are two types of queries issued:

1. **Recursive** queries received by a server forces that server to find the information requested or post a message back to the querier that the information cannot be found.
2. **Iterative** queries allow the server to search for the information and pass back the best information it knows about. This is the type that is used between servers. Clients used the recursive query.
3. **Reverse** - The client provides the IP address and asks for the name. In other queries the name is provided, and the IP address is returned to the client. Reverse lookup entries for a network 192.168.100.0 is "100.168.192.in-addr arpa".

Generally (but not always), a server-to-server query is iterative and a client-resolver-to-server query is recursive. You should also note that a server can be queried or it can be the person placing a query. Therefore, a server contains both the server and client functions. A server can transmit either type of query. If it is handed a recursive query from a remote source, it must transmit other queries to find the specified name, or send a message back to the originator of the query that the name could not be found.

DNS Transport protocol

DNS resolvers first attempt to use UDP for transport, then use TCP if UDP fails.

The DNS Database

A database is made up of records and the DNS is a database. Therefore, common resource record types in the DNS database are:

- A - Host's IP address. Address record allowing a computer name to be translated into an IP address. Each computer must have this record for its IP address to be located. These names are not assigned for clients that have dynamically assigned IP addresses, but are a must for locating servers with static IP addresses.
- PTR - Host’s domain name, host identified by its IP address
- CNAME - Host’s canonical name allows additional names or aliases to be used to locate a computer.
- MX - Host’s or domain’s mail exchanger.
- NS - Host’s or domain’s name server(s).
- SOA - Indicates authority for the domain

- TXT - Generic text record
- SRV - Service location record
- RP - Responsible person
- HINFO - Host information record with CPU type and operating system.

When a resolver requests information from the server, the DNS query message indicates one of the preceding types.

DNS Files

- CACHE.DNS - The DNS Cache file. **This file is used to resolve internet DNS queries**. On Windows systems, it is located in the WINNTROOT\system32\DNS directory and is used to configure a DNS server to use a DNS server on the internet to resolve names not in the local domain.

Example Files

Below is a partial explanation of some records in the database on a Linux based system. The reader should view this information because it explains some important DNS settings that are common to all DNS servers. An example /var/named/db.mycompany.com.hosts file is listed below.

```
mycompany.com.          IN      SOA     mymachine.mycompany.com.
root.mymachine.mycompany.com. (
                1999112701          ; Serial number as date and two digit number
YYMMDDXX
                10800               ; Refresh in seconds 28800=8H
                3600                ; Retry in seconds 7200=2H
                604800              ; Expire 3600000=1 week
                86400 )             ; Minimum TTL 86400=24Hours
mycompany.com.                  IN      NS      mymachine.mycompany.com.
mycompany.com.                  IN      MX              10
mailmachine.mycompany.com.
mymachine.mycompany.com.        IN      A       10.1.0.100
mailmachine.mycompany.com.      IN      A       10.1.0.4
george.mycompany.com.           IN      A       10.1.3.16
```

A Line by line description is as follows:

1. The entries on this line are:
    1. mycompany.com. - Indicates this server is for the domain mycompany.com.
    2. IN - Indicates Internet Name.
    3. SOA - Indicates this server is the authority for its domain, mycompany.com.
    4. mymachine.mycompany.com. - The primary nameserver for this domain.
    5. root.mymachine.mycompany.com. - The person to contact for more information.

    The lines in the parenthesis, listed below, are for the secondary nameserver(s) which run as slave(s) to this one (since it is the master).
2. 1999112701 - Serial number - If less than master's SN, the slave will get a new copy of this file from the master.
3. 10800 - Refresh - The time in seconds between when the slave compares this file's SN with the master.
4. 3600 - Retry - The time the server should wait before asking again if the master fails to respond to a file update (SOA request).
5. 604800 - Expire - Time in seconds the slave server can respond even though it cannot get an updated zone file.
6. 86400 - TTL - The time to live (TTL) in seconds that a resolver will use data received from a nameserver before it will

ask for the same data again.

7. This line is the nameserver resource record. There may be several of these if there are slave name servers.

```
mycompany.com.                  IN        NS      mymachine.mycompany.com.
```

   Add any slave server entries below this like:

```
mycompany.com.                  IN        NS      ournamesv1.mycompany.com.
mycompany.com.                  IN        NS      ournamesv2.mycompany.com.
mycompany.com.                  IN        NS      ournamesv3.mycompany.com.
```

8. This line indicates the mailserver record.

```
mycompany.com.                  IN        MX              10
mailmachine.mycompany.com.
```

   There can be several mailservers. The numeric value on the line indicates the preference or precedence for the use of that mail server. A lower number indicates a higher preference. The range of values is from 0 to 65535. To enter more mailservers, enter a new line for each one similar to the nameserver entries above, but be sure to set the preferences value correctly, at different values for each mailserver.

9. The rest of the lines are the name to IP mappings for the machines in the organization. Note that the nameserver and mailserver are listed here with IP addresses along with any other server machines required for your network.

```
mymachine.mycompany.com.        IN        A       10.1.0.100
mailmachine.mycompany.com.      IN        A       10.1.0.4
george.mycompany.com.           IN        A       10.1.3.16
```

Domain names written with a dot on the end are absolute names which specify a domain name exactly as it exists in the DNS hierarchy from the root. Names not ending with a dot may be a subdomain to some other domain.

Aliases are specified in lines like the following:

```
mymachine.mycompany.com          IN      CNAME   nameserver.mycompany.com.
george.mycompany.com    IN       CNAME   dataserver.mycompany.com.
Linux1.mycompany.com    IN       CNAME   engserver.mycompany.com.
Linux2.mycompany.com    IN       CNAME   mailserver.mycompany.com.
```

When a client (resolver) sends a request, if the nameserver finds a CNAME record, it replaces the requested name with the CNAME, then finds the address of the CNAME value, and return this value to the client.

A host that has more than one network card which is set to address two different subnets can have more than one address for a name.

```
mymachine.mycompany.com          IN      A       10.1.0.100
                                 IN      A       10.1.1.100
```

When a client queries the nameserver for the address of a multi homed host, the nameserver will return the address that is closest to the client address. If the client is on a different network than both the subnet addresses of the multi homed host, the server will return both addresses.

For more information on practical application of DNS, read the DNS section of the Linux User's Guide.

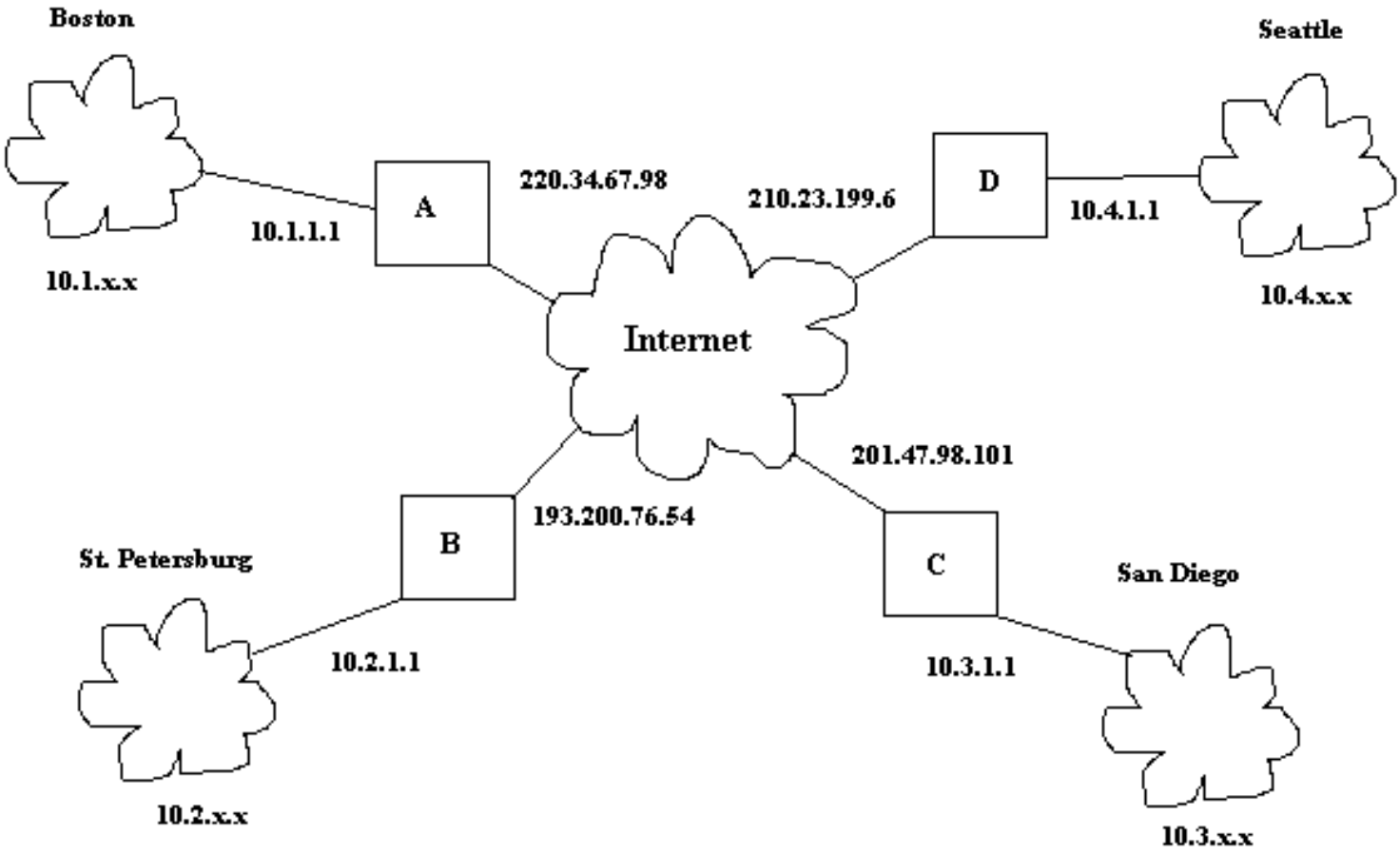
Virtual Private Networking

If you've understood most of this document so far, the principles of Virtual private networking (VPN) will be easy to understand. The most confusing part of VPN is that many acronyms show up. This is partly because VPN requires data encryption to be "private" and there are many encryption techniques and terms. Also there are many complicated security issues relating to VPN concerning encryption and user authentication. This section will first explain the concept and methodology behind VPN, then explain some of the acronyms. I can't explain them all, there will be more tomorrow.

Purpose of VPN

The function of VPN is to allow two computers or networks to talk to each other over a transport media that is not secure. To do this VPN uses a computer at each of the two or more points on the various ends of the transport media such as the internet. Each point at the end of the transport media (internet) is called a point of presence (POP). In this example, the transport media is the internet. In the example below our company "Boats and More, Inc." has four offices. One in Boston, St Petersburg, Seattle, and San Diego. The owner wants a networking setup so he can access any of the 4 network locations at any time through the internet. He wants his data secure since some of it is confidential. His offices are set up on networks 10.1.x.x, 10.2.x.x, 10.3.x.x, and 10.4.x.x. Each of the four networks, when they need to send a data packet to one of the other networks, will route its data packet to its respective router, A, B, C, or D. For example if a computer on the 10.1.x.x network in Boston needs to send a packet to a computer with address 10.3.6.1 on the network in San Diego at 10.3.x.x, it will send its packet to its router, A. Since the network number, 10.x.x.x, is reserved for private use, the packet can't be sent going from computer A with 10.3.6.1 as its intended address. This is because the routers on the internet will not recognize this address as a valid destination. IP masquerading won't solve this problem since the computer on the other end would have no way of knowing that a packet that it didn't send was a masqueraded packet. Tunneling is the technique used to solve this problem.

VPN Setup for Multiple Points of Presence



Tunneling means that the complete IP packet to be sent from Boston to San Diego must be encapsulated into another IP packet. This new packet will have a legal internet IP address. Therefore, machine A will take the packet it needs to route (already has destination address 10.3.6.1) and roughly the following will happen:

1. Machine A will extract the IP packet.
2. Machine A will encrypt the packet.
3. Machine A will wrap the original IP packet in a new IP packet with destination address 201.47.98.101, which is machine C's true internet address.
4. Machine A will wrap the new IP packet in an ethernet packet and send it to the network.
5. The packet will be routed through the internet until it reaches machine C.
6. Machine C will extract the outer IP packet.
7. Machine C will determine that the IP packet contains another IP packet and extract it.
8. Machine C will decrypt the packet.
9. Machine C will examine the destination address of the inner IP packet, wrap it in an ethernet packet with the correct ethernet address, and send it to the internal network on its port 10.3.1.1.

This description is simplistic, but it is essentially what happens. This did not account for authentication and being sure machine C had the authority or ability to decrypt the packet. Therefore VPN can be examined in two main functional areas which are the tunneling mechanism and the security mechanisms.

VPN tunneling Protocols

The list below describes the tunneling protocols which may be used for VPN.

- L2F - Layer2 Forwarding, works at the link layer of the OSI model. It has no encryption. Being replaced by L2TP.
- PPTP - Point-to-Point Tunneling Protocol (RFC 2637) works at the link layer. No encryption or key management included in specifications.
- L2TP - Layer2 Tunneling Protocol. (RFC 2661) Combines features of L2F and PPTP and works at the link layer. No encryption or key management included in specifications.
- IPSec - Internet protocol security, developed by IETF, implemented at layer 3. it is a collection of security measures that address data privacy, integrity, authentication, and key management, in addition to tunneling. Does not cover key management.
- Socks - handled at the application layer

VPN Security

In addition ot tunneling, VPN needs to provide for authentification, confidentiality, data integrity and key management. This is important if you need to keep your data going across the transmission media, secret. The capability of sending the data is easy, but the security measures necessary make VPN a much more complex subject. Security functions that must be covered are:

- Authentification - Making sure the data is from where it is supposed to be from.
- Confidentiality - Keeping any third parties from reading or understanding the data.
- Data integrity - Being sure the data received was not changed by a third party and that it is correct.
- Access control - Keeping third parties without authorization from getting access to your data or network.

Essentially the part of the system that must make the data secure, must encrypt the data and provide a method to decrypt the data. There are many different encryption formulas, but typically handling of decryption is usually done by providing a "key" to the party that must decrypt the data. Keys are secrets shared between two parties, that allow one party to pass encrypted information from one to the other without third parties being able to read it. It is similar to a house or car key that allows only members of your family to enter the house or use the car. Keys are a digital code that will allow the second party to decrypt the data. The digital code must be long enough to keep any third parties from being able to break the code by guessing. Key management can be a complex subject since there are many ways to implement it, but it needs to be secure so no third party gets, intercepts, or guesses the key.

There are many different protocols used to support each of the above functions. Each have various advantages and disadvantages including the fact that some are more secure than others. If you are going to use VPN as a data exchange method, and you want secure data, you or someone on your staff had better know what they're doing (Knowledge of the strengths and weaknesses of the protocols and how to implement them properly), or sooner or later, you may get burned.

Managing user access rights and Key Management or Authentification

Systems

Two key management protocols are:

1. RADIUS - Remote Authentication Dial-In User Service is used for dial in clients to connect to other computers or a network. It provides authentication and accounting when using PPTP or L2TP tunneling.
2. ISAKMP/Oakley - Internet Security Association and Key Management Protocol Authentication uses one of the following three attributes to authenticate users.
    1. Something you have such as a key.
    2. Something you know such as a secret.
    3. Something you are such as your fingerprint.

    More than one means of authentification is recommended for stronger security.

VPN terms

VPN Protocols:

- PPTP - Point to point tunneling protocol (RFC 2637)
- L2TP - Layer 2 tunneling protocol (RFC 2661)
- IPIP tunneling - Tunneling IP packets in IP packets.

Encryption protocols, methods and terms:

- CIPE - Crypto IP Encapsulation
- SSL - Secure sockets layer
- IPSEC - Internet protocol security

Authentication Protocols:

- PAP - Password Authentification Protocol is a two way handshake protocol designed for use with PPP.
- CHAP - Challenge Handshake Authentication Protocol is a three way handshake protocol which is considered more secure than PAP.
- TACACS - Offers authentication, accounting, and authorization.
- S/Key - A one time password system, secure against replays. RFC 2289.

Projects and software:

- SWAN - Secure wide area network
- PoPToP Point to point tunneling protocol server.

DHCP

Dynamic Host Configuration Protocol (DHCP)

This protocol is used to assign IP addresses to hosts or workstations on the network. Usually a DHCP server on the network performs this function. Basically it "leases" out address for specific times to the various hosts. If a host does not use a given address for some period of time, that IP address can then be assigned to another machine by the DHCP server. When assignments are made or changed, the DHCP server must update the information in the DNS server.

As with BOOTP, DHCP uses the machine's or NIC ethernet (MAC) or hardware address to determine IP address assignments. The DHCP protocol is built on BOOTP and replaces BOOTP. DHCP extends the vendor specific area in BOOTP to 312 bytes from 64. RFC 1541 defines DHCP.

DHCP RFCs

DHCP RFCs are 1533, 1534, 1541, and 1542. Sent from DHCP server:

- IP address
- Netmask
- Default Gateway address
- DNS server addresse(s)
- NetBIOS Name server (NBNS) address(es).
- Lease period in hours
- IP address of DHCP server.

DHCP Lease Stages

1. Lease Request - The client sends a broadcast requesting an IP address
2. Lease Offer - The server sends the above information and marks the offered address as unavailable. The message sent is a DHCPOFFER broadcast message.
3. Lease Acceptance - The first offer received by the client is accepted. The acceptance is sent from the client as a broadcast (DHCPREQUEST message) including the IP address of the DNS server that sent the accepted offer. Other DHCP servers retract their offers and mark the offered address as available and the accepted address as unavailable.
4. Server lease acknowledgement - The server sends a DHCPACK or a DHCPNACK if an unavailable address was requested.

DHCP discover message - The initial broadcast sent by the client to obtain a DHCP lease. It contains the client MAC address and computer name. This is a broadcast using 255.255.255.255 as the destination address and 0.0.0.0 as the source address. The request is sent, then the client waits one second for an offer. The request is repeated at 9, 13, and 16 second intervals with additional 0 to 1000 milliseconds of randomness. The attempt is repeated every 5 minutes thereafter. The client uses port 67 and the server uses port 68.

DHCP Lease Renewal

After 50% of the lease time has passed, the client will attempt to renew the lease with the original DHCP server that it obtained the lease from using a DHCPREQUEST message. Any time the client boots and the lease is 50% or more passed,

the client will attempt to renew the lease. At 87.5% of the lease completion, the client will attempt to contact any DHCP server for a new lease. If the lease expires, the client will send a request as in the initial boot when the client had no IP address. If this fails, the client TCP/IP stack will cease functioning.

DHCP Scope and Subnets

One DHCP scope is required for each subnet.

DHCP Relay Agents

May be placed in two places:

- Routers
- Subnets that don't have a DHCP server to forward DHCP requests.

Client Reservation

Client Reservation is used to be sure a computer gets the same IP address all the time. Therefore since DHCP IP address assignments use MAC addresses to control assignments, the following are required for client reservation:

- MAC (hardware) address
- IP address

Exclusion Range

Exclusion range is used to reserve a bank of IP addresses so computers with static IP addresses, such as servers may use the assigned addresses in this range. These addresses are not assigned by the DHCP server.

Sample DCHP Configuration File

In Linux, a sample configuration file is:

```
subnet 192.168.199.0 netmask 255.255.255.0 {
# --- default gateway
        option routers                  192.168.199.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "mynet.net";
        option domain-name              "mynet.net";
        option domain-name-servers      192.168.199.1;

        option time-offset              -5;     # Eastern Standard Time
#       option ntp-servers              192.168.199.1;
#       option netbios-name-servers     192.168.199.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;
```

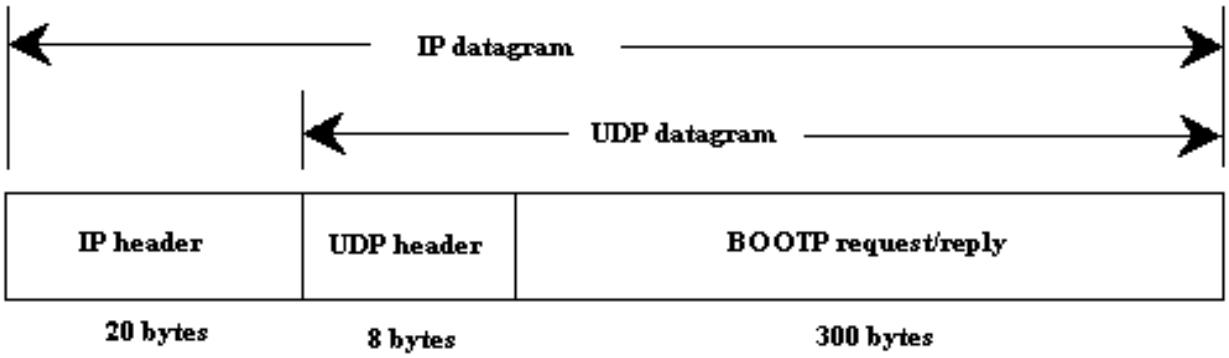
```
        default-lease-time 1209600;  # 2 weeks
        max-lease-time 1814400;          # 3 weeks

        range 192.168.199.10 192.168.199.250;

        # we want the nameserver to appear at a fixed address
        host nameserver {
                next-server nameserver.mynet.net;
                hardware ethernet 00:10:4b:ca:db:b5;
                fixed-address 192.168.199.1;
        }
}
```

This demonstrates that the IP addresses are based on lease times to the various clients. If they are not used within the period of their lease time by the client, those IP addresses are freed up for use by other clients.

BOOTP

BOOTP (Boot Protocol) may be used to boot remote computers over a network. BOOTP messages are encapsulated inside UDP messages and therefore it's requests and replies are forwarded by routers. BOOTP is defined by RFCs 951 and 1542. The drawing below illustrates the data encapsulation:

BOOTP Data Encapsulation



The diskless system reads its unique hardware address from its network interface card then sends a BOOTP request. The table below shows the BOOTP package format from most significant bit to least significant bit.

Bit range	# of Bits	Name	Description
0-7	8	Op code	Tells if the message is a BOOTP request or reply. Request=1, reply=2
8-15	8	Hardware type	Indicates the type of hardware (link level). A value of 6 indicates ethernet
16-23	8	Hardware address length	Tells the length in bytes of the hardware address number. Ethernet addresses are 6 bytes long.
23-31	8	Hop count	Initially set to 0. Incremented each time it is forwarded.
32-63	32	Transaction ID	A random number set by the client and returned by the server. Used to match replies with requests
64-79	16	Number of seconds	The time since the client started trying to bootstrap. Used to tell if a backup BOOTP server should respond.
80-95	16	unused	not used
96-127	32	Clients IP address	The clients IP address. If a request, it is normally 0.0.0.0
128-159	32	IP address for client	The server sets this in the reply message.

160-191	32	Server IP address	Filled in by the server.
192-223	32	Gateway IP address	Returned by the server.
224-351	128	Clients hardware address	Provided by the client.
352-1375	1024	Server hostname	A null terminated string optionally filled in by the server.
1376-3423	2048	Boot filename	A fully qualified boot file name with path information, terminated with a null. Supplied by the server.
3424-4447	1024	Vendor information	Used for various options to BOOTP including the subnet mask to the client.

The BOOTP server uses port 67 and the BOOTP client uses port 68. The following is a brief explanation of what happens when a remote client boots:

1. BOOTP request. The client sends a BOOTP request from 0.0.0.0.68 to 255.255.255.255.67 with its ethernet address and number of second's fields filled in.
2. BOOTP reply. The server responds with the client's IP address, the server's IP address (it's own), and the IP address of a default gateway.
3. ARP request. The client issues an ARP to tell if the IP address it just received is being used. It uses 0.0.0.0 as it's own address
4. ARP request. The client waits 0.5 seconds and repeats the same ARP request.
5. ARP request. The client waits another 0.5 seconds and repeats the ARP request with it's own address as the senders address.
6. BOOTP request. The client waits 0.5 seconds and sends another BOOTP request with its own IP address in the IP header
7. BOOTP reply. The server sends the same BOOTP reply it sent the last time.
8. ARP request. The client outputs an ARP request for the server hardware address
9. ARP reply. The server replies with its own ethernet address.
10. TFTP read request. The client sends a TFTP read request asking for its specified boot file.

RPC and NFS

Network File System (NFS)

NFS, defined by RFC 1094, is a method for client systems to use a filesystem on a remote host computer. NFS uses the UDP protocol and is supported by RPC.

Remote Procedure Call (RPC)

RPC, defined by RFC 1057, is a set of function calls used by a client program to call functions in a remote server program. The port mapper program is the program used to keep track of which ports programs supporting RPC functions use. The port mappers port is 111. In Redhat Linux the portmapper daemon is started in the /etc/rc.d/init.d/portmap and the daemon program is called "portmap".

The rpcinfo command

The command "rpcinfo -p" will show the port numbers that are assigned to the RPC services.

```
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100011    1   udp    747  rquotad
    100011    2   udp    747  rquotad
    100005    1   udp    757  mountd
    100005    1   tcp    759  mountd
    100005    2   udp    762  mountd
    100005    2   tcp    764  mountd
    100003    2   udp   2049  nfs
```

Services that may be listed include:

- rquotad - Enforces the set quotas for remote mounted NFS systems.
- mountd - Performs the requested mounts.
- nfs - Handles the user interface to the kernel module that performs NFS.

NFS related services in Linux include:

- amd - Runs the automount daemon for automatic remote filesystem mounting such as nfs. It is especially worthwhile for working with removeable media such as floppies or CD ROM disks.
- autofs - This is the startup, stop, and status script for the automount program used to configure

mount points for automatic mounting of file systems.

- nfs - Provides Network File System server services.
- netfs - Mounts and unmounts Network Fils System (NFS), Windows (SMB), and Netware (NCP) file systems. The mount command is used to perform this operation and no daemon is run in the background.

The /etc/exports file is used to configure exported filesystems.

Network Broadcasting and Multicasting

Network interface cards are usually programmed to listen for three types of messages. They are messages sent to their specific address, messages broadcast to all NICs, and messages that qualify as a multicast for the specific card. There are three types of addressing:

1. Unicast - A transmission to a single interface card.
2. Multicast - A transmission to a group of interface cards on the network.
3. Broadcast - A transmission to all interface cards on the network. RFC 919 and 922 describe IP broadcast datagrams.
    - Limited Broadcast - Sent to all NICs on the some network segment as the source NIC. It is represented with the 255.255.255.255 TCP/IP address. This broadcast is not forwarded by routers so will only appear on one network segment.
    - Direct broadcast - Sent to all hosts on a network. Routers may be configured to forward directed broadcasts on large networks. For network 192.168.0.0, the broadcast is 192.168.255.255.

All other messages are filtered out by the NIC software unless the card is programmed to operate in promiscuous mode to perform network sniffing.

Broadcasting

The types of broadcasting uses on TCP/IP that I know about are:

1. ARP on IP
2. DHCP on IP
3. Routing table updates. Broadcasts sent by routers with routing table updates to other routers.

The ethernet broadcast address in hexadecimal is FF:FF:FF:FF:FF:FF. There are several types of IP broadcasting:

1. The IP limited broadcast address is 255.255.255.255. This broadcast is not forwarded by a router.
2. A broadcast directed to a network has a form of x.255.255.255 where x is the address of a Class A network. This broadcast may be forwarded depending on the router program.
3. A broadcast sent to all subnetworks. If the broadcast is 10.1.255.255 on network 10.1.0.0 and the network is subnetted with multiple networks 10.1.x.0, then the broadcast is a broadcast to all subnetworks.
4. A broadcast sent to a subnet in the form 10.1.1.255 is a subnet broadcast if the subnet mask is 255.255.255.0.

Multicasting

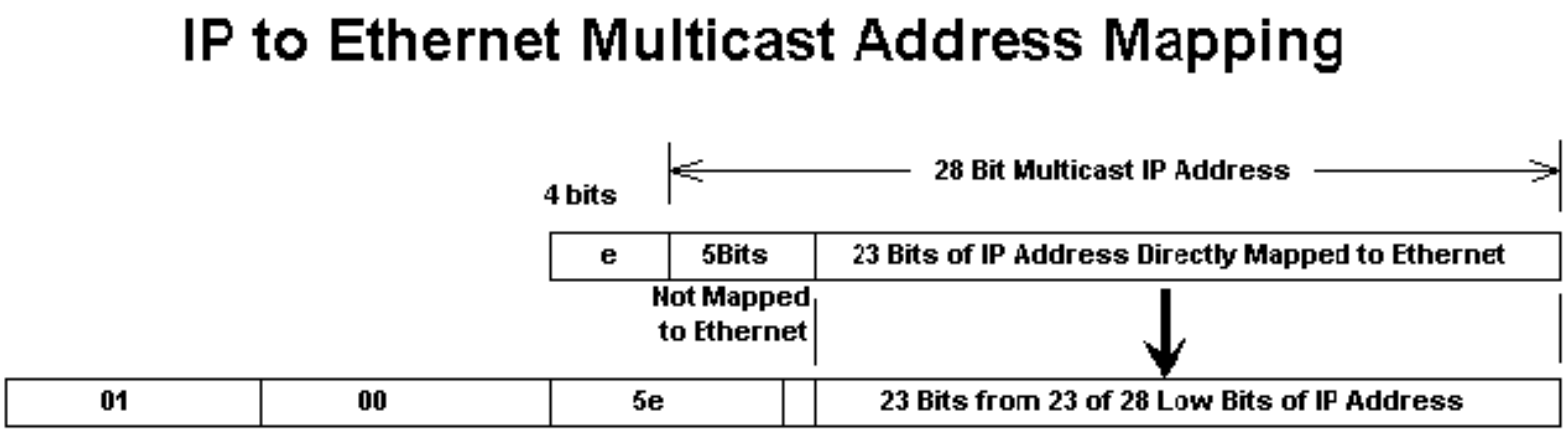
Multicasting may be used for streaming multimedia, video conferencing, shared white boards and more as the internet grows. Multicasting is still new to the internet and not widely supported by routers. New routing protocols are being developed to enable multicast traffic to be routed. Some of these routing protocols are:

- Hierarchical Distance Vector Multicast Routing Protocol (HDVMRP)
- Multicast Border Gateway
- Protocol Independent Multicast

Since IP is not a reliable network protocol, a new reliable multicast protocol that works at the transport layer and uses IP at the network layer has been developed. It is called Multicast Transport Protocol (MTP)

Ethernet Addressing:
The internet assigned numbers authority (IANA) allocates ethernet addresses from 01:00:5E:00:00:00 through 01:00:5E:7F:FF:FF for multicasting. This means there are 23 bits available for the multicast group ID.

IP Addressing:
An IP multicast address is in the range 224.0.0.0 through 239.255.255.255. In hexadecimal that is E0.00.00.00 to EF.FF.FF.FF. To be a multicast address, the first three bits of the most significant byte must be set and the fourth bit must be clear. In the IP address, there are 28 bits for multicasting. Therefore there are 5 multicasting bits that cannot be mapped into an ethernet data packet. The 5 bits that are not mapped are the 5 most significant bits.



The 28 IP multicast bits are called the multicast group ID. A host group listening to a multicast can span multiple networks. There are some assigned hostgroup addresses by the internet assigned numbers authority (IANA). Some of the assignments are listed below:

- 224.0.0.1 = All systems on the subnet
- 224.0.0.2 = All routers on the subnet
- 224.0.1.1 = Network time protocol (NTP)
- 224.0.0.9 = For RIPv2
- 224.0.1.2 = Silicon graphic's dogfight application

Being on the MBONE means you are on a network that supports multicasting. Usually you must check with your internet service provider (ISP) to see if you have this capability. IGMP described in the next section is used to manage broadcast groups.

Internet Group Management Protocol

Internet Group Management Protocol (IGMP) is the protocol used to suooprt multicasting. To use multicasting, a process on a host must be able to join and leave a group. A process is a user program that is using the network. Group access is identified by the group address and the interface (NIC). A host must keep track of the groups that at least one process belongs to and the number of processes that belong to the group. IGMP is defined in RFC 1112.

IGMP messages are used by multicast routers to track group memberships on each of its networks. It uses these rules:

1. The first time a process on a host joins a multicast group, the host will send an IGMP report. This means that every time the host needs to receive messages from a new group to support its processes, it will send a report.
2. Multicast routers will send IGMP queries regularly to determine whether any hosts are running processes that belong to any groups. The group address of the query is set to 0, the TTL field is set to 1, and the destination IP address is 224.0.0.1 which is the all hosts group address which address all the multicast capable routers and hosts on a network.
3. A host sends one IGMP response for each group that contains one or more processes. The router expects one response from each host for each group that one or more of its processes require access to.
4. A host does not send a report when its last process leaves a group (when the group access is no longer required by a process). The multicast router relies on query responses to update this information.

IGMP is defined in RFC 1112. Hosts and routers use IGMP to support multicasting. Multicast routers must know which hosts belong to what group at any given point of time. The IGMP message is 8 bytes. consisting of:

1. Bits 0 to 3 - IGMP version number
2. Bits 4 to 7 - IGMP type. 1=query sent by a multicast router. 2 is a response sent by a host.
3. Bits 8 to 15 - unused
4. Bits 16 to 31 - Checksum
5. The last 4 bytes - 32 bit group address which is the same as the class D IP address.

IGMP message formats are encapsulated in an IP datagram which contain a time to live (TTL) field. The default is to set the TTL field to 1 which means the datagram will not leave its subnetwork. an application can increase its TTL field in a message to locate a server distance in terms of hops.

Addresses from 224.0.0.0 to 224.0.0.255 are not forwarded by multicast routers since these addresses are intended for applications that do not need to communicate with other networks. Therefore these

addresses can be used for group multicasting on private networks with no concern for addresses being used for multicasting on other networks.

Dynamic Routing

Dynamic routing performs the same function as static routing except it is more robust. Static routing allows routing tables in specific routers to be set up in a static manner so network routes for packets are set. If a router on the route goes down the destination may become unreachable. Dynamic routing allows routing tables in routers to change as the possible routes change. There are several protocols used to support dynamic routing including RIP and OSPF.

Routing cost

Counting route cost is based on one of the following calculations:

- Hop count - How many routers the message must go through to reach the recipient.
- Tic count - The time to route in 1/18 seconds (ticks).

Dynamic routing protocols do not change how routing is done. They just allow for dynamic altering of routing tables.
There are two classifications of protocols:

1. IGP - Interior Gateway Protocol. The name used to describe the fact that each system on the internet can choose its own routing protocol. RIP and OSPF are interior gateway protocols.
2. EGP - Exterior Gateway Protocol. Used between routers of different systems. There are two of these, the first having the same name as this protocol description:
    1. EGP - Exterior Gateway Protocol
    2. BGP - Border Gateway Protocol.

The daemen "routed" uses RIP. The daemon "gated" supports IGP's and EGP's.

Route Discovery Methods

- Distance vector - Periodically sends route table to other routers. Works best on LANs, not WANs.
- Link-state - Routing tables are broadcast at startup and then only when they change. OSPF uses link-state.

Routing Information Protocol (RIP)

The RIP RFC is 1058.
The routing daemon daemon adds a routing policy to the system. If there are multiple routes to a destination, it chooses the best one. The RIP message can con contain information on up to 25 routes.
The RIP message contains the following components:

1. Command
2. Version - Normally 1 but set to 2 for RIP version 2.
3. family - Set to 2 for IP addresses.
4. IP address - 32 bit IP address
5. Metrics - Indicate the number of hops to a given network, the hop count.

RIP sends periodically broadcasts its routing table to neighboring routers. The RIP message format contains the following commands:

- 1 - request
- 2 - reply
- 3 & 4 - obsolete
- 5 - poll entry
- 6 - Asks for system to send all or part of routing table

When the daemon "routed" starts, it sends a request out all its interfaces for other router's routing tables. The request is broadcast if the network supports it. For TCP/IP the address family in the message is normally 2, but the initial request has address family set to 0 with the metric set to 16.

Regular routing updates are sent every 30 seconds with all or part of the route table. As each router sends routing tables (advertises routes to networks its NICs interface to) routes are determined to each network.

Drawbacks of RIP:

- RIP has no knowledge of subnet addressing
- It takes a long time to stabilize after a router or link failure.
- Uses more broadcasting than OSPF requiring more network bandwidth.

RIP Version 2

Defined by RFC 1388. It passes further information in some of the fields that are set to 0 for the RIP protocol. These additional fields include a 32 bit subnet mask and a next hop IP address, a routing domain, and route tag. The routing domain is an identifier of the daemon the packet belongs to. The route tags supports EGPs.

Open Shortest Path First (OSPF)

OSPF (RFC 1257) is a link state protocol rather than a distance vector protocol. It tests the status of its link to each of its neighbors and sends the acquired information to them. It stabilizes after a route or link failure faster than a distance vector protocol based system. OSPF uses IP directly, not relying on TCP or UDP. OSPF can:

- Have routes based on IP type of service (part of IP header message) such as FTP or Telnet.
- Support subnets.
- Assign cost to each interface based on reliability, round trip time, etc.
- Distribute traffic evenly over equal cost routes.
- Uses multicasting.

Costs for specific hops can be set by administrators. Adjacent routers swap information instead of broadcasting to all routers.

Border Gateway Protocol (BGP)

Described by RFC 1267, 1268, and 1497. It uses TCP as a transport protocol. When two systems are using BGP, they establish a TCP connection, then send each other their BGP routing tables. BGP uses distance vectoring. It detects failures by sending periodic keep alive messages to its neighbors every 30 seconds. It exchanges information about reachable networks with other BGP systems including the full path of systems that are between them.

Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) is used to send mail across the internet. There are four types of programs used in the process of sending and receiving mail. They are:

- MUA - Mail users agent. This is the program a user will use to type e-mail. It usually incorporates an editor for support. The user types the mail and it is passed to the sending MTA.
- MTA - Message transfer agent is used to pass mail from the sending machine to the receiving machine. There is a MTA program running on both the sending and receiving machine. Sendmail is a MTA.
- LDA - Local delivery agent on the receiving machine receives the mail from its MTA. This program is usually procmail.
- Mail notifier - This program notifies the recipient that they have mail. Normally this requires two programs, biff and comsat. Biff allows the administrator or user to turn on comsat service.

The MTA on both machines use the network SMTP (simple mail transfer protocol) to pass mail between them, usually on port 25.

Other components of mail service include:

- Directory services - A list of users on a system. Microsoft provides a Global Address List and a Personal Address Book.
- Post Office - This is where the messages are stored.

Mail Protocols

- SMTP - Simple Mail Transport Protocol is used on the internet, it is not a transport layer protocol but is an application layer protocol.
- POP3 - Post Office Protocol version 3 is used by clients to access an internet mail server to get mail. It is not a transport layer protocol.
- IMAP4 - Internet Mail Access Protocol version 4 is the replacement for POP3.
- MIME - Multipurpose Internet Mail Extension is the protocol that defines the way files are attached to SMTP messages.
- X.400 - International Telecommunication Union standard defines transfer protocols for sending mail between mail servers.
- MHS - Message Handling Service by Novell is used for mail on Netware networks.

Directory Services

- Lightweight Directory Access Protocol (LDAP)
- X.500 - This is a recommendation outlining how an organization can share objects and names on a

large network. It is hierarchical similar to DNS, defining domains consisting of organizations, divisions, departments, and workgroups. The domains provide information about the users and available resources on that domain, This X.500 system is like a directory. Its recommendation comes from the International Telegraph and Telephone Consultative Committee (CCITT)

Mail API

Mail application programming interfaces (APIs) allow e-mail support to be integrated into application programs.

- MAPI - Microsoft's Messaging API which is incorporated throughout Microsoft's office products supports mail at the application level
- VIM - Vendor-Independent Messaging protocol from Lotus is supported by many vendors exclusive of Microsoft.

Three parts of a mail message:

1. Envelope - Includes recipient and sender addresses using the MAIL and RCPT commands.
2. Headers - Each header has a name followed by a colon and its value. Some headers are From, Date, Reply To, Received, Message ID, To, and Subject.
3. Body - The contents of the message sent in 7 bit ASCII code.

SMTP Commands:

- HELO - Sent by client with domain name such as mymachine.mycompany.com.
- MAIL - From <myself@mymachine.mycompany.com>
- RCPT - To <myfriend@theirmachine.theirorg.org>
- DATA - Sends the contents of the message. The headers are sent, then a blank line, then the message body is sent. A line with "." and no other characters indicates the end of the message.
- QUIT

If you recall from the DNS section mail servers are specified in DNS configuration files as follows:

```
dept1.mycompany.com.    IN      MX      5       mail.mycompany.com.
dept1.mycompany.com.    IN      MX      10      mail1.mycompany.com.
dept1.mycompany.com.    IN      MX      15      mail2.mycompany.com.
```

The host dept1.mycompany.com may not be directly connected to the internet or network but may be connected periodically using a PPP line. The servers mail, mail1, and mail2 are used as mail forwarders to send mail to the host dept1. The one with the lowest number, 5, is normally used for sending the mail, but the others are used when the first one or ones are down.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is used as the transport protocol for network management. Network management consists of network management stations communicating with network elements such as hosts, routers, servers, or printers. The **agent** is the software on the network element (host, router, printer) that runs the network management software. Therefore when the word agent is used it is referring to the network element. The agent will store information in a **management information base (MIB)**. Management software will poll the various network devices and get the information stored in them. RFC 1155, 1157, and 1213 define SNMP with RFC 1157 defining the protocol itself. The manager uses UDP port 61 to send requests to the agent and the agent uses UDP port 62 to send replies or messages to the manager. The manager can ask for data from the agent or set variable values in the agent. Agents can reply and report events.

There are three supporting pieces to TCP/IP network management:

1. Management Information BASE (MIB) specifies variables the network elements maintain.
2. A set of common structures and a way to reference the variables in the database.
3. The protocol used to communicate between the manager and the network element agent which is SNMP.

SNMP collects information two ways:

1. The devices on the network are polled by management stations.
2. Devices send alerts to SNMP management stations. The public community may be added to the alert list so all management stations will receive the alert.

SNMP must be installed on the devices to do this. SNMP terms:

- Baseline - A report outlining the state of the network.
- Trap - An alert that is sent to a management station by agents.
- Agent - A program at devices that can be set to watch for some event and send a trap message to a management station if the event occurs.

The network manager can set the threshold of the monitored event that will trigger the sending of the trap message. SNMP enables counters for monitoring the performance of the network used in conjunction with Performance Monitor.

SNMP Communities

An SNMP community is the group that devices and management stations running SNMP belong to. It

helps define where information is sent. The community name is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are:

- Write = private
- Read = public

SNMP Security

SNMP should be protected from the internet with a firewall. Beyond the SNMP community structure, there is one trap that adds some security to SNMP.

- Send Authentication Trap - When a device receives an authentication that fails, a trap is sent to a management station.

Other configuration parameters that affect security are:

- Accepted Community Names - Only requests from computers in the list of community names will be accepted.
- Accept SNMP Packets from Any Host - This is checked by default. Setting specific hosts will increase security.
- Only Accept SNMP Packets from These Hosts - Only requests from hosts on the list of IP addresses are accepted. Use IP, or IPX address or host name to identify the host.

SNMP Message Types

There are five types of messages exchanged in SNMP. They are referred to by Protocol Data Unit (PDU) type.

PDU Type	Name	Description
0	get-request	Get one or more variables .(manager to element)
1	get-next-request	Get next variable after one or more specified variables. (manager to element)
2	set-request	Set one or more variables. (manager to element)
3	get-response	Return value of one or More variables. (element to manager)
4	trap	Notify manager of an event. (element to manager)

The SNMP message with PDU type 0-3 consists of:

1. Version of SNMP
2. Community - A clear text password character string
3. PDU type
4. Request ID - Used to associate the request with the response. For PDU 0-2, it is set by the manager.
5. error status - An integer sent by the agent to identify an error condition

Error	Name	Description
0	no error	OK
1	too big	Reply does not fit into one message
2	no such name	The variable specified does not exist
3	bad value	Invalid value specified in a set request.
4	read only	The variable to be changed is read only.
5	general error	General error

6. error index - Specifies which variable was in error when an error occurred. It is an integer offset.
7. name - The name of the variable (being set or read).
8. value - The value of the variable (being set or read)
9. any other names and values to get/set

The SNMP message with PDU type 4 (trap) consists of:

1. PDU type
2. Enterprise - The agents OBJECT IDENTIFIER or system objects ID. Falls under a node in the MIB tree.
3. agent addr - The IP address of the agent.
4. Trap type - Identifies the type of event being reported.

Trap Type	Name	Description
0	cold start	Agent is booting
1	warm start	Agent is rebooting
2	link down	An interface has gone down
3	link up	An interface has come up
4	authentification failure	An invalid community (password) was received in a message.
5	egp neighbor loss	An EGP peer has gone down.
6	enterprise specific	Look in the enterprise code for information on the trap

5. Specific code - Must be 0.
6. Time stamp - The time in 1/100ths of seconds since the agent initialized.
7. name
8. Value
9. Any other names and values

Types of data used:

- INTEGER - Some have minimum and maximum values.
- OCTET STRING - The number of bytes in the string is before the string.
- DISPLAY STRING - Each byte must be an ASCII value
- OBJECT IDENTIFIER - Specifies a data type allocated by an organization with responsibility for a group of identifiers. A sequence of integers separated by decimals which follow a tree structure.
- NULL - Used as the value of all variables in a get request.
- IpAddress - A 4 byte long OCTET STRING. One byte for each byte of the IP address.
- PhysAddress - A 6 byte octet string specifying an ethernet or hardware address.
- Counter - A 32 bit unsigned integer
- GaugeAn unsigned 32 bit integer with a value that can increase or decrease but wont fall below a minimum or exceed a maximum.
- TimeTicks - Time counter. Counts in 1/100 of seconds.
- SEQUENCE - Similar to a programming structure with entries of type IPAddress called udpLocalAddress and type INTEGER called udpLocalPort.
- SEQUENCE OF - An array with elements with one type.

The MIB data structure RFC 1213

In the above list the data type "OBJECT IDENTIFIER" is listed as a part of the management information database. These object identifiers are referenced very similar to a DNS tree with a directory at the top called root. Each node in the tree is given a text name and is also referenced numerically similar to IP addresses. There are multiple levels in the tree with the bottom level being variables, and the next one up is called group. The packets sent in SNMP use numeric identifiers rather than text. All identifiers begin with iso(1).org(3).dod(6).internet(1).mgmt(2).mib(1). Numerically, that is 1.3.6.1.2.1. In text it is "iso.org.dod.internet.mgmt.mib". Under mib are the following groups. The information in these groups is not complete and you should refer to the RFC for full information.

1. system
    1. sysDesc (DisplayString) - Description of entity
    2. sysObjectID (ObjectID) - Vendors ID in the subtree (1.3.6.1.4.1.
    3. sysUPTime (Timer) - Time the system has been up
    4. sysContact (DisplayString) - Name of contact person
    5. sysName (DisplayString) - Domain name of the element such as mymachine.mycompany.com
    6. sysLocation (DisplayString) - Physical location of the element.
    7. sysServices 0x1-physical, 0x02-datalink, 0x04-internet, 0x08 end to end, 0x40-application. If the bit is set the service is provided
2. interfaces
    1. ifNumber (INTEGER) - Number of network interfaces
    2. ifTable (table)

1. ifIndex
2. ifDescr - Description of interface
3. ifType - 6=ethernet, 7=802.3 ethernet, 9=802.5 token ring, 23 = PPP, 28=SLIP
4. ifMtu
5. ifSpeed - Bits/second
6. ifPhysAddress
7. ifAdminStatus - Desired state of interface 1=up, 2=down, 3=testing
8. ifOperStatus - Current state of interface 1=up, 2=down, 3=testing
9. ifLastchange
10. ifInOctets - Total bytes received
11. ifInUcastPkts
12. ifInNUcastPkts
13. ifInDiscards
14. ifInErrors
15. ifInUnknownProtos
16. ifOutOctets
17. ifOutUcastPkts
18. ifOutNUcastPkts
19. ifOutDiscards
20. ifOutErrors
21. ifOutQLen
22. ifSpecific

3. at - Address translation group
    1. atIfIndex (INTEGER) - Interface number
    2. atPhysAddress (PhyAddress)
    3. atNetAddress (NetworkAddress) - IP address
4. ip
    1. ipForwarding
    2. ipDefaultTTL (INTEGER)
    3. ipInReceives (counter)
    4. ipInHdrErrors (counter)
    5. ipInAddrErrors (counter)
    6. ipForwDatagrams (counter)
    7. ipInUnknownProtos (counter)
    8. ipInDiscards (counter)
    9. ipInDelivers (counter)
    10. ipOutRequests (counter)
    11. ipOutDiscards (counter)
    12. ipOutNoRoutes (INTEGER)
    13. ipReasmTimeout (counter)
    14. ipReasmReqds (counter) - Number of IP fragments received that need to be reassembled.
    15. ipReasmOKs (counter)
    16. ipReasmFails (counter)

17. ipFragOKs (counter)
18. ipFragFails (counter)
19. ipFragCreates (counter)
20. ipRoutingDiscards (counter)
21. ipAddrTable (table)
    1. ipAddrEntry (index)
        1. ipAdEntAddr
        2. ipAdEntIfIndex
        3. ipAdEntNetMask
        4. ipAdEntBcastAddr
        5. ipAdEntReasmMaxSize
5. icmp
6. tcp
7. udp
    1. udpInDatagrams (counter) - UDP datagrams delivered to user processes.
    2. udpNoPorts (counter) - UDP datagrams which were not received at the port since there was no application to receive it.
    3. udpInErrors (counter) - Number of UDP datagrams not delivered for reasons other than no applications available to receive them.
    4. udpOutDatagrams (counter) - Number of UDP datagrams sent.
    5. udpTable (table)
        1. udpEntry - Specifies the table entry number
            1. udpLocalAddress
            2. udpLocalPort

The ordering of data in the MIB is numeric. When the getnext function is used it gets the next data based on the numeric ordering.

Network Services

Networking Services and Ports

There are two general types of network services, which are connection less and connection oriented. Connection oriented service performs connection establishment, data transfer, and connection termination.

Ping

The "ping" program uses ICMP echo message requests and listens for ICMP echo message reply messages from its intended host. Using the -R option with ping enables the record route feature. If this option is used ping will set the record route (RR) in the outgoing ICMP IP datagram

Traceroute

The "traceroute" program uses ICMP messaging and the time to live (TTL) field in the IP header. It works by sending a packet to the intended host with a TTL value of 1. The first router will send back the ICMP "time exceeded" message to the sending host. Then the traceroute program will send a message with a TTL of 2, then 3, etc. This way it will get information about each router using the information received in the ICMP packets. To get information about the receiving host, the message is sent to a port that is not likely to be serviced by that host. A ICMP "port unreachable" error message is generated and sent back.

Telnet

Some telnet command codes and their meanings

Command Code	Description
236	EOF
237	SUSP - Suspend the current process
238	ABORT - Abort process
239	EOR - End of record
240	SE - Suboption end
241	NOP - No operation
242	DM - Data Mark
243	BRK - Break

244	IP - Interrupt process
245	AO - Abort output
246	AYT - Are you there
247	EC - Escape character
248	EL - Erase Line
249	GA - Go ahead
250	SB - Suboption begin
251	WILL - Sender wants to enable option / Receiver says OK
252	WONT - Sender wants to disable option / Receiver says not OK
253	DO - Sender wants receiver to enable option / Receiver says OK
254	DONT - Sender wants receiver to disable option / Receiver says not OK

On items 251 through 254 above, a third byte specifies options as follows:

ID	Name	RFC
1	Echo	857
3	Supress go ahead	858
5	Status	859
6	Timing Mark	860
24	Terminal type	1091
31	Window size	1073
32	Terminal speed	1079
33	Remote flow control	1372
34	Line mode	1184
36	Environment variables	1408

Network Drivers

Driver interfaces allow multiple protocol stacks to use one network interface card. The two in use today are listed below. they are not compatible with each other.

Open Driver Interface (ODI)

ODI is normally found on NetWare networks and was developed by Novell and Apple. It consists of:

- Multiple Protocol Interface - Provides connectivity from the data link layer to the network layer.
- Link Support Layer - It includes functions for managing protocol stack assignments and coordinating numbers assigned to MLIDs.
- Multiple-Link Interface Driver (MLID) - Passes data between the data link layer and the hardware or the network media. The drivers are protocol-independent.

Allows multiple drivers to be used on one card and lets one protocol use multiple cards.

Network Driver Interface Specification (NDIS)

NDIS, from Microsoft, is used on Microsoft networks. It allows multiple protocols to be used on a network card and supports the data link layer of the network model.

Transport Driver Interface (TDI)

This is a standard for passing messages between the drivers at the data link layer and the protocols working at the network layer such as IP or NetBEUI. It was produced by Microsoft.

Network Operating Systems

Network operating systems (NOS) typically are used to run computers that act as servers. They provide the capabilities required for network operation. Network operating systems are also designed for client computers and provide functions so the distinction between network operating systems and stand alone operating systems is not always obvious. Network operating systems provide the following functions:

- File and print sharing.
- Account administration for users.
- Security.

Installed Components

- Client functionality
- Server functionality

Functions provided:

- Account Administration for users
- Security
- File and print sharing

Network services

- File Sharing
- Print sharing
- User administration
- Backing up data

Universal Naming Convention (UNC)

A universal naming convention (UNC) is used to allow the use of shared resources without mapping a drive to them. The UNC specifies a path name and has the form:

\\servername\pathname

If I have a Linux server called "linux3" with a folder named "downloads" with a file called "readme.txt" in the folder, the UNC is:

\\linux3\downloads\readme.txt

Network Applications

There are three categories of applications with regard to networks:

1. Stand alone applications - Includes editors
2. Network versions of stand alone applications - May be licensed for multiple users.
3. Applications only for a network include databases, mail, group scheduling, groupware.

Models for network applications

1. Client-server - Processing is split between the client which interacts with the user and the server performing back end processing.
2. Shared file systems - The server is used for file storage and the processing of the file is done on the client computer.
3. Applications that are centralized - An example is a Telnet session. The data and the program run on the central computer and the user uses an interface such as the Telnet client or X server to send commands to the central computer and to see the results.

E-mail Systems

- Novell GroupWise - Also called Windows Messaging
- Microsoft Mail
- Microsoft Exchange - This is for the Microsoft Exchange Server. There is a Microsoft Exchange client for the Microsoft Exchange server and a client for an internet mail account only.
- Lotus Notes
- cc:Mail - From Lotus and IBM

There are several types of programs used in the process of sending and receiving mail. They are:

- MUA - Mail users agent. This is the program a user will use to type e-mail. It usually incorporates an editor for support. The user types the mail and it is passed to the sending MTA. This may also be called the user agent (UA).
- MTA - Message transfer agent is used to pass mail from the sending machine to the receiving machine. There is a MTA program running on both the sending and receiving machine. Sendmail is a MTA.
- MS - Message Store is a storage area for messages that can't be delivered immediately when the recipient is off-line.
- AU - Access Unit provides access to resources like fax, telex, and teletex.
- LDA - Local delivery agent on the receiving machine receives the mail from its MTA. This program is usually procmail.
- Mail notifier - This program notifies the recipient that they have mail. Normally this requires two

programs, biff and comsat. Biff allows the administrator or user to turn on comsat service.

Other components of mail service include:

- Directory services - A list of users on a system. Microsoft provides a Global Address List and a Personal Address Book.
- Post Office - This is where the messages are stored.

Mail API

Mail application programming interfaces (APIs) allow e-mail support to be integrated into application programs.

- MAPI - Microsoft's Messaging API incorporated throughout Microsoft's office products provides support for mail at the application level.
- VIM - Vendor-Independent Messaging protocol from Lotus is supported by many vendors exclusive of Microsoft.

Message Handling Service (MHS)

- MHS and Global MHS by Novell
- MHS by OSI - It is called MOTIS (message-oriented text interchange system).

X.500

This is a recommendation outlining how an organization can share objects and names on a large network. It is hierarchical similar to DNS, defining domains consisting of organizations, divisions, departments, and workgroups. The domains provide information about the users and available resources on that domain, This X.500 system is like a directory. Its recommendation comes from the International Telegraph and Telephone Consultative Committee (CCITT).

Scheduling systems

- Microsoft Schedule+
- Lotus Organizer

Groupware

Used for various electronic communication to enable a group to work together better. Functions may include group discussion, submission of reports and time sheets electronically, an on line help desk

database, forms design and access, and creating a document as a group such as configuration management.

Database Management Systems (DBMS)

They are used to share data on a network. DBMS standards for distributed databases:

- SQL - Structured Query Language is a database access language. It is used by most client/server database applications.
- ODBC - Open Database Connectivity (ODBC) from Microsoft lets application developers integrate database connections in applications. It is an application programming interface (API). ODBC drivers convert an application's query int SQL and send it to the database engine program.
- DRDA - Distributed Relational Database Architecture is from IBM.

When information is processed in a distributed database, it is called a transaction. The two phases of a transaction are:

1. Write or Update - The data is temporarily updated. An abort can cancel what this phase did by removing the changed data from a temporary storage area.
2. Commit - The changed data is made permanent in the database.

Databases store multiple copies of the data which is called replication. They must be sure the various copies of the database on various servers is accurate with identical data. Data is also partitioned into smaller blocks of data.

Wide Area Networks

Wide Area Networks (WAN) refers to the technologies used to connect offices at remote loactions. The size of a network is limited due to size and distance constraints. However networks may be connected over a high speed communications link (called a WAN link) to link them together and thus become a WAN. WAN links are usually:

- Dial up connection
- Dedicated connection - It is a permanent full time connection. When a dedicated connection is used, the cable is leased rather than a part of the cable bandwidth and the user has exclusive use.
- Switched network - Several users share the same line or the bandwidth of the line. There are two types of switched networks:
    1. Circuit switching - This is a temporary connection between two points such as dial-up or ISDN.
    2. Packet switching - This is a connection between multiple points. It breaks data down into small packets to be sent across the network. A virtual circuit can improve performance by establishing a set path for data transmission. This will shave some overhead of a packet switching network. A variant of packet switching is called cell-switching where the data is broken into small cells with a fixed length.

WAN Connection Technologies

- **X.25** - This is a set of protocols developed by the CCITT/ITU which specifies how to connect computer devices over a internetwork. These protocols use a great deal of error checking for use over unreliable telephone lines. Their speed is about 64Kbps. Normally X.25 is used on packed switching PDNs (Public Data Networks). A line must be leased from the LAN to a PDN to connect to an X.25 network. A PAD (packet assembler/disassembler) or an X.25 interface is used on a computer to connect to the X.25 network. CCITT is an abbreviation for International Telegraph and Telephone Consultative Committee. The ITU is the International Telecommunication Union.
- **Frame Relay** - Error checking is handled by devices at both sides of the connection. Frame relay uses frames of varying length and it operates at the data link layer of the OSI model. A permanent virtual circuit (PVC) is established between two points on the network. Frame relay speed is between 56Kbps and 1.544Mbps. Frame relay networks provide a high-speed connection up to 1.544Mbps using variable-length packet-switching over digital fiber-optic media.
- **Switched Multi-megabit Data Service (SMDS)** - Uses fixed length cell switching and runs at speeds of 1.533 to 45Mbps. It provides no error checking and assumes devices at both ends provide error checking.
- **Telephone connections**
    - Dial up
    - Leased lines - These are dedicated analog lines or digital lines. Dedicated digital lines are

called digital data service (DDS) lines. A modem is used to connect to analog lines, and a Channel Service Unit/Data Service Unit or Digital Service Unit(CSU/DSU) is used to connect to digital lines. The DSU connects to the LAN and the CSU connects to the line.

- T Carrier lines - Multiplexors are used to allow several channels on one line. The T1 line is basic T Carrier service. The available channels may be used separately for data or voice transmissions or they may be combined for more transmission bandwidth. The 64Kbps data transmission rate is referred to as DS-0 (Digital Signal level 0) and a full T1 line is referred to as DS-1.

Signal	System	Total Kbps	Channels	Number of equivalent T1 lines
DS-1	T1	1544	24	1
DS-2	T2	6312	96	4
DS-3	T3	44736	672	28
DS-4	T4	274760	4032	3668

T1 and T3 lines are the most common lines in use today. T1 and T2 lines can use standard copper wire. T3 and T4 lines require fiber-optic cable or other high-speed media. These lines may be leased partially called fractional T1 or fractional T3 which means a customer can lease a certain number of channels on the line. A CSU/DSU and a bridge or router is required to connect to a T1 line.

- Integrated Services Digital Network (ISDN) - Comes in two types and converts analog signals to digital for transmission.
  - Basic Rate ISDN (BRI) - Two 64Kbps B-channels with one 16Kbps D channel. The D-channel is used tor call control and setup.
  - Primary Rate ISDN (PRI) - 23 B-channels and one D channel.

  A device resembling a modem (called an ISDN modem) is used to connect to ISDN. The computer and telephone line are plugged into it.
- Switched-56 - A switched line similar to a leased line where customers pay for the time they use the line.

- **Asynchronous Transfer Mode (ATM)** - May be used over a variety of media with both baseband and broadband systems. It uses fixed length data packets of 53 bytes called cell switching. 5 bytes contain header information. It uses hardware devices to perform the switching of the data. Speeds of up to 622 Mbps can be achieved. Error checking is done at the receiving device, not by ATM. A permanent virtual connection is established (PVC).
- **Synchronous Optical Network (SONET)** - a physical layer standard that defines voice, data, and video delivery methods over fiber optic media. It defines data rates in terms of optical carrier (OC) levels. The transmission rate of OC-1 is 51.8 Mbps. Each level runs at a multiple of the first. The OC-5 data rate is 5 times 51.8 Mbps which is 259 Mbps. SONET also defines synchronous transport signals (STS) for copper media which use the same speed scale of OC levels. STS-3 runs at the same speed of OC-3. Mesh or ring topology is used to support SONET. SONET uses multiplexing. The ITU has incorporated SONET into their Synchronous Digital Hierarchy (SDH) recommendations.

Network Backup

Items to do when considering network backups.

- Set a backup schedule
- Determine data to be backed up and its importance to determine a backup schedule.
- Determine backup methods, media, and equipment to use. Backup methods include full backup, file copy, backup changed files without marking files as backed up (differential backup), or backup only the files that have changed since the last backup and mark them as backed up (incremental backup).
- Determine where to store backup information such as a safe.
- Test the backup and restore capability of the backup system and its media to be sure it really works.
- Maintain backup logs.
- Create and maintain a disaster recover plan. Rotate tapes so you could recover your data if your server room or main place of operations was destroyed.

Network Fault Tolerance

Redundant Array of Inexpensive disks (RAID)

RAID is a fault tolerant method of storing data, meaning that a failure can occur and the system will still function. The various RAID categories are:

- 0 - Disk striping - Data is written across multiple drives in parallel. Different parts of the data is written at the same time to more than one drive. If there are two drives, half the data is written to one drive, while the rest of the data is written to the other drive. All partitions on striped drives must be the same size. No fault tolerance is provided with RAID-0.
- 1 - Disk mirroring - All the data is written to two drives so each drive has a complete of all stored data. If one drive fails, the other can be used to get a copy of the data. To be more fault tolerant, more than one controller card may be used to control the mirrored hard drives. This is called disk duplexing and will allow the system to keep functioning if one controller card fails.
- 2 - Disk striping with error correction codes (ECC).
- 3 - Disk striping with ECC parity information stored on a separate drive.
- 4 - Disk striping with blocks with parity information stored on a separate drive.
- 5 - Disk striping with blocks with parity information stored using multiple drives. Uses five disks with one fifth of each one to store parity information.

Sector Sparing

Sector sparing will detect when data is going to be read from or written to a bad sector on the hard drive and will move the data to a good sector. The bad sector is marked as not available so it is not used again.

Windows NT support

Supports RAID-0,1, and 5 along with sector sparing.

Terms:

- DAT - Digital Audio Tape
- Sector Sparing - A method of fault tolerance that automatically identifies and marks bad sectors as not available. It is also called hot-fixing.
- SLED - Single Large Inexpensive disk - The concept that a large disk costs less per amount of storage than several smaller ones. Somehow this concept is used as a means of fault tolerance.

Network Troubleshooting

Documentation

Document the network installation and configuration

- Cable installation information - Cable types with network diagrams showing jacks
- Equipment information - Where the equipment was purchased with serial numbers, vendors and warranty information.
- Network resources - Document commonly used resources including drive mappings.
- Network addressing - Record the allocation of network addresses with diagrams.
- Network connections - Document or diagram how your network is connected to other networks.
- Software configuration - Software is installed on each network node outlining the sequence of software and driver installation required. Also document configuration files.
- User administration - Determine methods and policies for user names, passwords, and groups.
- Policies and procedures - Be sure network policies and procedures are defined and necessary personnel are aware of them.
- Base network performance - Determine normal traffic levels on the network.
- Hardware or software changes - document all changes to the network and record dates.
- Software licenses - Be sure you have valid software licenses for all software with license serial numbers recorded.
- Keep a history of troubleshooting - Record network problems and their solutions.

Troubleshooting and network management tools

- SMS - Systems Management Server from Microsoft can collect information of software on each computer and can install and configure new software on the client computers. It will also monitor network traffic.

Performance Monitoring Benefits

- Identify network bottlenecks.
- Identifying network traffic pattern trends.
- Provide information to help develop plans for increasing network performance.
- Determine the effects of hardware or software changes.
- Provide information to help forecast future needs.

Microsoft Complex Problem Structured Approach

1. Set the problem's priority

2. Identify the symptoms.
3. Determine possible causes.
4. Perform tests to determine the problem cause.
5. Identify a solution by studying the test results.

Troubleshooting Tools

- DVM - Digital volt meter.
- TDR - Time-domain reflectometer sends a sonar like electrical pulse down a cable and can determine the location of a break in the cable. The pulse is reflected back to the TDR and the TDR can tell where the break is by timing the time it takes for the pulse to return.
- Advanced Cable testers -
- Protocol analyzers - They are usually a mix of hardware and software and may also be referred to as network analyzers. They monitor network traffic and examining packets, collecting data that helps determine the network performance. They can locate:
    - Faulty NICs or components
    - Network bottlenecks
    - Abnormal network traffic from a computer
    - Conflicting applications
    - Connection errors

  Windows NT Server 4.0 includes the Network Monitor tool which is a software based protocol analyzer.
- Advanced cable testers - Can determine a cable's impedance, resistance, attenuation, and if the cable is broke or shorted. Advanced cable testers can acquire information about message network collisions, frame counts, and congestion errors.

  If thinnet cable is broken its resistance would go from the normal of 50 ohms to infinity.

- Network monitors - Used to monitor network traffic. They can examine network packets, where they are from and where they are going. They can also generate reports and shows graphic statistics about the network. The network monitors work through all layers of the OSI model except the hardware layer. Windows NT provides the Performance Monitor tool software as a network monitor.
- Terminators - They are placed on one end of a network cable so the cable will have proper impedance. This is also a way to check the cable to be sure it is not broken.

Network Ports

Not all ports are included here, just the most common ones:

Keyword	Number	Protocol(s)	Description
tcpmux	1	TCP, UDP	TCP Port Service Multiplexer
echo	7	TCP, UDP	Echo
discard	9	TCP, UDP	Discard
systat	11	TCP	Active Users
daytime	13	TCP, UDP	Daytime (RFC 867)
qotd	17	TCP	Quote of the Day
msp	18	TCP, UDP	message send protocol
chargen	19	TCP, UDP	Character Generator
ftp-data	20	TCP, UDP	File transfer default data
ftp	21	TCP, UDP	File transfer control
ssh	22	TCP, UDP	Remote login protocol
telnet	23	TCP, UDP	Telnet
smtp	25	TCP, UDP	Simple Mail Transfer
time	37	TCP, UDP	Time
rlp	39	TCP, UDP	Resource location protocol
nameserver	42	TCP, UDP	Host name server
whois	43	TCP, UDP	Who is
re-mail-ck	50	TCP, UDP	Remote mail checking protocol
domain	53	TCP, UDP	Domain name server
bootps	67	TCP, UDP	Bootstrap protocol server
bootpc	68	TCP, UDP	Bootstrap protocol client
tftp	69	TCP, UDP	Trivial file transfer protocol
gopher	70	TCP, UDP	Gopher
finger	79	TCP, UDP	Finger
www	80	TCP, UDP	World wide web or HTTP
kerberos	88	TCP, UDP	Kerberos
supdup	95	TCP, UDP	SUPDUP
hostname	101	TCP, UDP	NIC Host Name Server
iso-tsap	102	TCP, UDP	ISO-TSAP Class 0
csnet-ns	105	TCP, UDP	CCSO name server protocol
rtelnet	107	TCP, UDP	Remote Telnet Service
pop-2	109	TCP, UDP	Post Office Protocol - Version 2
pop-3	110	TCP, UDP	Post Office Protocol - Version 3
sunrps	111	TCP, UDP	SUN Remote Procedure Call
auth	113	TCP, UDP	Authentication Service
sftp	115	TCP, UDP	Simple File Transfer Protocol
uucp-path	117	TCP, UDP	UUCP Path Service
nntp	119	TCP, UDP	Network News Transfer Protocol

nyp	123	TCP, UDP	Network Time Protocol
netbios-ne	137	TCP, UDP	NETBIOS Name Service
netbios-dgram	138	TCP, UDP	NETBIOS Datagram Service
netbios-ssn	139	TCP, UDP	NETBIOS Session Service
imap	143	TCP, UDP	Internet Message Access Protocol
snmp	161	TCP, UDP	SNMP
snmp-trap	162	TCP, UDP	SNMPTRAP
cmip-man	163	TCP, UDP	CMIP/TCP Manager
cmip-agent	164	TCP, UDP	CMIP/TCP Agent
xdmcp	177	TCP, UDP	X Display Manager Control Protocol
nextstep	178	TCP, UDP	NextStep Window Server
bgp	179	TCP, UDP	Border Gateway Protocol
prospero	191	TCP, UDP	Prospero Directory Service
irc	194	TCP, UDP	Internet Relay Chat Protocol
smux	199	TCP, UDP	SMUX

```
at-rtmp         201/tcp                         # AppleTalk routing
at-rtmp         201/udp
at-nbp          202/tcp                         # AppleTalk name binding
at-nbp          202/udp
at-echo         204/tcp                         # AppleTalk echo
at-echo         204/udp
at-zis          206/tcp                         # AppleTalk zone information
at-zis          206/udp
qmtp            209/tcp                         # The Quick Mail Transfer Protocol
qmtp            209/udp                         # The Quick Mail Transfer Protocol
z3950           210/tcp         wais            # NISO Z39.50 database
z3950           210/udp         wais
ipx             213/tcp                         # IPX
ipx             213/udp
imap3           220/tcp                         # Interactive Mail Access
imap3           220/udp                         # Protocol v3
rpc2portmap     369/tcp
rpc2portmap     369/udp                         # Coda portmapper
codaauth2       370/tcp
codaauth2       370/udp                         # Coda authentication server
ulistserv       372/tcp                         # UNIX Listserv
ulistserv       372/udp
https           443/tcp                         # MCom
https           443/udp                         # MCom
snpp            444/tcp                         # Simple Network Paging Protocol
snpp            444/udp                         # Simple Network Paging Protocol
saft            487/tcp                         # Simple Asynchronous File Transfer
saft            487/udp                         # Simple Asynchronous File Transfer
npmp-local      610/tcp         dqs313_qmaster  # npmp-local / DQS
npmp-local      610/udp         dqs313_qmaster  # npmp-local / DQS
npmp-gui        611/tcp         dqs313_execd    # npmp-gui / DQS
npmp-gui        611/udp         dqs313_execd    # npmp-gui / DQS
hmmp-ind        612/tcp         dqs313_intercell# HMMP Indication / DQS
hmmp-ind        612/udp         dqs313_intercell# HMMP Indication / DQS
```

```
#
# UNIX specific services
#
exec            512/tcp
biff            512/udp         comsat
login           513/tcp
who             513/udp         whod
shell           514/tcp         cmd             # no passwords used
syslog          514/udp
printer         515/tcp         spooler         # line printer spooler
talk            517/udp
ntalk           518/udp
route           520/udp         router routed   # RIP
timed           525/udp         timeserver
tempo           526/tcp         newdate
courier         530/tcp         rpc
conference      531/tcp         chat
netnews         532/tcp         readnews
netwall         533/udp                         # -for emergency broadcasts
uucp            540/tcp         uucpd           # uucp daemon
afpovertcp      548/tcp                         # AFP over TCP
afpovertcp      548/udp                         # AFP over TCP
remotefs        556/tcp         rfs_server rfs  # Brunhoff remote filesystem
klogin          543/tcp                         # Kerberized `rlogin' (v5)
kshell          544/tcp         krcmd           # Kerberized `rsh' (v5)
kerberos-adm    749/tcp                         # Kerberos `kadmin' (v5)
#
webster         765/tcp                         # Network dictionary
webster         765/udp
#
# From ``Assigned Numbers'':
#
#> The Registered Ports are not controlled by the IANA and on most systems
#> can be used by ordinary user processes or programs executed by ordinary
#> users.
#
#> Ports are used in the TCP [45,106] to name the ends of logical
#> connections which carry long term conversations.  For the purpose of
#> providing services to unknown callers, a service contact port is
#> defined.  This list specifies the port used by the server process as its
#> contact port.  While the IANA can not control uses of these ports it
#> does register or list uses of these ports as a convienence to the
#> community.
#
ingreslock      1524/tcp
ingreslock      1524/udp
prospero-np     1525/tcp                        # Prospero non-privileged
prospero-np     1525/udp
datametrics     1645/tcp        old-radius      # datametrics / old radius entry
datametrics     1645/udp        old-radius      # datametrics / old radius entry
sa-msg-port     1646/tcp        old-radacct     # sa-msg-port / old radacct entry
sa-msg-port     1646/udp        old-radacct     # sa-msg-port / old radacct entry
radius          1812/tcp                        # Radius
radius          1812/udp                        # Radius
```

```
radacct         1813/tcp                        # Radius Accounting
radacct         1813/udp                        # Radius Accounting
cvspserver      2401/tcp                        # CVS client/server operations
cvspserver      2401/udp                        # CVS client/server operations
venus           2430/tcp                        # codacon port
venus           2430/udp                        # Venus callback/wbc interface
venus-se        2431/tcp                        # tcp side effects
venus-se        2431/udp                        # udp sftp side effect
codasrv         2432/tcp                        # not used
codasrv         2432/udp                        # server port
codasrv-se      2433/tcp                        # tcp side effects
codasrv-se      2433/udp                        # udp sftp side effect
mysql           3306/tcp                        # MySQL
mysql           3306/udp                        # MySQL
rfe             5002/tcp                        # Radio Free Ethernet
rfe             5002/udp                        # Actually uses UDP only
cfengine        5308/tcp                        # CFengine
cfengine        5308/udp                        # CFengine
bbs             7000/tcp                        # BBS service
#
#
# Kerberos (Project Athena/MIT) services
# Note that these are for Kerberos v4, and are unofficial.  Sites running
# v4 should uncomment these and comment out the v5 entries above.
#
kerberos4       750/udp         kerberos-iv kdc # Kerberos (server) udp
kerberos4       750/tcp         kerberos-iv kdc # Kerberos (server) tcp
kerberos_master 751/udp                         # Kerberos authentication
kerberos_master 751/tcp                         # Kerberos authentication
passwd_server   752/udp                         # Kerberos passwd server
krb_prop        754/tcp                         # Kerberos slave propagation
krbupdate       760/tcp         kreg            # Kerberos registration
kpasswd         761/tcp         kpwd            # Kerberos "passwd"
kpop            1109/tcp                        # Pop with Kerberos
knetd           2053/tcp                        # Kerberos de-multiplexor
zephyr-srv      2102/udp                        # Zephyr server
zephyr-clt      2103/udp                        # Zephyr serv-hm connection
zephyr-hm       2104/udp                        # Zephyr hostmanager
eklogin         2105/tcp                        # Kerberos encrypted rlogin
#
# Unofficial but necessary (for NetBSD) services
#
supfilesrv      871/tcp                         # SUP server
supfiledbg      1127/tcp                        # SUP debugging
#
# Datagram Delivery Protocol services
#
rtmp            1/ddp                           # Routing Table Maintenance Protocol
nbp             2/ddp                           # Name Binding Protocol
echo            4/ddp                           # AppleTalk Echo Protocol
zip             6/ddp                           # Zone Information Protocol
#
# Services added for the Debian GNU/Linux distribution
poppassd        106/tcp                         # Eudora
```

```
poppassd        106/udp                         # Eudora
mailq           174/tcp                         # Mailer transport queue for Zmailer
mailq           174/tcp                         # Mailer transport queue for Zmailer
ssmtp           465/tcp                         # SMTP over SSL
gdomap          538/tcp                         # GNUstep distributed objects
gdomap          538/udp                         # GNUstep distributed objects
snews           563/tcp                         # NNTP over SSL
ssl-ldap        636/tcp                         # LDAP over SSL
omirr           808/tcp         omirrd          # online mirror
omirr           808/udp         omirrd          # online mirror
rsync           873/tcp                         # rsync
rsync           873/udp                         # rsync
simap           993/tcp                         # IMAP over SSL
spop3           995/tcp                         # POP-3 over SSL
socks           1080/tcp                        # socks proxy server
socks           1080/udp                        # socks proxy server
rmtcfg          1236/tcp                        # Gracilis Packeten remote config
server
xtel            1313/tcp                        # french minitel
support         1529/tcp                        # GNATS
cfinger         2003/tcp                        # GNU Finger
ninstall        2150/tcp                        # ninstall service
ninstall        2150/udp                        # ninstall service
afbackup        2988/tcp                        # Afbackup system
afbackup        2988/udp                        # Afbackup system
icp             3130/tcp                        # Internet Cache Protocol (Squid)
icp             3130/udp                        # Internet Cache Protocol (Squid)
postgres        5432/tcp                        # POSTGRES
postgres        5432/udp                        # POSTGRES
fax             4557/tcp                        # FAX transmission service
(old)
hylafax         4559/tcp                        # HylaFAX client-server protocol
(new)
noclog          5354/tcp                        # noclogd with TCP (nocol)
noclog          5354/udp                        # noclogd with UDP (nocol)
hostmon         5355/tcp                        # hostmon uses TCP (nocol)
hostmon         5355/udp                        # hostmon uses TCP (nocol)
ircd            6667/tcp                        # Internet Relay Chat
ircd            6667/udp                        # Internet Relay Chat
webcache        8080/tcp                        # WWW caching service
webcache        8080/udp                        # WWW caching service
tproxy          8081/tcp                        # Transparent Proxy
tproxy          8081/udp                        # Transparent Proxy
mandelspawn     9359/udp        mandelbrot      # network mandelbrot
amanda          10080/udp                       # amanda backup services
kamanda         10081/tcp                       # amanda backup services (Kerberos)
kamanda         10081/udp                       # amanda backup services (Kerberos)
amandaidx       10082/tcp                       # amanda backup services
amidxtape       10083/tcp                       # amanda backup services
isdnlog         20011/tcp                       # isdn logging system
isdnlog         20011/udp                       # isdn logging system
vboxd           20012/tcp                       # voice box system
vboxd           20012/udp                       # voice box system
binkp           24554/tcp                       # Binkley
```

```
binkp           24554/udp                       # Binkley
asp             27374/tcp                       # Address Search Protocol
asp             27374/udp                       # Address Search Protocol
tfido           60177/tcp                       # Ifmail
tfido           60177/udp                       # Ifmail
fido            60179/tcp                       # Ifmail
fido            60179/udp                       # Ifmail

# Local services

linuxconf 98/tcp
swat            901/tcp                         # Add swat service used via inetd
```

Network Terms

1. ADSP - AppleTalk data stream protocol manages the flow of data between two established socket connections.
2. AEP - AppleTalk echo protocol uses echoes to tell if a computer, or node, is available.
3. AFP - AppleTalk Filing protocol - Makes network files appear local by managing file sharing at the presentation layer.
4. AGP - Accelerated Graphics Port. This bus is developed for fast video cards. It is currently up to 4X mode speed.
5. AMPS - Advanced Mobile Phone Service is analog cellular phone service.
6. API - Application Programming Interface.
7. APPC - Advanced Peer-to-Peer Communications provides peer to peer services at the transport and session layer.
8. APPN - Advanced Peer-to-Peer Networking supports the computer connections at the network and transport layers.
9. Architecture - The method that is used to transmit packets on a network. Sometimes the term architecture includes topology. An example is ethernet.
10. ARCnet - Attached Resource Computer Network is an architecture using star and bus topology.
11. ARP - Address resolution Protocol is used to resolve the hardware address of a card to package the ethernet data. It works at the data link layer. RFC 826.
12. ARUP - AppleTalk update routing is a newer version of RTMP.
13. ASP - AppleTalk session protocol controls the starting and ending of sessions between computers called nodes. It works at the session level.
14. ASP - Active Server Pages is Microsoft's web server technology which can run Visual Basic or JAVA script.
15. ATM - Asynchronous Transfer Mode may be used over a variety of media with both baseband and broadband systems. It uses fixed length data packets of 53 bytes called cell switching.
16. ATP - AppleTalk Transaction Protocol provides a Transport Layer connection between computers.
17. attenuation - signal loss due to impedance.
18. AU - Access Unit provides access to resources like fax, telex, and teletex.
19. Backbone - Main cable used to connect computers on a network.
20. Bandwidth - Indicates the amount of data that can be sent in a time period. Measured in Mbps which is one million bits per second.
21. Baseband - Data bits are defined by discrete signal changes.
22. BDC - Backup Domain Controller is a backup for a PDC
23. BGP - Border Gateway Protocol, a dynamic routing protocol. RFC 1267.
24. BNC - British Naval Connector.
25. BOOTP - Boot Protocol. RFC 951, 1542.
26. Bridge - Read 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 but only sends packets intended for that segment they are attached to.

27. 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.
28. Broadcast - A transmission to all interface cards on the network.
29. Brouter - Will function similar to a bridge for network transport protocols that are not routable, and will function as a router for routable protocols.
30. BSC - Binary Synchronous Communication sends bits in frames which are timed sequences of data. A possible SNA communications architecture,
31. CCITT - International Telegraph and Telephone Consultative Committee.
32. CDMA - Code division multiple access allows transmission of voice and data over a shared part of radio frequencies. This is also called spread spectrum.
33. CDPD - Cellular Digital Packet Data will allow network connections for mobile users using satellites.
34. cellular - An 800 Mhz band for mobile phone service.
35. CHAP - Challenge Handshake Authentication Protocol is a three way handshake protocol which is considered more secure than PAP.
36. CIDR - Classless Inter Domain Routing.
37. Client - This computer requests resources for its use from a computer that provides the resource (a server).
38. CRC - Cyclic Redundancy check is a set of trailing data bytes in a message used to determine if an error occurred in a message.
39. CSMA/CD - Carrier-sense multiple-access with collision detection for controlling access to the network media.
40. CSU - Channel service unit used to connect to digital leased lines on the line side.
41. D-AMPS - Digital AMPS using TDMA to divide the channels into three channels.
42. DAS - Dual attachment stations are used by FDDI networks for servers and concentrators are attached to both rings.
43. DAT - Digital Audio Tape
44. Datagram - IP header and what is called a message or segment. The message or segment is a transport header (TCP or UDP) and application data. The term datagram is used to describe the information before IP fragmentation or after reassembly.
45. DBMS - Database Management Systems are used to share data on a network.
46. DDE - Dynamic data exchange.
47. DDP - Datagram Delivery Protocol is a routable protocol that provides for data packet transportation. It operates at the network layer at the same level of the IP protocol.
48. DDS - Digital data service is a leased dedicated digital line.
49. DECnet - From Digital Equipment Corporation is a suite of protocols which may be used on large networks that integrate mainframe and minicomputer systems
50. DHCP - Dynamic Host Configuration Protocol is used to assign IP addresses dynamically to network cards works at the application layer. RFC 1541.
51. Direct sequence modulation - The data is broken into parts and transmitted simultaneously on multiple frequencies.
52. DLC - Data Link Control operates at the data link layer and is designed for communications between Hewlett-Packard network printers and IBM mainframe computers on a DECnet network.

53. DNA - Digital Network Architecture is a term from DECNet
54. DNS - Domain Name System is used on the internet to correlate between IP address and readable names. RFC 1034, 1035, 1535-1537, 1591.
55. DRDA - Distributed Relational Database Architecture is from IBM.
56. DSU - Digital service unit used to connect to digital leased lines on the LAN side.
57. DTD - Document Type Definition.
58. DUN - Dial up networking.
59. DVM - Digital volt meter.
60. EGP - Exterior Gateway Protocol. Used between routers of different systems.
61. EIA - Electronic Industries Association .
62. EIGRP - Enhanced Interior Gateway Routing Protocol integrates the bese capabilities of link-state protocols with distance vector protocols capabilities.
63. EISA - Extended ISA used when the 80286 through 80486 series microprocessors were being produced. It is backward compatible with ISA.
64. EMI - Electromagnetic Interference.
65. Ethernet - A network architecture that uses carrier-sense multiple-access with collision detection (CSMA/CD) for controlling access to the network media and baseband broadcasts. It uses star topology.
66. FDDI - Fiber Distributed Data Interface is a network architecture normally used to send longer distances. Topology is ring with two counter rotating rings for reliability with no hubs. Cable type is fiber-optic.
67. FDMA - Frequency Division Multiple Access divides the cellular network into 30Khz channels.
68. Frame - The unit of transmission in a link layer protocol, consisting of a link-layer header (ethernet) followed by a packet (IP header and data). It may be a part of a fragmented datagram.
69. Frame Relay - Error checking is handled by devices at both sides of the connection. Frame relay uses frames of varying length and it operates at the data link layer of the OSI model. A permanent virtual circuit (PVC) is established between two points on the network. Frame relay speed is between 56Kbps and 1.544Mbps.
70. Frequency hopping - The transmitter and receiver change predetermined frequencies at the same time (in a synchronized manner).
71. FTP - File Transport Protocol is a TCP/IP protocol running at the application layer.
72. 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. Not the same as a default gateway used by a client to send packets to.
73. GSM - Global System for Mobile Communications.
74. HDML - Handheld Device Markup Language is a version of HTML only allowing text to be displayed.
75. HTML - Hypertext Markup Language is the format many files for web viewing are in. It is a language with "mark-up" text included for formatting.
76. HTTP - Hypertext Transfer Protocol is the protocol used to communicate between web servers and web browser software clients.
77. Hub - A type of repeater used on several network architectures which usually connects several

stations.

78. IAB - Internet Architecture Board
79. IANA - Internet Assigned Numbers Authority.
80. ICMP - Internet Control Message Protocol is used to perform network error reporting and status. It works at the transport layer. RFC 792.
81. IDC - Internet Database collector.
82. IETF - Internet Engineering Task Force. Sets Internet technical standards.
83. IGMP - Internet Group Management Protocol, used for managing multicast groups. RFC 1112.
84. IMAP4 - Internet Mail Access Protocol version 4 is the replacement for POP3
85. Impedance - The amount of resistance to the transmission device.
86. Infared - Infared is just below the visible range of light between 100Ghz and 1000Thz.
87. Interference - Electromagnetic Interference (EMI). Crosstalk - When wires pick up electromagnetic signals from nearby wires also carrying signals.
88. Internetwork - Several subnets connected together using routers.
89. InterNIC - Internet Network Information Center, the authority for allocating internet addresses.
90. Intranet - Refers to using internet technologies such as a web server on an internal network.
91. IP - Internet Protocol os used for software addressing of computers and works at the data link layer. RFC 791.
92. IPIP tunneling - Tunneling IP packets in IP packets. Used for VPN tunneling.
93. IPSec - Internet protocol security, developed by IETF, implemented at layer 3. it is a collection of security measures that address data privacy, integrity, authentication, and key management, in addition to tunneling. Used for VPN.
94. IPX - Internetwork Packet Exchange supports the transport and network layers of the OSI network model. Provides for network addressing and routing. It provides fast, unreliable, communication with network nodes using a connection less datagram service.
95. IRQ- Interrupt Request
96. IRTF - Internet Research Task force.
97. ISA - Industry Standard Architecture internal computer bus. Used when the original 8088 8bit microprocessor based personal computers were produced. (16 bit).
98. ISAKMP/Oakley - Internet Security Association and Key Management Protocol Authentication.
99. ISAPI - Internet Server Application Programming Interface
100. ISDN - Integrated Services Digital Network is a method of sending voice and data information on a digital phone line. Two 64Kbps B-channels with one 16Kbps D channel is provided with basic ISDN service
101. ISP - Internet Service Provider
102. ISOC - Internet Society, promotes internet policies.
103. ITU - International Telecommunication Union.
104. FTP - File Transfer Protocol.
105. L2F - Layer2 Forwarding, works at the link layer of the OSI model. It has no encryption. Being replaced by L2TP. It is used for VPN.
106. L2TP - Layer 2 tunneling protocol (RFC 2661). Used for VPN tunneling.
107. LAN - Local Area Network
108. LDA - Local delivery agent on the receiving machine receives the mail from its MTA. This

program is usually procmail.
109. LCP - Link Control Protocol
110. Link - Connects two network devices. Implemented by the data link layer.
111. LLC - Loc\gical link control is the interface between the lower and upper layer networking protocols.
112. LU - Logical Units are ports that users use to access network resources is an SNA term.
113. MAC - Media Access Control address. Basically a network card unique hardware address.
114. Mail notifier - This program notifies the recipient that they have mail. Normally this requires two programs, biff and comsat. Biff allows the administrator or user to turn on comsat service.
115. MAN- Metropolitan area network refers to a network which connects several LANS over various media that is large enough to cover an area the size of a city.
116. MAPI - Microsoft's Messaging API which is incorporated throughout Microsoft's office products supports mail at the application level.
117. MAU - Multistation access unit used by Token Ring Networks.
118. MBONE - Being on the MBONE means you are on a network that supports multicasting.
119. MCI - Microchannel architecture by IBM and used mainly on IBM brand computers for the internal bus. Established in 1988. (16 or 32 bits).
120. MDBS - Mobile Data Base Station reviews all cellular channels at cellular sites.
121. Media - The hardware method used to connect computers over a network. The three main types are copper cable, fiber optic cable, and wireless.
122. Message - The unit of transmission in a transport layer protocol. A TCP segment is a message which consists of a transport protocol header followed by application data.
123. MHS - Message Handling Service by Novell is used for mail on Netware networks.
124. MIB - Management Information BASE specifies variables the network elements maintain. Works with the TCP/IP protocol SNMP.
125. MIME - Multipurpose Internet Mail Extension is the protocol that defines the way files are attached to SMTP messages.
126. MOTIS - Message-oriented text interchange system.
127. MS - Message Store is a storage area for messages that can't be delivered immediately when the recipient is off-line.
128. MTA - Message transfer agent is used to pass mail from the sending machine to the receiving machine. There is a MTA program running on both the sending and receiving machine. Sendmail is a MTA.
129. MTP - Multicast Transport Protocol is a new transport layer protocol designed for reliable multicast network message transport.
130. MTU - Maximum Transmission Unit is the maximum size of each data packet for the ethernet protocol.
131. MUA - Mail users agent. This is the program a user will use to type e-mail. It usually incorporates an editor for support. The user types the mail and it is passed to the sending MTA. This may also be called the user agent (UA).
132. Multicasting - Transmitting to a group of interface cards on the network.
133. Multihomed - A host with multiple IP addresses.
134. NADN - Nearest Active Downstream Neighbor is a Token ring Architecture term.

135. NAU - Network Addressable Units is an SNA term.
136. NAUN - Nearest Active Upstream Neighbor is a Token ring Architecture term.
137. NAT - Network Address Translation.
138. NBF - NetBIOS Frame Protocol.
139. NBNS - NetBIOS Name Server. A server that maps NetBIOS names to IP addresses. This service is provided by the nmbd daemon on Linux.
140. NBP - Name-binding protocol of the AppleTalk suite of protocols translates addresses into names.
141. NBT - NetBIOS over TCP/IP defined by RFC 1002.
142. NCP - NetWare Core Protocol provides for client/server interactions such as file and print sharing. It works at the application, presentation, and session levels.
143. NCP - Network Control Program performs routing, session management tasks. It runs in the communications controller. It is an SNA networking term.
144. NDIS - Network Driver Interface Specification from Microsoft, is used on Microsoft networks. It allows multiple protocols to be used on a network card and supports the data link layer of the network model.
145. NetBEUI - NetBIOS Extended User Interface works at the transport layer and provides data transportation. It is not a routable transport protocol which is why NBT exists on large networks to use routable TCP protocol on large networks.
146. NetBIOS - Network Basic Input Output System by Microsoft.
147. NetDDE - Network dynamic data exchange.
148. Network Operating System - Typically used to run computers that act as servers, but may be used on various types of computers today.
149. NFS - Network File System. A protocol that allows UNIX and Linux systems remotely mount each other's file systems. RFC 1094
150. NIC - Network interface card. Also called LAN adapters.
151. NNTP - Network News Transport Protocol is used to link newsgroups for discussions on the web
152. OC - Optical Carrier level, see SONET.
153. ODBC - Open Database Connectivity (ODBC) from Microsoft lets application developers integrate database connections in applications. It is an application programming interface (API). ODBC drivers convert an application's query int SQL and send it to the database engine program.
154. ODI - Open Data-link Interface operates at the data link layer allowing IPX to work with any network interface card.
155. OSI - Open Systems Interconnect is a suite of protocols developed by the International Standards Organization (ISO) which corresponds with the layers of the OSI model.
156. OSPF - Open Shortest Path First, a dynamic routing protocol. RFC 1247.
157. Packet - Includes an IP header and data. It may be a complete IP datagram or a fragment of an IP datagram.
158. PCI - Peripheral Component Interconnect internal computer bus. The popular expansion bus of choice. It is significantly faster than EISA. This is a 32bit bus with plug and play capability from Intel.
159. PDC - Primary Domain Controller is an NT server providing central control of user access permissions and accounts on a network.
160. PAP - Password Authentification Protocol is a two way handshake protocol designed for use with

PPP.

161. PAP - Printer access protocol of the AppleTalk suite of protocols manages information between workstations and printers.
162. PCS - Personal communications Service is a 1.9 Ghz band for mobile phones.
163. Peer - A computer that can act as both a client and a server.
164. 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.
165. POP - Point of presence is each point at the end of the transport media (internet) when talking about VPN.
166. POP3 - Post Office Protocol version 3 is used by clients to access an internet mail server to get mail. It is not a transport layer protocol.
167. Protocol - A set of standards sets of standards that define all operations within a network. There are various protocols that operate at various levels of the OSI network model such as transport protocols include TCP, SPX.
168. PPP - Point to Point Protocol, used for serial connections to a network ot the internet. (RFC 1332, 1548)
169. PPTP - Point to point tunneling protocol (RFC 2637) Used for VPN tunneling.
170. PU - Physical Units are a network device used to communicate with hosts. It is an SNA term.
171. RADIUS - Remote Authentication Dial-In User Service is used for dial in clients to connect to other computers or a network. It provides authentication and accounting when using PPTP or L2TP tunneling.
172. RAID - Redundant Array of Inexpensive disks is a fault tolerant method of storing data, meaning that a failure can occur and the system will still function.
173. RARP -Reverse Address Resolution Protocol used for diskless computers to determine their IP address using the network. It works at the data link layer. RFC 903.
174. RAS - Remote Access Service (RAS) with Windows NT allows users connecting to the network using a modem to use network resources. The NT RAS server can handle 256 connections.
175. Redirector - it runs on a windows operating system and directs requests for network resources to the appropriate server and makes network resources seem to be local resources.
176. Repeater - Used on a network to regenerate signals to be sent over long distances or tie computers together on a network.
177. Resolver - Used as part of DNS, it is the client side asking for DNS information.
178. RIP - Routing Information Protocol, a dynamic routing protocol. A distance-vector algorithm is used to calculate the best route for a packet. RFC 1058, 1388 (RIP2).
179. Rlogin - Remote login between UNIX hosts. This is outdated and is replaced by Telnet.
180. Router - Routes data packets between two networks. It reads the information in each packet to tell where it is going.
181. RPC - Remote Procedure Call. A protocol invented by Sun Microsystem to allow remote computers to invoke functions on other hosts. RFC 1057.
182. RR - Resource Records are a part of the DNS database.
183. RTMP - Routing table maintenance protocol is used to update routers with information about network status and address tables. The whole address table is sent across the network.
184. S/Key - A one time password system, secure against replays. RFC 2289.

185. SAP - Service Advertising Protocol packets are used by file and print servers to periodically advertise the address of the server and the services available. It works at the application, presentation, and session levels.
186. SAS - Single Attachment stations attached to one ring and used by FDDI networks to attach workstations to concentrators.
187. SDH - Synchronous Digital Hierarchy
188. SDLS - Synchronous Data Link Control is a possible SNA communications architecture.
189. Sector Sparing - A method of fault tolerance that automatically identifies and marks bad sectors as not available. It is also called hot-fixing.
190. Segment - The unit of end-to-end transmission in the TCP protocol which consists of a TCP header followed by application data.
191. Server - For the most part it provides resources on the network for other computers to use.
192. SGML - Standardized General Markup Language is the base language for document publishing and is used to define XML, HTML and more.
193. Shielding - Used to minimize interference.
194. SLED - Single Large Inexpensive disk - The concept that a large disk costs less per amount of storage than several smaller ones. Somehow this concept is used as a means of fault tolerance.
195. SLIP - Serial Line interface Protocol used to connect serially to a network or internet. RFC 1055, 1144 (Compressed). Replaced by PPP.
196. SMAU - Smart Multistation Access Unit.
197. SMB - Server Message Block protocol works at the presentation level to provide peer to peer communication.
198. SMDS - Switched Multi-megabit Data Service uses fixed length cell switching and runs at speeds of 1.533 to 45Mbps.
199. SMS - SMS - Systems Management Server from Microsoft can collect information of software on each computer and can install and configure new software on the client computers. It will also monitor network traffic.
200. SMTP - Simple Mail Transfer Protocol is a TCP protocol for mail transport running at the application layer. RFC 821, 822.
201. SNA - System Network Architecture by IBM is a suite of protocols mainly used with IBM mainframe and AS/400 computers.
202. SNMP - Simple Network Management Protocol. RFC 1155, 1157, 1213, 1441.
203. SONET - Synchronous Optical Network is a physical layer standard that defines voice, data, and video delivery methods over fiber optic media. It defines data rates in terms of optical carrier (OC) levels.
204. Spread spectrum - It uses several frequencies at the same time.
205. SPX - Sequenced Packet Exchange operates at the transport layer providing connection oriented communication on top of IPX.
206. SQL - Structured Query Language is a database access language. It is used by most client/server database applications.
207. SSCP - Systems Services Control Point manages all resources in the host's domain. An SNA term.
208. STP - Shielded Twisted Pair cable. 100 meter maximum length. 16-155 Mbps speed. Lower electrical interference than UTP

209. Subnet - A part of a network. A class B network may have several class C subnets. Usually routers are used to connect subnets.
210. TACACS - Offers authentication, accounting, and authorization.
211. T Carrier - Multiplexors are used to allow several channels on one line. The T1 line is basic T Carrier service.
212. TCP - Transport Control protocol is a connection oriented reliable protocol working at the transport layer. RFC 793.
213. TDI - Transport Driver Interface is a standard for passing messages between the drivers at the data link layer and the protocols working at the network layer such as IP or NetBEUI. It was produced by Microsoft.
214. 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.
215. TDR - Time-domain reflectometer sends a sonar like electrical pulse down a cable and can determine the location of a break in the cable.
216. TFTP - Trivial File Transfer Protocol. RFC 1350.
217. Telnet - Remote session at the application layer. RFC 854.
218. 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).
219. 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.
220. TIA - Telecommunications Industries Association .
221. TLD - Top Level domain
222. Token Ring - A network architecture developed by IBM which sends tokens around a ring of computers to allow media access. Standardized to IEEE 802.5
223. Topology - The shape of the physical connection of a network with regard to repeaters and networked computers. The three main types are ring, bus, and star.
224. UA - Users agent. This is the program a user will use to type e-mail. It usually incorporates an editor for support. The user types the mail and it is passed to the sending MTA. This may also be called the mail user agent (MUA).
225. UDP - User Datagram Protocol is a connection less unreliable protocol working at the transport layer. RFC 768.
226. UNC - Universal Naming Convention is used to allow the use of shared resources without mapping a drive to them.
227. Unicast - A transmission to a single interface card.
228. URL - Universal Resource Relocator is a term used to describe the name of a web based resource such as a web page or location of a file for down loading.
229. UTP - Unshielded Twisted Pair cable. Normally UTP contains 8 wires or 4 pair. 100 meter maximum length. 4-100 Mbps speed.
230. VIM - Vendor-Independent Messaging protocol from Lotus supports mail at the application level and is supported by many vendors exclusive of Microsoft.
231. VPN - Virtual Private Networking. The function of VPN is to allow two computers or networks to talk to each other over a transport media that is not secure, but the network is made secure by VPN security protocols.

232. W3C - World Wide Web Consortium, sets standards for the web working with the IETF.
233. WAN - Wide Area Network is larger than a MAN and may be an enterprise network or a global network.
234. WINS - Windows Internet Name Service is the Microsoft implementation of NetBIOS name service.
235. wireless bridge - Microwave or infared is used between two line of site points where it is difficult to run wire.
236. WML - Wireless markup language is another name for HDML.
237. X.25 - This is a set of protocols developed by the CCITT/ITU which specifies how to connect computer devices over a internetwork.
238. X.400 - International Telecommunication Union standard defines transfer protocols for sending mail between mail servers.
239. X.500 - This is a recommendation outlining how an organization can share objects and names on a large network. It is hierarchical similar to DNS, defining domains consisting of organizations, divisions, departments, and workgroups.
240. XML - Extensible Markup Language is a subset of SGML and is used widely on the web.
241. ZIP - Zone information protocol used with RTMP to map zones. Routers use zone information tables (ZITs) to define network addresses and zone names.

Network RFCs

Network RFCs and Associated Protocols

The table below lists Protocols and their associated RFCs.

Protocol	Associated RFC
Port Numbers	1340, 1700
Official Protocol Standards	1600, 1610, 1720, 1800, 1880, 1920, 2000, 2200, 2300, 2400
Host Requirements	1122 (LINK, NETWORK, TRANSPORT, 1123 (Application)
Router Requirements	1009, 1812, 2644
IP Datagrams	894, 1042, 919, 922
SLIP	1055
Compressed SLIP	1144
PPP	1134, 1332, 1333, 1547, 1548, 1549, 1552, 1661, 2153
Path MTU Discovery	1191
IP	791
Checksum	1071, 1141, 1624
Assignment of Subnet Numbers	1219
ARP	826
RARP	903
ICMP	792, 950
RIP	1058
RIPv2	1388, 1723, 2453
OSPF	1247, 1583, 1246, 1245, 2178
BGP	1267, 1268, 1467, 1655, 1772
UDP	768
IGMP	1112, 2236 (IP multicasting)
Link Control Protocol (LCP)	1570
DNS	1034, 1035, 1065, 2308, 1101, 1183, 1348, 1876, 1982, 2065, 2535, 1995, 1996, 2136, 2137
ECHO	862
TFTP	783, 1350, 1782, 1783, 1784, 1785, 2347, 2348, 2349

BOOTP	951, 1395, 1497, 1532, 1542
TCP	793, 1323
SNMP	1157
SNMPv2	1441
Management Information Base (MBIB)	1213, 2011, 2012, 2013
Structure of Management Information (SMI)	1155
Rlogin	1282
Telnet	854
FTP	959, 2228, 2640
SMTP	821, 822, 1138, 1148, 1327, 2156
SMTP Message Transfer Agent (MTA)	821
RPC	1057
NFS	1094, 1813
Finger	1288
NetBIOS	1001, 1002
IP on Token Ring	1042
Line Printer	1179
IP on FDDI	1188
IP on ARCNet	1201
DHCP and BOOTP	1533, 1534, 1541, 1542
IPX	1553

Link to Listing of RFCs at Ohio State

Further Reading

Title:

TCP/IP Illustrated, Volume1, The Protocols

Author:

W. Richard Stevens

Publisher:

Addison Wesley

ISBN

0201633469

The CTDP Networking Guide Credits

Document:

The CTDP Networking Guide Version 0.6.3

Author:

Mark Allen