

i-Net+ Exam and Networking Study Guide

for the
The Beacon Institute for Learning

Table of Contents

| | |
|--|-----------|
| Table of Contents | 2 |
| Overview | 3 |
| Prosoft Foundations vs. iNet+ | 4 |
| i-Net+ Exam Blueprint | 6 |
| Question Domain breakdown for examination..... | 6 |
| What to Expect at the Testing Site | 9 |
| Test Statistic Summary | 9 |
| i-Net+ and Networking Topics | 10 |
| URLs, IP Addresses and Port Numbers | 10 |
| Site Performance and Caching | 11 |
| Search indexes | 14 |
| Client Software | 15 |
| Desktop Configuration..... | 16 |
| Browser Configuring and MIME Types | 18 |
| Legacy Issues | 19 |
| Patches, Bug Fixes, Security and Virus protection | 19 |
| Viruses | 20 |
| Cookies | 21 |
| Programming Environments | 21 |
| How Server side programming is used | 22 |
| Programming Languages | 23 |
| Databases, ODBC, JDBC and connectivity tools | 24 |
| HTML..... | 25 |
| Multimedia Plug-ins and File Formats..... | 28 |
| Pre-Launch Testing..... | 30 |
| Internet Infrastructure and Connectivity | 30 |
| Domain names and DNS..... | 31 |
| TCP/IP Essentials | 33 |
| Remote Access Protocols, Information Protocols and Services..... | 34 |
| Diagnostic Tools..... | 35 |
| Network Devices..... | 36 |
| Connection and Bandwidth..... | 39 |
| Servers | 41 |
| Encryption and Virtual Private Networks | 43 |
| Internet Security..... | 45 |
| Network and Server Security | 46 |
| Suspicious Activities..... | 47 |
| Security and Business Arrangements | 49 |
| Intellectual Property..... | 50 |
| Global Marketplace | 51 |
| Audience Development..... | 51 |
| E-Commerce terms and Concepts | 52 |
| The OSI Reference Model | 52 |
| Practice Questions | 55 |
| Index | 56 |

Overview

The i-Net+ exam was developed by CompTIA to test and certify that professionals understood the concepts of the Internet and how the World Wide Web operates. Unlike the CIW Examinations there is no definitive book on what is covered on the iNet+ exam. CompTIA has only issued a “blueprint” of the topic they will cover. There are many books to prepare you for the exam; you can find an annotated list of those books in the “Other iNet+ Review Sources” section of this booklet.

The material presented in class, along with the Prosoft CIW Foundations books, the Deitel, Deitel and Neito, *eCommerce How to Program* book and this guide will prepare you for the exam. You still need to read study and know these materials.

If you have not taken a standardized exam recently, you will want to take some standardized exams before taking the i-Net+ exam. There are a number of on-line sites to take sample, standardized exams. You will find them listed in the Practice section of this booklet.

CompTIA has broken down the job roles of the computer industry and has targeted the iNet+ to the following job roles:

- A. **Internet Systems Administrators.** Manage and tune corporate Internet and Intranet infrastructure (DNS, FTP and Web server). Manage machines running Internet services down to the operating system level.
- B. **Internet Security Specialists.** Define, develop and manage corporate security policies; audit security mechanisms such as firewall systems and attack recognition products and technologies; manage the deployment of security solutions.
- C. **Internet Application Developers.** Develop client side and server side Internet applications.
- D. **Internet Database Specialists.** Develop and implement solutions for integrating the back-end database systems with Internet applications for real-time access to customer and corporate information.
- E. **Internet E-Commerce Specialists.** Develop transaction-based systems including commerce, inventory and workflow-related systems.
- F. **Internet Network Specialists.** Manage and tune hardware, connectivity, network protocols, routing and switching.
- G. **Internet Site Designers.** Design Internet site structure and user interface.

We realize that you may not be interested in pursuing all these job domains. But having background knowledge for each of them will make you a more marketable job candidate.

Prosoft Foundations vs. iNet+

The Prosoft CIW Foundations examination and the iNet+ examination are both entry-level examinations for careers in the Internet world.

The chart below shows how the tests relate to certification. The iNet+ examination adds the iNet+ Certified Professional designation to your qualifications. This is an advantage since the iNet+ is coming from a better-known Certification organization, CompTIA. CompTIA is an industry-based membership organization with members such as IBM and Microsoft. It has a history of administering certifications, including the A+ and Net+, and is well known. Prosoft is relatively new in the field but has been making alliances with major companies in the past few years. The CIW certification is not yet well known but has gained the respect of major industry forces in the short time it has been in existence.

Any certification will assist you in becoming hired for a job. Given equal backgrounds employers will almost always choose the certified individual over one without certifications. Better known certifications will also help because hiring managers and supervisors will associate that certification with quality and expertise.

Notice the test numbers in the boxes on the certification paths chart below, you should always request your test by number and let the testing company verify its name. There are many tests with similar names but their numbers are different.

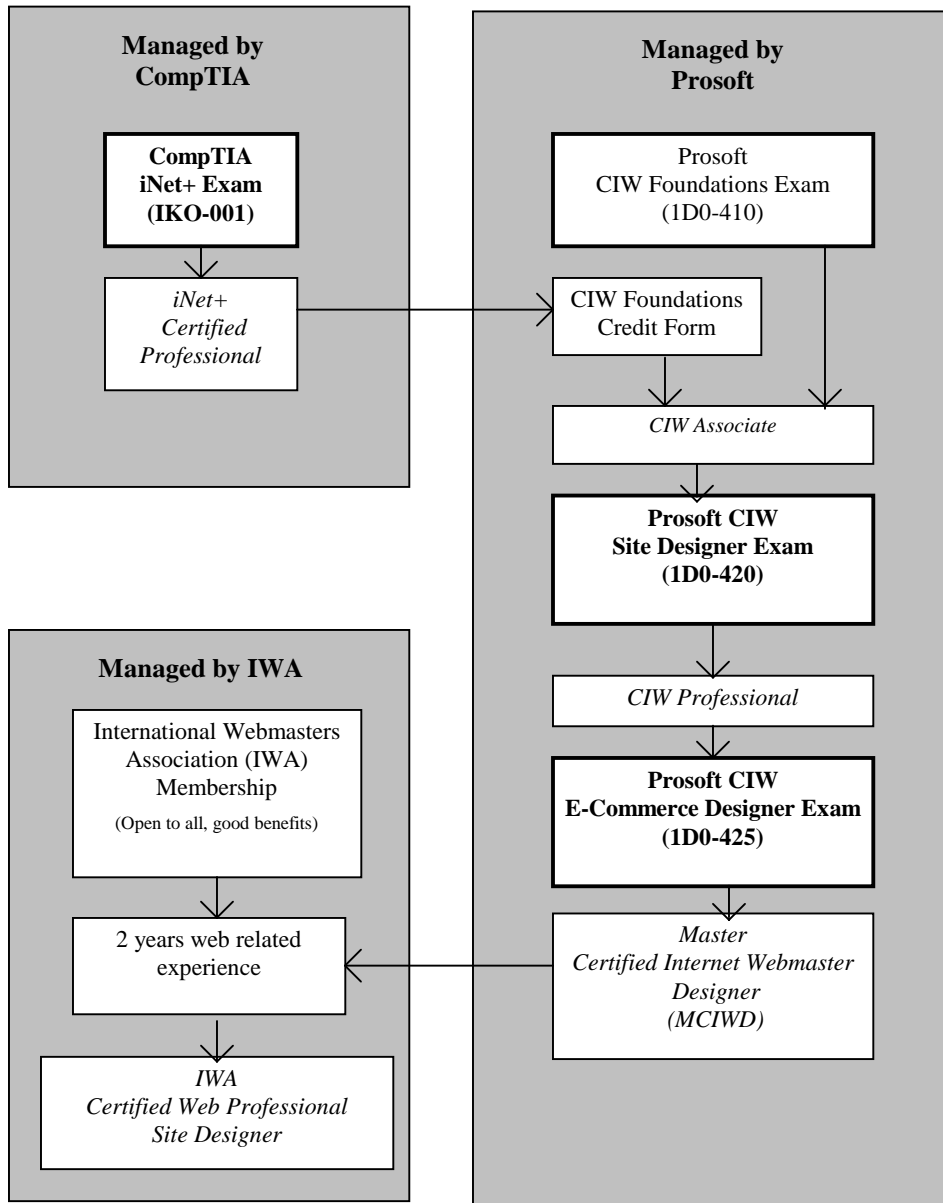
At this time (Spring 2001) there are no other widely recognized, entry level, certification tests for Internet skills. The World Organization of Webmasters (WOW) recently announced it would develop a certification exam system. WOW Certifications will not begin until late 2001 or early in 2002. The WOW certifications will be based on WOW developed courseware similar to the Prosoft CIW books.

CompTIA recently (Spring 2001) acquired a company, Gartner Institute, which was also marketing an eBusiness Fundamentals certification. They are in the process of reworking their test and marketing it as the CompTIA e-Biz+ exam. At the current time it is not widely available and there are few review materials available for it. Prometric plans to have this test distributed to its testing site systems by mid-summer 2001.

Certification Path(s) Overview.

Italicized items are the titles/certifications gained at each step of the process.

Bold items are the certification examinations you must take.



i-Net+ Exam Blueprint

This material is based on the July 1999 revision of the blueprint. Please check for updates at: <http://www.comptia.org/certification/inetplus>

CompTIA breaks down the skills you need for jobs in the Internet field and regroups them into “domains” of knowledge. The domains are then defined

This examination blueprint includes weighting, test objectives, and example content. Example topics and concepts are included to clarify the test objectives; they should not be construed as a comprehensive listing of the content of this examination. The blueprint may undergo additional minor modifications during the final test development workshop.

The table below breaks down the domains measured by this examination and the approximate percentage of questions on the exam they will represent. We will be dealing with each topic in more detail later in this booklet.

Question Domain breakdown for examination

| Domain | Topic | % of Questions on Examination |
|--------|-------------------|-------------------------------|
| 1.0 | i-Net Basics | 10% |
| 2.0 | i-Net Clients | 20% |
| 3.0 | Development | 20% |
| 4.0 | Networking | 25% |
| 5.0 | i-Net Security | 15% |
| 6.0 | Business Concepts | 10% |

Domain 1.0 I-NET BASICS

(1.1) Describe a URL, its functions and components, different types of URLs, and use of the appropriate type of URL to access a given type of server. Including: Protocol, Address, Port.

(1.2) Identify the issues that affect Internet site functionality (e.g., performance, security and reliability). Including: Bandwidth, Internet connection points, Audience access, Internet Service Provider (ISP), Connection types, Corrupt files, Files taking too long to load, Inability to open files, Resolution of graphics.

(1.3) Describe the concept of caching and its implications. Including: Server caching, Client caching, Proxy caching, Cleaning out client-side cache, Server may cache information as well, Web page update settings in browsers.

(1.4) Describe different types of search indexes – static index/site map, keyword index, full text index. Including: Searching your site, Searching content, Indexing your site for a search.

Domain 2.0 I-NET CLIENTS

(2.1) Describe the infrastructure needed to support an Internet client.; Including: TCP/IP stack;; Operating system; Network connection; Web browser; E-mail; Hardware platform (PC, handheld device, WebTV, Internet phone);

(2.2) Describe the use of Web browsers and various clients (e.g., FTP clients, Telnet clients, email clients, all-in-one clients/universal clients) within a given context of use. Including: When you would use each; Basic commands you would use (e.g., put and get) with each client (e.g., FTP, Telnet);

(2.3) Explain the issues to consider when configuring the desktop. Including: TCP/IP configuration (NetBIOS name server such as WINS, DNS, default gateway, subnet mask, Host file configuration; DHCP versus static IP; Configuring browser (proxy configuration, client-side caching).

(2.4) Describe the MIME types and their components. Including: Whether a client can understand various email types (MIME, HTML, uuencode); The need to define MIME file types for special download procedures such as unusual documents or graphic format.

(2.5) Identify problems related to legacy clients (e.g., TCP/IP sockets and their implication on the operating system). Including: Checking revision date, manufacturer/vendor; Troubleshooting and performance issues; Compatibility issues; Version of the Web browser.

(2.6) Explain the function of patches and updates to client software and associated problems. Including: Desktop security; Virus protection; Encryption levels; Web browsers; E-mail clients.

(2.7) Describe the advantages and disadvantages of using a cookie and how to set cookies. Including: Setting a cookie without the knowledge of the user; Automatically accepting cookies versus query; Remembering everything the user has done; Security and privacy implications.

Domain 3.0 DEVELOPMENT

(3.1) Define the programming-related terms as they relate to Internet applications development. Including: API; CGI; SQL; SAPI; DLL – dynamic linking and static linking; Client and server-side scripting;

(3.2) Describe the differences between popular client-side and server-side programming languages. Examples could include the following: Java; JavaScript; Perl; C; C++; Visual Basic; VBScript; Jscript; XML; VRML; ASP. Including: When to use the languages; When they are executed.

(3.3) Describe the differences between a relational database and a non-relational database.

(3.4) Identify when to integrate a database with a Web site and the technologies used to connect the two.

(3.5) Demonstrate the ability to create HTML pages. Including: HTML document structure; Coding simple tables, headings, forms; Compatibility between different browsers; Difference between text editors and GUI editors; Importance of creating cross-browser coding in your html;

(3.6) Identify popular multimedia extensions or plug-ins. Examples could include the following; QTVR (quick time); Flash; Shockwave; RealPlayer; Windows Media Player.

(3.7) Describe the uses and benefits of various multimedia file formats. Examples could include the following: GIF; GIF89a; JPEG; PNG; PDF; RTF; TIFF; PostScript; EPS; BMP; MOV; MPEG; AVI; BINHex; Streaming media; Non-streaming media;

(3.8) Describe the process of pre-launch site/application functionality testing. Content could including the following: Checking hot links; Testing different browsers; Testing to ensure it does not corrupt your web commerce site; Load testing; Access to the site; Testing with various speed connections.

Domain 4.0 NETWORKING AND INFRASTRUCTURE

(4.1) Describe the core components of the current Internet infrastructure and how they relate to each other. Including: Network access points; Backbone.

(4.2) Identify problems with Internet connectivity from source to destination for various types of servers. Examples could include the following: E-mail; Slow server; Website.

(4.3) Describe the Internet domain names and DNS. Including: DNS entry types; Hierarchical structure; Role of root domain server; Top level or original domains – edu, com, mil, net, gov, org; Country level domains -- uk, us, mx, de, fr, ru, jp, etc.;

(4.4) Describe the nature, purpose, and operational essentials of TCP/IP.

Including: What addresses are and their classifications (A, B, C,D); Determining which ones are valid and which ones are not (subnet masks); Public versus private IP addresses;

(4.5) Describe the purpose of remote access protocols. Including: SLIP; PPP; PPTP; Point-to-point/multipoint.

(4.6) Describe how various protocols or services apply to the function of a mail system, Web system, and file transfer system. Including: POP3; SMTP; HTTP; FTP; NNTP (news servers); TCP/IP; LDAP; LPR; Telnet; Gopher.

(4.7) Describe when to use various diagnostic tools for identifying and resolving Internet problems. Including: Ping; WinIPCfg; IPConfig; ARP; Trace Routing Utility; Network Analyzer; Netstat.

(4.8) Describe the hardware and software connection devices and their uses. Including: Network interface card; Various types of modems including analog, ISDN, DSL, and cable; Modem setup and commands; Adapter; Bridge; Internet-in-a-box; Cache-in-a-box; Hub; Router; Switch; Gateway; NOS; Firewall.

(4.9) Describe various types of Internet bandwidth technologies (link types). Including: T1/E1; T3/E3; Frame relay; X.25; ATM; DSL.

(4.10) Describe the purpose of various servers – what they are, their functionality, and features. Including: Proxy; Mail; Mirrored; Cache; List; Web (HTTP); News; Certificate; Directory (LDAP); E-commerce; Telnet; FTP;

Domain 5.0 I-NET SECURITY

(5.1) Define the following Internet security concepts: access control, encryption, auditing and authentication, and provide appropriate types of technologies currently available for each. Examples could include the following: Access control – access control list, firewall, packet filters, proxy; Authentication – certificates, digital signatures, non-repudiation; Encryption – public and private keys, secure socket layers (SSL), S/MIME, digital signatures, global versus country-specific encryption standards; Auditing – intrusion detection utilities, log files, auditing logs; SET (Secure Electronic Transactions).

(5.2) Describe VPN and what it does. Including: VPN is encrypted communications; Connecting two different company sites via an Internet VPN (extranet); Connecting a remote user to a site.

(5.3) Describe various types of suspicious activities. Examples could include the following: Multiple login failures; Denial of service attacks; Mail flooding/spam; Ping floods; Syn floods.

(5.4) Describe access security features for an Internet server (e.g., email server, Web server). Examples could include the following: User name and password; File level; Certificate; File-level access: read, write, no access;

(5.5) Describe the purpose of anti-virus software and when to use it. Including: Browser/client; Server.

(5.6) Describe the differences between the following as they relate to security requirements: Intranet; Extranet; Internet.

Domain 6.0 BUSINESS CONCEPTS

(6.1) Explain the issues involved in copyrighting, trademarking, and licensing. Including: How to license copyright materials; Scope of your copyright; How to copyright your material anywhere; Consequences of not being aware of copyright issues, not following copyright restrictions.

(6.2) Identify the issues related to working in a global environment. Including: Working in a multi-vendor environment with different currencies, etc.; International issues – shipping, supply chain; Multi-lingual or multi-character issues (Unicode); Legal and regulatory issues;

(6.3) Define the following Web-related mechanisms for audience development (i.e., attracting and retaining an audience): Push technology; Pull technology.

(6.4) Describe the differences between the following from a business standpoint: Intranet; Extranet; Internet.

(6.5) Define e-commerce terms and concepts. Including: EDI; Business to Business; Business to Consumer; Internet commerce; Merchant systems; Online Cataloging; Relationship management; Customer self-service; Internet marketing;

What to Expect at the Testing Site

Both Vue and Sylvan Prometric are usually very good about test security. This means there are many rules that you will need to be prepared for before and while you take your test.

You need to arrive on time or slightly early for your testing appointment. Your test is not transferred to the testing site until a short time before the appointment. If you are too early you may have to wait for the test to transfer to their system.

You may not bring anything into the testing room that could help you with answers. Many testing sites do not provide a storage area or lockers for anything you may have brought with you. You need to plan ahead and only bring the essentials: Two forms of ID and any payment needed (if you did not pay online).

The testing center will provide you with a pencil and paper for notes during the tests, you may not bring in anything else. The following may NOT be brought to a test: Cell phones, pagers, calculators, pens, notebooks, books, children, computer, PDAs, purses, etc.

When you arrive you'll go to the front desk and present your ID and payment. You will then sign a log of the time you arrived. When there is a place available you will be seated in the testing room and the test administrator will sign-you onto the computer for your test. The computer will usually ask a few basic questions before the main test begins.

Once the test begins, it is almost identical to the Transcender including the ability to mark answers that you want to review. Take your time and read every question carefully as you test. Do not get stressed if there appear to be errors or confusing phrasing. Just find the best answer for each question. Once you answer the last questions you will be given a last opportunity to review to your answers before the test is scored.

If anything goes wrong during the test, let the front desk know immediately. At the end of the test you will usually be asked a few questions about the testing center. If you are hot or cold, if there is too much glare on the screen, anything that could affect your performance should be noted on these blanks.

The test is scored automatically and before you standup from your seat you will be told if you have passed the test. Once the test is over take your pencil and paper and return to the front desk where they should have your score report. You should turn in your materials to the front desk and they will give you your score report.

Test Statistic Summary

| | |
|-----------------------------------|-------------------------------|
| Number of Scored Questions | 72 |
| Passing Score | 73% (53 correct) |
| Time Allowed | 90 minutes |
| Average Time needed | 35 minutes |
| Managing Body | CompTIA |
| Standard Price | \$190 (as of 01 January 2001) |
| Beacon Coupon Price | \$144 (as of 01 March 2001) |
| Testing Centers | Vue, Prometric |

i-Net+ and Networking Topics

URLs, IP Addresses and Port Numbers

URLs are Uniform (or Universal) Resource Locators. They are a method to uniquely identify a computer, directory or file on any computer attached to the Internet. URLs are made up of a protocol, hostname, port number, directory and filename. They can also include user and password information. As follows:

```
protocol://hostname:port/directory/filename.type
```

```
protocol://user:password@host:port/directory/filename.type
```

The protocol must be recognized by the client computer to connect properly. The user and password fields are sometimes used with gopher, wais, ftp and other connections. They allow the user to login to the server when dialog boxes are not available. The hostname can be an IP address, or a domain name. The port can be any number from 0 through 65,535. The directory needs to be a valid directory name and you may have multiple directories, each separated by a slash. The filename and type are specific to the server computer. Usually the filename and type are recognizable as a common file name and extension, but they do not have to be.

A protocol and hostname are required for an address to be valid. The other items are optional. The port is used, but is fairly uncommon. Different protocols may have other requirements for their syntax to be valid. That information is not required for the iNet+ test.

The following are all valid URLs. Notice that mailto and news protocols do not use the colon-slash-slash syntax between the protocol and hostname.

| | | |
|------------------------------|--|-------------------------|
| http://www.yahoo.com | http://go.to | ftp://simtel.com/public |
| mailto:student@edutech.net | http://svr.mysite.com/files/mine/more/here/graphic.gif | |
| gopher://gopher.yoyodyne.com | telnet://training:secret@corporate.net:21/ | |
| news:rec.gardening | http://www.yoyodyne.com:1234/pub/files/foobar.html | |

IP addresses are most often written as four sets of numbers from 0 to 255 separated by periods, like this: 178.122.34.250. Each set is called an octet. In the example the second octet is 122 and the third octet is 34.

IP addresses were originally assigned in blocks of different sizes. The governments and major corporations purchased large blocks of IP addresses and smaller companies bought smaller blocks of IP addresses. The different block sizes of IP address are called classes. There are officially 5 classes, named A,B,C,D, and E. Classes D is reserved for special uses we'll talk about later and class E is reserved for future use.

The number in an IP address's first octet identifies what class of IP address an IP address is originally from. It is important to also note that within the set of IP addresses there are reserved blocks of IPs. Every class of IP has a reserved block of addresses that are not for Internet use. The reserved blocks are used for special network configurations and testing. Those are noted in the table below.

| Class | First octet(s) | Reserved Block | Default Subnet Mask | Number of IPs per block | Comment |
|-------|----------------|--------------------------------|---------------------|-------------------------|-------------|
| A | 001 to 126 | 10.0.0.0 to 10.255.255.255 | 255.0.0.0 | 116,777,214 | |
| | 127 | 127.0.0.0 to 127.255.255.255 | | | Loopback. |
| B | 128 to 191 | 172.16.0.0 to 172.31.255.255 | 255.255.0.0 | 65,534 | |
| C | 192 to 223 | 192.168.0.0 to 192.168.255.255 | 255.255.255.0 | 254 | |
| D | 224 to 239 | None | | | Multicast |
| E | 240 to 255 | None | | | Future use. |

For the i-Net+, remember the groupings of the first octet and the reserved blocks. You need to associate those with the class letter and the default subnet mask.

The 127 IP block is a special case of reserved IP address. Any IP address starting with 127 is known as a loopback address. These IP addresses are used for internal testing of components and are setup to not be transmitted by most network cards. Traffic sent to an 127.anything address never leaves the computer.

Subnet masks set the rules for a computer about which computers are on its local network and which need to go through a gateway. Note that the A, B, and C class default subnet masks have 1, 2 and 3 octets of 255 respectively. (You'll read more about subnet masks on page 17)

Port numbers are associated in a computer with a particular listening program called a daemon. These daemons are generally associated with a particular protocol. As an example, the program that responds to HTTP requests in servers will usually listen to traffic marked for port 80. At the same time the program that responds to FTP requests listens to port 21. If no port number is specified for a packet the default or "well known port number" will be handed the traffic.

For the i-Net+ you need to know the following "well known port numbers".

| Port | Service/Protocol | Port | Service/Protocol |
|------|------------------|------|------------------|
| 21 | FTP | 80 | HTTP or WWW |
| 23 | Telnet | 110 | POP3 |
| 25 | SMTP | 119 | NNTP |
| 53 | DNS | 389 | LDAP |

All ports with numbers from 0 through 1023 are considered "well known port numbers". They are to not be used for a service or protocol other than the "well known" service or protocol associated with that port. Some port numbers between 1024 through 49151 have a default associated protocol or service, but can be used for any protocol the user wishes. Port numbers from 49152 through 65535 are open and can be used by any service or protocol. Client computers use these higher numbered ports to send requests to servers and to listen for the response to each request on a separate port.

Site Performance and Caching

Web sites need to be configured to maximize performance, security and reliability. The factors most often responsible for good or poor site performance are: bandwidth issues, internet connection points problems, audience access, internet service provider (ISP) speed, connection types, corrupt files, files taking too long to load, the inability to open files, and the resolution of graphics.

Bandwidth is the amount of data that can be simultaneously transmitted on a medium. Usually, the amount of bandwidth that can be used by a site is equal to the amount of bandwidth that can reach the site.

Bandwidth can be a problem at both ends of the connection. The user may not have a fast enough or reliable enough connection to receive the page content within a reasonable amount of time. The server might also be receiving more requests per second than it can handle or need to transfer more content per second that it's connection to the Internet can handle. It is generally assumed that between the Server's ISP/Hosting Company and the user's ISP there is enough bandwidth to handle the content's transfer. There have been instances of bandwidth outages on backbones of the Internet but these are rare.

If a server is primarily a web server but starts receiving and handling a high percentage of mail or FTP requests this can affect the web site's performance. A server can change how it responds to requests, however, by invoking "bandwidth throttling." Throttling allows you to reduce the amount of bandwidth the site will offer for any one task, thus leaving the server hosting the site with additional bandwidth that can be allocated to other services on the same server, or other servers in the same location which host other sites or services.

The majority of users access the Internet through **Internet Service Provider (ISP)**. ISPs buy their connection from another ISP or, more often, a **Network Access Point (NAP)**. These major connection points were sometimes called a **Metropolitan Area Exchange (MAE)**. Originally there were three major NAPs in the United States, located in the Chicago, New York and San Francisco areas. The New York and San Francisco MAEs were

also known as MAE East and MAE West respectively. More recently, most large cities and all state capitals have a local NAP used to provide high-speed connections.

Audience access is a major factor of how web sites are perceived and used. The audience are the users you are publishing your site to attract. Their access determines how they use your site. The target audience of a site should be defined and the site should be designed for their experience level. For low-experience users you may want to include the words “click here” with links, though most users, and especially advanced users, consider this very poor design. The language and technical terminology used in web page instructions or text should also reflect your target audience’s knowledge base.

The users’ connection speed should also be considered. If your users are predominantly low-speed dial-up users, such as rural or home users, then files to be downloaded should be compressed, and you should use simple graphics and avoid large, full-color pictures on your site’s most used pages.

Connection types determine how your site will be designed. Connections can be established through dial-up service, proxy service, dedicated lines (ISDN, T1, etc.), these connections are discussed more later in this booklet (see page 39). Not all connections are available in all areas. DSL, T-1, T-3 connections are only available within about 3 miles of a telephone switching office or NAP.

Bandwidth is amount of bits of data flowing at any given time. For example, a 56K modem may transmit at 57,600 bps (bits per second), so it has (up to) 57,600 bps bandwidth. Unfortunately, American residential quality phone lines usually can handle only 53,000 bps of signal in analog mode. Other transmission factors such as interference, signal quality and static can also affect be a top speed a computer can connect. It is not unusual for a home user to only be able to connect at 33,000 bps. This difference in connection speed can significantly change how you need to design your web site. The user or can only receive sixty percent as much information in the 10 seconds most are willing to wait.

File corruption can occur at any time and prevent users from accessing your resources successfully. **Corrupt files** happen. There is no one reason for files becoming corrupt. Anything from a power surge to an error in a computer program can cause a file to become corrupt. Because of this, it is important to test your files before posting/uploading them, and to continue to check them for corruption and correct, as needed. Users reporting that a file is not working, needs to be investigated because the file may have become corrupt since you last checked.

Files taking too long to load will drive away many users. A well-designed site can have the problem of being too complicated for normal users to receive within the time they’re willing to wait. Most users will wait 10 seconds or less for a page to load. Users may be willing to wait longer if they know what they are loading. When planning your site consider the bandwidth of the median audience is using to reach your site.

To solve the issue of long or large pages the site creator can beak a large file into smaller files. For example, instead of posting one 88-page PDF file that will take forever for a slow connection to load, break the file into eleven 8-page segments that can be loaded individually.

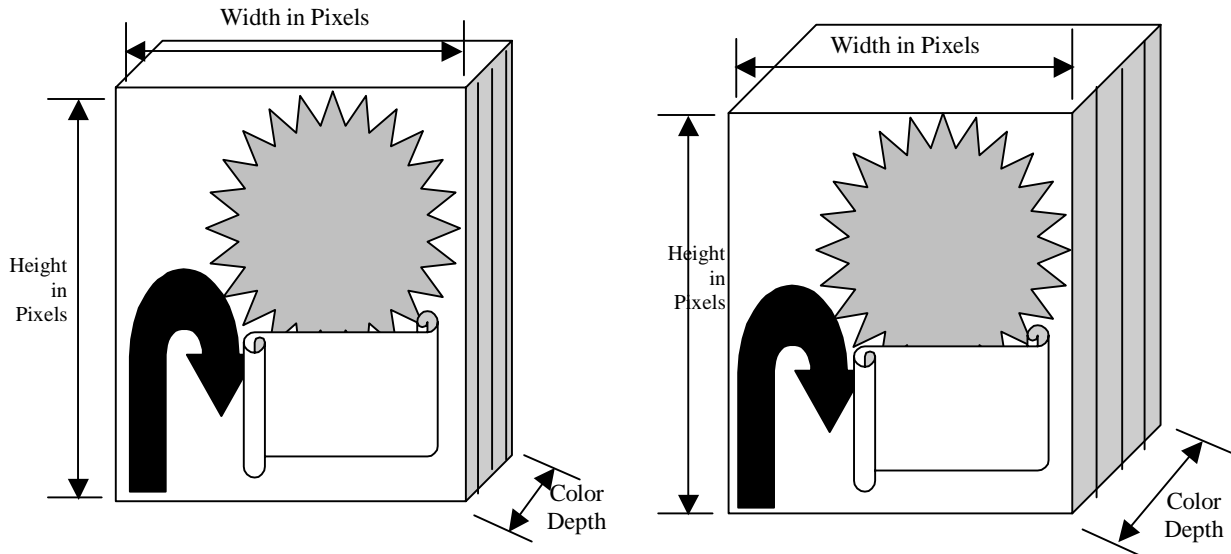
Inability to open files also will prevent users from exploring your site. Different browsers and computers have different file types that they know how to receive and open. For example Macintosh computers generally do not know about the BMP file type while Internet Explorer on a Windows computer opens it up as a native file format. Netscape Navigator on a Windows computer also will usually not open a BMP file within the web page but may try download it as a separate file. Try to avoid browser dependencies whenever and wherever possible. You should stick with well-known file formats that are accessible across most platforms.

When you do use plug-ins, such as Flash, Comet Cursor, or other special programs, you should provide a link to a site where the user can download the appropriate plug-in.

Resolution of graphics – Graphics are described in their resolution two ways, first in the number of pixels wide or high they are; and also in the number of colors each of those pixels can be.

The saved width and height in pixels of a graphic should match as closely as possible the number of pixels that will be used when the web page displays that graphic. Saving a file with many more pixels than when it is displayed will lead to a longer download times for the user. Saving a file with many fewer pixels than it will be displayed with will make the image graphic appear grainy or pixilated and jagged in the users’ browser.

Color depth is the determining factor of the accuracy of color in graphics. It is based on the total number of colors a picture can display; and is expressed in bits: the greater the number of bits, the better the graphic. While 24-bit graphics are perfect for an ideal world, if you want to serve all users, you should use 8-bit graphics. There are still 256-color (8-bit) monitors in use. Using eight-bit graphics instead of 24-bit graphics can also speed downloading because the file will be significantly smaller.



Caching

A cache is a place to store something temporarily. When pages are transferred from a web site to your computer a number of different devices may temporarily store them in hopes of being able to bring them to you more quickly, if someone requests them again.

Server caching stores page information on a server to speed up requests for a page. Instead of the reading the web page again from its hard drive the Web server will keep a copy of that page in memory. This not only improves the speed with which the computer can answer a page request that also can reduce the wear and tear on the server hard drive. To cache more pages and to respond to users more quickly, high traffic servers will have large amounts of RAM installed so they can keep more pages cached in RAM.

Client caching enables the client's computer to load a page from its own hard drive instead of again requesting it through the Internet. Recently viewed pages are stored on the client computer hard drive. The speeds up the time it takes to display the web page, since it does not have to wait for a connection to be made to the remote Web server. Unfortunately if a web page's content has changed, the reload from cache will not reflect the changed Web contents. This can cause problems for the user, as well as lead to confusing and complaints and help desk calls for the server operator. Internet browsers have the ability to check to see if content has changed but many browsers are set to only check for new contents once a day rather than every visit to the web site.

Proxy caching occurs between the server and the client. Again the files are stored temporarily in hopes a request can be answered more quickly. They're a number of places this can occur. In small businesses the proxy server itself will be doing the proxy cache operation. For home users, the ISPs will often perform the proxy cache operation. In those situations this reduces the amount of bandwidth the ISPs or small business is using and can save on their monthly connection bill. Sites like Yahoo and eBay may be cached so that users will get their requested page very quickly. Depending on how the proxy is configured it may not check for new contents on cached pages for 10 seconds, a minute or maybe up to a half-hour.

Cleaning out the client-side cache is important to solve the most common caching issues. Users should know how to clear their own cache to avoid problems with cached pages. For the i-Net+ exam you should know the steps to clear the client side cache and Internet Explorer 4 and Netscape Navigator 4.5. You should also know how to reset the amount of time a page is cached on the browsers.

It is possible for a cache file to be corrupt on the proxy, the server or the client. This of course causes unpredictable web page responses from the where the corrupt cached page is.

You can clean out a client-side cache using third party utilities or Internet Options in IE and Preferences in Netscape. This frees up hard drive space and allows a fresh page to be loaded from the server. A server may cache information as well, which will show you a older page than what is currently available. A web designer can put code in a page showing it as expired, always making your browser load a recent version. In your Internet Options or Preferences, you can also change how much cache and how often pages are downloaded.

Search indexes

Web sites need to consider the user searching their contents three different ways. They are: the static index or site map; the keyword index, and the full text index. Users visiting sites will use whatever index is available to search the site to more quickly find what they are looking for. The better you are index were search service is the more pleased your users will be.

A **static index** or site map is a web page produced by the computer user or buy computer program that lists the contents of a site by their main topics. This type of search indexes needs to be updated regularly or with every major web sites updates said it correctly reflects the content and organization of the web site.

A **keyword index** is used to only search for certain words on a web site. These keywords are stored in META tags on the web pages or the administrator can create a file of what words he or she wants to be indexed on the site. A program similar to a spider or robot then goes through all the pages on the site and collects the words that are in the keyword list or the keyword META tags.

A **full text index** of a web site uses all the words on all the connected pages in the web site to build a list of the words on that site. This index of words is then searchable using a search engine. Search engine software can be installed on the Web server and a version of a search engine does come with the MS Front Page extensions.

Commercial search engines, such as AltaVista or Google, perform full text indexes of web page, which have been suggested to them. Some commercial search engines will not list or index all words, and may exclude the common words such as articles and propositions. A list of words to not index is called a “noise” list.

Commercial web site directories, like Yahoo and DMOZ, are more similar to a keyword index. Certain words and page descriptions are given into the directory services that are then used in user searches to match results.

Most search and directory engines have shortcuts to help you find what you're looking for more quickly. Using plus and minus signs and quotation marks in your search request will narrowed the results that are reported by the search or directory engines. The basics of rules for searching include:

| Search Request | Search Result |
|----------------|---|
| A | Finds pages with word A |
| B | Finds pages with word B |
| A B | Will find words A and words B |
| “A B” | Will find the words A and B together |
| +A B | Requires word A to be in the search results |
| A -B | Will find words A that do not contain words B |

Both network intranet and Internet files can be indexed using an index server. An index server is a computer running software that searches and indexes files for full text or keywords. The user can then use the result of the index server’s search and index to find their needed information quickly.

Infrastructure needed for an Internet client

In order to connect to the intranet the client must have five specific pieces of hardware and software.

First, and maybe the most obvious piece is a **hardware platform** such as a personal computer, PDA, WebTV, or Internet enabled phone.

Second, a **network connection** of some sort is required for computers this is most often getting to be a a modem or network a connection. For PDAs and cell phones this is often a wireless connection. WebTV and other devices may use other connections such as broadcast television signal or cable a television signal.

Whatever the hardware platform is, it needs to have installed on it an appropriate **operating system** with a compatible **TCP/IP stack**. For personal computers an appropriate operating system is something like a Windows or Mac OS. The TCP/IP stack often comes with the operating system as is the case with Windows, Mac and Linux computers. Web TV and cell phones have their own built-in operating system and TCP/IP connection system.

Once all the above pieces have been assembled, software needs to be installed or activated on the device that enables Internet transmission and reception. This is software such as a Web browser or an e-mail program. The most common examples of these would be Internet Explorer, Netscape Navigator, Microsoft Outlook or Outlook Express or the Eudora e-mail program. The software packages are known as client software.

TCP/IP is Transmission Control Protocol/Internet Protocol. TCP/IP is the basic communication language of the Internet. TCP manages the assembling of files or messages into packets. IP handles the address part of the delivery. TCP/IP is a point-to-point protocol, packets are sent from one computer to another. TCP/IP allows the client to communicate across the Internet to different types of systems and computers.

Client Software

In addition to Web browsers and e-mail programs there are other Internet client software packages. He needs know the basics of how to use many common Internet client software packages.

Web browsers and **e-mail programs** are probably the programs you are most familiar with. Web browsers to use HTTP protocol to connect to Web servers and many browsers can use other protocols. Email programs use SMTP to send mail to other computers and use POP3 to receive mail from their mail server.

FTP clients allow the user to use FTP protocol commands. FTP is a protocol that allows for a user or to request files from our remote computer or send files to a remote computer. The commands used most often are put and get. Once you're connected to a FTP server, you type the put command and your computer will transfer the named file to the FTP server. You could also type the get command and your computer will get the filename you entered from the FTP server. In addition to get and put, mput and mget allow user or to put or get multiple files.

| Command | Example Syntax | Summary |
|---------|--|---|
| put | put <i>filename</i> | Send a single file to the remote computer |
| get | get <i>filename</i> | Receive a single file from the remote computer |
| mput | mput <i>filename filename filename</i> | Send multiple files to the remote computer |
| mget | mget <i>filename filename filename</i> | Receive multiple files form the remote computer |

Telnet clients allow the user to use Telnet protocol commands. Telnet is a way to type information as though you are sitting at a remote computer's keyboard. The Telnet protocol replies to your computer with the information that appears on the screen of the remote computer. This allows clients to issue command line instructions for the remote computer and have the remote computer execute those commands. This is often used as a method for checking the status of UNIX computers and other devices that are connected to a network such as routers.

The command to start a Telnet connection is usually connect or Telnet with an IP address or domain name. Once you're connected to the remote computer what ever you type at the command line is sent to a to the remote computer. When you are done you type the command **exit**. On Windows-based computers you'll double-click a Telnet program and it will prompt you for what IP address or domain name you wish to connect to.

| Command | Example Syntax | Summary |
|------------|------------------------|--|
| telnet | telnet 100.125.199.207 | Connect to the remote computer |
| telnet | telnet yahoo.com | Connect to the remote computer |
| (commands) | (command host OS) | Commands during the telnet session are based on the remote computer's OS or environment. |
| exit | exit | Disconnect from the remote computer |

There are other clients for other protocols. Usually a client designed to handle a single protocol. An **All-in-one client** is made to handle many protocols. For example, Netscape Communicator is designed to handle NNTP protocol and FTP as well as HTTP, POP3 and SMTP. Microsoft Outlook handles SMTP, POP3, and NNTP protocols.

Desktop Configuration

In order for a desktop computer to connect to the Internet it needs to be properly configured. Using a dial-up connection the Internet service provider provides you with a phone number to connect to them through. SLIP or PPP protocols (see page 34) are used to connect from your computer to the ISPs equipment. Your ISP has already configured their equipment to correctly connect to the intranet.

When your computer is connecting through DSL, cable modem or is attached to a local area network it needs to be configured with basic information about how well connect to the Internet. The basic information needed is: an IP address, DNS addresses, a default gateway address, and a subnet mask. This information can be configured in the appropriate setup tool for the operating system; or it can be gathered through a DHCP request.

When a computer is configured to use **Dynamic Host Configuration Protocol (DHCP)**, the **network interface card (NIC)** sends a request onto the network for its network configuration information as it boots. Any DHCP server on the network responds to that DHCP request. Whichever DHCP request the computer receives first is acknowledged and that DHCP server's information is used to configure the computer. With DHCP, the DHCP server is responsible for managing the DNS information, IP addresses, the gateway address, and subnet mask information. The server administrator or network administrator sets up the basic settings for the DHCP server.

DHCP is based on **BOOTP** (Boot Protocol). The IP addresses received by DHCP are "leased" from a set of IPs that is setup and reserved for the DHCP server to assign. At any time, the leases can be renewed or released. Usually they are renewed halfway through the term of the lease. When and if the lease expires, such as when a computer is turned off, the IP address is placed back in the DHCP server's available list of IPs for use by another client.

If DHCP is not used, this configuration information comes from either your ISP or your network administrator. Every network is has a set of IP addresses to use for computers on that network. These IPs are rented from an IP assignment agency such as ARIN (the **American Registry of Internet Numbers**) in North and South America, and RIPE and APNIC in other areas of the world. No two computers on the same network are allowed to have the same IP address. No two computers connected directly to the Internet are allowed to have the same IP address.

Somewhere on every network will be a computer or device that is configured to relay traffic from within the network to outside of the network. That computer or device is called the **gateway**. The gateway computer's IP address is used by the computer being configured as the target address for traffic to that is going to the Internet. On large networks there may be more than in one computer configured as a gateway. The network administrator will choose which gateway device your computer uses as its default. Thus the name default gateway. A gateway is any device that can translate data from one network to another.

The **subnet mask** tells your computer which IP addresses are parts of its own network. The subnet mask value is based upon the class of network you have. The default values by class, and the maximum number of hosts are:

| Class | Default Subnet Mask | Total number of Hosts for Network |
|-------|---------------------|-----------------------------------|
| A | 255.0.0.0 | > 16 million |

| | | |
|---|---------------|---------|
| B | 255.255.0.0 | >65,000 |
| C | 255.255.255.0 | 254 |

Network engineers can calculate custom subnet masks to fit particular networking situations. Most organizations with a Class A IP address blocks will further mask their network; but for other organizations the default subnet masks, above, still remain the most used.

Your computer addresses traffic on its own network directly to the IP address that needs to go to. Any traffic that needs to go outside of its own network is addressed to go through the **default gateway**. The source computer makes the decision based on the source computer's subnet mask and the target's computers IP address. If the sending computer's IP address and the receiving computer's IP address are the same in the octets that are nonzero in the subnet mask, it can send the traffic directly to the target computer; because it is on the same network. If the source IP address and the target IP address are different in any of the parts of the subnet mask that are nonzero, then the information must be addressed to go through the gateway; because the computers are on separate networks.

| Source IP | Source subnet mask | Target IP | Octets where source and target are different | Value of different octets | Traffic directed to |
|---------------|--------------------|----------------|--|---------------------------|---------------------|
| 7.141.12.24 | 255.0.0.0 | 7.141.0.5 | 3 and 4 | Zero | Target computer |
| 7.141.12.24 | 255.0.0.0 | 208.141.12.24 | 1 | Nonzero | Gateway |
| 7.141.12.24 | 255.0.0.0 | 208.1.45.178 | 1,2,3,4 | Zero and nonzero | Gateway |
| 208.141.12.24 | 255.255.255.0 | 208.141.12.159 | 4 | Zero | Target computer |
| 208.141.12.24 | 255.255.255.0 | 208.141.15.24 | 3 | Nonzero | Gateway |
| 208.141.12.24 | 255.255.255.0 | 7.141.0.5 | 1,2,3,4 | Zero and nonzero | Gateway |
| 131.27.12.45 | 255.255.0.0 | 208.141.12.24 | 1, 2, 4 | Zero and nonzero | Gateway |
| 131.27.12.45 | 255.255.0.0 | 131.27.45.237 | 3, 4 | Zero | Target computer |

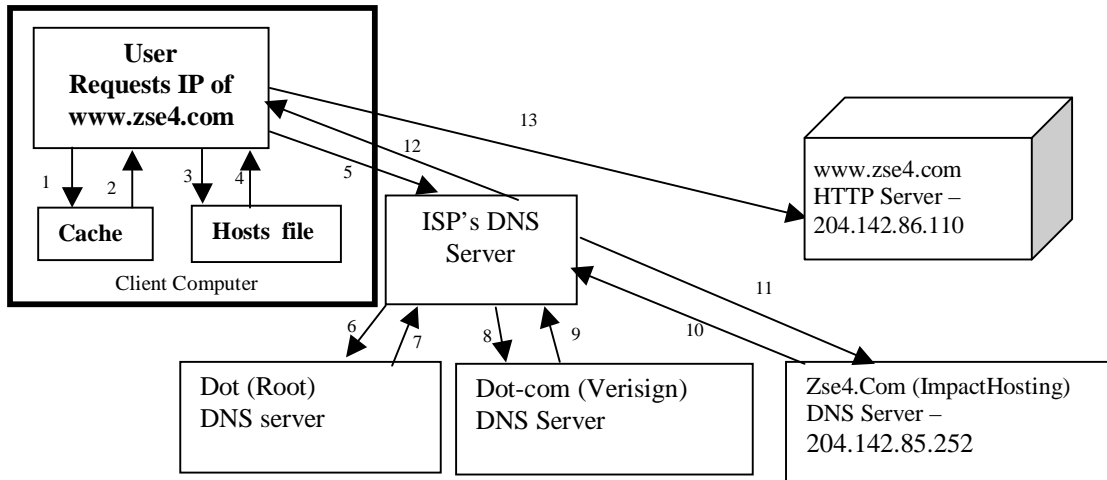
The above assumes that the source computer knows the target computer's IP address. There are two major systems used by a computer to hook up the target computers IP address: DNS and HOSTS.

For **DNS**, the source computer sends to a DNS server the domain name that it needs to contact. The DNS server then replies with what the IP address of that domain name's server is. In order to connect to the DNS server the computer must be given the IP address of that DNS server. The DNS system expects that there are two servers or two IP addresses available to answer any DNS request. That way of one of the DNS servers is too busy the other one can be used to answer the DNS request. More about DNS can be found on page 31.

Using **HOSTS**, the source computer has a file on its hard drive that lists names of computers and their matching IP address. This file, which is usually named HOSTS, is simply a list of the names and IP addresses for all the computers that system needs to connect with. There is no need for the computer to contact a DNS server to ask what an IP address is, it already has the address in its hosts file. The **Host file** allows a local computer to hardcode addresses. For example, the HOSTS file on a Windows NT system would allow you to code an address like MAIL_US001 to an IP Address 197.154.165.45. If you are having difficulty reaching a specific name on your network, placing an entry in your HOSTS file could eliminate the problem.

When using a web browser to connect to www.zse4.com, the following process takes place as shown in the drawing below. For simplicity this example assumes that zse4.com has not been contacted recently from the client computer or it's ISP. First, the client computer checks its own (1) cache of recent DNS lookups. The local cache returns (2) that it does not have the IP address of www.Zse4.Com. The browser then checks (3) its local HOSTS file for any entry for www.zse4.com. The HOSTS file reports (4) that it does not have www.zse4.com. The computer then send the DNS request to the DNS server (5) that is named in its configuration. That is usually the DNS of the ISP providing the connection for the client. If the ISP knows the IP address of our selected site it returns it without asking any other servers for that information. Since this is a first request, the ISP's DNS server sends a request to the Root DNS server (6), called "dot", for the DNS entry for www.zse4.com. The root DNS always answers that it does not know that site, but does provide (7) the IP address of the primary DNS server for all dot-Com sites. The ISP's DNS server, then requests (8) the IP address of www.zse4.com from the Dot-com DNS server. The dot-com DNS server replies (9) that it does not know www.zse4.com, but does know the IP address for zse4.com's DNS services.

The ISP's DNS server then requests (10) the IP address of www.zse4.com from the ZSE4.Com DNS server at 204.142.85.252. This DNS server then replies (11) that the IP address of www.zse4.com is 204.142.86.110. The ISP's DNS server then returns this IP address to the client computer (12). And finally the Client computer sends its HTTP request (13) to the IP address 204.142.86.110, which replies with the requested web page.



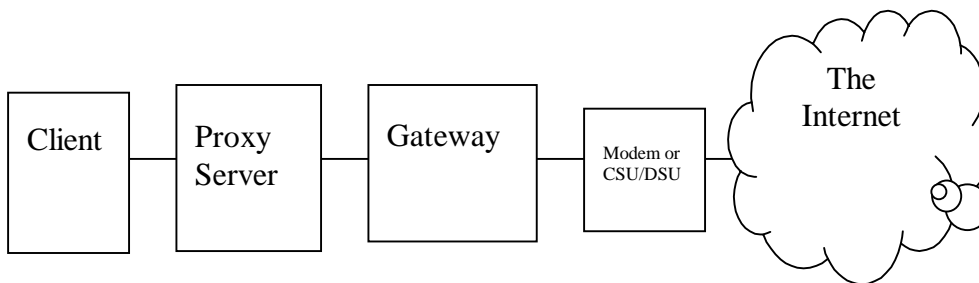
Windows computers also maintain a list of computers they can connect to directly on their own network using a **WINS** system. Some networks use NetBIOS or WINS instead of TCP/IP. The computer name that is set up on your computer and the Windows operating system is part of the **NetBIOS** system of computer name. This is the name that appears in the Network Neighborhood window of your computer. NetBIOS-to-IP resolution can be done through static files (LMHOSTS) or dynamically with a Windows Internet Naming Service (WINS) server. When a difference local network system is used such as winds instead of TCP/IP the gateway is not only sending things to the Internet it is translating the traffic to TCP/IP format.

Browser Configuring and MIME Types

In addition to configuring the network connection for your computer, some systems are setup to require additional configuration for the Client software. For security and access control, networks may have a proxy server that is used to regulate traffic going to the Internet.

The IP address of the proxy server must be entered into each client program that connects to the Internet. On Internet Explorer, you can configure the **proxy** under Internet Options. On Netscape, you can configure those to options under Preferences.

In addition to browsers, mail programs, chat clients, ftp programs and other client software needs to be configured to use the proxy. Most networks will have a single proxy server for all protocols of traffic. Some will have separate proxy servers for each type of traffic or block certain type of traffic by not allowing it through the proxy server.



MIME (Multi-Purpose Internet Mail Extensions) was originally developed to allow Internet email to contain something other than just simple ASCII characters. When a server sends a file to a client application, it specifies the MIME type in the header and the browser either displays it with its built in players or plug-ins, or the

item downloaded so the client computer can open it with a separate application. Email attachments are each marked with its MIME type so the correct program can use them when they are saved.

You can define MIME file types on the client and on the server. You may need to define a MIME type for a non-standard extension on a page or in an email. For example, if you are using the scripting language PHP, you will need to define the extension PHP or PHP3 in the configuration on the server so the browser can interpret it correctly. On the client you might have to associate ZIP file extensions with WinZip. On windows computers this is usually done automatically when a program is installed.

Some example MIME types below.

| MIME type | Description |
|------------|------------------|
| text/html | HTML documents |
| text/plain | ASCII text files |
| image/gif | GIF images |
| image/jpeg | JPEG images |

| MIME type | Description |
|--------------------|------------------------|
| audio/x-wav | WAV format audio files |
| video/quicktime | QuickTime Movies |
| application/msword | MS Word Documents |
| Application/pdf | Adobe Acrobat file |

When the client does not know a MIME type that is sent to it, the file can usually be saved for later use. If the MIME type is known it will usually be opened by the default application associated with that MIME type.

Legacy Issues

Older software may not work the same as the current version. When **troubleshooting** problems, look for revision dates, and manufacturer/vendor values and use them to determine if you have the most current software available. Troubleshooting problems and performance issues can often be tied to compatibility issues and differing versions of the Web browser.

Problems can arise on older systems with TCP/IP sockets and older browsers. On older systems, such as Windows 3.1, one independent TCP/IP socket only allows one program to access the Internet at one time. Without a stable TCP/IP socket, your operating system could experience problems with connection and transfer. You should check the revision date of the TCP/IP driver, the vendor, and if there is an upgrade available. You can monitor the performance of your connection and troubleshoot your connection using different applications.

Another factor that has to be taken into consideration is the **version of the web browser**. Older browsers lack support for present day Internet standards such as PNG graphics, XML or XHTML.

A patch or update usually updates software to account for security holes, new functionality, or performance issues. Patches should be tested before they are applied en masse on your network, problems may arise. For example, when Microsoft first released Service Pack 6, it fixed a lot of problems in Windows NT, however, it caused compatibility problems with Lotus Notes. If your IT department blindly deployed this Service Pack in a Lotus Notes environment, it would have been very difficult to undo what is done.

Virus Protection needs to be regularly updated to protect your system from new viruses that appear. Keeping your system updated keeps your risk at a lower level than with no protection.

Patches, Bug Fixes, Security and Virus protection

As noted above, patches should never be blindly applied as you run the risk of taking a working system and making changes that can adversely affect performance. When new patches become available, you should always download them and carefully read the documentation, which accompanies them. If you are experiencing none of the problems addressed by the patch, or there would be no performance gain by applying it, then do not apply it. If the patch looks beneficial, then try it on a single system first to look for problems that might arise before rolling it out to all computers.

Windows Update will check for patches and security fixes available for Windows computers. It is best to check for a patch or fix on a regular basis. If symptoms of a problem are occurring on more than one computer, there may be a fix available for the problem.

The data being sent from server to client is encrypted so that other computers cannot interpret the data. There are different **encryption levels** for different software applications and browsers. An encryption level is the strength of the keys used to encrypt and decrypt information sent. The higher the number of bits of encryption the more complex the encryption is and the more time consuming it is to decrypt.

Standard security has been 56-bit encryption. Many banks are now requiring that use 128-bit encryption be used to connect to their site. Until 1999, encryption stronger than 56-bit was illegal to export or transmit out of the country via Internet. Since then most downloaded browsers include 128-bit or stronger encryption.

Desktop Security is an important issue in today's always-connected networks. All operating systems experience security holes and applying regular updates from vendors or the open source community helps keep security problems to a minimum. Ways have been discovered to capture passwords and defeat passwords on many common operating systems.

Many client programs have security problems as well that can cause damage to the files on the computer. Recently, the ability of Microsoft Outlook to execute VBScript files attached to emails has been exploited to damage computer files. These programs that run without the user's knowledge are generally called viruses. They come in a number of categories based on how they are written and how they hide from the system.

Antivirus Software is used to detect viruses and virus-like activity on a computer. Usually these programs use a list of known viruses to detect them on the computer hard drive. This means that only viruses known to the scanning program can be detected on the computer. Antivirus software needs to be updated with a current list of viruses in order to remain effective. Any time a new virus is discovered antiviral software companies will update their virus lists and issue a new list file. It is a good idea to check for these updates on a weekly to monthly basis.

Antivirus software needs to be installed on both servers and clients for it to be most effective. Since viruses can infect servers and clients, the server needs to also be protected. Just protecting clients is not enough. Any particular client may not update their virus list and this would leave the server open to infection if it were not also protected.

Viruses

Viruses are computer programs. They can do whatever a computer program can do, from reset the clock, to display information on the computer screen. Many viruses do nothing dangerous to a computer's data. Other, more malicious and therefore significant viruses cause files to be renamed, altered or erased. Some viruses take the extreme step of changing disk and drive information so disks and drives become unusable.

Historically viruses are communicated by shared diskettes or shared files on a computer or network system. More recently, the most popular forms of viruses are tied to email programs and send themselves to other computers through apparently friendly email messages. Any file coming from an unprotected source needs to be scanned for viruses. Since it is difficult to know what other computers have protection, it is better to scan all computer files.

Macros are small programs written in macrocode for word processing or spreadsheet applications. The Microsoft Office suite includes macro programming ability in all of its programs.

Executables are viruses that attach themselves to executable files and are activated when the program is launched. Sometimes these viruses pose as a application or utility or sometimes these viruses "piggy-back" their code onto another application or utility. Either way, when the application with the virus code is executed, the virus does as it is programmed to do.

Boot Sector viruses copy themselves to the boot sector of hard drives allowing them to be loaded into memory each time a system is started. This makes them especially difficult to eradicate since they can reappear every time the computer is booted from an infected disk.

Stealth viruses attempt to avoid detection by redirecting virus scanning software as it reads the hard drive.

Polymorphic viruses are the most difficult to detect. They have the ability execute differently each time the virus runs. It avoids detection by constantly changing its code so there is no single pattern a virus scanner can detect.

Cookies

When a user visits a web page, each page served is independent of one another. As a user travels through the site, the website doesn't have a way of identifying the user using HTTP 1.0. With HTTP 1.1, cookies can be used to track a user as they travel through a web site. Cookies are text files written to a user's hard drive by their browser. These cookies contain information sent from the web server(s) they are accessing. A cookie file can be used in identifying the user as they travel through the sending server's other pages or to remember a user when they return to the web site on a future visit.

Since they are text files the cookies are considered unencrypted; but the text stored is entirely up to the server sending the cookie and may be difficult for humans to interpret.

Cookies are stored on the client's computer with, or without, the user's knowledge. The most common use of cookies is for user identification. Cookies also commonly hold values about the user or the user's preferences and history, such as a shopping cart. They can be used for other purposes, but that is extremely rare and usually not productive for a web site. All cookies contain expiration dates; dates last modified, last accessed, and last checked. Cookies can be read and written any time the user accesses a file on a web server through HTTP 1.1.

The server that created the cookie is the only server that can read that cookie, in theory. However, since information and especially graphics on a web page can come from many servers, it is possible for a set of web sites to share information through common files referenced all their sites. Banner ads, such as those from Doubleclick.net, are on a great many web sites. This allows those placing the banner ads to follow a browser's visits to many web pages. The data gathered about the user and their habits can be used to better target the banner ads.

Whether cookies are accepted, and from whom, is controlled by the browser software. In Internet Explorer, you can choose to set whether cookies will: 1. Always be accepted, 2. Require prompting before accepting, or 3. Not be accepted. Sites that use cookies to track or customize information may not work properly if cookies are disabled or rejected. For the i-Net+ exam you need to know where the setting are in Netscape 4.5 and Internet Explorer 4 and 5.

The **security and privacy implications** of cookies should be readily evident. Doubleclick.net was severely criticized by privacy advocates for tracing users' activities across the Internet and attempting to associate names with users. Other companies have also seen their privacy policies subject to review after linking names with Internet travels. Websites should exercise caution when storing cookies on website visitors' computers.

Programming Environments

To customize web pages based on user information or custom information on the web site a programming environment and programming language is needed. The programming environment sets the abilities for the programming language to use and controls what data comes in and goes out of the program itself.

The common programming environments on web servers are: API, CGI, SQL, SAPI, and DLL. The languages used to program in these environments are covered later. This is separate from how client-side programs are written and controlled.

CGI is the Common Gateway Interface. It is the most common way to communicate between the data being received by the web server and the programs on the server. Following the CGI rules, almost any command line program can be converted into a web-based application. This allowed people with prior programming experience to write web-based applications without a lot of more training. Other web programming environments usually emulate the CGI for simplicity and compatibility.

CGI does not have the interactivity with the Windows Operating System that is was desired by Microsoft. So Microsoft built their own custom system called ISAPI based on their existing programming technologies API and SAPI. **API** is Microsoft's Application Programming Interfaces. This system is the building block by which Windows-based software applications are built by programmers. Its partner systems: SAPI and **ISAPI** are also necessary for interactive web pages. SAPI is the Server API is simple server applications running between servers on a network. And ISAPI is the Internet Server API that attaches programs to be used by the Microsoft IIS server. All these APIs are used exclusively on Microsoft servers.

DLL are Microsoft's Dynamic Linking Libraries. These are the method by which common executable routines are made available in the Windows-based environment. Drivers and executables depend upon DLLs to provide functionality that can be accessed, making programming much easier. Adding a DLL that knows about ISAPI can add a new programming language to a Microsoft server or enable a new set of commands or routines in a already installed programming language.

Within CGI and API programs, a method for sending request to databases to retrieve data for the programs to use is needed. **SQL**, the Structured Query Language, is standard way to send requests to relational database systems RDBMS and collect the results. More recently, a system called **OQL**, or Object Query language, is being used with object-oriented database systems, ODBMS.

Both SQL and OQL need the database they are communicating with to have a connection established within the computer's operating system. These connections are made using **ODBC**, Open Database Connectivity, or **JDBC**, Java Database Connectivity. ODBC was originally designed for use with SQL and the Windows OS but is now used on a number of different platforms. JDBC is used with Java and is better suited for use with OQL, but also supports SQL.

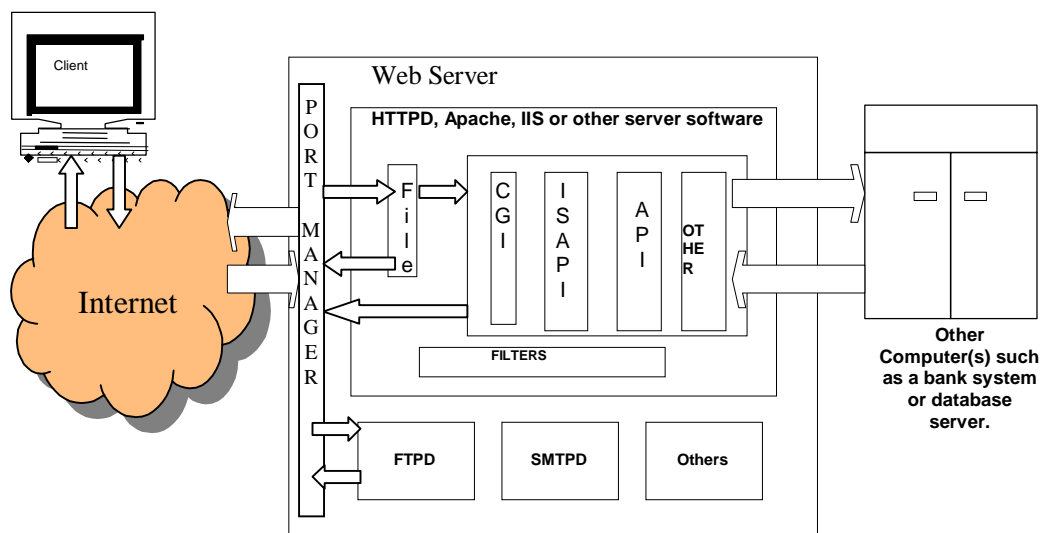
How Server side programming is used

When someone sitting at a PC goes to a web page and clicks on something, a request is sent to the appropriate web server. This request is then received and interpreted by the web server software. In the simplest situation, the server software responds to the request by sending an already saved file in return. With CGI or ISAPI requests the file request triggers a program to be executed. It is the result of the program that is then sent back to the requesting computer.

With CGI and ISAPI server systems there is the possibility to request information that is on the server in a form other than a pre-written file. In this case, when the request comes into the server, it is passed to the appropriate program or library and the results are returned to the client as though it were a file. The program or library has the ability to request the information it needs to build this resulting file. These added requests can go to other systems on the web server or even be directed to other computers so the work can be shared for faster responses.

This is what happens with an online credit card system. The processing request goes to another computer, actually many, to verify the credit card before the page that indicates approval is sent in response to your submission.

Server-side scripting model



Programming Languages

The i-Net+ covers the most common programming languages being used on the web today. With the CGI or ISAPI environment you still need a programming language to write the instructions the computer will execute to produce its response. Additionally there are programming languages that are designed so that the actual program is sent to the client computer to be executed. The advantage of sending the program to the client is that the server does not have to process the specifics of the program and is free to respond to more requests. However the program being sent to the client raises security concerns and removes the program from the controlled server environment.

The common programming languages used on servers to perform file access and to save data about the client would be dangerous on a client where the same program could erase or alter files. The programming languages used with the web to send short programs to the client and browser for execution are intentionally limited in how they can read and write from the user's computer.

On the client-side the most common programming languages are JavaScript, Java and VBScript. Along with these programming languages there are markup languages that are sent to the client computer to be displayed and interpreted. The most common markup language is, of course, HTML; but also there are XML and VRML. On the server side, the most common programming languages are Perl, C, C++, Visual Basic and ASP.

| Language | Primary use | Category | Description | File extension | Other uses |
|--------------|-------------|------------------------------|---|--------------------------------|--|
| C | Server-side | Traditional, Compiled | Used to write complex programs on the server side. Favored by UNIX programmers. Developed in the 1970s on UNIX computers at BellLabs. | .c then .exe | |
| C++ | Server-side | Object-Oriented, Compiled | Used to write complex programs on the server side. Favored by UNIX programmers. Based on C, developed in universities to expand on C's abilities. | .cpp then .exe | Used to write operating systems and many common programs on computers today. |
| Java | Client-Side | Object-Oriented, Precompiled | Based on C++. Sent as an "Applet" to the client it can not perform file access to files the applet did not originally create. Developed by Sun Microsystems. Requires a version of the Java Virtual Machine, or JVM, to actually run the compiled program. This JVM allows the same program to be run on many different computer types. | .class, .java | Also used to write "servlets" for server side use. |
| JavaScript | Client-side | Object-based, Interpreted | Interpreted in the browser to perform functions within a web page. Developed by Netscape. It is Not related to Java, there merely have a similar name. | .js (also part of .htm files) | There is now a server side version, which is not covered on the i-Net+. |
| Jscript | Client-side | Object-based, Interpreted | Microsoft's version of JavaScript. | .js (also part of .htm files) | |
| Visual Basic | Server-side | Object-based, Interpreted | Microsoft's native programming language to interface with the API of Windows. | .vb, .vbs | Used to write freestanding windows-programs. |
| VBScript | Client-side | Object-based, Interpreted | Microsoft's stripped-down version of Visual Basic for use in browsers. | .vbs (also part of .htm files) | Also used as the Macro scripting language in MS Office. |
| ASP | Server-side | Object-based, Interpreted | Based on VBScript, it is used to quickly produce interactive web pages on Microsoft servers. | .asp | IIS 5.0 uses a revision called ASP+. |
| Perl | Server-side | Traditional, interpreted | Based on a number of early programming languages, Perl is good at processing data in text files to make reports or customized results. | .pl, .pls | Used to process text for reports separate from web pages as well. |
| XML | Client-side | Markup, interpreted | eXtensible Markup Language. A data description system. Used to make customized data processing possible. Version 5+ browsers natively interpret some XML. | .xml, .xsl, .dtd | Also used on the server side as a data source to build custom HTML or other pages. |
| VRML | Client-side | Markup, interpreted | Virtual Reality Modeling Language. Markup to describe three-dimensional space and objects in that space. Newer browsers require a plug-in to view VRML. | .vrm | |

Databases, ODBC, JDBC and connectivity tools

Databases are collections of data that can be used to answer questions call queries and to record events.

Some databases are designed so each item of data is independent of the others while others are designed to maintain relationships between the data they contain. The database file where data is independent is often called a flat-file database, each flat-file can contain only one set of data. A relational database stores data in different tables (each of which can be in a different format). Relational databases are far more complicated than flat-file databases, but also much more flexible and scalable for big installations.

A database should be integrated with a web site anytime you need to return values from it to the user, or input values from the user into it. In the first scenario, a database could be used to show inventory on hand when queried by partners in your extranet or web site users. In the second scenario, a database could be used to collect mailing addresses from users who want to receive your catalog.

The software that is used to interact with a database is called a **DBMS** or Database Management System. Non-relational databases that are often designed to treat the data like an index card system. An **RDBMS** or Relational Database Management System lets you manage not only the data but the relationships between the data. An RDBMS lets you define rules and define relationships by using a query language such as SQL. Common RDBMS systems are Oracle, Microsoft SQL, MySQL, and Microsoft Access 97 and above.

In the last decade a new theory for organizing database data has been developed: **ODBMS**, the Object Oriented Database Management System. ODBMS allows for more complex relationships between data than an RDBMS or SQL system can manage. Instead of SQL, OQL is used to access the data. Sun Microsystems is the big name promoting OQL and ODBMS. OQL is new, but losing its glamour; a shortage of trained technicians and training problems have limited its distribution and use.

As noted above, connecting to a database requires a connectivity tool to associate the program that is using the database to the file itself. Microsoft servers favor the **ODBC**, Open Database Connectivity, system with ISAPI programs for making this connection. ODBC can also be used on UNIX and Microsoft systems with CGI based programs. To register a database with the operating system you must create a DSN, Data Source Name. This DSN is what is used in the program to connect to the database. ODBC is the intermediary between the program, the DBMS and the files actually storing the data.

Databases using the ODBC must be ODBC compliant. Almost all common databases have ODBC drivers. As Microsoft has moved from Windows 3.1 with Dos to Windows 95 and Nt/2000 there have been changes to the ODBC. Older systems used 16-bit ODBC drivers. Those older drivers are not compatible with newer servers. Since 1995, 32-bit drivers are the preferred ODBC version now.

JDBC, Java Database Connectivity, developed by Sun Microsystems works like ODBC but uses slightly different internal information and is compatible with both SQL and OQL. ODBC is SQL based only.

Most server-side programming languages are capable of using ODBC or JDBC to connect to a database. ColdFusion or CFML, Java Server Pages or JSP, Active Server Pages or ASP and Personal Home Page or PHP are all common tools used to quickly write web pages that use database connections.

HTML

For the HTML section of the i-Net+ you need to recognize the following basic HTML tags.

| TAG | Attributes | Description | Gotchas |
|-------------------------------|------------|--|--|
| <HTML></HTML> | | Creates your HTML document | |
| <HEAD></HEAD> | | The header information for the page, not displayed on the main page. | |
| <TITLE></TITLE> | | Use this to put a title at the top bar of the browser. | Must be between head tags |
| <BODY> </BODY> | | Signifies the portion that will be shown in the browser. | |
| | BGCOLOR | Sets the background color of your page using the hex values or name. | |
| | TEXT | Sets the text color using names or hex values. | |
| | LINK | Sets the color of links on your page. | |
| | VLINK | Sets the color of followed links on your page. | |
| <H1></H1> <H6></H6> | | Creates headings. <h1> is the largest to the smallest <h6>. | Valid values are 1 through 6. |
| | SIZE | Sets font size. | |
| | FACE | Sets font face. | |
| | COLOR | Sets the color of the font using a name or hex values. | |
| | | Bold prints your text. | |
| <I></I> | | Sets the text to Italics. | |
| <A > | HREF | Creates a link to a website, or to send you mail, or to an anchor somewhere else on the same page. | Remember quotation marks around URL. Or # before an internal link. |
| | NAME | Defines an anchor within a page. | |
| <P></P> | | New paragraph. | |
| | ALIGN | Align your paragraph to right, left, or center. | |
| | | Line break. | No ending tag needed in HTML. |
| <BLOCKQUOTE> </BLOCKQUOTE> | | Creates an indented text block. | |
| | | Creates a bulleted list structure. | |
| | | Creates a numbered list structure. | |
| | | List item | Must be between OL or UL tags |
| | SRC | Marks where an image goes and the source of the image. | Check spelling, watch for quotation marks. There is no ending IMG tag in HTML. |
| | ALT | Add alternate text to an image. | |

On the i-Net+ plus, remember that the best answer will always have the tags in **nested pairs**. All attributes will have quotation marks around the values.

Every page has a begin HTML command, <HTML>. Next is the <HEAD> tag which opens the HEAD area of the page which is not displayed in your browser, but commands like <TITLE> appear at the top of your screen. Inside the <BODY> tags appears the stuff that is shown on the page. All of the scripts, tables, tags, and text on this page are contained inside a set of <BODY> </BODY> tags. Finally, a close HTML command, </HTML>, tells the browser where the HTML ends.

Links are created using the **anchor** or <a> tag. The <a> tag has a required attribute of href. The attribute's value is whatever URL or relative file path you are linking to. For example, to link to the domain Learnthat.com, you can type this on your page: Click here for free training!

As you see, the <a> tag is like all others, it has a close tag to tell it when to stop linking. The above example links to another page on a different site, or one that is not easily linked to on your site. You can also link to a local page easily, here is an example: Click here to learn about us.

This would assume the page "about.html" is in the same directory as the page you are linking from. To link to a page in a deeper directory, you can specify the directory first: `Click here to learn about us.`

The above would link to a document in a subdirectory off the one you are in.

Instead of text, just put an img source tag in there, for example: ``

The last thing to learn about linking is how to create one of those links where it opens a new mail message. Here's an example: `Click here to email me!`

For the exam you will also need to know **TABLE** tags.

Netscape originated tables, and as such, made the commands for them. To open a table, the `<TABLE>` command should be used. The other tags you need to know are Table Row `<TR>` and Table Cell `<TD>`. One key thing to remember is that a `<TD>` is always enclosed in a `<TR>` which is always enclosed in a `<TABLE>` tag.

First, let's create a basic table with 4 cells:

| | |
|------------|-------------|
| First Cell | Second Cell |
| Third Cell | Fourth Cell |

The code for this table is:

```
<TABLE BORDER="1">
<TR>
<TD>First Cell</TD>
<TD>Second Cell</TD>
</TR>
<TR>
<TD>Third Cell</TD>
<TD>Fourth Cell</TD>
</TR>
</TABLE>
```

In this code, you can see that there are two `<TR>` tags, or two rows. Within the first row is the First Cell and Second Cell, each inside a set of `<TD>` tags. In the second row, the Third Cell and Fourth Cell is enclosed in their `<td>` set of tags. As you see with the `<TABLE BORDER>` tag, the border was added so we could see it. To see a border of a different size, set the border equal to a number, such as `<TABLE BORDER="3">`.

Now, let's learn some important attributes of Tables. These are the main attributes of a table: border, width, cellpadding, cellspacing, bgcolor, and background. **Border** sets the size of the border around the table. **Width** can be expressed in pixels or %, it specifies the width of the tag it is in, it is available to all of the table tags. **Cellpadding** determines the padding width between each of the table's cells. **Cellspacing** specifies the spacing width between each of the table's cells. **Bgcolor** specifies a background color of the table and background specifies a background image in the table.

An example of using several of these commands is:

```
<TABLE BORDER="3" WIDTH="75%" BGCOLOR="#CC0000">
```

The **FORM** tags start and end a form (all input fields of the form are placed between these two tags). **METHOD** specifies which technical protocol the web server will use to pass the form data to the program which processes it (always set it to POST), and **ACTION** tells the server exactly which program that is. *Note:* POST must be capitalized; otherwise the method defaults to "GET".

```
<FORM METHOD="POST" ACTION="http://www.webcom.com/cgi-bin/form">
Enter your name: <INPUT TYPE="text" NAME="your_name">
<INPUT TYPE="submit" VALUE="Test this form">
</FORM>
```

The above code creates the text input box for the user's name in our example form. **NAME** defines the name of the data for the field; it's how the program that processes the form references the data from this field.

Some other things we can do with a text input field are define an initial value for the field, and make it longer (or shorter):

```
<INPUT TYPE="text" NAME="your_name" SIZE="50" VALUE="Joe Schmoe">
```

Difference between text editors and GUI editors;

To insert a command to run a script, use the syntax: `<script language="JavaScript">`.

The "©" syntax produces the copyright symbol - ©.

It is important to create **cross-browser compatible code** on your web pages to appeal to the widest audience possible. With about 75% of users using Internet Explorer and 22% more using Netscape, it's important to design so all of the users can view your pages and website. The two main browsers are Netscape Navigator and Internet Explorer. Each has its similarities and differences. Incompatibilities in the browsers are usually found in its implementation of newer technologies such as CSS (Cascading Style Sheets) and DHTML (Dynamic HTML).

Text editors allow you to create web pages by typing in the HTML code yourself. **GUI editors** allow you to design web pages with WYSIWYG (What You See Is What You Get) results. You can enter things and choose stylings, insert tables, pretty much do anything you want with HTML without knowing any code.

Multimedia Plug-ins and File Formats

To add increased interactivity to a web site the designer may add non-HTML Tools to the page. These often take the form of Plug-ins. QuickTime VR, Macromedia Flash, Macromedia Shockwave, RealPlayer and Windows Media Player are all common plug-ins for Web Browsers.

QTVR (QuickTime) - developed by Apple, it allows video, audio, and animation to be displayed with its strength lying in the ability to show 3-D photos and artwork.

Flash - developed by Macromedia, allows video, audio, animation to be shown. A **vector** file format, so result animations/videos are small.

Shockwave - also developed by Macromedia, allows video, audio, and animation to be shown.

Realplayer - developed by RealMedia, plays RealAudio and RealVideo. Streaming video and audio as well as downloadable files.

Windows Media Player - originally designed to play .AVI files, now has been extended to play many different multimedia types. It also allow for streaming of content to the desktop.

The common file formats for Web Graphics are GIF; GIF89a; JPEG; and PNG. PNG is a relatively new format and version 3.0 and before browsers do not support it.

CompuServe developed **GIF**, the Graphics Interchange Format, in 1987. GIF uses the LZW compression algorithm, which is owned by Unisys. GIF is one of the two most commonly used file formats on the web, the other being JPEG. Benefits of using GIF is its wide spread support among browsers and software applications. GIF uses the 24-bit color palette, but is limited by only allowing 256 different colors in any file. The copyright for writing a GIF file is still protected by CompuServe.

GIF89a is an update to the original GIF file format. It is a version of the GIF format, which allows for animated graphics, usually small in size.

The Joint Photographic Experts Group developed the **JPEG** standard. After GIF, JPEG graphic files are the second most popular graphics files found on the web. JPEG uses different levels of compression to control the quality and size of images.

The **PNG** or Portable Network Graphic file format was designed as a replacement for GIFs. PNG is free from any restrictions due to copyrights. It can be used with newer browsers and software, but has not caught on with web developers yet.

In addition to the above formats there are many other graphical file formats in use on computers. While these however are not web browser compatible, they can be used with Plug-ins or separate programs.

The Adobe Acrobat **PDF**, Portable Document Format, file format was developed by Aldus Inc., now part of Adobe. It allows a document to be printed to a file, similar to a graphic. The PDF contains all of the elements of the document, such as text, graphics, movies. It allows the user to zoom in and out and to navigate several pages of the document. Adobe's Acrobat Reader is free and assures that the PDF data will be displayed identically on all platforms. Great for converting non-web documents to be available on the web and for documents which are difficult to recreate in HTML. It also allows for the source data to be protected so it can not be altered by other people.

Rich Text Format, **RTF**, was standardized by Microsoft, and based on a number of similar formats. RTF is designed to store formatted text and can be read by most word processors and platforms. It is an excellent alternative to raw text for transferring files that need to retain, font, indentation or tabular information.

The Tagged Image File Format or **TIFF** is a graphics file format similar to JPEGs but less utilized by developers. It is excellent for printed output but not a good choice for Web graphics due to its generally a larger file size than other graphic types.

Postscript is a page description language developed by Adobe for use with its line of printer control software. Postscript is vector based and used in most laser printers and higher end printers. Postscript files are complex and not easily scaled for display purposes. Adobe also created the Encapsulated Postscript or **EPS** format. It is a vector-based file format for images and can easily be used in desktop publishing programs. Due to its internal complexity it is slow to display on video screens and is not used for Web graphics.

The **BMP** or Windows Bitmap File Format is the original file format used for screen display in Windows 3.0. BMPs are limited in the colors they can display and are generally larger than the other popular file formats with less compression options.

In addition to the above formats, there are many multimedia file formats that are becoming accepted as the web grows. These include the non-streaming MOV, MPEG and AVI formats but also include a few streaming formats. **Non-streaming video** is video, which is not streamed. The files have to be downloaded in its entirety before the user can view it. **Streaming video** allows small portions of a video to be sent at a given time, and then played in the related player. This allows a large video file to be viewed by someone with a slow Internet connection. Examples of streaming video include RealVideo RM, format and Windows streaming media, ASF format. There are also streaming audio formats, such as RealAudio's RAM format and the MP3 streaming format.

Apple's **MOV** or QuickTime movie format is a widely used multimedia video format. Since 1992 it has been available on the Mac, and was available on Microsoft Windows computers in 1993.

MPEG, developed by the Moving Pictures Expert Group. Is a widely used standard for video and audio formats. It offers variable image size and frame rates along with high quality compression. The MPEG standard has been updated through various versions. MPEG-2 is used on the web and also by small-dish satellite and digital cable systems. One of the audio formats (Layer #3) used with MPEG is also now being used as the MP3 file format. MPEG has also had additions to its format options, which are being numbered. MPEG-4 version 2 was adopted by the ISO as the ISO/IEC 14496 standard for both streaming and non-streaming multimedia files.

The Video for Windows format, **AVI**, was one of the first audio video format for the Windows computers. It is limited to a 320 by 240 pixel image size with 30 frames per second. Though it is mainly used on the Windows platform, it is now available across many platforms.

To make transmission of complex data files across the once text-only email system a special file format was created. It translates the binary data of computer files into a text-only format so it can be efficiently sent through e-mail. **BINHex** is now built into many e-mail clients as the default encoding/decoding system, which encodes attachments, files, or emails and sends them over the Internet to be decoded on the receiving end. First and primarily used on the Macintosh platform, Netscape and some email programs have the encoding/decoding system built in. Raw BINHex data is usually stored with a HQX file extension.

BINHex has largely been replaced by the internet standard Uuencode (UNIX to UNIX encoding) system, but is still used for some transmissions.

Pre-Launch Testing

To assure good customer service and satisfaction with your web site, you must: check hot links, test different browsers, test to ensure the new site does not corrupt your e-commerce sites and that it can be accessed, perform load testing, and test with various speed connections. Any of these factors could limit your audience or even make your site inoperable.

Before launching a site, a thorough **review of the hot links** and checking the hyperlinks for dead links and mistyped links should be performed. Visitors have short attention spans for sites with broken links.

Before launching a site **access to the site** must be checked. Computers involved in the site's original development should not be used test the site. Sometimes a file link or graphic will only work in the development environment or when viewed from the authoring computers.

You should also check your site in **different browsers**, especially the most popular versions of Internet Explorer & Netscape Navigator. You should preview your site in several different versions of the browsers, as different versions render the screen differently.

If you are running an **e-commerce site**, you should have a test version of the site available for reliability testing and run tests which look like actual customers using your site. It is possible for bad programming to lose orders or to prevent users to not be able to complete the order process. The e-commerce sites should be tested with different levels of inventory and payment options.

You should also test the access to your site and the ability of your servers to handle volumes of visitors and customers. This is called **load testing**. Software is available which runs scripted tests on your server and records how well your server handles the sample visitors.

Another test, which should be run on your site, is testing your site with various connection **speeds and technologies**, including 28.8K, 33.6K, and 56.6K dialup, DSL, Cable Modem, ISDN, and T1. Testing your site with the various connections can show slow spots where a majority of customers (dialup) will experience problems or become frustrated with your site.

Internet Infrastructure and Connectivity

The Internet is made up of a number of interconnected networks. The network with the highest capacity and which connects long distance Internet traffic is known as a **backbone**. A number of different companies now provide backbone services across the country. These companies install their equipment connect at certain interconnection points known as **Network Access Points** or NAPs. NAPs are where Internet Service Providers connect to the Internet backbone services. Different backbones come together at points called an **interchange**. As different companies expand their networks more and more interchanges are made. Originally there were three major interchanges known as Metropolitan Area Exchanges or MAEs. The three major original MAEs were near San Francisco, Chicago and New York. An MAE was added in suburban Washington D.C. shortly after the original three.

Today the backbones are usually made of high-capacity fiber-optic cable. Communication companies install fiber-optic cable along their old telephone lines as well as in rural road right-of-ways and along the old oil pipelines. This allows for multiple paths to reach any city, interchange or Network Access Point. Since multiple paths, any one path can be a broken or disconnected for service and Internet traffic will still be able to reach its intended destination.

Probably the most common problem with Internet connectivity is a slow server or a server that is not fast enough to handle the traffic it is receiving. A web site does not predicting how much traffic they will receive can result in users becoming frustrated with trying to use their service and choosing the other providers for their service. It is also possible for none Web traffic to slow down the web server. The computer used in the web site may also be being used for e-mail or ftp services. If a high quantity of e-mail or ftp traffic occurs the server may not be able to respond to its HTTP traffic.

Along with slow servers it is possible for the network connection going to the server to be broke in debt or out of service. Web servers can also crash, switches and routers connecting their traffic can fail, as can the DSU that connects between the service provider and the LAN.

All Internet traffic is sends with a maximum of number of connections that it is allowed to make in a maximum amount of time it is allowed to exist. If the packet of traffic cannot reach its intended destination within the 127 connection hops or 127 seconds allowed it will be automatically destroyed by the network hardware.

Email servers can have similar problems to web servers in that they can crash or have connection problems. Also incorrectly formatted or intentionally ill-formatted mail messages can cause web servers to fail. A high quantity of oversized e-mails can fill a mail server's hard drive and prevent it from accepting other pieces of email.

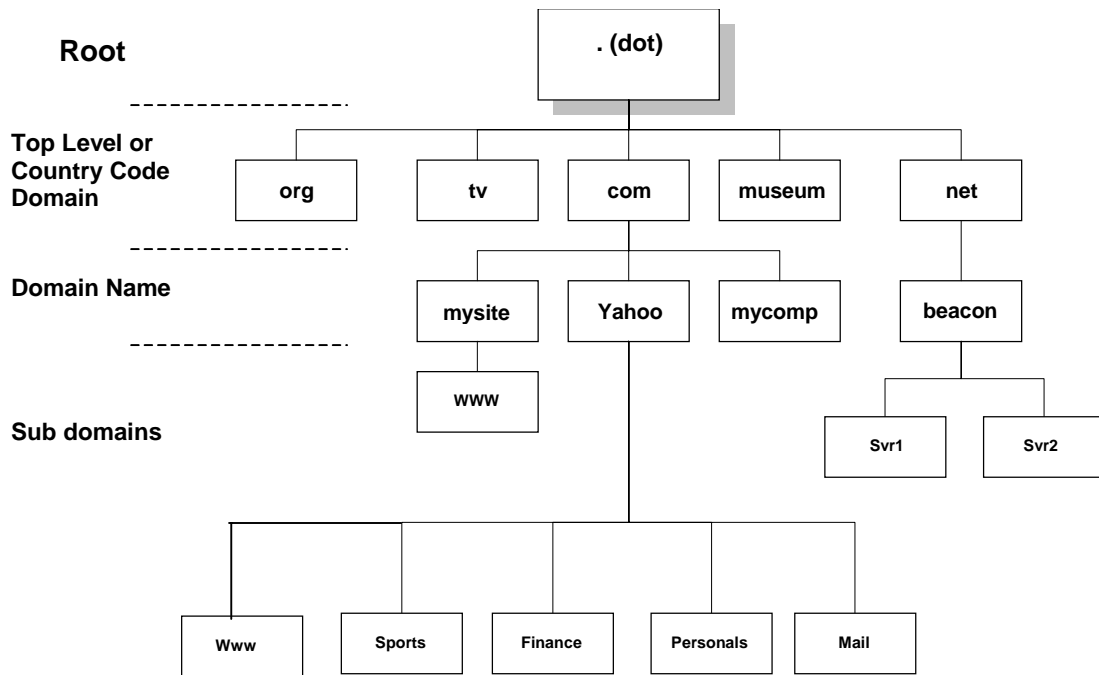
Poorly designed CGI or API programs on Web sites can also cause slow performance. A request that causes an infinite loop in a program, or retrieves too much data for the program to handle, can quickly crash a web site.

Domain names and DNS

As noted above domain name servers provided the interpretation of common domain names to the IP address that the TCP/IP system uses to connect Web traffic. To result in the domain names into their IP addresses the client computer has to send a request to a DNS server. This DNS server then affords a request for any domain names it has not catch on its frequently requested list. Each top-level domain has a DNS server responsible for answering all domain name service requests within that top-level domain. VeriSign is currently responsible for answering DNS requests for .com, .net and .org domains. Each country code top-level domain also has a particular company responsible for answering requests for it. In some countries this is the national telecommunications agency in others that has been contracted to a private company.

These top-level domain servers give the client computer's domain name server the IP address of the requested domain's domain name server. Each domain handles its own and subdomain domain name services. So if your computer requests to connect to www.yahoo.com, your computer will request from its local domain name of server the IP address. That's domain name server will request from VeriSign's .com domain name server what the IP address of the domain name server for yahoo is. This IP address is returned to your local domain name server, which then requests from that IP address what the IP address for the www server at yahoo.com it is.

When diagramed, all the possible domain name of servers forms a large tree of possible domain names. In theory in at the top on of all the possible domain names is the root domain known as dot.



Since each domain is responsible for its own sub domains the must keep a DNS server available for any DNS requests for their domain. The DNS server can be the same server as the web server although this is rare. On the DNS server is a DNS records file that contains all of the information for the sub domains and that domain. This usually includes the sub domain name for the mail server the web server the ftp server and whatever other or sub domain servers are set up in that domain.

DNS records consist of different types of information. The types to know for the I-Net+ are:

| Entry | Name | Description |
|-------|------------------------|--|
| A | IPv4 Address (32 bits) | The IP address corresponding to a sub domain |
| Cname | Canonical Name | A given host can have several DNS names. One of these is the canonical or reference name. This is listed under this title. |
| MX | Mail Exchange Record | The IP address of the Mail server. |
| NS | Name Server | Gives the domain names or IP addresses of the computers acting as name servers for this domain. |
| SOA | Start of Authority | Points to the IP address or domain name of the computer responsible to find this computer's domain name. |

For the i-Net+ exam you need to recognize the top level and country code domains. Below are the most common domains that they use on the exam.

| gTLD | Original assignees | DNS Managed by | ccTLD | Country | Managed by |
|------|---------------------------|---|-------|----------------|---|
| edu | Educational Institutions | VeriSign (soon Educause) | uk | United Kingdom | Nominet UK |
| com | Commercial groups | VeriSign (until 2007) | us | United States | United States Domain Registry - VeriSign |
| net | Network service providers | VeriSign (until 2006) | de | Germany | DENIC eG |
| gov | Government institutions | U.S. Government, Dept. of Commerce – contracted | fr | France | Association Française pour le Nommage Internet en Coopération |

| | | | | | |
|-----|------------------------------|-----------------------|----|--------------------|---------------------------------------|
| | | to Verisign. | | | |
| org | Not-for-profit organizations | VeriSign (until 2002) | ru | Russian Federation | Russian Institute for Public Networks |

Other top level domains to know.

| | | | | | |
|--------|-------------------------------------|---|----|--------|---|
| mil | US Military Installations | U.S. Government, Department of Defense | mx | Mexico | Department for Networking and Telecommunications – NIC Mexico |
| int | International treaty organizations. | IANA, (negotiating to transfer it to the ITU) | jp | Japan | Japan Network Information Center |
| museum | Museums | Museum Domain Management Association, (MDMA) | tv | Tuvalu | “Tuvalu Ministry of Finance and Tourism” assigned to “The .TV Corporation” Canada |

Country code top level domains, ccTLDs, are two letter "codes" at the end of the domain name to signify which country the domain name is registered in. Every country that is a member of the International Telecommunications Union, ITU, has a ccTLD. For example, .uk are domains in the United Kingdom, .fr in France, and many more. Some countries sell their country codes to companies who make money from the registrations. For example, .cc is the country code for the Cocos (Keeling) Islands that is leased to the Internet Services Corporation in Seattle, Washington who are registering .cc domain names. Another highly publicized country code is Tuvalu’s .tv, was perpetually leased to an Idealab backed venture, The .tv Corporation.

TCP/IP Essentials

An IP Address is a four-byte value that is expressed by converting each byte into a decimal number (0-255) with a period in between each byte. The IP address is made up of an Network ID and a host ID. Different classes of IP address use different lengths of Network and Host IDs. The Host IDs identify the individual computer or device on the network.

The first octet of the IP address tells what class it belongs to: Class A addresses range from 1-126, Class B addresses range from 128-191, and Class C range from 192-223.

A Class A address uses the first byte to specify the network ID and the last three bytes to specify the host ID. An example would be on Network 80 with host ID 124.23.241. Thus the IP address is 80. 124.23.241.

A Class B address uses the first two bytes specify the network ID and the last two specify a host ID. Class B networks can have of up to 64,000 individual hosts.

A Class C address uses the first three bytes specify the network and the last byte specifies the host ID in that network. A class C network can have up to 254 hosts.

Class D addresses are not assigned to networks, but are used for multicasting technologies.

The 127.x.x.x IP addresses are reserved for local loopback and self-diagnostic testing use.

The host ID portion of an IP address cannot be all 0’s or all 255’s. The network portion can also not be all 0’s or all 255’s, these are used for DHCP and Multicasting services.

IP Addresses reserved for internal use and which will not route on the Internet:

Public versus private IP addresses – when connecting to the Internet (meaning the world), you must have a unique IP address for every single host within the world. When you are not connecting to the world, however, then the addresses must only be unique within your network. Public addressing requires the uniqueness, while private addressing suggests that the following ranges be used:

| Class of private network desired | Starting address | Last available address |
|----------------------------------|------------------|------------------------|
| A | 10.0.0.0 | 10.255.255.255 |
| B | 172.16.0.0 | 172.31.255.255 |

| Class of private network desired | Starting address | Last available address |
|----------------------------------|------------------|------------------------|
| C | 192.168.0.0 | 192.168.255.255 |

Remote Access Protocols, Information Protocols and Services

The purpose of remote access protocols is to allow remote workstations, terminals, and servers to connect to the Internet. Most often, this connection is from a computer system to an Internet Service Provider (ISP), but could be many other combinations.

Serial Line Internet Protocol, **SLIP**, is an older used connection protocol used to connect to a computer over a dial-up connection. The use of PPP has mostly replaced SLIP.

Point-to-point protocol, **PPP**, is a connection protocol which uses TCP/IP and allows you to connect to a remote server. Better than SLIP as it supports synchronous and asynchronous communication. It also has error correcting features that result in fewer disconnects and lost packets.

Point-to-point tunneling protocol, **PPTP**, is a protocol that allows private networks to connect to one another via a public network (the Internet). The information sent via PPTP is encrypted between the two computers. This system is used to build Virtual Private Networks. Using encryption, PPTP allows companies to securely connect LANs together over the Internet. That eliminates the need for dedicated network connections or dedicated phone lines and ISDN lines to form secure corporate networks.

Layer 2 Tunneling Protocol, **L2TP**, combines PPP and PPTP with Cisco's Layer 2 Forwarding, **L2F**, protocol to build more secure VPN networks.

Information Protocols

For each of the services that make up the Internet and World Wide Web there is a protocol that provides the communication for that service. A protocol is simply a set of conventions for two machines sending information to each other. Each client computer and each server has the appropriate software installed to listen to the network for that protocol and to send messages using the matching protocol. TCP/IP ports provide an easy way for computers to receive traffic of a particular protocol. Servers have a program, service or background process that answers requests for each protocol. On UNIX computers these listener programs are called **daemons** on Windows they are called **System Agents**.

Mail Protocols: POP3, SMTP, and IMAP.

Post Office Protocol, **POP**, has gone through a few versions; The most recent version of the protocol for receiving email is **POP3**. When you are sent an email, your ISP's servers receive and store that email. When you are ready to receive the mail, your email client uses POP3 to transfer all the email on the server to your email local computer. POP3 is only for receiving mail, SMTP is used for sending email. The associated daemon for SMTP is `smtpd`.

Internet Message Access Protocol, **IMAP**, like POP is used to access the mail on your mail server. Like POP, it has gone through a few different versions. The current version is IMAP4. IMAP allows your client to search and delete mail while it is still on the mail server. To read email, the email is transferred to your local computer.

Simple Mail Transfer Protocol, **SMTP**, is used in sending mail across the Internet. (SMTP was the original system used for both sending and receiving email. POP and IMAP are based on SMTP.) Today SMTP is used exclusively for sending mail. SMTP relays mail messages to the destination server so the addressee can retrieve it. SMTP also has the protocols for delaying delivery when target mail server is not responding.

File Protocols: HTTP, NNTP, TCP/IP, LDAP, Telnet, and Gopher.

Hypertext Transfer Protocol, **HTTP**, is the application protocol that describes the transfer of the text, images, and multimedia elements that make up the World Wide Web. When a user types in a URL, the web browser processes the request and sends the necessary HTTP requests to the appropriate web server, which sends the information back to the client. HTTP 1.0 has been replaced with HTTP 1.1, a more efficient and feature filled protocol. The associated daemon for HTTP is `httpd`.

File Transfer Protocol, **FTP**, as noted above, is a protocol which is a simple way to transfer files between networked computers. The associated daemon for FTP is `ftpd`. In addition to FTP there is also the Trivial File transfer protocol, **TFTP**. TFTP does not include confirmation messages that the file was successful or correct when the client computer received it. The daemon for TFTP is `tftpd`.

Usenet services predate the World Wide Web and provide bulletin board systems on the Internet. Usenet was born in 1979 when Tom Truscott and Jim Ellis, graduate students at Duke University, conceived of creating a computer network to link together those in the Unix community. The computers would exchange files automatically so all computers had the most up to date files. The Usenet newsgroup data was organized into topics so it could be retrieved quickly and articles about a research topic could be browsed.

Each Usenet group was a public area that members could post messages for others to view. There are over 14,000 Usenet group topics, also called newsgroups, on the Internet. To access the Usenet, Network News Transfer Protocol, **NNTP**, is used.

Communication Protocols: TCP/IP, Telnet, Gopher, and LDAP.

TCP/IP, the Transmission Control Protocol/Internet Protocol, is the basic protocol for transferring information on the Internet and most private networks. TCP/IP is actually a suite of protocols. The TCP protocol manages connections between computers and verifies that messages are receivable by the target computer. IP, the Internet Protocol, is the protocol that provides for computer addressing and identification. IP is also responsible for converting information into small and efficient packets.

Telnet is a utility to log into a remote system using a command line prompt. It is mainly used on Unix systems to login and administer the system. Telnet is the main Internet protocol for creating a connection with a remote machine. It gives the user the opportunity to be on one computer system and do work on another, which may be across the street or thousands of miles away. Telnet is also used to configure some routers. The associated daemon for Telnet is `telnetd`.

Gopher is a text-based information system that pre-dates the World Wide Web. IT was used to browse menus on servers around the world. The menus would provide links to text files or FTP addresses. Gopher was developed at the University of Minnesota and named after the school's mascot. Two systems, Veronica and Jughead, let you search global indices of resources stored in Gopher systems.

Phone companies and other communication systems maintain large databases of searchable information on their users. The system used to communicate and update their complex directory information is called X.500. Unfortunately X.500 is not TCP/IP compatible. To bring this type of service to the Internet the Lightweight Directory Access Protocol or **LDAP** was developed based on the X.500 standard. LDAP is a set of protocols for accessing information directories. Because it's a simpler version of X.500, LDAP is sometimes called X.500-lite.

LDAP is not widely implemented. It makes possible for almost any application running on virtually any computer platform to obtain directory information, such as contact information like email addresses and encryption public keys.

Diagnostic Tools

To identify and isolate problems with networks and the Internet technicians use a number of diagnostic tools. Each provides a different way to test a network connection or service.

Ping is a utility that sends a small amount of information to an Internet host to get a reply. Ping measures how long it took to send this information and get it back. Ping can be used to check to see if a site, server, or computer is operating on the network. Ping is also used to see if a particular service or site is reachable from the pinging computer.

WinIPCfg and **IPConfig** are programs that come with the Windows OS that give IP Address & network information for that computer. Both names stand for IP Configuration, with the WinIPCfg allowing for that data to be viewed in Windows itself. WinIPCfg is only on Windows 95, 98 and ME. IPConfig is a DOS based program available on all Windows computers.

ARP, or Address Resolution Protocol gives network devices the information they need to send transmissions efficiently. ARP is a TCP/IP protocol used to translate IP addresses to hardware addresses such as Ethernet or MAC address. A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.

There is also Reverse ARP, or **RARP**, which can be used by a host to discover its IP address. On a network there are server computers that listen for ARP traffic and then store the Ethernet address and IP address information. When a computer or technician requests RARP information a host broadcasts the desired computer's physical address and a RARP server replies with the host's IP address.

A **Trace Routing Utility, Tracert** on Windows NT/2000, is a utility that allows you to trace the connection between two computers. In other words, tracert sends out a request that shows you the path from one computer to another. Tracert can be used to show the list of routers you go through to reach a certain site. This is used to identify slow connections and where traffic is lost as it attempts to reach a target computer.

A **Network Analyzer**, also known as a sniffer, collects information about packets and their movement throughout the network. They are used to analyze problems or see how much traffic is moving in your network. One popular software network sniffer is Sniffer Pro. Sniffer Pro allows you to monitor the network or specific machines to determine problems or the amount of traffic flowing. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This allows unauthorized users to view all packets on a network and their contents, such as unencrypted passwords.

Netstat is used too identify what services are currently active on a computer and which IP ports are in use. Netstat can also report what IP address is connecting to each active port. Netstat is a command line utility on UNIX and Windows computers. Ports that are unexpectedly open can be a sign of network problems or an attempt to break into a computer. Using netstat in constant mode can give a system administrator an idea of the amount of time each port is in use on their system.

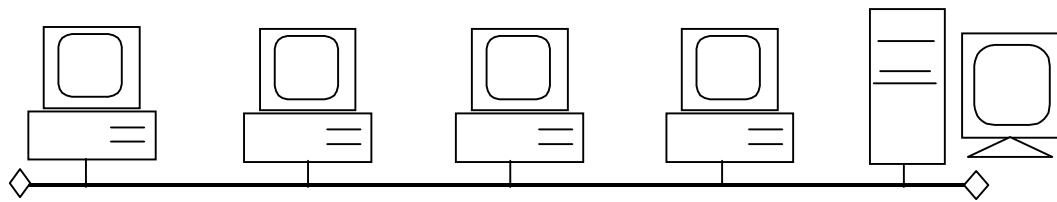
Network Devices

For a network to operate there must be some form of connection between its constituent computers. The most common devices are described here.

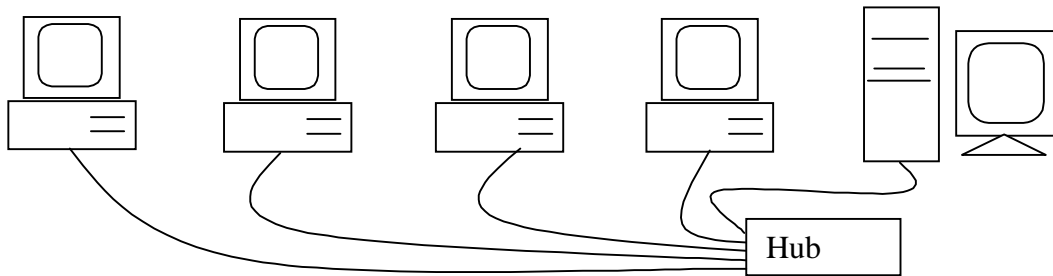
For the simplest network only two computers and a connection are needed. The connection will usually be a set of wires connecting to each computer through a Network Interface Card. Once you are connecting more than two computers some connection device is needed to connect each computer to all the others.

A slightly confusing term used with the physical network devices is **port**. These are different from the TCP/IP ports discussed above. A port is simply the jack that a network cable's jack can be inserted into.

At first computers needing this common connection were hooked onto a common pair of network wires, called a bus. The bus was organized like Christmas tree lights; the single strand travels past every node on the network or light on the strand. And just like Christmas tree lights, if the wires were broken, the entire network would go out. To solve this problem, a system was developed that allowed each computer to be independently connected to a central, **hub** device. Hubs send all traffic they receive on one port out all the ports of the hub.

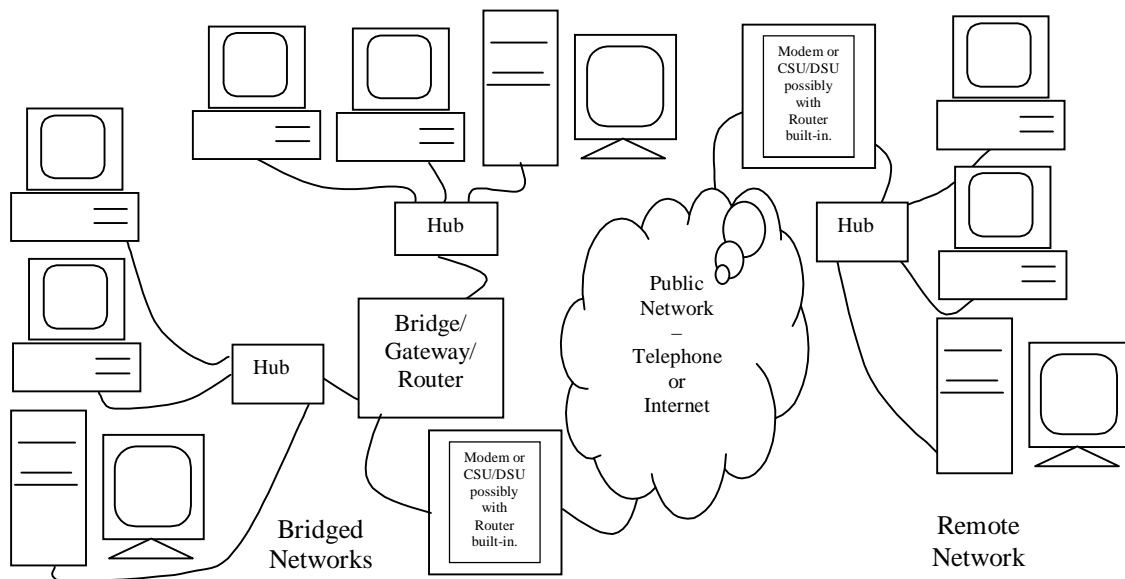


Bus Topology, single wire pair past all computers.



Hub or Star Topology, wires go to central, hub device to connect all computers.

These kinds of network connections, bus and hub, are limited by the physical characteristics of copper wire. For a network to operate effectively, it must not exceed 300 meters in length along its longest path of copper wire. To get past this problem other network devices are added to the network that break the single network into segments or multiple networks. Additionally, distant networks need to be connected; such as when a company has offices in multiple cities that need to share data.



A **bridge** is the simplest device that allows two (only two) networks to be joined so they can share data. A Bridge simply repeats all data that comes in one port to all the other ports by making its network information match the target network. A bridge can change the format of data so it is compatible with the other network. A bridge that does not convert signals to a different network number or type is sometimes called a **repeater**.

A **gateway** is a step above a bridge for complexity. Gateways are a combination of hardware and software that can connect different protocols of data intelligently. Gateways are customizable.

Bridges, gateways and hubs are starting to be replaced by switches and routers. A **switch** performs instantaneous connections for network traffic between whatever two network lines or ports that need to handle the traffic. This allows for traffic to be better directed to its destination, in some switches two simultaneous communications can be directed between two pairs of computers.

A **router** is one of the most complex devices used to connect networks. Routers examine the network traffic coming to them and only allow it to be repeated on the other side if it needs to be communicated to that part of the network. Routers can be setup with multiple ports and sets of instructions about what addresses are allowed to use which ports or what protocols are allowed to pass through the router. It is at routers that private network traffic is blocked and prevented from going to other networks.

Routers also allow for another layer of the network design. Routers can communicate with other routers to find the most efficient path for traffic to use to get to its destination and to automatically correct for network problems and outages. Routers with multiple connections to other routers form a very reliable connection system since any single failure can be corrected by re-routing traffic. The original design of the Internet is based on this kind of a mesh of routers to make its communication system nuclear war survivable.

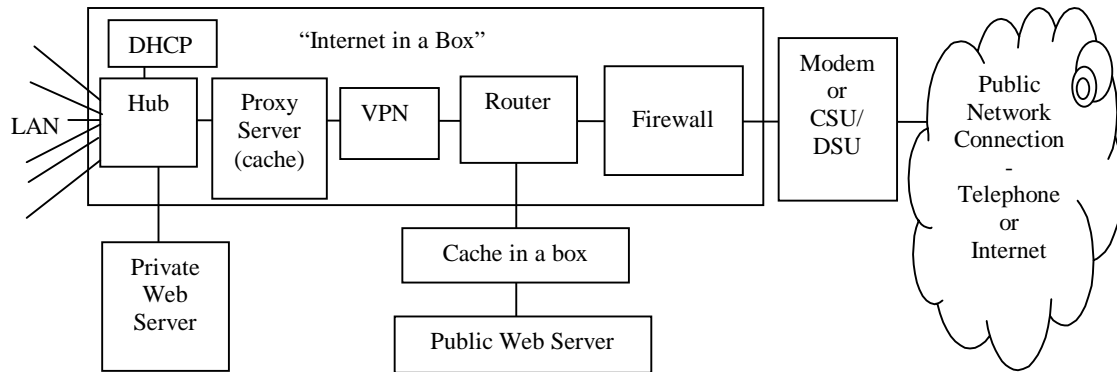
The **modem** (modulator-demodulator) or **CSU/DSU** (Channel Service Unit/Data Service Unit) is a device that interfaces with the Internet Service Provider. On home computers this is usually a card within your computer, on more complex networks it is a device that attaches to the network on one side and the outside service on the other. Officially, modems are used with analog lines and the CSU/DSU is used with digital service lines. Many people with call any device that connects to outside service providers a modem.

Today, most CSU/DSUs include a router. The reason for this is that it protects private network traffic from being sent to the ISP. Some ISPs also bill, based on the number of bytes sent through the CSU/DSU so by including a router, only traffic directed to the outside world will be sent to the ISP. On the ISP end of the connection is another CSU/DSU and network that connects to another CSU/DSU to connect to the ISP's customer traffic to their service provider or backbone service.

Modems, today are usually automatically setup for use by the operating system. It is useful to know the setup commands to better troubleshoot Modem connections. The I-Net+ includes these commands on the test. All commands start with AT, the modem attention signal.

| AT-code | Command | AT-code | Command |
|-------------|------------------------------------|---------|---|
| ATD | Dial | ATH0 | Hang-up line (on-hook) |
| ATDT | Dial, touch-tone | ATH1 | Pickup line (off-hook) |
| ATDP | Dial, pulse | ATM0 | Speaker Off |
| ATDT5551212 | Dial, touch-tone with phone number | ATM1 | Speaker on during dial, until connected |
| ATA | Auto Answer | ATM2 | Speaker on while off-hook |
| ATZ | Reset modem to factory specs | ATX | Do not wait for Dial tone detection (ATX is not for Exit) |

To help secure a network from outside attacks there are a number of devices. Used together with the equipment above and when properly configured it becomes increasingly difficult to gain unauthorized access to a computer network through its public Internet connection. The order things are drawn in the diagram below is a general order for how things would be connected. Depending on the security risks and target audience, the order the items are organized in can be changed between the CSU/DSU and the Hub.



Firewall – either a hardware or software entity that protects a network by stopping network traffic from passing through it. In most cases, a firewall is placed on the network to allow all internal traffic to leave the network (emails to the outside world, web access, etc.), but stop all traffic from the outside world from entering the internal network

Since many companies need most or all of the above units for their network installation and connection many companies are marketing all-in-one solutions that provide the above services in one configurable unit. This kind of all-in-one unit is sometimes called an “Internet-in-a-box”. Though often they are called by one of the component names and it is understood that the other services are included. In the drawing above you can see the Internet in a box can encompass everything from the Firewall to the Hub. Cisco is already selling units that also include the CSU/DSU with all the other items. Internet-in-a-box are also an effective solution for attaching multiple computers to a single DSL or Cable Modem for home use. Home versions cost less than \$200 and can provide Firewall, DHCP and Proxy services for up to 200 hosts.

Proxy servers will often also provide a cache service for the local network. They are a good choice to provide this since they are already readdressing traffic and checking traffic. Proxy servers are also commonly setup with content filtering software that block access to particular web sites or services. The limitations of traffic and hardware can sometimes cause the proxy server to become the weak point in the network setup as it takes on a number of roles.

Another Internet connection device that is available is the “**Cache-in-a-box**”. This is basically a hard drive with network connections and software that tries to provide efficient caching service of the files people request most often. These are placed in the network between the device it is caching for and the users who access that device.

Connection and Bandwidth

Communication speeds are measured in bits per second or **bps**. Faster connections can also be measured in Kbps (1024 bits per second) and Mbps (1048576 bps, or 1024 Kbps). Both ends of the connection must be able to communicate at the same speed. Modems can negotiate their fastest reliable speed. This is why 56 Kbps modems often connect at 33 Kbps, that is the fastest speed they could make a reliable connection at. Some modems have the ability to perform data compression as they transmit. The modems must also negotiate this and both modems must be using the same compression method to get full advantage. Since many files sent over the Internet are already compressed, the amount or speed gained by attempting re-compression is minimal.

| Modem type | Top speed | Description |
|------------|---|---|
| Analog | 57,600 bps by technology. 53,000 bps for compatibility with US phone networks. | Traditional modem – requires a single voice telephone line for a connection. It transmits sounds over the phone lines that correspond to the bits of data to be communicated. |
| ISDN | Single - 64,000 bps or Dual - 128,000 bps | Integrated Services Digital Network, basically equivalent to two telephone lines. One of those two can be used for voice and one for data. This is very rare now. |
| DSL | 1.5 to 9 Mbps. | Digital Subscriber Line, uses copper phone lines (only!), and is |

| | | |
|------------|--|--|
| | <p>Sold by guaranteed minimum speed up and down stream (up/down). Such as:</p> <p>256 Kbps/64 Kbps.</p> <p>1.5 Mbps/768 Kbps.</p> <p>768 Kbps/768 Kbps.</p> | <p>available only within about 3 miles of the phone company switching office. The distance from the switching office also affects the line's top speed. DSL works by sending digital pulses in the high-frequency area of telephone wires. Since these high frequencies are not used by normal voice communications, DSL can operate simultaneously with voice connections over the same wires.</p> <p>ADSL – Asymmetric DSL – allows for more traffic to be transmitted in one direction than the other. ADSL has speeds like 768 Kbps download and 128Kbps upload.</p> <p>SDSL – Symmetric DSL – allows equal upload and download speeds. SDSL has speeds like 512 Kbps download and 512 Kbps upload.</p> |
| Cable | <p>2 Mbps to 8 Mbps</p> <p>Bandwidth is shared for all users on the same segment of the cable system.</p> | <p>Because the coaxial cable used by cable TV provides much greater bandwidth than telephone lines, a cable modem can be used to achieve extremely fast access to the World Wide Web. This, combined with the fact that millions of homes are already wired for cable TV, has made the cable modem something of a holy grail for Internet and cable TV companies.</p> |
| High-Speed | <p>Voice = 64 Kbps (DS-0)</p> <p>T-1 = 1.544 Mbps (DS-1)</p> <p>E-1 = 2.048 Mbps (DS-1)</p> <p>T-3 = 44.736 Mbps (DS-3)</p> <p>E-3 = 34.368 Mbps (DS-3)</p> <p>OC-3 = 155 Mbps (STS-3)</p> | <p>Originally intended for inter-office and long distance connections, high-speed service is now being used for data transmission.</p> <p>The T in these names refers to the Transmission protocol standard that puts it on the physical Digital Signal (DS) line. OC stands for Optical Carrier.</p> <p>T-1 is a high-speed digital network developed by AT&T in 1957 to support long-haul pulse-code modulation [digital] voice transmission. T-1 created a network fully capable of digitally representing what was up until then, a fully analog telephone system. A T-1 line carries the equivalent of 24 voice phone lines.</p> <p>T-3 is equivalent to 28 T-1 lines or 672 voice lines. There was a T-2, but most companies no longer sell it.</p> <p>E-1 and E-3 are the similar European standard to the North American T-1 and T-3. Europe uses 32 lines in a bundle instead of the 24 that the US phone companies chose to use.</p> <p>Higher capacity connections are not on the i-Net+ test.</p> <p>OC-128 (6.4 Gbps) and OC-192 (9.9 Gbps) are currently used in backbones and OC-768 (39.8 Gbps) is an existing technology.</p> |

In addition to the above connection technologies, there are a number of related transmission methods that use the same lines but provide different service structures, namely: X.25, ATM and Frame Relay.

While standard T-1 service is a continuous connection designed for continuous traffic, to a single destination, a **frame relay** connection allows for multiple shared destinations for the traffic. It is more like a computer network than the point-to-point phone network. Traffic is sent in packets and routed to the intended destination. Frame relay is used when a company has multiple locations that need to share a high-speed private network.

Frame Relay networks in the U.S. support data transfer rates at T-1 (1.544 Mbps) and T-3 (45 Mbps) speeds. In fact, you can think of Frame Relay as a way of utilizing existing T-1 and T-3 lines owned by a service provider. Most telephone companies now provide Frame Relay service for customers who want connections at 56 Kbps to T-1 speeds. In the U.S., Frame Relay is quite popular because it is relatively inexpensive. However, it is being replaced in some areas by faster technologies, such as ATM.

ATM, Asynchronous Transfer Mode, uses easily switched cells of a fixed size to achieve high speed connections. Each user of the ATM system is guaranteed to be able to send a certain number of these cells or packets per second, if there is extra bandwidth available, the more cells than the guaranteed number of cells can be used by

those needing the capacity. The small, constant cell size allows ATM equipment to transmit video, audio, and computer data over the same network, and assure that no single type of data hogs the line.

Current implementations of ATM support data transfer rates of from 25 to 622 Mbps (megabits per second). ATM creates a fixed channel, or route, between two points whenever data transfer begins. This differs from TCP/IP, in which messages are divided into packets and each packet can take a different route from source to destination. This difference makes it easier to track and bill data usage across an ATM network, but it makes it less adaptable to sudden surges in network traffic or equipment failure.

X.25 is another popular standard for packet-switching networks. The X.25 standard was approved and adopted ITU (then CCITT) in 1976, making it an international standard. X.25 utilizes a Connection-Oriented service, which insures that packets are transmitted in order. It enables a computer to “dial” other X.25 hosts and exchange data at high speed almost instantly. Once the transmission is done, it disconnects from that host and can connect with another host.

X.25 has the advantage of being an international standard and allows for as-needed connections making is a good choice when transmissions are not constant.

Servers

Generally, a server is simply a computer or device attached to a network that handles a particular type of traffic or service. Servers can be dedicated to only being used as a server, or simply software running on a computer used for other things. Servers that do other things besides just servicing their traffic often run more slowly and take longer to reply to traffic. Non-dedicated servers are often more prone to crash or fail.

A number of protocols and their purposes have been described above. For each protocol there is a related server: **Web servers** handle HTTP requests and files; **News servers** handle NNTP requests and files; **Directory servers** handle LDAP requests and data; **Telnet servers** handle telnet connections; **Mail Servers** handle SMTP, POP and IMAP traffic; and **FTP servers** handle FTP traffic. All these different services and their server software can be installed on a single computer unit that will act as all of the needed servers based on the traffic it receives. Microsoft’s IIS 4.0 (and 5.0) provide all the above services and Apache handles most of the above, with other freeware products taking up what Apache does not include.

File Servers are computers with special software installed that allow them to easily share files with other computers. In fact, all Windows computers have the ability to share files and can be used as file servers. Special software however makes them more efficient. Faster processors and larger Hard Disk Drives also help to make a computer into an effective file server. File servers can often play other roles on a network and are very often also **printer servers** for queuing and managing user’s print jobs.

To make a dedicated file server you would normally purchase a **NOS**, or **Network Operating System**. There are many choices for this but the most common NOSs are Novell Netware, Microsoft Windows 2000 and UNIX/Linux. These operating systems are optimized for users to retrieve data and files quickly and without errors. NOSs also provide security services for the files and data so that only authorized users can access particular directories or files on the hard drive.

Since File servers and web servers can hold a large quantity of valuable data they need backup systems that allow for the data to still be retrieved if the server or its hard drive fails. **Mirror servers** and **mirrored hard drives** play this role on a network.

A mirrored hard drive is simply a second hard drive installed in a server that also receives all the data written to the server’s main hard drive. This arrangement is also called a level 1 **RAID** or Redundant Array of Independent (or Inexpensive) Disks. Additional hard drives allow for better error correction and disaster survivability for server data. A level 5 raid uses systems that spread the data over the drive surface so less data is lost in the event of a hard drive failure and a third drive for error correction data so the two different drives can be compared and automatically corrected.

A **mirror server** is a second server that copies the files from a main server on a regular basis so the mirror server acts as a backup of the main server. Mirror servers not only provide for backup of the data on the main server, but can also be configured to answer requests for the files on the main server so the main server has less

traffic. Very popular downloads, like Internet Explorer or Netscape software, are often mirrored so no one web host receives the overwhelming traffic that occurs when a new version is released.

Mirrored servers are also setup on separate continents to reduce the time it takes for downloads. You have probably seen web sites that offer you the choice of what continent or country to download a file from. Windows 2000 Advanced Server provides server mirroring that is very similar to a RAID system across multiple PCs. In the UNIX/Linux world Beowulf Cluster, or “Beowulf Class Cluster Computers”, are the name given for this type of multiple, shared, mirrored computer technology.

File servers and mirror servers are not exclusively used for Internet traffic. **Cache servers** also are not exclusively used for the web. Cache servers are simply a server that provides quick replies to user requests of another server using cached information. It is more common to have a cache on the main server but there are independent cache servers.

Back on the Internet side of servers, we have a special kind of mail server called a List Server. **List Servers** allow people to subscribe to receive newsletters or other items in their email. Many hobbies, and businesses use List servers to simplify their communication. Someone interested in home automation would locate a list server for home automation topics and send that list’s subscribe address an email with their name and email address. From that point on, all mail sent to the messages address of the home automation list server will be forwarded to the subscriber. To unsubscribe, the list server subscriber send a message to the subscribe address with the word UNSUBSCRIBE in the message.

Since people can subscribe and unsubscribe themselves, they can effectively manage their own mail preferences. This frees staff of a business of club to do other things. Businesses can send emails to subscribers with new sales or promotion information and also quickly communicate any updates their customers need. Within large companies a list server would also allow all people in a particular department or role to be contacted.

List servers pre-date the World Wide Web and have are beginning to be absorbed by the various Web Groups that perform similar services. With a list server, the server receives its subscribe and unsubscribe information by email instead of through web sites. Web groups will have web-page-based subscription setup, and preference controls.

Certificate Servers are a large, almost invisible, part of the Internet. When a user connects to a secure web site, their browser validates or certifies that the site reached is actually the site the user intended to reach. This is accomplished through certificates. A certificate is similar to a driver’s license. It contains identifying information about the holder that can be used to verify if the bearer is the actually who it was issued to or not. These certificates, like drivers licenses are also kept on file by a central database that can be used to see if they are valid or out of date. This central repository resides on a certificate server.

When a user connects to a secure site, a certificate is sent to the user’s browser from that secure site. The browser then looks in the certificate to see what **Certificate Authority** issued the certificate and directly contacts that authority’s certificate server to verify that it is a trusted and valid certificate. To further verify the process, each certificate authority is issued a certificate from a higher-level authority that is, usually, already known to the browser. If necessary, this higher authority’s certificate server is contacted to verify that the lower certificate authority is still trusted.

A certificate whose sending server: cannot be verified, is listed as not trusted, or whose certificate authority is not trusted, will result in an error being displayed on the receiving browser. The user can then decide if they want to continue on that site or not. This verification system allows for identities of servers to be verified so it is difficult to setup a malicious or fake bank web site or store site that collects sensitive user information.

Related to the certificate servers are **e-Commerce Servers**. These are the computers that process the business transactions of the Internet. All e-commerce servers should hold identifying certificates so those involved know what server and company they are doing business with. These e-commerce servers connect with bank systems and credit card and check clearing systems to verify that money is available for the business transaction being processed. E-commerce servers vary in how they are setup and in how they connect with banking systems, but all e-commerce servers have the role of performing transactions between businesses and consumers.

Encryption and Virtual Private Networks

Encryption is the method of securing data by coding it so others cannot easily decode it.

In web commerce, encryption systems protect information and packets, as they are en-route from a commerce server to the user's workstation. Any certificate-holding server can implement Secure Sockets Layer, SSL. SSL provides a simple system to securely encrypt a server's traffic before it leaves the computer itself. This traffic is only decrypted once it gets to the addressed recipient. This encryption also protects traffic sent from the client to the server. Packet sniffers can then not easily decipher the contents of the packets and will not be able to view password, username, or financial information being sent with this system. The SSL encryption is a version of MIME called **S/MIME** or Secure MIME. As the name implies it was originally designed for encrypted mail messages but is now being used for Web traffic.

VPNs also use encryption while their traffic is on the public network. All traffic intended for the remote part of the private network are encrypted at the VPN unit with a code only known to the VPN unit it is intended to be received by.

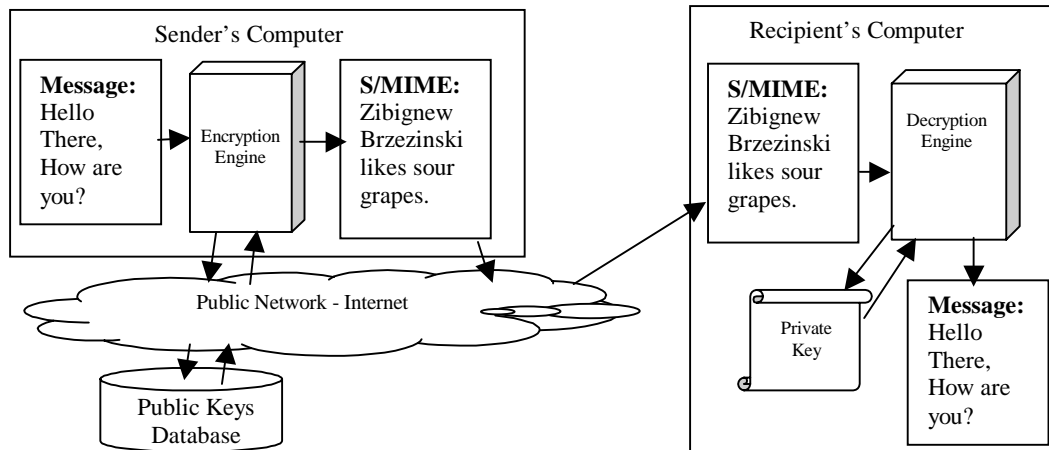
Due to privacy and national security issues in different countries, encryption should be studied carefully before it is implemented for international commerce. The usual rule of thumb is that the encryption used in a country should be able to be decoded by that country's government if necessary for police or security reasons. Until 1999 it was unlawful for any strong encryption (128-bit or above) hardware or software to be exported from the United States or Canada.

All of the most used encryption systems used today are based on public and private "keys". A cryptography key is a method or rule used to encode or decode a message. In traditional encryption the key might be something like the rule to shift all letters to the next letter in the alphabet for encryption and then to shift all letters to the previous one for decryption. Thus the message "Hello There" would be encoded as "Ifmmp Uifsf" and could then be decrypted using the key back to its original "Hello There".

With advanced mathematics a more secure method of encryption was discovered. The "Trapdoor algorithm" allows for the two, mathematically related, keys to be created. The two keys are related but neither key can reveal what the other key is. One of these keys is made public and one is kept private. One key is used for encryption and the other is used for decryption. The method that is being used to send a message determines which key, public or private, is used for encryption and which is used for decryption.

Public keys need to be in the hands of whoever is going to use them. They can be sent as a file or more often, public keys are stored in an online database that encryption-enabled programs use to find the keys when needed. Verisign, and its subsidiary Thawte, are one of the main holders and issuers of key certificates. Thawte certificates are free to create and use. Thawte verifies basic identifying information and will issue a certificate within 24 hours in most cases.

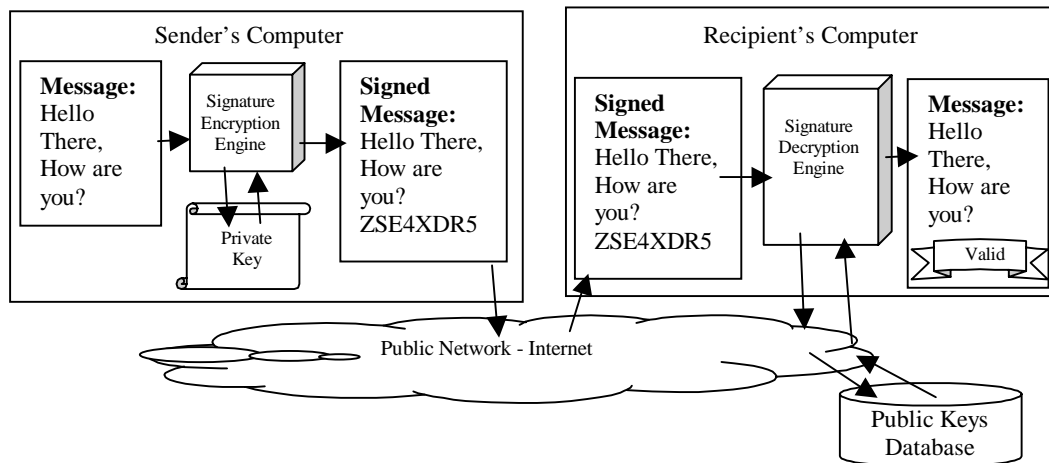
When mail is addressed to someone with a public key and marked for encryption, the client software searches its known local and online databases for the addressee's public key. If one is available, it is used to encrypt the message. Once encrypted, the message can only be decrypted by the addressee's private key. The message is then sent, and the addressee's client software uses their private key to decrypt the message. This guarantees that only the person it was addressed to reads the message.



Also related to public and private keys are **digital signatures**. These are a method of verifying who has created a file and that the file has not been changed. A U.S. law signed in mid-2000 made digital signatures legally binding on some electronic documents for business. Digital signatures provide **non-repudiation** for the signed document similar to how a store receipt proves that you bought an item at that store. Non-repudiation is basically positive proof that the item came from where it claims to have come from.

The most common format of digital signature is the X.509 standard based on X.500. The X.509 standard is still under review and currently has competing interpretations. It has been studied by a special working group of the IETF known as PKIX. PKIX has made a number of RFCs that are becoming standards and has defined a number of protocols that are used for exchanging and verifying Public Keys.

A digital signature is added onto the end of the message and contains two pieces of information: the identity of who signed the message; and a code, called a hash, which matches or verifies the contents of the document. If the document is changed, then the hash will not match the document. The recipient's computer verifies the identity information through a public key database. This verifies that the hash and identification are based on the correct sender's private key, which means the document was sent by that sender and has not been changed since it was sent.



Digital signatures and encryption can also be used together for even greater security. This verifies both the sender and the recipients are the only one who can access the message and that it is valid and being viewed by only those who are intended to view it. To gain this security, the sender's private key is used to sign the document and the recipient's public key is used to encode that signed document. Once received, the recipient's computer uses its own private key to decrypt the document and the sender's public key to verify its contents. This is the method used for SSL connections, the client's browser generates a unique key-pair and the public key is sent to the server the server

also sends a digitally signed public key to the recipient. The server's identity is verified and it can be assured that only the intended recipient is receiving its traffic.

With digital signatures, a document can be sent to multiple recipients and proved valid. Documents encoded with a recipient's public key cannot be sent to a group since each person's private key is different.

Drivers for Windows 2000 are required to be digitally signed by their creator. Unsigned drivers could be hazardous and will trigger warnings to the user that they are not trusted on the system.

A virtual private network allows two computer networks or a user and a network to exchange files and data over the Internet while still keeping the files and data a secure. VPNs are commonly used between different branches of the same company or between two companies that have a business relationship for their also used with work at home employees. When a VPN is set up between two companies with the business relationship this is considered to be an extranet.

At either end of the Internet connection between the two sites there is a device called a VPN. While today's VPNs are usually set up using hardware and is possible to set them up with software.

VPNs are set up to use the same encryption team so that's the user or can send encrypted data to the server and vice versa. Any traffic leaving one of the networks that is directed to the other or network is encrypted before it is put onto the public network or intranets. Traffic that is not intended for the other network is not encrypted. When the traffic is received by the partner network, it is decrypted and placed on the partner network and so were normal traffic.

Setting of VPNs can be difficult it is getting to be routine for many businesses. The tens of the connection need to have the same encryption methods and need to know the public key of the other VPN.

VPNs are based on standard Internet protocols that additionally can use point-to-point tunneling protocol to the secure transmission of data. More recently Cisco Systems and some other partners have added level to tunneling protocol has another protocol to be used for VPNs.

Internet Security

Any time that people are allowed to connect to a computer, there is the risk of their being able to change data on that computer. To reduce the risk of someone maliciously changing data on the computer certain security procedures and systems need to be put into place. All web commerce servers should have this procedures and systems; namely: an access control system, an encryption system, a log and auditing system, and user authentication. Along with these, for higher security a Secure Electronic Transactions system, or SET, can also be implemented. The general rule of thumb for deciding how much to spend on security is that it should be more money and time consuming to steal or alter data than the data or the result of its alteration is worth.

The first line of defense against malicious users is simply an **access control system**. It can be thought of as being like a turnstile or door that users pass through before they can access they server. Firewalls, packet filters and proxy servers all provide parts of this service. **Firewalls** (including **packet filters**) can block unauthorized TCP/IP packets or packets for services the public should not have. Firewalls can also block repeated ping requests and Synchronization requests that can overload a server with work. **Proxy Servers** provide the ability to screen what addresses connections are coming from via an **access control list** and to redirect or block traffic based on its apparent origin. These access control systems, when installed properly and working together can effectively restrict access to those who have business on the server.

Internet security is strengthened by **authentication**, a method for each party to prove who they are. Most noticeably, users authenticate themselves when they give their username and password to a server. Digital signatures and certificates also authenticate messages to and from servers. Authentication is based on "what you have" and "what you know". Similar to having the correct key for a give door, knowing what server a password matches and having that password are usually enough to authenticate a user and let them in. Additionally there are more sophisticated methods for authentication: Iris patterns are being used by some ATMs to verify a bank patron's identity. Companies and government agencies are using thumbprint scanners to replace manually typing names or passwords. Card-keys are widely used for door access in secure office buildings in place of keypads. American

Express Blue comes with a special card reader that allows the user to use their Blue card information for online-authentication on their home computer.

Good authentication and access control is a very effective start to securing a web site. Additionally Web site owners need to watch for signs that malicious users are targeting their site. All web servers have the ability to list suspicious events in a log file. This log needs to be audited on a regular basis to see what kinds of unusual activities are happening. **Auditing** log files and adding other intrusion detection utilities can keep a web site secure. Log files should be checked for repeated wrong password login attempts, wrong username password attempts and attempts to gain access to secure directories without authorization. For higher security you can check logs of users normal login frequency and see if their usual time of day or frequency has changed. If you suddenly not that many users are login in more often than usual, you may have connectivity problems or your traffic is being sniffed.

SET (Secure Electronic Transactions) is a slightly different approach to online money transaction security. With SET the user adds a browser plug-in, known as a **wallet**, to their system that can be triggered by the checkout system of web commerce merchant sites. The wallet is pre-made with certain of the users' credit cards being registered in the wallet. After checkout the wallet holds receipts and other information about the purchases made with the wallet. Some wallet plug-ins also allow for automatically filling in name/address forms and login forms on many sites to make the web easier to use.

The SET system is used when a wallet-user is ready to checkout of a merchant site. Instead of typing in information to the website they are ordering from with their payment information, they click a "Pay with e-Wallet" button that sends transaction information to their Payment wallet. The payment wallet then displays the purchase information on the client's computer where the user selects which payment method they will use and then approves the purchase. A certificate is sent to credit card holder's bank, the merchant and merchant's bank. These three institutions verify the certificate with the SETco Certificate Authority and have the transaction instantly approved. The actual credit card number is not sent to any of those institutions thus reducing the possibility of fraud. The certificate is a one-time use certificate so it can not be reused.

SET is widely used in Japan and Denmark. MasterCard and its member banks started a push toward SET in the United States in Spring 2001. Due to the existing ease of using credit cards in forms on web sites, SET has caught on more slowly here than in some other countries.

Network and Server Security

When malicious users attempt to compromise your network or network connection, there are four types of assets that they will focus upon: local resources, network resources, server resources and database and information resources.

Local resources include workstations and users that might be used to access your server, network or database information. Often, users will have login passwords saved on their hard drive or written next to their workstations. If a malicious user can use this information to gain access to your network, they can do as they wish under the guise of being that trusted user or workstation. Local resources also include gullible users or administrators who can be convinced to change passwords or to disclose their password through deception. Server administrators are often suckers for a sweet voice asking for help.

Network resources are hardware assets such as routers and communications networks that provide access to your IP addresses. If a malicious user can make your equipment think that their computer is within a trusted network or if they can redirect traffic from your network to their computer they can capture information and data they should not have. Network resources are also a location where the user can "sniff" packets from the network and perhaps capture passwords and other critical information.

If a company's network routers can be redirected, or if the ISP's routers can be redirected then another user can receive the company's web traffic. A web server could be setup to act like a bank's customer web server and then simply display "server-busy" after login information is gathered, a malicious user could gather hundreds of usernames and passwords for the real bank site. By rerouting traffic to the real site after a short period, the malicious user could then identify large accounts and perform money transfers to charities or other worthy causes.

There have been a number of cases where the DNS entries for a web server were maliciously changed and users redirected to fake web sites. Even similar sounding domain names can be used: `www.gatt.org` appears to be a website made by the World Trade organization about the General Agreement on Tariffs and Trade (GATT). It is in fact a spoof site run by “The Yes Men”.

Server resources are your website, e-mail and FTP servers. Since these resources contain important data and often contain passwords they are prime targets for attacks. Once a user gains access to a server or email they can possibly change passwords or send requests and upload files that will make further access easier to accomplish and harder to detect.

Many servers have their passwords and backup passwords and account noted in a notebook kept near the server. By overcoming local resources, it could be easy to gain higher access to the server and then gain server resources. This is a common attack method used by company insiders or in industrial espionage.

Database and information resources are proprietary information such as employee information, customer information and financial data. In the business world this is one of the main targets for malicious users. Numerous companies have reported that their database of past customer transactions have been stolen. These databases often include credit card numbers, addresses and sometimes verification information such as social security number or mother’s maiden name. With these pieces of information, malicious users can perform identity theft for many users.

Server Security

All networked computers that can share services or files should be given extra attention for security issues. At a minimum, all access to that a server needs to be protected by **name and password authentication** for all services. If there are services that are to be public, such as a web page, logging needs to be installed so basic information about users and user requests can be stored.

Once a user has been authenticated, the server’s file permissions can be used. A server has the right to grant access to files to some users but not others. Access generally falls into three categories: Read, Write and none. Each directory can have a separate setting for each user. **Read access** allows the user to see what files are on the server and to read files and from the server. **Write access** allows the user to read and write files on the server. Write access usually includes the ability to create, modify and delete files. **No access** prevents the user from reading files or even directory entries. The server administrator is usually in charge of setting directory permissions for directories on servers.

As an example: On our server we have two users: “jdoe” and “hjmudd”. We also have at least two directories on our server, we’ll call them “filedir” and “empdata”. In the filedir directory, user jdoe has write access and in the empdata directory jdoe user has no access. This means that anyone logged in as jdoe will be able to save and change files in the filedir, but not able to even see files in empdata. Our other user, hjmudd, has been given read access to filedir and write access to empdata. So hjmudd can change files in empdata, and can see but not change files in the filedir.

Most network operating systems have more complex abilities to set access on directories, and some even have the ability to set similar permissions on each individual file for each individual user.

Suspicious Activities

Above, we discussed some of the various methods that are used to gain unauthorized access to a server. There are other systems for causing trouble within a computer network. The most common suspicious activities that the administrator needs to be aware of are: multiple login failures, denial of service attacks, mail flooding or spam, ping floods, and syn floods.

Login failures, brute force attacks

Multiple **login failures** are usually an indication of someone trying to repetitively guess a password on the server. Since most users choose a guessable password, hackers assume that they will be would break into the system. During the early days of ATM cards it is estimated that over two-thirds of those cards had the Personal Identification Number 1234. System administrators should coach their users to not choose easily guessed passwords. Many people will choose a child’s name, pets name, street name or favorite musician as their password. Simply adding

digits to a simple password or adding a second word can greatly increase the difficulty of guessing a password and therefore make it harder for a malicious user to break into the system.

Multiple login failures should be able to be noticed from the server logs. Regularly auditing the logs should allow the administrator to identify where the login failures are coming from and take the appropriate actions. These actions could include things such as contacting the highest ISP the attacks coming from, or finding what workstation in their own company network is responsible for the multiple login failures.

Malicious users can attempt to defeat password security by repeatedly trying common passwords until they find the correct one. This repeated attempt is known as a **brute force attack**.

Denial of Service and Flooding

Another suspicious activity is a sudden burst in the amount of traffic a host receives. Programmers have written programs that can be installed on multiple computers and then triggered to make multiple, rapid requests of a single server. This category of attack is known as a **Denial of Service (DoS)** attack. Many of these attacks originate in offices or schools where there are many computers in one location that can all be setup and triggered at once.

Denial of service attack programs have even been concealed in other programs to propagate like a virus. The DoS program can be set to start at a particular time or even triggered by an Internet broadcast or other signal. This distribution of the attack across multiple machines in multiple locations makes the attack more difficult to block and gains the particular name **Distributed Denial of Service (DDoS)** attack.

This flood of traffic from a DoS causes the server to slow down and/or crash and prevents other users from being able to connect to the server. The burst of traffic can take many forms. Any Internet request that can be generated will slow down a web server if enough of that request can be generated. Common types of requests used in DoS are HTTP, FTP, SMTP, Ping or TCP/IP Syn requests.

Above you have seen examples of HTTP, FTP, SMTP and Ping requests. The TCP/IP Syn request is a request for a host to respond with an available port number to be used in making a connection. If enough Syn's are generated the server will run out of available port numbers. These attacks have gained more specific nicknames. A Ping DoS attack is known as **Ping Flooding** or Smurfing. Syn DoS attacks are called **Syn Floods**.

SMTP requests can be incomplete mail messages or complete mail messages. Mass mailing can cause DoS like effects. Malicious mailings, known as Mail Bombs, can overwhelm a user's mailbox and eventually the mail server if enough mail requests are generated. SMTP mail request DoS attacks can also take the form of mass quantities of **unsolicited email**, known as **Spam**. Large quantities of Spam have recently overwhelmed many large mail servers. States such as Virginia, Utah and Washington have passed laws restricting unsolicited email. Some mailers have even been taken to court and fined for the damages they have caused to mail services.

All of these attacks have the basic symptom of causing the server to slow down and eventually stop or crash. Obviously preventing other users from being able to use the server can be measured as success for the malicious user, but also there is another possible reason for this type of attack. The advantage of causing a server or other host to crash for the malicious user is that some operating systems such as Microsoft Windows NT 4.0 and some Cisco routers have a bug that allows the user to gain supervisor rights by logging in while the device reboots.

Gaining supervisor rights means the user can copy, replace, modify or delete all files and sometimes settings on the device. As supervisor the malicious user can also add additional supervisor user accounts that can be used to gain access again in the future. Also as supervisor it is possible to install software that records keystrokes or automatically changes settings at certain times of day to make future attacks easier. These changes that allow for future access are known as **trap door attacks**.

Stopping DoS attacks usually centers on identifying what IP addresses are creating the traffic and blocking those IP addresses at a router before they arrive at the IP address that is being targeted by the attack. Doing this with a Distributed DoS is obviously a greater problem since it is more likely that there will not be an easily defined set of IPs to block but many single IPs that each must be blocked one-by-one.

Man in the middle or hijacking attack

In a different category of attack, a malicious user or can place a packet sniffer onto a network between the server and client. This lets the sniffer receive all the information that is being sent between the server and the client. In doing this, the hope is to capture unencrypted text information such as business secrets or usernames and passwords. This attack is called a **man in the middle attack** and requires some form of access to the network being attacked. Depending on how the network is set up that can be very easy or very difficult.

A company with multiple locations without a properly configured VPN will have a great deal of public traffic that can be sniffed if it can be found on the larger public network. In an office building it is possible to find network devices in unlocked closets or utility rooms that can be used for the attack. In a more complicated attack, the company's routers can be reprogrammed to send local traffic through an outside router where it can be captured. This redirection is called a **hijacking** attack.

Man in the middle attacks are especially difficult to detect because the data continues on to where it was intended to go, and there is virtually no sign that it has been in the tampered with.

Spoofing or Masquerade attacks

A computer can be made to act like another computer and traffic intended for the other server can be directed to the imposter. This is a spoofing attack. As noted above, spoofing a bank site could be lucrative for a malicious user.

Insider and Replay Attacks

A malicious user who already has an account on a server or system can examine parts of the system and gain insight into ways to compromise the system security. Insiders can watch other users and even read memos and notes that may be saved in common areas of the server to gain access to the other parts of the server.

Malicious users can even install software or hardware on other users machines that records keystrokes of users as they use their computer. This allows for commands and passwords to be recorded for future use.

At the network level a user can record network traffic and replay it on the network to cause a server to provide access to information or trigger similar events at a different time. This is one of the few successful attacks that was used on banking machine networks.

Trojan horse attacks

Trojan Horse attacks involve hiding an unauthorized command within a commonly used command or program to cause a breach of security. For example the login command can be replaced with a similar attack that captures the users password sends it to the malicious user and then logs the person into the system as though nothing happened. Trojan horses can take many forms, any programmable event can be hidden as another program and used to gain access to a system or cause problems on the server.

Social Engineering Attacks

Probably the most successful attack for malicious users is the **social engineering attack**. The user impersonates a supervisor or a needy user and has people with system access give them information or access to the system. Some hackers claim that a sweet female voice is the best method of attack on system administrators. Claiming to be a temp for a mean boss or otherwise a helpless figure can gain great sympathy for them and get the supervisor to reset passwords or disclose useful information about their system.

In a reverse social engineering attack: during the 1960s the hackers at MIT used social engineering to explore the still under construction WATS-Toll free phone service. The hackers are credited with speeding the toll free systems implementation by posing as system technicians and reporting problems to Phone company service supervisors.

Security and Business Arrangements

Networks can be described and categorized by how they connect with other networks.

The network we have been talking about most if the Internet. It is a worldwide collection of networks that all work together to route traffic and handle user's requests. Unlike online services, which are centrally controlled, the Internet is decentralized by design. Each Internet computer, called a host, is independent. Its operators can

choose which Internet services to use and which local services to make available to the global Internet community. Remarkably, this anarchy by design works exceedingly well.

A TCP/IP network that is wholly owned by a company or organization and only available to its employees or members is called an **Intranet**. The web sites and servers on an Intranet operate just like an Internet except outside traffic to them is blocked at a firewall. Since intranets can use Internet compliant hardware and software they are usually much less expensive to setup than other private networks.

An **Extranet** refers to an intranet that is partially accessible to authorized outsiders. Extranets are becoming a very popular means for business partners to exchange information. While an intranet resides behind a firewall and is accessible only to people who are members of the same company or organization, an extranet provides various levels of accessibility to outsiders. You can access an extranet only if you have a valid username and password or are connecting from a trusted IP address. Your identity determines which parts of the extranet you can view.

Intellectual Property

To promote the production of new creation, governments around the world have given exclusive rights to profit from ideas to each idea's creator. For print materials and art this protection to profit is called **copyright**.

A copyright is automatically granted to the creator of a work or the creator's employer at the time of creation. No copyright or circle-c mark needs to be written on a work for a copyright to be valid. Stronger protections can be gained by filing a copyright with the Library of Congress, but it is not necessary.

Copyrights apply only to original written or artistic works. This includes computer graphics and programming or markup language code. Adding a copyright notice to the creation in the form of the "©", or "Copyright" along with a date or year of creation and the creator's name provide the best protection in case of a copyright dispute.

For works made after 1978, the creator of a work has the exclusive right to profit from the work for a period of time equal to the life of the creator plus seventy years (the i-Net+ sometimes uses the older figure of life plus 50 years). If the work is made from a corporate entity or business entity that does not have a life span, the protection is the shorter of 95 years from publication or 120 years from creation. After that point the work is considered, under copyright law, to be in the public domain. However, the growing idea of intellectual property gives eternal protection to the work and its creator.

The following cannot be copyrighted: (1) Works that have not been fixed in a tangible form of expression. For example, choreographic works that have not been notated or recorded and improvisational speeches or performances, which have not been written or recorded, are not protected. (2) Titles, names, short phrases, and slogans; familiar symbols or designs; mere variations of typographic ornamentation, lettering, or coloring; or mere listings of ingredients or contents. (3) Ideas, procedures, methods, systems, processes, concepts, principles, discoveries, or devices, though their description, explanation, or illustration can be protected. (4) Works consisting entirely of information that is common property and containing no original authorship. For example: standard calendars, height and weight charts, tape measures and rulers, and lists or tables taken from public documents or other common sources.

There are exceptions for using someone else's copyrighted work for the purposes of criticism, commentary or parody. Despite what is often claimed, there is no exception for educational or academic use of a work.

Violations of copyright are generally handled in civil courts. The owner of a copyright can file a civil suit in court to collect damages from those using their work. Federal courts can also become involved, though this is rare for small cases. The minimum statutory fine for copyright infringement is \$200 per copy. If intent and knowledge can be proven the fine rises to \$100,000 per copy. A first offence can generate up to a five-year prison sentence and further offences have a 10-year maximum penalty.

In addition to copyright, trademarks also protect a creator's intellectual property. As noted above, logos or symbols and short phrases cannot be protected by copyright. The U.S. **Trademark** laws provide protection for creators of logos, symbols and short phrases that are used to identify a service, product or business entity.

Most copyrighted works can be **licensed** for use on the web or in print. Contacting the copyright holder or an agency that is managing their licensing is usually a very easy way to secure legal use of another person's work.

Many licensing companies will charge a small fee for the use of their work to affirm that they are the owner of the copyright. Bertelsmann Music Group and/or ASCAP usually handle musical works' licensing. Major art works' rights are managed by the museum holding them or may have been sold to a licensing company such as Getty Communications, Image Bank and Corbis.

Copyright, trademarking, and licensing are very important issues in today's Internet society. As recent copyright infringement lawsuits have shown, making sure your website and company are following copyright laws strictly is very important.

The Digital Millennium Copyright Act of 1998 and the No Electronic Theft Act of 1997 have added copyright restrictions. They make it clearly illegal to circumvent anti-piracy tools in software or web sites; and add the requirement that material sent through steaming media follow the same rules as broadcast media for paying copyright fees. The acts also allow ISPs to no longer be responsible for the contents of their web servers placed there by customers or others.

Global Marketplace

Since the Internet connects almost every country in the world, it is possible for any web site to be viewed in almost any country of the world. This allows goods, services and products to be traded across national boundaries and for goods to be ordered from overseas.

International issues of shipping and supply chain need to be taken into consideration when developing an international business. Shipping across countries and through customs can take a considerable amount of time and expense, and supplying partners through long ship times can affect business operations. Since each country has slightly different import and export laws, legal and regulatory issues will arise when conducting international business. Issues such as taxes, local laws, and customs are issues to consider before supplying other countries, and thus need to be taken into consideration prior to designing business systems.

Other than being aware and doing research, there is no one answer for international issues.

To better represent each country's native language it may be necessary for an international business to translate their web site into multiple languages. For correct and efficient representation of characters and ideas in the other languages it is often necessary to use the Unicode character set which includes the characters of most human languages. Unicode is an international standard that is being used by most countries as they update computers to be Internet compatible.

The constantly changing currency market also makes it important for the terms of a sale to be clearly defined for exchange rate and payment terms. Fluctuations can make an expensive item cheap and bankrupt a company counting on a higher exchange rate.

Audience Development

The Internet is designed to transport information from user to user and server to client efficiently. To effectively move information and to broaden their audience, web sites need to identify people who are interested in their content. There are two general technologies that perform this function: push technology and pull technology.

Push technology: Push technology is one that was developed to send information out to a client without a request for the specific information being sent. This information could be of many forms, stock quotes, news, programs, etc. The information is automatically sent to the client, which could use it at their discretion and on their schedule. Examples of this are the Internet Explorer 4.0 and Windows 98 Channels and the Infogate screen saver and ticker (formerly PointCast and Entry Point). A preferences file is stored on the user's hard drive that keeps their preferences and settings for what information they wish to receive. This **Channel Definition File** or CDF determines which information is collected by their computer for display as requested by the user's software.

Pull technology: Pull technology brings users to a site to retrieve information from the site. This is the normal method that web pages work. The user actively selects what information they wish to view and it is sent to their computer when requested.

These two technologies can be used effectively to develop and retain an audience. Push technology was a hit among the investment and analyst sector several years ago, though has not proved popular among users.

E-Commerce terms and Concepts

Web commerce has created a stir in most of the world. Web commerce, **Internet Commerce** or e-Commerce all refer to the idea that the exchange of goods or services for money is done electronically through the international computer network. In particular **Business-to-Business (B2B)** sales technologies have been highly touted for their possibilities.

B2B is simply sales targeted toward businesses rather than consumers. The assumption that businesses will buy greater quantities of products than consumers allows for B2B companies to offer lower prices to their customers. This large quantity small profit margin theory was expected to greatly improve the efficiency of the purchasing process for businesses.

B2B contrasts with the **B2C** or **Business-to-Consumer** sales model, where small quantities of each product are sold for a larger profit each than in B2B. Since B2B allows for businesses to invoice their purchases electronically rather than through the expensive credit card system it is expected to gain once more companies install electronic invoicing or EDI based accounting systems.

EDI, Electronic Data Interchange, is the transfer of data between different companies using networks, such as the Internet. As more and more companies get connected to the Internet, EDI is becoming increasingly important as an easy mechanism for companies to buy, sell, and trade information. ANSI has approved a set of EDI standards known as the X12 standards. EDI is designed to simplify the purchase, invoicing and payment process to save businesses money.

In addition to EDI, which is almost exclusively for large companies, **Online Transaction Processing, OLTP** is being used to facilitate payment and data entry for companies and consumers. SET is a form of OLTP. Officially OLTP, is a class of program that facilitates and manages transaction-oriented applications, typically for data entry and retrieval transactions in a number of industries, including banking, airlines, mail-order, supermarkets, and manufacturers. Today, online transaction processing increasingly requires support for transactions that span a network and may include more than one company.

In order for people to purchase products online, users need to be able to compare the products they are considering ordering. **Online Cataloging** provides the system for these products to be indexed and retrieved so users can make their purchase decision. Once items are selected and the user chooses to make their purchase, **Merchant systems** provide the back end that process the order and payments in real-time. The merchant system is required for the transaction to be finalized online.

Customers who are indecisive about a purchase can be aided in their decision using customer service technologies online. **Customer self-service** systems allow customers to help themselves without human intervention. Oftentimes used in software companies to let customers help themselves using knowledge databases. Customer self-service also is used to reduce after-purchase product support, by allowing customers to search for answers to their questions on-line without taking the time of a phone operator or other staff person.

After the purchase, a Web commerce site will try to retain the customer as a client for future purchases. This is done through additional backend software known as **Relationship management** software. This relationship management software uses backend software which helps generate more leads and sales. It feeds promotional materials to the user to encourage the user to return to the store. These promotions are a form of Internet marketing. **Internet marketing** includes any form of advertising and marketing your products via the Internet. These could be banner advertising, site sponsorships, viral marketing, email lists, or other on-line promotions and partnerships.

The OSI Reference Model

The **International Organization for Standardization (OSI)** developed the **OSI Reference Model** or **OSI/RM** as a guide for defining a set of open protocols to be used by computers and computer networks.

The OSI/RM divides the network connection and communication process into seven layers. Different descriptions of the process number these seven layers in different ways, but usually they are numbered with the Physical layer being layer 1 and the Application layer being 7.

| No. | Title | Role at sending computer | At receiving computer | Examples |
|-----|--------------|---|--|---|
| 7 | Application | Allows the user to input information to be sent via network. | Displays the received information in for the user. | Web Browsers, mail programs and other software that is network enabled. |
| 6 | Presentation | Responsible for translating data from an application's format to a network compatible format, often using data encryption and compression | Responsible for translating data from the network compatible format to application readable formats which can include decryption and decompression | Rarely implemented, or often part of the software application. |
| 5 | Session | Controls and manages dialog control between network hosts. | Controls and manages dialog control between network hosts. | |
| 4 | Transport | Divides messages into fragments that fit within the size limitations established by the network. It also marks the order the packets should be reassembled in. For example, Ethernet, limits the size of the data field to 1500 bytes and ATM connections are limited to 48 bits of data per packet. It is also used for detecting errors in transmitting data. | Reassembles the fragments based on their original order to recover the original message. Detects errors in transmitted data and signals the sender if redelivery is necessary. | TCP/IP Port. And port management software |
| 3 | Network | Adds a header to the messages that includes the source and destination network address. | Checks headers to verify that the received message is for the receiving computer and from a valid source. | IP address. Driver software and Routers. |
| 2 | Data Link | Provides an address mechanism that enables messages to be delivered to the correct nodes. Translates messages from into bits that the physical layer can transmit. The data units at the data link layer are most commonly called frames, although the term packet is used with some protocols. | Determines if the target address of a packet of frame is for the receiving computer. Throws out all other traffic. | Network interface card and driver software. MAC address. Bridges. |
| 1 | Physical | Places bits or signal directly on the communication medium. | Detects bits and signal on the communication medium. | Wire, fiber optic cable, hubs. |

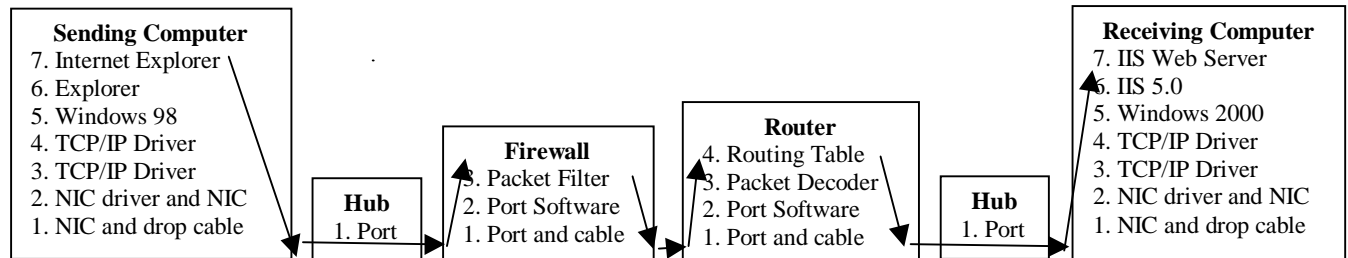
There are a number of mnemonics to remember the layer names, the most common are:

| OSI/RM | Physical | Data link | Network | Transport | Session | Presentation | Application |
|--------|----------|-----------|---------|-----------|---------|--------------|-------------|
| 1 | Please | Do | Not | Tell | Sales | People | Anything |
| 2 | Please | Do | Not | Throw | Sausage | Pizza | Away |

The **transport layer** can perform two general categories of error detection: **Reliable delivery** where errors are detected if they do occur; and **Unreliable delivery** where the transport layer does not check for errors.

The **Session Layer** communications can take place in one of three dialog modes, which are: Simplex, half duplex, and full duplex. Sessions enable nodes to communicate in an organized manner. Each session has three phases: Connection establishment, Data transfer, Connection release; the Connection establishment is where the TCP/IP Syn command is used..

On the network traffic's route to its destination, it is encoded and decoded a number of times using the OSI/RM. This process allows the packet to be appropriately addressed and screened and routed so it arrives at the target computer as efficiently as possible.



Each device that alters the packet also alters its **Time To Live** or TTL setting. TTL is a measure of the number of times a packet can be repeated before it must be killed. This prevents a packet from being forwarded around the Internet eternally. Usually a TTL is set to be 127 or 255. Trace route software and Pings show the TTL's value as part of their statistic report.

The OSI/RM is merely a model. Different protocol suites and operating systems implement its design in different ways. The TCP/IP suite predates the OSI/RM model and does not entirely match the models layers for how it is implemented. Only Macintosh System 7 implements the full seven-layer model in their operating system. All other OSs use a slightly different layering to implement their network connection.

Practice Questions

It is recommend that you use the questions below to review for the examination. You also have been given a Transcender Review tool for the test. The Transcender will give you a good feel for how the testing software works at the testing center.

There are some questions on the Transcender that are more difficult than the exam and some questions that cover topics that are not on the exam. If a Transcender question's content is not covering one of the topics listed in the Exam Blueprint above; it will not be on the real i-Net+ exam.

For the best results using the Transcender:

- A. Use Tests A and B as practice tests, but save test C for a final review before the exam. Do not take test C until you are very comfortable with the contents of Tests A and B.
- B. When you are done with an exam, print out the correct answers and explanations from the questions you missed. Review the material that those questions covered and retake the same exam.
- C. Beware of memorizing questions on the Transcender. You can get all the Transcender questions correct by memorizing the correct answers rather than learning the materials. That cause you damage when you take the real exam. Be certain that you know why the answers you choose are correct.
- D. When you have a doubt about a particular questions on the Transcender, make a note of the topic or questions number and review that material so you understand all your answers.

Note: Transcender will be releasing an update to their i-Net+ software during the third quarter of 2001.

For the questions below, you should fold the page in half and note your answers on a separate paper before you check each answer. That way you can reuse the questions and you will not be tempted to peek at the answers.

When a question says "Select all that apply" it is a sign that there are multiple correct answers. You must choose all the correct answers to get the answer correct. On the computerized tests you will find that instead of round "radio buttons" for a single correct answer, the test will give you square checkboxes to mark all the correct answers.

Index

- 127 11, 31, 33, 54
- 128-bit 20, 43
- 24-bit graphics 13
- 256-color 13
- access .3, 6, 7, 8, 11, 12, 19, 23, 24, 25, 30, 34, 35, 38, 39, 40, 41, 44, 45, 46, 47, 48, 49, 50
- access control 8, 45
- Active Server Pages 25
- Adapter 8
- Address 6, 18, 32, 33, 35
- Administrators 3
- Adobe Acrobat 19, 29
- ADSL 40
- agency 31, 51
- ALIGN 26
- all-in-one clients 6
- Alta Vista 14
- American Registry of Internet Numbers 17
- Analog 39
- anchor** 26
- ANSI 52
- Antivirus** 20
- anti-virus software 8
- API 7, 22, 24, 31
- APNIC 17
- application 7, 19, 22, 34, 35, 53
- Application** 3, 19, 22, 53
- ARIN 17
- ARP 8, 35, 36
- ASCAP 51
- ASCII 19
- ASF 29
- ASP 7, 23, 24, 25
- assets 46
- Asymmetric DSL 40
- asynchronous 34
- AT&T 40
- AT-code** 38
- ATM 8, 40, 41, 47, 53
- Audience 6, 11, 12, 51
- audit 3
- auditing 8, 45, 48
- Auditing 8, 46
- authentication 8, 45, 46, 47
- Authentication 8, 45
- authority 42
- authorship 50
- AVI 7, 28, 29
- B2B** 52
- bandwidth 8, 11, 12, 14, 40, 41
- Bandwidth 6, 11, 12, 39, 40
- banner advertising 53
- Beacon 1, 9
- BellLabs 24
- Beowulf 42
- Bertelsmann Music Group 51
- BGCOLOR 26, 27
- BINHex 7, 29
- bits per second 12, 39
- BLOCKQUOTE 26
- BMP 7, 13, 29
- Boot Sector** 21
- BOOTP** 16
- Border** 27
- bps 12, 39
- Bridge 8, 37
- browser 6, 7, 13, 14, 15, 18, 19, 20, 21, 23, 24, 26, 28, 34, 42, 44, 46
- Browser 8, 19
- browsers 6, 7, 12, 14, 15, 19, 20, 24, 28, 30
- brute force attack 48
- Business 6, 8, 49
- business relationship 45
- Business to Consumer 8
- Business-to-Business 52
- Business-to-Consumer 52
- C 7, 10, 11, 17, 23, 24, 30, 33, 55
- Cable Modem 30, 39
- cache 6, 13, 14, 18, 39, 42
- Cache 8, 39, 42
- Cache-in-a-box 8, 39
- caching 6, 13, 14, 39
- calculators 9
- Canada 33, 43
- Canonical Name 32
- CCITT *See*
- ccTLD 32, 33
- CDF 52
- Cell phones 9
- Cellpadding** 27
- Cellspacing** 27
- Certificate 8, 46
- Certificate Authority 42
- Certificate Servers 42
- certificates 8, 42, 43, 45
- certifications 4, 5
- CFML 25
- CGI 7, 22, 23, 25, 31
- Channel Definition File** 52
- Channel Service Unit 38
- Channels 51
- character 8, 51
- check clearing 43
- children 9
- Cisco 34, 39, 45, 48
- CIW 3, 4
- class 3, 10, 11, 17, 24, 33, 52
- Class** 11, 17, 33, 42
- Classes 10
- client .. 3, 6, 7, 8, 10, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 31, 34, 35, 43, 44, 46, 49, 51, 52

| | | | | | |
|---------------------------------------|-------------------------------------|--|-------------------------|---|-----------------------------------|
| Client..... | 6, 7, 11, 13, 15, 18, 19, 24 | DHCP | 6, 16, 17, 33, 39 | exchange rate | 51 |
| Cocos (Keeling) Islands | 33 | dialup..... | 30 | exit | 16 |
| ColdFusion..... | 25 | digital signatures..... | 8, 44, 45 | Explorer . | 12, 14, 19, 21, 28, 30, 42 |
| Compiled..... | 24 | Digital Subscriber Line..... | 40 | extension..... | 10, 19, 24, 29 |
| CompTIA | 3, 4, 6, 9 | directories | 10, 14, 35, 41, 46, 47 | extranet | 8, 25, 45, 50 |
| CompuServe..... | 28 | directory | 10, 14, 27, 35, 47 | Extranet..... | 8, 50 |
| computer3, 9, 10, 11, 12, 13, 14, 15, | 16, 17, 18, 19, 20, 21, 22, 23, 24, | distant networks..... | 37 | fiber optic cable | 53 |
| 29, 30, 31, 32, 33, 34, 35, 36, 38, | 40, 41, 42, 43, 44, 45, 46, 47, 49, | Distributed Denial of Service | 48 | file formats..... | 7, 13, 28, 29 |
| 50, 52, 53, 54 | | DLL | 7, 22 | filename | 10, 15, 16 |
| connection speed..... | 12 | DMOZ..... | 14 | firewall..... | 3, 8, 39, 50 |
| cookies | 7, 21, 22 | DNS. 3, 6, 7, 11, 16, 17, 18, 31, 32, | 47 | Firewall..... | 8, 39 |
| Cookies | 21 | domain7, 10, 16, 17, 26, 31, 32, 33, | 47, 50 | Flash | 7, 28 |
| copyright | 8, 28, 50, 51 | domain name | 16, 17, 31, 32, 33 | flat-file | 25 |
| copyright infringement..... | 50 | domains | 3, 6, 7, 31, 32, 33 | Flooding | 48 |
| Corbis..... | 51 | DoS | 48 | floods | 8, 47 |
| corrupt..... | 7, 12, 14, 30 | dot-com..... | 18 | FONT..... | 26 |
| Corrupt files | 6, 11, 12 | Drivers..... | 22, 45 | form . | 16, 23, 27, 28, 31, 34, 36, 38, |
| country code..... | 31, 32, 33 | DS-1 | 40 | 48, 49, 50, 52 | |
| CSU | 38, 39 | DSL | 8, 12, 16, 30, 39, 40 | fragments | 53 |
| Customer | 8, 52 | DSN..... | 25 | frame relay | 40 |
| customers | 30, 40, 42, 51, 52 | DSU | 31, 38, 39 | FTP3, 6, 7, 8, 11, 12, 15, 16, 34, 35, | 41, 47, 48 |
| daemons | 11, 34 | Duke University..... | 35 | full text | 6, 14, 15 |
| damages..... | 48, 50 | E-1 | 40 | gateway..... | 6, 11, 16, 17, 18, 37 |
| Data Link | 53 | E-3 | 40 | Gateway | 8, 17, 22 |
| Data Service Unit | 38 | e-commerce | 8, 30, 42 | GATT..... | 47 |
| Data Source Name..... | 25 | EDI..... | 8, 52 | General Agreement on Tariffs and | Trade |
| database3, 7, 22, 25, 42, 43, 44, 46, | 47 | Electronic Data Interchange ... | 52 | get .. | 6, 9, 14, 15, 16, 35, 38, 39, 49, |
| Database | 3, 22, 25, 47 | email 6, 7, 8, 19, 21, 27, 29, 34, 35, | 42, 47, 53 | 52, 55 | |
| Databases | 25 | Email | 15, 19 | Getty Communications | 51 |
| DBMS | 25 | Encapsulated Postscript..... | 29 | GIF..... | 7, 19, 28 |
| DDoS | 48 | encoding..... | 29 | GIF89a..... | 7, 28 |
| decoding..... | 29 | encryption 8, 20, 34, 35, 43, 44, 45, | 53 | global | 8, 35, 50 |
| dedicated lines..... | 12 | Encryption | 7, 8, 43 | Google | 14 |
| default subnet mask..... | 11 | engines..... | 14 | Gopher | 7, 34, 35 |
| Denial of service | 8, 48 | EPS..... | 7, 29 | graphics ...6, 11, 12, 13, 20, 21, 28, | 29, 50 |
| Denial of Service..... | 48 | errors | 9, 41, 53 | Graphics Interchange Format..... | 28 |
| Denmark..... | 46 | Ethernet | 36, 53 | GUI..... | 7, 28 |
| Department of Defense..... | 33 | Eudora e-mail | 15 | hackers..... | 47, 49 |
| Designers | 3 | exam | 3, 4, 6, 14, 27, 32, 55 | | |
| Desktop | 7, 16, 20 | | | | |

| | | | |
|------------------------------------|---|--|--|
| hard drive | 13, 14, 18, 20, 21, 31, 39, 41, 46, 51 | | |
| Hardware | 6 | | |
| HEAD | 26 | | |
| headings | 7, 26 | | |
| hijacking | 49 | | |
| holy grail | 40 | | |
| host | 10, 12, 32, 33, 35, 36, 41, 42, 48, 50 | | |
| hostname | 10 | | |
| HOSTS | 17, 18 | | |
| HREF | 26 | | |
| HTML | 7, 19, 23, 24, 25, 26, 28, 29 | | |
| HTTP | 7, 8, 11, 15, 16, 18, 21, 30, 34, 41, 48 | | |
| HTTP 1.0 | 34 | | |
| HTTP 1.1 | 34 | | |
| hub | 36, 37 | | |
| Hub | 8, 38, 39 | | |
| Hypertext Transfer Protocol | 34 | | |
| | | | |
| IANA | 33 | | |
| identity theft | 47 | | |
| IE 14 | | | |
| IETF | 44 | | |
| IIS | 24, 41 | | |
| image | 13, 19, 26, 27, 29 | | |
| Image Bank | 51 | | |
| IMAP | 34, 41 | | |
| IMG | 26 | | |
| index | 6, 14, 15, 25, 27 | | |
| index server | 15 | | |
| indexes | 6, 14, 15 | | |
| i-Net+ | 1, 3, 14, 23, 32, 50, 55 | | |
| infrastructure | 3, 6, 7 | | |
| INPUT | 27, 28 | | |
| Insider | 49 | | |
| Intellectual Property | 50 | | |
| interface card | 8, 16, 53 | | |
| International | 8, 33, 51, 53 | | |
| International treaty organizations | 33 | | |
| Internet | 3, 4, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 28, 29, 30, 31, 32, 33, 34, 35, 38, 39, 40, 42, 45, 48, 50, 51, 52, 54 | | |
| Internet Explorer | 15, 28 | | |
| Internet marketing | 52 | | |
| Internet Message Access Protocol | 34 | | |
| Internet Protocol | 35 | | |
| Internet-in-a-box | 39 | | |
| interpreted | 22, 23, 24 | | |
| Intranet | 3, 8, 50 | | |
| intrusion detection | 8, 46 | | |
| IP | 6, 7, 10, 11, 15, 16, 17, 18, 19, 31, 32, 33, 35, 36, 46, 48, 50, 53 | | |
| IP addresses | 10, 11, 18, 31, 48 | | |
| IPConfig | 8, 35 | | |
| ISAPI | 22, 23, 25 | | |
| ISDN | 8, 12, 30, 34, 39 | | |
| ISP | 6, 11, 12, 16, 17, 18, 34, 38, 46, 48 | | |
| ISPs | 12, 14, 16, 38, 51 | | |
| ITU | 33, 41 | | |
| | | | |
| Japan | 33, 46 | | |
| Japan Network Information Center | 33 | | |
| Java | 7, 22, 23, 24, 25 | | |
| Java Database Connectivity | 22 | | |
| JavaScript | 7, 23, 24, 28 | | |
| JDBC | 22, 25 | | |
| Joint Photographic Experts Group | 28 | | |
| JPEG | 7, 19, 28 | | |
| Jscript | 7 | | |
| JSP | 25 | | |
| Jughead | 35 | | |
| JVM | 24 | | |
| | | | |
| Kbps | 39, 40 | | |
| keyword | 6, 14 | | |
| knowledge databases | 52 | | |
| | | | |
| Language | 12, 22, 24 | | |
| languages | 7, 22, 23, 24, 25, 51 | | |
| laws | 48, 51 | | |
| Layer 2 Forwarding | 34 | | |
| LDAP | 7, 8, 11, 34, 35, 41 | | |
| | | | |
| legacy | 7 | | |
| Legal | 8 | | |
| LI 26 | | | |
| license | 8, 42 | | |
| licensed | 51 | | |
| licensing | 8, 51 | | |
| links | 7, 12, 26, 27, 30, 35 | | |
| List | 8, 26, 42 | | |
| LMHOSTS | 18 | | |
| log files | 8, 46 | | |
| login | 8, 10, 35, 46, 47, 48, 49 | | |
| login failures | 8, 47, 48 | | |
| loopback | 11, 33 | | |
| Lotus Notes | 20 | | |
| LPR | 7 | | |
| | | | |
| MAC | 36, 53 | | |
| Macintosh | 12, 29, 54 | | |
| Macromedia | 28 | | |
| Macros | 21 | | |
| MAE | 12, 30 | | |
| MAE East | 12 | | |
| MAE West | 12 | | |
| Mail | 8, 19, 32, 34, 41 | | |
| Mail Bombs | 48 | | |
| Mail Exchange Record | 32 | | |
| Malicious | 48, 49 | | |
| man in the middle attack | 49 | | |
| mask | 6, 16, 17 | | |
| Masquerade | 49 | | |
| MasterCard | 46 | | |
| mathematics | 43 | | |
| Mbps | 39, 40, 41 | | |
| Merchant systems | 8, 52 | | |
| METHOD | 27 | | |
| Metropolitan Area Exchange | 12 | | |
| Metropolitan Area Exchanges | 30 | | |
| mget | 15, 16 | | |
| Microsoft | 4, 15, 20, 21, 22, 24, 25, 29, 41, 48 | | |
| Microsoft IIS | 22 | | |
| Microsoft Outlook | 15, 20 | | |
| Military | 33 | | |

| | | | | | |
|---|---|--|--------------------------------------|-------------------------------------|--|
| MIME..... | 7, 8, 19, 43 | NOS..... | 8, 41 | permissions..... | 47 |
| Mirror servers | 41 | notebooks..... | 9 | Personal Home Page..... | 25 |
| Mirrored..... | 8, 42 | | | Personal Identification Number..... | 47 |
| mirrored hard drives | 41 | Object Oriented..... | 25 | phone..... | 6, 12, 15, 16, 34, 38, 39, 40, 49, 52 |
| MIT..... | 49 | Object Query language..... | 22 | PHP..... | 19, 25 |
| modem | 12, 15, 16, 38, 39, 40 | Object-based..... | 24 | PHP3..... | 19 |
| modulator-demodulator..... | 38 | Object-Oriented..... | 24 | Physical..... | 53 |
| monitors..... | 13 | OC-3..... | 40 | Ping..... | 8, 35, 48 |
| MOV..... | 7, 29 | octet..... | 10, 11, 33 | Ping Flooding..... | 48 |
| Moving Pictures Expert Group..... | 29 | octets..... | 11, 17 | pixels..... | 13, 27 |
| MP3..... | 29 | ODBC..... | 22, 25 | PKIX..... | 44 |
| MPEG..... | 7, 29 | ODBMS..... | 22, 25 | platform..... | 6, 15, 29, 35 |
| mput..... | 15, 16 | OL..... | 26 | PNG..... | 7, 20, 28 |
| Museum Domain Management Association..... | 33 | OLTP | 52 | Point-to-point..... | 7, 34 |
| | | Online Cataloging..... | 8, 52 | Polymorphic | 21 |
| Name Server..... | 32 | Online Transaction Processing | 52 | POP..... | 34, 41 |
| NAP | 12 | operating system..... | 3, 7, 15, 16, 18, 19, 22, 25, 38, 54 | POP3..... | 7, 11, 15, 16, 34 |
| NAPs..... | 12, 30 | Operating system..... | 6 | port..... | 10, 11, 36, 37, 48, 53 |
| NetBIOS..... | 6, 18 | OQL | 22, 25 | Port..... | 6, 11, 53 |
| Netscape..... | 13, 14, 15, 16, 19, 24, 27, 28, 29, 30, 42 | Oracle..... | 25 | Portable Network Graphic..... | 28 |
| netstat..... | 36 | ordering..... | 46, 52 | Postscript | 29 |
| Netstat..... | 8, 36 | OS..... | 15, 16, 22, 35 | PostScript..... | 7 |
| network..... | 3, 11, 15, 16, 17, 18, 19, 20, 21, 22, 30, 31, 33, 34, 35, 36, 37, 38, 39, 40, 41, 43, 45, 46, 47, 48, 49, 50, 52, 53, 54 | OSI | 53, 54 | PPP..... | 7, 16, 34 |
| Network Access Point | 12, 30 | OSI Reference Model | 53 | PPTP..... | 7, 34 |
| Network Access Points | 30 | OSI/RM | 53, 54 | Presentation..... | 53 |
| network connection | 15, 19, 31, 35, 46, 53, 54 | Outlook Express..... | 15 | printer servers | 41 |
| Network ID..... | 33 | | | privacy..... | 7, 22, 43 |
| Network Interface Card..... | 36 | packet filters..... | 8, 45 | private..... | 7, 8, 31, 33, 34, 35, 38, 40, 43, 44, 45, 50 |
| Network News Transfer Protocol..... | 35 | paragraph..... | 26 | Professional..... | 4 |
| Network Operating System | 41 | partnerships..... | 53 | profit margin..... | 52 |
| Networking..... | 1, 6, 33 | password..... | 8, 10, 43, 45, 46, 47, 48, 49, 50 | Prometric..... | 4, 9 |
| News..... | 8, 41 | passwords..... | 20, 36, 45, 46, 47, 48, 49 | Prosoft..... | 3, 4 |
| NNTP..... | 7, 11, 16, 34, 35, 41 | patch..... | 20 | protocol..... | 10, 11, 15, 16, 27, 34, 35, 40, 41, 45, 54 |
| No access | 47 | payment..... | 9, 30, 46, 51, 52 | Protocol..... | 6, 11, 15, 16, 34, 35 |
| nodes..... | 53 | payments..... | 52 | proxy..... | 6, 8, 12, 14, 19, 39, 45 |
| non-repudiation | 8, 44 | PDA..... | 15 | Proxy..... | 6, 8 |
| North American..... | 40 | PDA's..... | 9, 15 | Proxy servers..... | 39 |
| | | PDF..... | 7, 12, 29 | Public..... | 7, 33, 43, 44 |
| | | performance..... | 6, 7, 9, 11, 12, 19, 20, 31 | Pull..... | 8, 52 |
| | | Perl..... | 7, 23, 24 | Pull technology..... | 52 |
| | | | | Push..... | 8, 51, 52 |

| | | |
|---|--|--|
| Push technology.....51 | secure socket layers 8 | Stealth 21 |
| put6, 14, 15, 16, 26, 27, 45 | security 3, 6, 7, 8, 9, 11, 19, 20, 22, 23, 36, 38, 41, 43, 44, 45, 46, 47, 48, 49 | stolen..... 47 |
| QTVR7, 28 | Security..... 3, 6, 7, 20, 45, 46, 49 | Streaming media 7 |
| QuickTime 19, 28 | segments 12, 37 | subnet..... 6, 7, 11, 16, 17 |
| RAID41 | self-service..... 8, 52 | Subnet Mask 11, 17 |
| RAM 13, 29 | server. 3, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 27, 30, 31, 32, 34, 35, 36, 39, 41, 42, 43, 45, 46, 47, 48, 49, 51 | supervisor..... 48, 49 |
| RARP36 | Server 6, 8, 23, 47 | switch 38 |
| raw text.....29 | servers.. 7, 8, 11, 12, 13, 15, 17, 18, 19, 20, 21, 22, 23, 24, 25, 30, 31, 32, 34, 35, 39, 41, 42, 45, 46, 47, 48, 50, 51 | Switch 8 |
| RDBMS22, 25 | Server-side..... 24 | switching office..... 12, 40 |
| Read access47 | service.... 11, 12, 14, 16, 30, 31, 32, 34, 35, 38, 39, 40, 41, 45, 47, 49, 51, 52 | Sylvan 9 |
| Realplayer28 | Service 6, 11, 12, 18, 20, 30, 34, 48 | Symetric DSL 40 |
| RealPlayer7, 28 | Session 53 | Syn 8, 48, 53 |
| RealVideo28, 29 | SET..... 8, 45, 46, 52 | Syn floods 8 |
| Redundant Array of Independent (or Inexpensive) Disks.....41 | SETco 46 | Syn Floods48 |
| relational database.....7, 25 | share data..... 37 | Synchronization 45 |
| Relational Database Management System.....25 | shipping 8, 51 | T1..... 8, 12, 30 |
| Relationship management 8, 52 | Shockwave..... 7, 28 | T-1 12, 40 |
| reliability 6, 11, 30 | site sponsorships..... 53 | T-3 12, 40 |
| Remote Access34 | SLIP..... 7, 16, 34 | TABLE..... 27 |
| remote user.....8 | slogans..... 50 | Tagged Image File Format 29 |
| repeater37 | SMTP 7, 11, 15, 16, 34, 41, 48 | tangible form..... 50 |
| Replay Attacks49 | Smurfing..... 48 | taxes 51 |
| Reserved Block 11 | sniffer 36, 49 | TCP/IP . 6, 7, 15, 18, 19, 31, 33, 34, 35, 36, 41, 45, 48, 50, 53, 54 |
| Resolution6, 11, 13, 35 | Sniffer Pro 36 | telephone companies..... 40 |
| Rich Text Format29 | Social Engineering 49 | telnet 10, 16, 41 |
| RIPE.....17 | software7, 8, 14, 15, 19, 20, 21, 22, 25, 28, 29, 34, 36, 37, 39, 41, 42, 43, 45, 48, 49, 50, 51, 52, 53, 54, 55 | Telnet 6, 7, 8, 11, 16, 34, 35, 41 |
| root.....7, 18, 31 | spam 8, 47 | terminology..... 12 |
| Root..... 18 | Spam 48 | The .TV Corporation 33 |
| router38, 48, 49 | Spoofing 49 | The Yes Men.....47 |
| Router.....8 | SQL 7, 22, 25 | TIFF 7, 29 |
| RTF7, 29 | SSL..... 8, 43, 44 | Time To Live 54 |
| Russian Federation33 | Start of Authority..... 32 | TITLE 26 |
| SAPI.....7, 22 | static 6, 7, 12, 14, 18 | Trace Routing 8, 36 |
| SDSL.....40 | | Tracert 36 |
| search6, 14, 15, 34, 35, 52 | | traffic 11, 13, 17, 18, 19, 30, 31, 34, 36, 38, 39, 40, 41, 42, 43, 45, 46, 48, 49, 50, 53, 54 |
| Searching.....6 | | transactions 42, 47, 52 |
| Secure Electronic Transactions8, 45, 46 | | Transcender..... 9, 55 |

| | | | |
|--|-------------------------------|---|--|
| Transmission | 15, 35, 40 | users. 12, 13, 14, 22, 25, 28, 30, 35, | web site.. 12, 13, 14, 21, 22, 25, 28, |
| transmit..... | 12, 20, 39, 41, 53 | 36, 39, 40, 41, 45, 46, 47, 48, 49, | 30, 31, 42, 46, 51 |
| Transport..... | 53 | 52 | Website |
| transport layer | 53 | Utah | 7 |
| trap door attacks | 48 | 48 | WebTV |
| Trojan Horse attacks..... | 49 | | 6, 15 |
| troubleshooting | 19 | VBScript..... | well known port |
| Troubleshooting | 7, 19 | 7, 20, 23, 24 | 11 |
| TTL | 54 | vector | Width |
| Tuvalu | 33 | 28, 29 | 27 |
| Tuvalu Ministry of Finance and Tourism | 33 | VeriSign | Windows.. 7, 12, 15, 16, 18, 19, 20, |
| | 33 | 31, 32, 33 | 22, 24, 25, 28, 29, 34, 35, 36, 41, |
| | | Veronica | 42, 45, 48, 51 |
| | | 35 | Windows Media Player..... |
| | | version... 14, 20, 24, 25, 28, 29, 30, | 7, 28 |
| | | 34, 35, 42, 43 | WinIPCfg..... |
| | | Video..... | 8, 35 |
| | | 29 | WINS |
| | | viral marketing..... | 6 |
| | | 53 | WinZip..... |
| | | Virginia | 19 |
| | | 48 | World Organization of Webmasters |
| | | Virtual Machine..... | |
| | | 24 | 4 |
| | | Virtual Private Networks | World Wide Web. 3, 34, 35, 40, 42 |
| | | 34, 45 | WOW..... |
| | | Virtual Reality Modeling..... | 4 |
| | | 24 | Write access |
| | | virus..... | 47 |
| | | 8, 20, 21, 48 | |
| | | Virus..... | X.25 |
| | | 7, 20 | 8, 40, 41 |
| | | viruses..... | X.500 |
| | | 20, 21 | 35, 44 |
| | | Visual Basic..... | X.509 |
| | | 7, 23, 24 | 44 |
| | | VPN..... | XML |
| | | 8, 34, 43, 45, 49 | 7, 20, 23, 24 |
| | | VRML | |
| | | 7, 23, 24 | Yahoo |
| | | Vue..... | 14 |
| | | 9 | yahoo.com..... |
| | | wallet | 10, 16, 31 |
| | | 46 | |
| | | Washington..... | ZIP |
| | | 30, 33, 48 | 19 |
| | | Web ... 3, 6, 7, 8, 11, 13, 14, 15, 19, | |
| | | 28, 29, 30, 31, 41, 42, 43, 46, 52, | |
| | | 53 | |
| | | web server12, 22, 23, 30, 32, 46, 48 | |
| | | | |
| UL..... | 26 | | |
| Unicode..... | 8, 51 | | |
| United Kingdom..... | 32, 33 | | |
| United States Domain Registry | 32 | | |
| universities | 24 | | |
| University of Minnesota..... | 35 | | |
| Unix | 35 | | |
| UNIX 16, 24, 25, 29, 34, 36, 41, 42 | | | |
| Unreliable delivery | 53 | | |
| unsolicited email | 48 | | |
| URL..... | 6, 26, 34 | | |
| URLs..... | 6, 10 | | |
| Usenet | 35 | | |
| user | 3, 7, 10, 11, 12, 13, 14, 15, | | |
| 16, 20, 21, 22, 23, 25, 27, 29, 34, | | | |
| 35, 41, 42, 43, 45, 46, 47, 48, 49, | | | |
| 50, 51, 52, 53 | | | |
| usernames..... | 46, 49 | | |