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

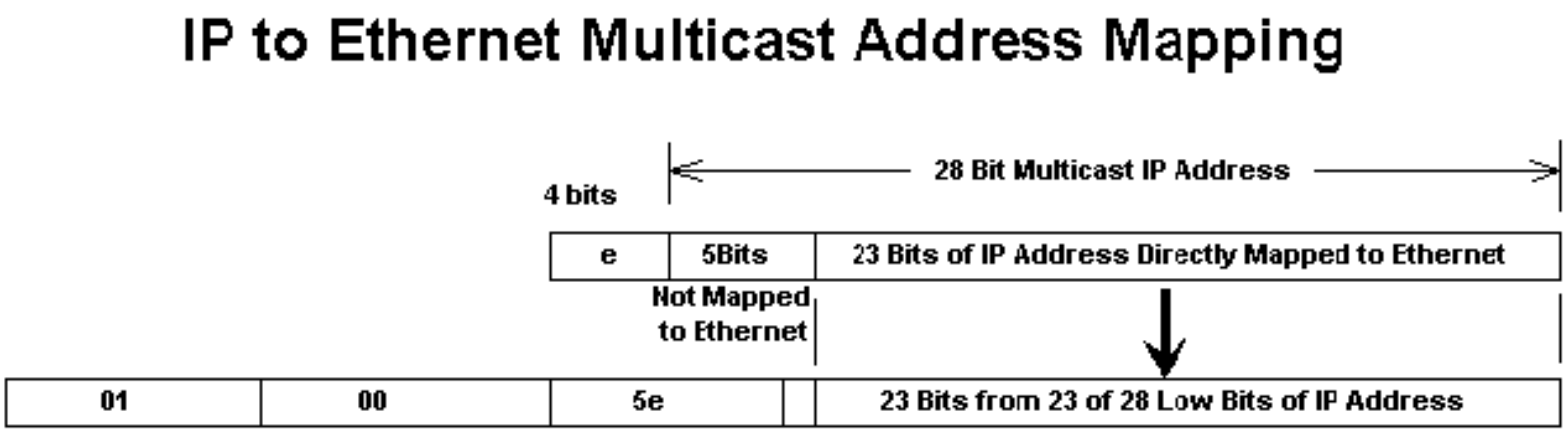
Multicasting may be used for streaming multimedia, video conferencing, shared white boards and more as the internet grows. Multicasting is still new to the internet and not widely supported by routers. New routing protocols are being developed to enable multicast traffic to be routed. Some of these routing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

This document avalable at the Computer Technology Documentation Project at http://www.comptechdoc.org