i-Net+ CertNotes

Acronyms

- DSL stands for Digital Subscriber Line
- DHCP stands for Dynamic Host Configuration Protocol
- PPP stands for Point to point protocol
- HTTP stands for Hyper Text Transfer Protocol
- WWW stands for World Wide Web
- HTML stands for Hyper Text Markup Language
- PPTP stands for Point to Point Tunneling Protocol
- L2F stands for Layer 2 Forwarding
- L2TP stands for Layer 2 Tunneling Protocol
- MIME stands for Multipurpose Internet Mail Extensions.
- CA stands for Certificate Authority.
- DLL stands for Dynamic Link Labrary
- ODBC stands for Open Data Base Connectivity.
- VRML stands for Virtual Reality Modeling Language
- JPEG stands for Joint Photographic Experts Group.
- PNG stands for portable Network Graphics
- TIFF stands for Tag image File Format
- MPEG stands for Moving Pictures Experts Group
- PDF stands for Portable Document Format.
- AVI stands for Audio Video Interleaved.
- PKI stands for Public Key infrastructure.

1. Internetwork IP addressing:

IP addresses are written using decimal numbers separated by decimal points. This is called dotted decimal notation of expressing IP addresses.

The different classes of IP addresses is as below:

Class	Format	Leading Bit Pattern	N/W Addr Range	Max Networks	Max Hosts/ Nodes
A	N.H.H.H	0	0-126	127	16,777,214
B	N.N.H.H	10	128-191	16,384	65,534
C	N.N.N.H	110	192 -223	2,097,152	254

N: Network address part

H: Host address part

- Network address of all zeros means "This network or segment".

- Network address of all 1s means " all networks", same as hexadecimal of all Fs.

- Network number 127 is reserved for loop-back tests.

- Host (Node) address of all zeros mean "This Host (Node)".

- Host (Node) address of all 1s mean "all Hosts (Nodes) " on the specified network.

- The range of numbers from 224.0.0.0 to 239.255.255.255 is used for multicast packets. This is known as Class D address range.

- The default subnet mask for

    o Class A network: 255.0.0.0

    o Class B network: 255.255.0.0

    o Class C network: 255.255.255.0

2. TCP/IP protocol suite was initially developed based on Unix operating system and it is native to Unix. TCP/IP protocol suite was added to other operating systems like Windows later.

3. ATM:

- ATM, Asynchronous Transfer Mode, uses 53 byte cells for all transmissions All cells are 53 byte long and consist of a 5 byte header and 48 bytes of data.

4. T1,T2, and T3 connections:

- The speeds of the Tx connections are as given below:

    o T1: 1.544 MBPS consisting of 24 channels of 64 kBPS

- o T2: 6.312 MBPS consisting of 96 channels of 64 kBPS
- o T3: 43 MBPS consisting of 672 channels of 64 KBPS

5. DSL:

- DSL uses existing copper phone lines. The access speeds can be up to 9 MBPS. but has distance limitations and available in only certain exchange areas.

- There are several categories of DSL:

- o Asymmetric DSL (ADSL): Here data flow is asymmetric. Data flow in one direction is different from that in the other direction.
- o Symmetric DSL (SDSL): Here the data flow is symmetric, that the data flows equally in both directions.
- o Other not so much used or known types of DSL are BDSL, HDSL, and VDSL.

6. The range of numbers from 224.0.0.0 to 239.255.255.255 is used for multicast packets. This is known as Class D address range.

7. Telnet, FTP, and TFTP:

- TCP/IP is the protocol used when you are Telnetting to a remote host. Telnet is used for terminal emulation that runs programs remotely.

- FTP is used to transfer files. FTP is a connection-oriented protocol. It uses TCP/IP for file transfer.

- TFTP (Trivial File Transfer Protocol) uses UDP. TFTP is a connectionless protocol.

8. A valid IP address on a host / node can't start with 127; 127.X.X.X is reserved for local loop back. A valid IP address can't be larger than 255 (in any octet), The maximum allowed value is 255 in any or combination of octets. For example, 150.206.256.31 is an invalid IP, since one octet exceeded the value 255. An example of valid IP is 202.122.154.11.

9. Tracert, Ping use ICMP as their base protocol. ICMP messages are carried in IP data grams.

10. SMTP is used to upload mail to the mail server. POP3 is used for downloading mail from a mail server to a client machine running POP3 client.

11. A firewall is a security mechanism, which prevents unauthorized access to a network or a resource on a network.

12. Important port numbers:

The port numbers used by different programs are as below:

- FTP: Port #21

- Telnet: Port #23

- SMTP: Port #25

- SNMP: Port #161

- WWW: port 80,

- NNTP: port 119,

- POP: port 110.

It is also important to know that FTP, Telnet, SMTP use TCP; whereas TFTP, SNMP use UDP.

13. Repeaters, Bridges, and Routers:

- Repeaters work at Physical layer (Layer 1),

- Bridges and simple switches work at Data Link Layer (Layer 2),

- Routers work at Network Layer (Layer 3) of ISO Reference Model.

14. Gateway is used to translate protocols, as it works at application layer.

15. Telnet requires an username and password to access.

16. ISDN:

- ISDN specifies two standard access methods:

- BRI (Basic Rate Interface):

    o Consists of two B channels (64Kbps) and one D channel (16Kbps).

    o The B channels can be used for digitized speech transmission or for relatively high-speed data transport.

    o The D channel carries signaling information (call setup) to control calls on B channels.

    - PRI (Primary Rate Interface):

    o Consists of 23 B channels and one D channel with a bandwidth of 1.544Mbps.

    o PRI uses a DSU/CSU for a T1 connection. B stands for Bearer Channel.

17. TCP/IP port assignments used in the Internet: Originating source port numbers are dynamically assigned by source host, and usually greater than 1023. The following are the recommended port numbers:

- Numbers 0 - 255 are used for public applications

- Numbers 255 - 1023 are assigned to companies so that they can use these port numbers in their applications.

- Numbers above 1023 are used by upper layers to set up sessions with other hosts and by TCP to use as source and destination addresses.

18. Some of the important commands useful in trouble shooting TCP/IP networks:

I. Ipconfig: Displays TCP/IP configuration values, including IP address, subnet mask, and default gateway.

II. Ping: This command can be used to verify whether the target ip address or host name is present. You need to specify the target IP address or host name.

III. Route: Displays and manipulates route information.

IV. Tracert: Determines the route packets take to reach the specified destination.

19. HTTP is the protocol used for accessing the World Wide Web services. HTTP operates over TCP/IP. TCP/IP is the protocol, which is used by all internet applications such as WWW, FTP, Telnet etc. IPX/SPX is proprietary protocol stack of Novell NetWare.

20. TCP is a full-duplex, connection-oriented protocol. It incorporates error checking as well. UDP (User Data gram Protocol): UDP is a thin protocol. UDP is a connectionless protocol. It doesn't contact the destination before sending the packet and doesn't care whether the packet is reached at the destination. UDP uses port number 6.

21. The core administrative unit in DNS is called "zone". A zone is a physical file composed of resource records that define a group of domains. A domain is a node in the DNS namespace and all sub-domains below it.

22. Telnet is used for terminal emulation that runs programs remotely.
FTP is used to transfer files.

23. To see TCP/IP configuration on a Windows 95 / 98 computer in a graphical format, use WINIPCFG. It will display your IP address, subnet mask, default gateway, hardware MAC address and other details.

To see TCP/IP configuration in a non-graphical format or on an NT machine, use IPCONFIG. It will also display the IP configuration information on an NT machine. To get more details, use IPCONFIG/ALL.

24. A valid IP address on a host / node can't start with 127; 127.X.X.X is reserved for local loop back. A valid IP address can't be larger than 255 (in any octet), The maximum allowed value is 255 in any or combination of octets. For example, 150.206.256.31 is an invalid IP, since one octet exceeded the value 255. An example of valid IP is 202.122.154.11.

25. TCP/IP utilities:

- NBTSTAT: This utility displays current NetBIOS over TCP/IP connections, and display NetBIOS name cache.

- NETSTAT: Displays protocol statistics and current TCP/IP connections since the server was last booted.

- TRACERT: This command is used to determine which route a packet takes to reach its destination from source.

- IPCONFIG: Displays Windows IP configuration information.

- NSLOOKUP: This utility enables users to interact with a DNS server and display resource records.

- ROUTE: This command can be used to display and edit static routing tables.

26. PAP and CHAP:

- PAP uses 2-way handshaking. Passwords are sent in clear text across the link. Therefore, PAP is to be used only when it not possible to use CHAP.

- CHAP uses 3-way handshaking. CHAP uses Challenge/ Response method that provides protection against the password capture while authenticating the user. One should use CHAP whenever it is possible.

27. HOSTS file:

- HOSTS file is an ASCII file and can be edited using Notepad or any other text editor. The IP address and domain name ns.dname.com of a proper entry in a HOSTS file looks like: 196.54.202.16 ns.dname.com. Hash mark (#) is used before writing the comment in HOSTS file. The entire line after the # mark is treated as comment. You can enter any number of lines into a HOSTS file. But the number of characters that each line in a HOSTS file is limited to 255.

28. PPP&SLIP:

- PPP offers multi protocol support, error correction and compression.

- Multilink PPP allows multiple physical links be used to transfer information. The data passing through different physical connections form a single logical stream of data, thus increasing the effective bandwidth.

- PPP supports Password Authentication Protocol (PAP) and, Challenge Handshake Authentication Protocol (CHAP).

- SLIP is an older protocol and supports only TCP/IP. No error correction/ compression are offered by SLIP.

29. Some frequently occurring HTTP error messages:

1. Client side:

- 404-not found (specified file not found on server side)

- 401 - unauthorized

2. Server side:

- 500 - internal server error

- 502 - Server overloaded

- 503 - service unavailable

- 504 - gateway timeout

30. OSI 7 layers: The 7 layers of OSI model are:

1. The Application Layer: Application layer is responsible for identifying and establishing the availability of desired communications partner and verifying sufficient resources exist for communication. Some of the important application layer protocols are: WWW, SMTP, FTP, etc.

2. The Presentation Layer: This layer is responsible for presenting the data in standard formats. This layer is responsible for data compression, decompression, encryption, and decryption. Some Presentation Layer standards are: JPEG, MPEG, MIDI, PICT, Quick Time, TIFF.

3. The Session Layer: Session Layer is responsible for co-coordinating communication between systems/nodes. The following are some of the session layer protocols and interfaces: a) Network File System (NFS),SQL,RPC (Remote Procedure Call), X-Windows, ASP, DNA SCP.

4. The Transport Layer: The Transport Layer is responsible for multiplexing upper-layer applications, session establishment, and tearing-down of virtual circuits. This layer is also responsible for "flow control" to maintain data integrity.

5. The Network Layer: There can be several paths to send a packet from a given source to a destination. The primary responsibility of Network layer is to send packets from the source network to the destination network using pre-determined routing methods. Routers work at Network layer.

6. The Data Link Layer:

- Data Link Layer is layer 2 of OSI reference model. This layer is divided into two sub-layers:

A. Logical Link Control (LLC) sub-layer.

B. Media Access Control (MAC) sub-layer.

- The LLC sub-layer handles error control, flow control, framing, and MAC sub-layer addressing.

- The MAC sub-layer is the lower of the two sub-layers of the Data Link layer. MAC sub-layer handles access to shared media, such a Token passing or Ethernet.

7. Physical Layer: The actual flow of bits takes place through Physical layer. At Physical layer, the interface between the DTE and DCE is determined. The following are some of the standard interfaces are defined at Physical layer: A> EIA/TIA-232, EIA/TIA-449, V.24, V.35, X.21, G.703, HSSI (High Speed Serial Interface).

31. FTP utility is used for transferring files between server and client. It uses TCP/IP protocol and therefore connection oriented. The ftp is a reliable (since it is connection oriented) method of data transmission.

The syntax of ftp is as below:

ftp [-v] [-n] [-I] [-d] [-g] [-s:filename] [host name].

Where,

-v Suppresses any display of server responses (verbose)

-n Prevents automatic logon when the connection with the server has been established.

-I Turns off interactive prompting during file transfers

-d Displays all ftp commands exchanged between client and server. Useful during debugging.

-g Prevents the use of wildcard characters in path and file names.

-s: filename : Specifies a text file containing ftp commands and then runs the commands within the file. This is similar to running batch file in DOS.

Hostname Specifies the host to connect to and must be the last parameter to be specified.

FTP commands:

- To upload a single file using FTP, use the command "put",

- To download a single file using FTP, use the command "get",

- To upload multiple files using FTP, use the command "mput",

- To download multiple files using FTP, use the command "mget".

32. Search Engines:

- By placing the phrase in double quotes, the search engine returns all the pages that contain the phrase. For example, to return all pages with the phrase ‘space ship’ type in the same within double quotes “space ship”; On the other hand +space +ship return all pages that contain 'space' and 'ship' not necessarily together.

33. A computer on Internet having a unique IP address is known as HOST.

34. PPTP, L2TP, and L2F:

- PPTP: PPTP is Microsoft proprietary protocol and widely supported. PPTP supports wide range of protocols such as TCP, NetBEUI, IPX.

- L2F: It was developed by Cisco systems and is proprietary protocol. L2F uses UDP instead of TCP for forwarding the packets through the tunnel.

- L2TP: L2TP uses IPSec for encryption.

35. A DNS zone file contains the resource records for the part of the domain for which the zone is responsible. Some of the resource records are:

1. SOA (Start Of Authority Record): The first record in any zone file is the SOA record. The SOA file contains some general parameters such as contact e-mail of the person responsible for this zone file, the host on which zone file is maintained etc.

2. The NS Record (Name Server Record): NS Record contains the name servers for this domain. This will enable other name servers to look up names in your domain.

3. MX Record (Mail Exchange Record): MX record tells us which host processes mail for this domain.

4. Host Record (A Record): A host record is used to statically associate hosts names to IP addresses within a zone. The syntax for this is

5. <hostname> IN A <ip address of the host>

ex:

NameServer1 IN A 196.52.34.143

- Here 'NameServer1' is the host name and 196.52.34.143 is its ip address.

6. CNAME Record (Canonical name): These records allow you to use more than one name to point to a single Host. Using CNAME, you can host both WWW and FTP servers on the same machine.

7. Reverse Look up is useful when you want to implement security. Reverse look up ensures that the domain name is indeed the domain that it claims to be.

The correct format for Pointer record is

<ip reverse domain name> IN PTR <host name>

ex.: 16.12.54.204.in-addr.arpa. IN PTR services.yourcompany.com

Here the IP numbers are written in backward order and in-addr.arpa is appended to the end, creating a Pointer record.

36. ARP, RARP, and BootP:

- Since IP address is a logical address, if a packet is to be delivered to another machine, its physical address (MAC address) needs to be known. Address Resolution Protocol (ARP) is used to resolve or map a known IP address to a MAC sub-layer address to allow communication on a multi-layer access network such as the Internet.

- Reverse ARP (RARP) is used to obtain an IP address using an RARP broadcast. RARP is used to obtain IP address from a known MAC address.

BootP (Bootstrap Protocol): When a diskless workstation is powered on, it broadcasts a BootP request

on the network. A BootP server responds with its IP address, Default gateway, etc.

37. Proxy Server:

A Proxy server is primarily used in between the Web and the client machines that reside on a LAN / intranet. It serves multiple fuctions as required, including:

1. It receives the client requests for Web pages and forward the requests if necessary. If the pages are available in its cache (Don't confuse with L1/L2 cache of CPUs!), it immediately serves the pages to the clients. This improves response times and efficient bandwidth utilization.

2. A proxy server maps the IP addresses of the clients to one or more IP addresses for accessing the Internet. This way, a Proxy can be used to save precious IP addresses available on the Internet. At least, one valid IP address is required to access the Internet for multiple clients, that are connected to the Internet through Proxy.

3. A Proxy Server can also be used to secure the clients from possible security threats from the Internet by configuring appropriately. This improves the safety of the client machines malicious attacks.

38. Cookies:

- A cookie is a plain text file that sends out client information to the corresponding Web server, usually when the client makes a visit to the Web server. Disabling Cookies may result in improperly loaded Web pages.

39. A multi-homed computer will have atleast two IP addresses defined. These IP addresses can be defined to a single network card or there might be more than one network card with atleast one IP address defined to each. It is important to note that there can be more than one IP address defined to a single network card.

40. Only WINS update entries dynamically. All others require records to be entered manually. Remember that DNS and HOSTS resolve FQDN names to IP addresses, whereas, LMHOSTS and WINS resolve NetBIOS names to IP addresses.

41. Browsers:

- Configuring the browser not to show pictures enable the Web pages to load faster.

- A correctly formatted connection to access a Web site over a secure link will have "https://".

42. News Service:

- By installing Internet News service, you can enable all group members to exchange threaded messages.

- NNTP is a service. Users can connect to NNTP service using client software like Microsoft Internet Mail and News through TCP/IP.

43. The port number needs to be specified if you are accessing a website at a port other than the default port, the default port number for WWW traffic is port 80. By default, the Web page request is sent to port 80 unless otherwise specified. For example, if you want to access a web page at port number 5064, the correctly formatted URL is http://www.yoursite.com:5064/default.htm.

44. MIME specifies how non-ASCII (binary) messages such as graphics can be sent across the Internet.

45. Features supported by HTTP1.1:

1. Host headers enable a single IP address to be assigned to multiple web sites.
2. Persistent connections allow a single session between a client and server to transfer multiple objects, connected to a single resource.
3. Pipelining does not require clients to wait for a confirmation or completion of each request before sending another request.

Older browsers support only HTTP version 1.0, whereas most of the modern browsers support HTTP ver.1.1

46. Server Side Includes (SSI):

Server-side include (SSI) directives instruct the Web server to insert the contents of another file into an HTML page. This is a convenient way to store information used on many pages in a single file.

47. When you enable SSL communication on your Web site, you need to install a digitally certified key on your Web server.

48. At least first and second level domain names (in this case company.com) are to be registered with InterNIC for access over Internet. Third level and below can be resolved by installing DNS server.

49. FTP site can usually be configured with the following messages. Users (clients computers) get these messages when appropriate.

1. Welcome message: When a user enters an FTP site, this message is displayed.
2. Exit message: When a user exits an FTP site, this message is displayed.
3. Maximum connections: This is displayed when the maximum simultaneous connections limit is reached at the FTP server, and the user computer can not be connected because of this.

50. Certificate authority (CA) is any trusted third party that issues certificates and verifies the identity of a server or an individual for security purposes. A certificate is a digital signature containing the identity of a server or an individual.

51. Active Server Pages (ASP):

- ASP tags begin with "<%" and end with "%>". The tags are known as delimiters.

- ASP runs at the server side.

52. JScript, VBScript, and Java are some of the client side content tools that run on the client computers.

53. URL (Uniform Resource Locator):

A URL uniquely identifies the location of a computer, directory, or file on the Internet. The URL also specifies the appropriate port to be used (if different from default port value), Internet protocol, such as HTTP or FTP. The following is an example of a correctly formed URL: http://www.microsoft.com. When no file is specified in the URL, the default.htm or default.asp file, located in the home directory of the Web site is displayed by the client's browser.

54. File Extensions:

The extensions that are usually associated with some important file types are:

1. Active Server Pages -- .asp
2. Java source code -- .java
3. Java Script -- .js
4. Perl script -- .pl

55. CGI and ISAPI can only be used for server side scripting.

VBScript, JavaScript, ASP are used for client side scripting.

56. XML (Extensible Markup Language) is a reduced version of SGML.

57. A DLL is used in Microsoft operating systems. DLLs' are library routines that are called to perform some common tasks within Microsoft operating environment. DLLs can also be developed by third party vendors to enable integration of their programs into Microsoft environment. Multiple programs can call a DLL.

58. If you want to embed a Pert script into html page, the correct syntax for inserting PerlScript is

<SCRIPT LANGUAGE="PerlScript" SRC="mycode.js"> </SCRIPT>

Note that "/" is placed before the SCRIPT command as shown, to signify that it is the end of the script.

59. The correct syntax for inserting Java Script into html page is

<SCRIPT LANGUAGE="JavaScript" SRC="mycode.js"> </SCRIPT>

Note that "/" is placed before the SCRIPT command as shown, to signify that it is the end of the script.

60. ODBC is Microsoft's implementation for accessing Microsoft SQL Server / Access databases from a Web Server, and delivering the results over the Web in html format to client computers.

61. The correct sequence of tags in an html page is:

<html>

<head>

<title>

</title>

</head>

<body>

</body>

</html>

Please note that the tag "title" comes between "head" tags. "title" describes the title of the page and usually appears in the Title window of the browser.

62. Correct syntax to insert a comment into html page is:

The correct syntax is <!-- your message -->

An example is

<!-- BEGIN FASTCOUNTER LINK -->

Here 'BEGIN FASTCOUNTER LINK' is the comment that you have inserted into html code.

63. HTML:

- If you write <IMG SRC="myimage.gif">, the web server assumes that the image is in the same folder as that of the web page. If the image is in different folder, you need to specify the folder in the IMG directive ex: <IMG SRC="images/myimage.gif">.

- Correct syntax to insert a hyperlink to www.yahoo.com, when user clicks on "YAHOO" is <A HREF="http://www.yahoo.com">YAHOO</A>

- To include special characters, such as '<', '>' etc. we can use specified character entities.

This is required because, these characters have special meaning within html and therefore need to be specified otherwise.

Given below are some character entities used in HTML:

Less than (<): <

Greater than (>): >

Copyright: ©

Registered trademark: ®

- The attribute "ALT" provides an alternative description of an image. This is useful, for example if a

client has selected "Text Only" version and prevented any images to be down loaded for faster access to a web page. Also, it may so happen that a browser does not support the image format and can not display the image.

Common sytax for displaying alternate text is:

<IMG SRC="mypicture.gif" ALT="MY Picture">

64. Some of the image / video / audio file formats available are:

1. GIF (extension .gif): GIF is one of the most widely used formats for images on the World Wide Web. GIF images are very compact and have only 256 colours or 8 bit.

2. JPEG (Joint Photographic Expert Group, extension .jpg): JPEG is a 24 bit, 16-million colour graphic file format widely used on the Web. JPEG uses compression to reduce the file size and recommended for continuous tone images.

3. PNG (Portable network Graphics, extension .png): This is a new format, not yet widespread. Specifically designed for the Web.

4. MOV(Quick Time Movie, extension .mov): Quick Time Plug-in is required to play .mov files on the Internet.

5. MPEG (Extension .mpg): MPEG can provide full motion, full screen video with special software /or hardware.

6. PDF (Extension .pdf): This format is developed by Adobe Acrobat. It is used to display documents that are created using Adobe Acrobat. .pdf format is most widely used over the Internet to distribute the documents.

65. Web Graphics:

-VRML allows the display of 3D pictures with Web browsers.

- All .bmp,.gif, and .jpeg use raster graphics, where as Flash uses vector graphics. Vector graphics take less file space compared to raster graphics.

- VRML files use the extension .wrl.

66. A text editor such as Note pad can be used for writing HTML pages. But you need to enter all the code yourself (including html tags). On the other hand, if you are using a GUI editor to write HTML pages, inherent tags are inserted by the editor itself, such that you don't have to worry about the syntax. This will save time more efficient.

67. A Web page written in HTML can usually support the following lists:

1. Unordered lists:Unordered lists are bulleted and used when it is not required to number the lists.

2. Ordered lists: In an ordered list, the number precedes each list item.

3. Definition lists: A definition list typically lists each definition term followed by an indented description.

The correct syntax for writing Ordered lists is:

<OL>

<L1>Bulleted item 1

<L2>Bulleted item 2

</OL>

Note that there is no /L1 or /L2 tag.

The correct syntax for writing Unordered lists is:

<UL>

<L1>Bulleted item 1

<L2>Bulleted item 2

</UL>

Note that there is no /L1 or /L2 tag.

The correct syntax for writing Definition Lists is:

<DL>

<DT> Definition Term 1

<DD> Definition Description 1

<DT> Definition Term 2

<DD> Definition Description 2

</DL>

Remember that CompTIA expects you to be familiar with HTML tags and writing Web pages with pure HTML.

68. Flash: Flash is from Macromedia. Flash is based on vector graphics, and used for developing dazzling Web sites. You can also incorporate animation with Flash. Flash plug-in is required to display Flash content.

Shockwave: Shockwave is also from Macromedia. Shockwave is used for displaying interactive Web sites involving video, graphics, and Audio. Shockwave plug-in is required to display web pages with Shockwave content.

69. The correct syntax of html code to start an email client on client browser is

<A HREF="mailto:support@yahoo.com"> Email Yahoo Support </A>

This command will open the clients email program and puts "support@yahoo.com" in the "TO" address field. support@yahoo.com is taken only as an example.

70. A trademark is an original and unique name or symbol that is provided legal protection indefinitely.

71. A copyright applies to orignal works of "authorship". It is protected for the life of the author and an additional 50 years.

72. There are some occasions, where it will not constitute violation of copyright law:

1. Parody
2. Use by free educational institutions, where in portions of the material is used for non-profit
3. Limited use, wherein, the material is used only to quote some portions.
4. Archiving purposes.

73. The following are valid representations of copyright display:

© 2001 Sky Publications

Copyright 2001 Sky Publications

74. SSL, Secure Socket Layer, works by using a private key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, Web pages that require an SSL connection start with https: instead of http:.

Another protocol for transmitting data securely over the World Wide Web is Secure HTTP (S-HTTP). Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely, S-HTTP is designed to transmit individual messages securely. SSL and S-HTTP, therefore, can be seen as complementary rather than competing technologies. Both protocols have been approved by the Internet Engineering Task Force (IETF) as a standard.

75. Techniques for indexing a site:

- Keyword index uses only keywords as specified by the user for indexing.

- Stemming: Stemming is a technique that searches for the base of a work. For example, if you search for "tutoring", a word containing "tutor" may result.

76. When using "PUSH" technology, the server pushes the information to the browser, even if the browser doesn't request that information. This is different from PULL technology, wherein browser requests the information or pulls the information from the server.

77. X.509 is the most widely used standard for defining digital certificates.

78. S/MIME, Short for Secure/MIME, a new version of the MIME protocol that supports encryption of messages. S/MIME is based on RSA's public-key encryption technology.