PRTOCOLS

FTP - file transfer protocol

FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for controlling the conversation and a data channel for transmitting file content. Clients initiate conversations with servers by requesting to download a file. Using FTP, a client can upload, download, delete, rename, move and copy files on a server. A user typically needs to log on to the FTP server, although some servers make some or all of their content available without login, also known asanonymous FTP.

FTP sessions work in passive or active modes. In active mode, after a client initiates a session via a command channel request, the server initiates a data connection back to the client and begins transferring data. In passive mode, the server instead uses the command channel to send the client the information it needs to open a data channel. Because passive mode has the client initiating all connections, it works well across firewalls and Network Address Translation (NAT) gateways.

How FTP Works

FTP works in the same way as HTTP for transferring Web pages from a server to a user's browser and SMTP for transferringelectronic mail across the Internet in that, like these technologies.
FTP uses a client-server architecture. Users provide authentication using a sign-in protocol, usually a username and password, however some FTP servers may be configured to accepi anonymous FTP logins where you don't need to identify yourself before accessing files. Most often, FTP is secured with SSL/TLS.

Telnet

What is Telnet?

Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application and data on that computer.

A Telnet command request looks like this (the computer name is made-up):

telnet the.libraryat.whatis.edu

The result of this request would be an invitation to log on with a userid and a prompt for a password. If accepted, you would be logged on like any user who used this computer every day.
Telnet is most likely to be used by program developers and anyone who has a need to use specific applications or data located at a particular host computer.

Features:

- TELNET is a standard protocol. Its status is recommended.
- It is described in RFC 854 - TELNET Protocol Specifications and RFC 855 - TELNET Option Specifications.
- Telnet was the first application demonstrated on the four-IMP (Interface Message Processor) network installed by December 1969. The final edition took 14 more years to develop, culminating in Internet Standard #8 in 1983, three years after the final TCP specification was ratified.
- Telnet even predates internetworking and the modern IP packet and TCP transport layers.
- The TELNET protocol provides a standardized interface, through which a program on one host (the TELNET client) may access the resources of another host (the TELNET server) as though the client were a local terminal connected to the server.
- For example, a user on a workstation on a LAN may connect to a host attached to the LAN as though the workstation were a terminal attached directly to the host. Of course, TELNET may be used across WANs as well as LANs.
- Most TELNET implementations do not provide you with graphics capabilities.
- TELNET is a general protocol, meant to support logging in from almost any type of terminal to almost any type of computer.
- It allows a user at one site to establish a TCP connection to a login server or terminal server at another site.
- A TELNET server generally listens on TCP Port 23.

DNS (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.

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.

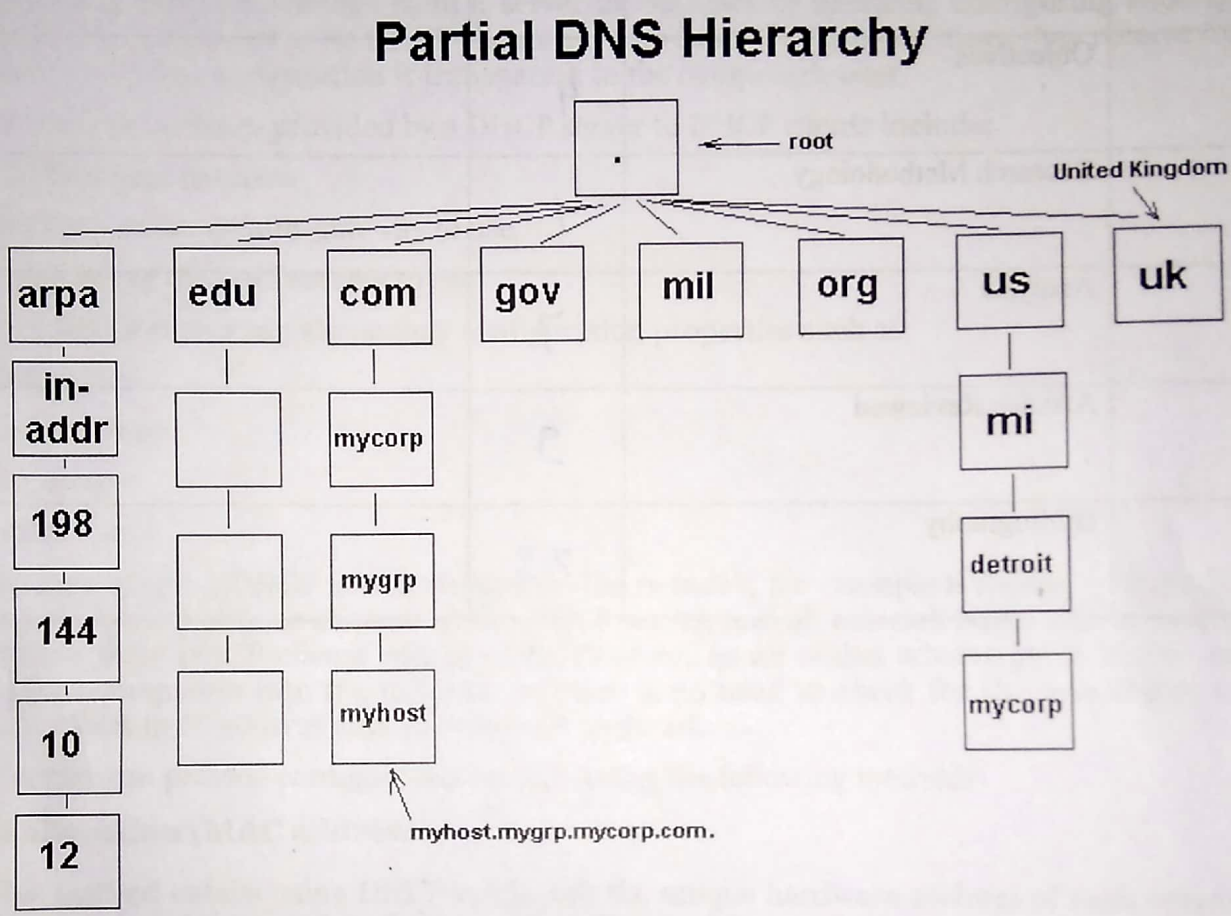
Main components of DNS

DNS can be confusing. It's made up of many different elements which control different aspects of your domain name. Here's a quick explanation of each one:

DNS Element	Description
Nameserver	Nameservers "point" your domain name to the company that controls its DNS settings. Usually, this will be the company where you registered the domain name. However, if your website is hosted by another company, sometimes you'll need to use their nameservers.
Zone File	Zone Files are simply the files that store all of your domain's DNS settings. Your domain name's Zone File is stored on the company's nameserver.
A Record	A Records point your domain name to an individual server using an IP address. An example IP address is 123.4.67.5. You can also use A Records to point subdomains (for examplesubdomain.coolexample.com) to a server's IP address. Every domain name has a primary A Record called "@," which controls what your domain name does when some visits it directly.
CNAME	CNAMEs point your subdomains to another server using a server name. Unlike A Records, CNAMEs cannot use IP addresses. Most domain names have many CNAMEs.
MX Records	MX Records point your domain name's email to its email provider.

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.

Dynamic Host Configuration Protocol (DHCP)

DHCP (Dynamic Host Configuration Protocol) is a communications protocol that network administrators use to centrally manage and automate the network configuration of devices attaching to an Internet Protocol (IP) network.

The Dynamic Host Configuration Protocol (DHCP) is a network service that enables host computers to be automatically assigned settings from a server as opposed to manually configuring each network host. Computers configured to be DHCP clients have no control over the settings they receive from the DHCP server, and the configuration is transparent to the computer's user.

The most common settings provided by a DHCP server to DHCP clients include:

1. IP address and netmask
2. IP address of the default-gateway to use
3. IP adresses of the DNS servers to use

However, a DHCP server can also supply configuration properties such as:

1. Host Name
2. Domain Name
3. Time Server
4. Print Server

The advantage of using DHCP is that changes to the network, for example a change in the address of the DNS server, need only be changed at the DHCP server, and all network hosts will be reconfigured the next time their DHCP clients poll the DHCP server. As an added advantage, it is also easier to integrate new computers into the network, as there is no need to check for the availability of an IP address. Conflicts in IP address allocation are also reduced.

A DHCP server can provide configuration settings using the following methods:

Manual allocation (MAC address)

This method entails using DHCP to identify the unique hardware address of each network card connected to the network and then continually supplying a constant configuration each time the DHCP client makes a request to the DHCP server using that network device. This ensures that a particular address is assigned automatically to that network card, based on it's MAC address.

Dynamic allocation (address pool)

In this method, the DHCP server will assign an IP address from a pool of addresses (sometimes also called a range or scope) for a period of time or lease, that is configured on the server or until the client informs the server that it doesn't need the address anymore. This way, the clients will be receiving their configuration properties dynamically and on a "first come, first served" basis. When a DHCP client is no longer on the network for a specified period, the configuration is expired and released back to the address pool for use by other DHCP Clients. This way, an address can be leased or used for a period of time. After this period, the client has to renegociate the lease with the server to maintain use of the address.

Automatic allocation

Using this method, the DHCP automatically assigns an IP address permanently to a device, selecting it from a pool of available addresses. Usually DHCP is used to assign a temporary address to a client, but a DHCP server can allow an infinite lease time.

The last two methods can be considered "automatic" because in each case the DHCP server assigns an address with no extra intervention needed. The only difference between them is in how long the IP

address is leased, in other words whether a client's address varies over time. Ubuntu is shipped with both DHCP server and client. The server is dhcpd (dynamic host configuration protocol daemon). The client provided with Ubuntu isdhclient and should be installed on all computers required to be automatically configured. Both programs are easy to install and configure and will be automatically started at system boot.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is an application–layer protocol defined by the Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices. It is a part of Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.

SNMP is one of the widely accepted protocols to manage and monitor network elements. Most of the professional–grade network elements come with bundled SNMP agent. These agents have to be enabled and configured to communicate with the network management system (NMS).

SNMP basic components and their functionalities

SNMP consists of :

- SNMP Manager
- Managed devices
- SNMP agent
- Management Information Database Otherwise called as Management Information Base (MIB)

SNMP Manager:

A manager or management system is a separate entity that is responsible to communicate with the SNMP agent implemented network devices. This is typically a computer that is used to run one or more network management systems.

SNMP Manager's key functions

- Queries agents
- Gets responses from agents
- Sets variables in agents
- Acknowledges asynchronous events from agents

Managed Devices:

A managed device or the network element is a part of the network that requires some form of monitoring and management e.g. routers, switches, servers, workstations, printers, UPSs, etc...

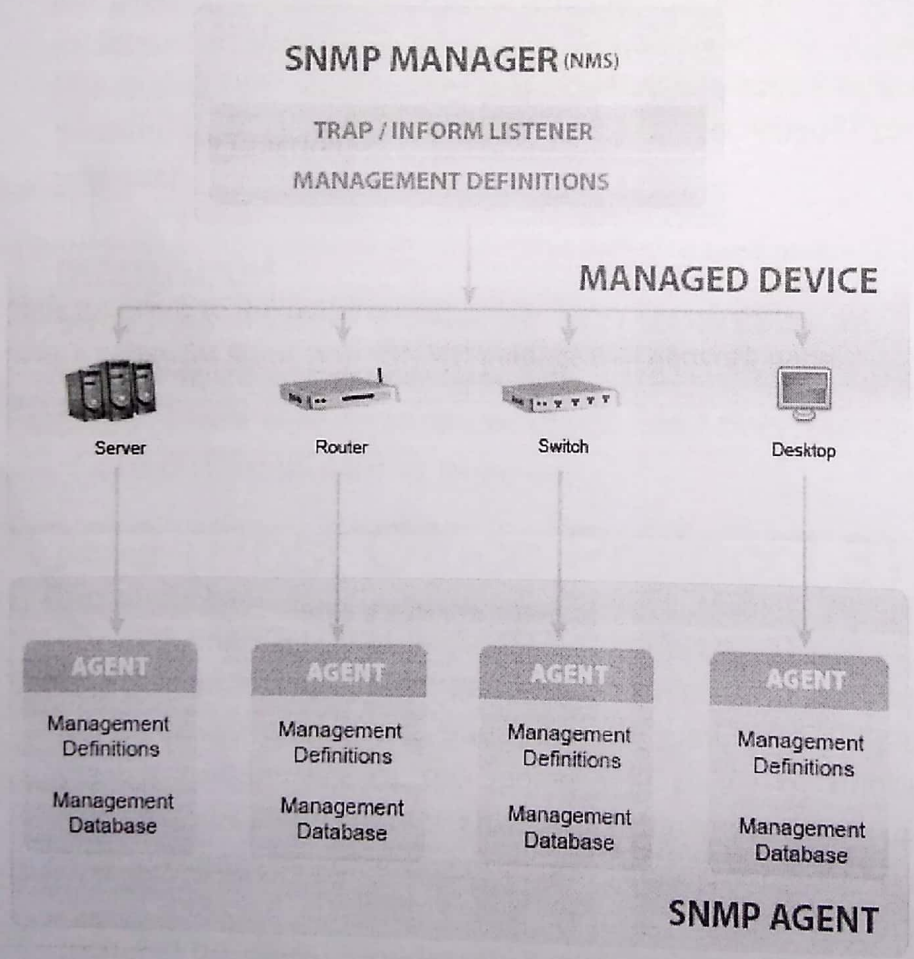
SNMP Agent:

The agent is a program that is packaged within the network element. Enabling the agent allows it to collect the management information database from the device locally and makes it available to the SNMP manager, when it is queried for. These agents could be standard (e.g. Net-SNMP) or specific to a vendor (e.g. HP insight agent)

SNMP agent's key functions

- Collects management information about its local environment
- Stores and retrieves management information as defined in the MIB.
- Signals an event to the manager.
- Acts as a proxy for some non–SNMP manageable network node.

Basic SNMP Communication Diagram



SMTP

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, sendmail is the most widely-used SMTP server for e-mail. A commercial package, Sendmail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

SMTP usually is implemented to operate over Internet port 25. An alternative to SMTP that is widely used in Europe is X.400. Many mail servers now support Extended Simple Mail Transfer Protocol (ESMTP), which allows multimedia files to be delivered as e-mail.

In other words :

- SMTP is used when email is delivered from an email client, such as Outlook Express, to an email server or when email is delivered from one email server to another. SMTP uses port 25.
- POP3 allows an email client to download an email from an email server. The POP3 protocol is simple and does not offer many features except for download. Its design assumes that the email client downloads all available email from the server, deletes them from the server and then disconnects. POP3 normally uses port 110.
- IMAP shares many similar features with POP3. It, too, is a protocol that an email client can use to download email from an email server. However, IMAP includes many more features than POP3. The IMAP protocol is designed to let users keep their email on the server. IMAP requires more disk space on the server and more CPU resources than POP3, as all emails are stored on the server. IMAP normally uses port 143. Here is more information about IMAP.

Examples

Suppose you use hMailServer as your email server to send an email to bill@microsoft.com.

1. You click Send in your email client, say, Outlook Express.
2. Outlook Express delivers the email to hMailServer using the SMTP protocol.
3. hMailServer delivers the email to Microsoft's mail server, mail.microsoft.com, using SMTP.
4. Bill's Mozilla Mail client downloads the email from mail.microsoft.com to his laptop using the POP3 protocol (or IMAP).

POP3 (Post Office Protocol 3)

POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail, probably using POP3. This standard protocol is built into most popular e-mail products, such as Eudora and Outlook Express. It's also built into the Netscape and Microsoft Internet Explorer browsers.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP), a protocol for transferring e-mail across the Internet. You send e-mail with SMTP and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP.

Broadband and Baseband Connection

Broadband is a term frequently used with accessing the Internet using high speeds, usually in excess of 248kbps. In general terms broadbandreferred to communication technology that can employ different channels of data or data streams by using any medium (air or Physical). Obviously, to transfer data at a higher rate, it requires more bandwidth (or frequencies). With wide band of frequencies, information can be multiplexed and sent on many different frequencies or channels within the band concurrently, allowing more information to be transmitted in a given amount of time.

Broadband can be provided over your phone line, via cable, or via satellite. It involves large volumes of information being carried at high speeds to your PC and vice versa. This allows graphics, music and videos to be experienced in real time by the user. Broadband, therefore, has many features that can be taken advantage of in the home or office:

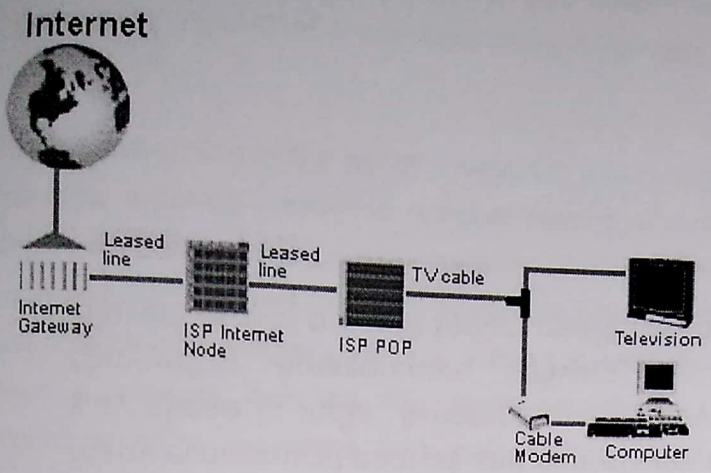
- The connection to the Internet is always on, allowing for instant Internet access and no need to wait for a connection to be made, as in dial up access.
- The phone line is unaffected; this means that you can make telephone calls whilst the Internet is on. This is due to the fact that voice and Internet data use different frequencies for transmission.
- Normally, you pay a standard monthly fee for unlimited Internet access, and you are not charged for the time you are connected to the Internet. There are certain broadband products now that also offer pay as you go access.
- Broadband allows music and videos downloaded at a faster rate.
- You can take advantage of instant messaging and online high-speed interactive games.
- You can receive uninterrupted real time services, such as Internet radio, streaming video and voice-over-ip, phone calls.

In the next section, we discuss about different types of broadband access technologies like wired broadband (includes xDSL, and Cable Modem), and wireless broadband access.

Wired broadband

a. Cable Broadband

The local cable TV provider provides the broadband cable modem connection. The cable modem should not be confused with dialup access modem. Both are different, and one can't be used in place of other. In fact, they are different animals! The cable Internet connection speed varies with the number of users on the service at a given point in time. Given a given geographical area, users of the broadband cable service share the connection bandwidth among themselves. As a result, the access speed may reduce to a noticeable extent at times. This is likely to occur at peak times, like late in the evenings after the work day is over when many people will be accessing the Internet. The cable company, however, claim the total bandwidth as available to the customer, as if you were the only person accessing the Internet using the cable. But that is clearly not the case.



A cable, as shown in the diagram, generally runs down your street and, if you choose to connect, a second cable is then run from the main line to your home. If you happen to already have cable TV installed, you won't need to get a professional installer to run this cable to your house – and that may mean savings on your set up fees.

Broadband cable Internet access requires a cable modem at the customer's premises and a cable modem termination system at a cable operator facility, typically a cable television head end. The two are connected via coaxial cable or a Hybrid Fiber Coaxial (HFC) plant. While access networks are sometimes referred to as *last-mile* technologies, cable Internet systems can typically operate where the distance between the modem and the termination system is up to 100 miles (160 km).

Using Cable Internet, downstream bit rates that can be typically reached at customer end are 30Mbit/s. Upstream traffic typically of range of 384Kbit/s or more at the customer premises. One downstream channel can handle hundreds of cable modems. As the system grows, the cable modem termination system (CMTS) can be upgraded with more downstream and upstream ports.

Advantages:

- Both ADSL and wireless users can experience degraded quality and reduced speeds if the customer premises is a long way from the Internet service provider (ISP). The quality issue is something cable surfers don't need to worry about.
- Cable Internet generally has a more constant top speed than thos available with traditional dial-up, DSL technology, or wireless.
- Your phone line is free from any interruption. You can make or receive call using your phone line because a cable modem is no way related with your phone line.

Disadvantages:

- You will need to buy a special cable modem hardware to send or receive information via a fiber-optic cable.
- The more people there are sharing the bandwidth, the slower your experience will be the quoted speeds are more like "theoretical maximums" speeds.
- If you haven't already connected to cable TV, you may need a professional to do the installation. Laying cable and related hardware increases the initial costs of having Cable modem service.
- Many packages place limits on downloads and uploads.

What Is a Baseline?

Sometimes when you talk to a seasoned system or network administrator, he'll tell you that he knows that something is wrong when things don't feel right. This isn't an admission of paranormal powers; it's just a shorthand method for explaining that these experts know how their system or network is supposed to

behave and that it isn't acting like that now. These administrators have created a baseline for their environment. Not all of them have done it formally, but the ones who have will have gained significant added benefits.

Network baselining is the act of measuring and rating the performance of a network in real-time situations. Providing a network baseline requires testing and reporting of the physical connectivity, normal network utilization, protocol usage, peak network utilization, and average throughput of the network usage.
Such in-depth network analysis is required to identify problems with speed and accessibility, and to find vulnerabilities and other problems within the network.
Once a network baseline has been established, this information is then used by companies and organizations to determine both present and future network upgrade needs as well as assist in making changes to ensure their current network is optimized for peak performance

A Baseline Defined

Several things make up a baseline, but at its heart, a baseline is merely a snapshot of your network the way it normally acts. The least effective form of a baseline is the "sixth sense" that you develop when you've been around something for a while. It seems to work because you to notice aberrations subconsciously because you're used to the way things ought to be. Better baselines will be less informal and may include the following components:

Network traces

- Summarized network utilization data
- Logs of work done on the network
- Maps of the network
- Records of equipment on the network and related configuration data

Network Traces

"Network Monitoring Tools" capability to save capture files (or traces) enables you to maintain a history of your network. If the only traces you have saved represent your troubleshooting efforts, you won't have a very good picture of your network.

You also need to be aware that a lot of things will influence the contents of the traces you collect. Weekend vs. weekday; Monday or Friday vs. the rest of the week; and time of day are all examples of the kinds of factors that will affect your data. Running ethereal (or some other analyzer) at least three times a day, every day, and saving the capture file will give you a much clearer idea of how things normally work.

Utilization Data

Several tools can give you a quick look at your network's behavior: netstat, traceroute, ping, and even the contents of your system logs are all good sources of information.

Wi-Fi Network

Wi-Fi is a wireless networking technology that allows computers and other devices to communicate over a wireless signal. It describes network components that are based on one of the 802.11 standards developed by the IEEE and adopted by the Wi-Fi Alliance. Examples of Wi-Fi standards, in chronological order, include:

- 02.11a
- 802.11b
- 802.11g
- 802.11n
- 802.11ac

Wi-Fi is the standard way computers connect to wireless networks. Nearly all modern computers have built-in Wi-Fi chips that allows users to find and connect to wirelessrouters. Most mobile devices, video game systems, and other standalone devices also support Wi-Fi, enabling them to connect to wireless networks as well. When a device establishes a Wi-Fi connection with a router, it can communicate with the router and other devices on the network. However, the router must be connected to the Internet (via a DSL or cable modem) in order to provide Internet access to connected devices. Therefore, it is possible to have a Wi-Fi connection, but no Internet access.

Since Wi-Fi is a wireless networking standard, any device with a "Wi-Fi Certified" wireless card should be recognized by any "Wi-Fi Certified" access point, and vice-versa. However, wireless routers can be configured to only work with a specific 802.11 standard, which may prevent older equipment from communicating with the router. For example, an 802.11n router can be configured to only work with 802.11n devices. If this option is chosen, devices with 802.11g Wi-Fi chips will not be able to connect to the router, even though they are Wi-Fi certified.

How Wi-Fi Works

Wi-Fi works with no physical wired connection between sender and receiver by using radio frequency (RF) technology -- a frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space.

The cornerstone of any wireless network is an access point (AP). The primary job of an access point is to broadcast a wireless signal that computers can detect and "tune" into. In order to connect to an access point and join a wireless network, computers and devices must be equipped with wireless network adapters

Bluetooth

Bluetooth is defined as being a *short-range radio technology* (or wireless technology) aimed at simplifying communications among Internet devices and between devices and the Internet. It also aims to simplify data synchronization between Internet devices and other computers.

Bluetooth products -- that is products using Bluetooth technology -- must be qualified and pass interoperability testing by the Bluetooth Special Interest Group prior to release. Bluetooth's founding members include Ericsson, IBM, Intel, Nokia and Toshiba.

We're all use to wireless communication by now, even if we don't always realize it. Radio receivers and television sets pick up programs beamed in radio waves hundreds (possibly even thousands) of km/miles through the air. Cordless telephones use similar technologies to carry calls from a handset to a base station somewhere in your home. If you use Wi-Fi (wireless Internet), your computer sends and receives a steady stream of Internet data to and from a router that's probably wired directly to the Net. All these technologies involve sending information back and forth not along copper cables but in radio waves buzzing invisibly through the air.

Bluetooth is a similar radio-wave technology, but it's mainly designed for communicating over short distances less than about 10m or 30ft. Typically, you might use it to download photos from a digital camera to a PC, to hook up a wireless mouse to a laptop, to link a hands-free headset to your cellphone so you can talk and drive safely at the same time, and so on. Electronic gadgets that work this way have built-in radio antennas (transmitters and receivers) so they can simultaneously send and receive wireless signals to other Bluetooth gadgets. Older gadgets can be converted to work with Bluetooth using plug-in adapters (in the form of USB sticks, PCMCIA laptop cards, and so on). The power of the transmitter governs the range over which a Bluetooth device can operate and, generally, devices are said to fall into one of three classes: class 1 are the most powerful and can operate up to 100m (330ft), class 2 (the most common kind) operate up to 10m (33ft), and class 3 are the least powerful and don't go much beyond 1m (3.3ft).

How does Bluetooth work?

Bluetooth sends and receives radio waves in a band of 79 different frequencies (channels) centered on 2.45 GHz, set apart from radio, television, and cellphones, and reserved for use by industrial, scientific, and medical gadgets. Don't worry: you're not going to interfere with someone's life-support machine by using Bluetooth in your home, because the low power of your transmitters won't carry your signals that far! Bluetooth's short-range transmitters are one of its biggest plus points. They use virtually no power and, because they don't travel far, are theoretically more secure than wireless networks that operate over longer ranges, such as Wi-Fi. (In practice, there are some security concerns.)

Bluetooth devices automatically detect and connect to one another and up to eight of them can communicate at any one time. They don't interfere with one another because each pair of devices uses a different one of the 79 available channels. If two devices want to talk, they pick a channel randomly and, if that's already taken, randomly switch to one of the others (a technique known as spread-spectrum frequency hopping). To minimize the risks of interference from other electrical appliances (and also to improve security), pairs of devices constantly shift the frequency they're using—thousands of times a second.

When a group of two or more Bluetooth devices are sharing information together, they form a kind of ad-hoc, mini computer network called a piconet. Other devices can join or leave an existing piconet at any time. One device (known as the master) acts as the overall controller of the network, while the others (known as slaves) obey its instructions. Two or more separate piconets can also join up and share information forming what's called a scatternet.