V Skills

Skills for a secure future

Certified Cyber Law Analyst
Sample Material

V-Skills Certifications

A Government of India
&
Government of NCT Delhi Initiative

V-Skills

Skills for a secure future

1. CYBER TECHNOLOGY

1.1. Networking

A network is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information. Networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software. A host device on a network can be computers, servers, laptops, Personal Digital Assistants (PDAs), or anything a person uses to access the network. Network devices are hubs, repeaters, bridges, switches, router and firewall.

Network Models (Peer-to-Peer and Client-and-Server)

The term computer network model defines the category in which a computer network can be grouped into. Networks are divided into peer to peer and client-server.

Peer To Peer Networks

When nodes or workstations perform the same communication functions, they are referred to as peers, in this network model, both server and client operations are performed by the same computer. Each user administers his/her workstation and the resources in it. There are no dedicated servers and no hierarchy among the computers. All the computers are equal and therefore are known as peers. Each computer functions as both a client and a server, and there is no administrator responsible for the entire network. The user on each computer determines which data on that computer is shared on the network.

Security is also managed by the user of the devices. This model is not quite secure and is suited for a small computer networks (with 10 computers or less) where users do not want to share files. User’s files are decentralized – they are not stored in a single location.

Client Server Networks

This network model offers centralized access to services and devices. One computer plays the role of a server. It is the most common type of network architecture today that provides centralized data storage, security, manning of applications and network administration. Most servers have operating system like Windows NT/2003 or later, Linux, Novel Netware etc.

Network Types (LAN,WAN,MAN,PAN)

Different types of networks are distinguished based on their size (the number of nodes), their data transfer speed, and their reach. Private networks are networks that belong to a single organization. There are usually of three categories

- ✓ LAN (local area network)
- ✓ MAN (metropolitan area network)
- ✓ WAN (wide area network)

There are two other types of networks as PANs (Personal Area Network), which are limited few feets, and CANs (Campus Area Networks), which are the same as MANs (with bandwidth limited between each of the network's LANs).

LAN

It's a group of computers which all belong to the same organization, and which are linked within a small geographic area using a network, and often the same technology (usually Ethernet). Data transfer speeds over a local area network can be up to 10 Mbps, 1 Gbps and 10 Gbps. LAN can reach to 100 or even 1000 users. LAN can be sub-divided as per the services that it provides and operating modes into, a "peer-to-peer" network (having no central computer and each computer has the same role) and a "client/server" network (with a central computer for services to users).

MAN

MANs (Metropolitan Area Networks) connect multiple geographically nearby LANs to one another (over an area of few kilometres) at high speeds. Thus, a MAN lets two remote nodes communicate as if they were part of the same local area network. A MAN is made from switches or routers connected to one another with high-speed links (usually fiber optic cables or microwave).

WAN

A WAN (Wide Area Network or extended network) connects multiple LANs to one another over vast geographic distances. The speed available on a WAN varies depending on the cost of the connections (which increases with distance) and may be low. WANs operate using routers, which can "choose" the most appropriate path for data to take to reach a network node. The most well-known WAN is the Internet.

Internet connection (DSL, Cable, Serial Link)

The need for speed has changed the options available to consumers and businesses. The connection speeds will change over time and also between Internet Service Providers (ISP). Various internet connection technologies have different characteristics and are discussed.

Dial-up Internet Access

It is called as dial-up access and is economical but slow. Users connect by a modem linked to PC by dialing a phone number (from ISP) but tying up phone line. It is an analog connection as data is sent over an analog, public-switched telephone network. The modem converts received analog data to digital and vice versa. Due to telephone lines usage, the quality of the connection is not always good and data rates are limited. The connection speeds range from 2400 bps to 56 Kbps.

ISDN - Integrated Services Digital Network

It is an international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires and speeds are from 64 Kbps to 128 Kbps.

B-ISDN - Broadband ISDN - Broadband ISDN is similar in function to ISDN but it transfers data over fiber optic telephone lines, not normal telephone wires. SONET is the physical transport backbone of B-ISDN. Broadband ISDN has not been widely implemented.

DSL – Digital Subscriber Line

DSL uses existing telephone line and gives internet simultaneously with telephone service without tying up phone line. Two main categories of DSL for home are called ADSL and SDSL. All types of DSL technologies are collectively called xDSL with speeds from 128 Kbps to 9 Mbps.

ADSL - Asymmetric Digital Subscriber Line - ADSL is the most commonly deployed types of DSL in North America. It supports data rates of from 1.5 to 9 Mbps when receiving data or downstream rate and from 16 to 640 Kbps when sending data or the upstream rate.

ADSL+2 - ADSL Extension - An extension to ADSL broadband technology with faster download speeds though similar as ADSL. Both use a special filter on a telephone line to split existing telephone lines (POTS) between regular telephone (voice) and ADSL+2.

Cable - Broadband Internet Connection

It uses a cable modem for Internet connection over cable TV lines. It works by using TV channel space for data transmission, with certain channels used for downstream transmission, and other channels for upstream transmission. As, the coaxial cable is used so, greater bandwidth is present. Cable speeds range from 512 Kbps to 20 Mbps.

Wireless Internet Connections

Wireless Internet, or wireless broadband is the newest Internet connection types. It uses radio frequency bands for transmission. It provides an always-on connection which can be accessed from anywhere but within a network coverage area hence, it is not present in some areas. It is usually more expensive and mainly available in metropolitan areas by cellular operators using 2Gor 3G.

T-1 Lines – Leased Line

T-1 lines are a leased line option connecting to the Internet backbone with a dedicated phone connection supporting data rates of 1.544Mbps. A T-1 line consists of 24 individual channels, each supporting 64Kbits per second and can be configured to carry voice or data traffic. One or some of individual channels can be taken, and called as fractional T-1access.

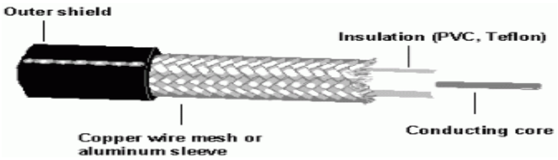
T-3 Lines – Dedicated Leased Line - T-3 lines are similar to T-1 with data rates of about 43 to 45 Mbps. It consists of 672 individual channels, each of which supports 64 Kbps.

Network Media

Network media is the actual path over which data travels as it moves from one component to another. The network transmission medium carry signals between computers. There is a variety of media that meet the varying needs and sizes of networks and the common types are coaxial, twisted-pair, unshielded twisted-pair, shielded twisted-pair, fiber-optic and wireless

Coaxial Cable

It has a hollow outer cylindrical conductor that surrounds a single inner wire made of two conducting elements usually copper and surrounding it, is a layer of flexible insulation. Over this insulating material is a woven copper braid or metallic foil that acts both as the second wire in the circuit and as a shield for the inner conductor. This second layer, or shield, can help reduce the amount of outside interference. Covering this shield is the cable jacket.



Coaxial Cable

Thicknet
Thinnet

Thicknet and Thinnet

It supports 10 to 100 Mbps and is more costly than UTP but, can be cheaper for a physical bus topology as less cable will be needed. Coaxial cable can be cabled over longer distances than twisted-pair cable usually 500m compared to 100m for UTP. The largest diameter (1 cm) coaxial cable is referred as Thicknet but, it is too rigid to install easily due to its thickness. A connection device called vampire tap connect network devices to Thicknet by attachment unit interface (AUI). Similarly, coaxial cable with an outside diameter of only 0.35 cm is referred as Thinnet and used with networks with many twists and turns. Thinnet uses BNC (British Naval Connector or Bayonet Neill Concelman) connectors which are a male type mounted at each end of a cable.

Twisted-Pair Cable

Twisted-pair cable is a type of cabling that is used for telephone communications and Ethernet networks. A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against crosstalk, the noise generated by adjacent pairs. Using cancellation with twisting the wires, self-shielding for wire pairs within the network media is provided. Two basic types of twisted-pair cable exist of unshielded twisted pair (UTP) and shielded twisted pair (STP).

Unshielded Twisted-Pair (UTP) Cable

It relies on cancellation effect by the twisted wire pairs to limit signal degradation due to electromagnetic interference (EMI) and radio frequency interference (RFI). The number of twists in the wire pairs varies to reduce crosstalk between the pairs. UTP cable has four pairs of either 22- or 24-gauge copper wire. UTP external diameter is 0.43 cm and is easy to install and less expensive than other types of media. It is installed by a Registered Jack 45 (RJ-45) connector. UTP cable is more prone to electrical noise and interference also, the distance between signal boosts is shorter for UTP than others. Commonly used types of UTP cabling are as follows

- ✓ Category 1—Used for telephone communications. Not suitable for transmitting data.
- ✓ Category 2—Capable of transmitting data at speeds up to 4 megabits per second (Mbps).
- ✓ Category 3—Used in 10BASE-T networks. Can transmit data at speeds up to 10 Mbps.
- ✓ Category 4—Used in Token Ring networks. Can transmit data at speeds up to 16 Mbps.
- ✓ Category 5—Can transmit data at speeds up to 100 Mbps.
- ✓ Category 5e —Used in networks running at speeds up to 1000 Mbps.
- ✓ Category 6—It has four pairs of copper wires and is the fastest standard for UTP.

Shielded Twisted-Pair (STP) Cable

Each of four pair of STP wires is wrapped in a metallic foil and then are wrapped in an overall metallic foil thus, reducing electrical noise within the cable (pair-to-pair coupling, or crosstalk) and from outside the cable (EMI and RFI). It is installed with STP data connector but, is more expensive and difficult to install. It's speed and throughput are from 10 to 100 Mbps with maximum cable length to 100 m.

Fiber Optic Cable

It is a flexible, transparent fiber made of glass (silica) or plastic, thicker than a human hair. It functions as a waveguide to transmit light between the two ends of the fiber. It enables transmission over longer distances and at higher data rates. Optical fibers have a transparent core surrounded by a transparent cladding material with a lower index of refraction. Light is kept in the core by total internal reflection. This causes the fiber to act as a waveguide. Fibers supporting many propagation paths are multi-mode fibers (MMF) and a single mode are called single-mode fibers (SMF). MMF has a wider core diameter, and is used for short-distance but SMF are used for links longer than 1 km. Each fiber can carry many independent channels, each using a different wavelength of light. Speed varies from 5Mbps to 50Gbps and newer are in Tbs.

Wireless

It avoids using cables by using radio communication. It is used by two-way radios, GPS units, cellular telephones, personal digital assistants (PDAs), wireless networking, wireless computer mice or keyboards or headsets, satellite television and cordless telephones. IEEE 802.x (Wi-fi) standards are used for wireless computer network and are of different speeds and coverage area as 802.11 a/b/g/n.

Layered Network Model

The layered network model defines a networking framework for implementing protocols in different layers. Control is passed from one layer to the next, starting at the top most layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

The International Standards Organization (ISO) defined a seven-layer model to standardize networking processes. The benefits to layering networking protocol specifications are many including

- ✓ Interoperability - Greater interoperability between devices from different manufacturers and between different generations of same type of device from the same manufacturer.
- ✓ Compatibility - Compatibility between devices, systems and networks that this delivers.
- ✓ Better Flexibility - Improved flexibility in options and choices for configuration and installation.
- ✓ Increased Life Expectancy - Devices from different technology generations can co-exist thus the older units do not get discarded immediately newer technologies are adopted.
- ✓ Scalability - Experience shows that a layered design scales better than the horizontal approach.
- ✓ Value Added Features - It is easier to add and implement value added features into products or services when the entire system has been built on the use of a layered philosophy.
- ✓ Modularity Plug-ins and add-ons are easily added from use of a layered approach.
- ✓ Standardization and Certification –The layered design specifications facilitate streamlined and simple standardization and certification process due to the clearer and more distinct definition.
- ✓ Portability - Layered networking protocols are much easier to port from one system to another.
- ✓ Compartmentalization of Functionality – It gives freedom to concentrate on a specific layer or specific functions without the need for concern or modification of any other layer.

TCP/IP Protocol Architecture

TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. The TCP/IP model and related protocols are maintained by the (IETF) or Internet Engineering Task Force. The Internet protocol suite and the layered protocol stack design were in use before the OSI model was established. It has four abstraction layers, each with its own protocols. It has four abstraction layers, each with its own protocols. From highest to lowest, the layers are

- ✓ **Application layer (process-to-process)**- It contains all protocols (like HTTP) for specific data communications services on a process-to-process level (for example how a web browser communicates with a web server). This is the scope within which applications create user data and communicate this data to other processes or applications on another or the same host. The communications partners are often called peers. This is where the "higher level" protocols such as SMTP, FTP, SSH, HTTP, etc. operate.

- ✓ **Transport layer (host-to-host)-** It handles host-to-host communication. The transport layer constitutes the networking regime between two network hosts, either on the local network or on remote networks separated by routers. The transport layer provides a uniform networking interface that hides the actual topology (layout) of the underlying network connections. This is where flow-control, error-correction, and connection protocols exist, such as TCP. This layer deals with opening and maintaining connections between Internet hosts.
- ✓ **Internet layer (internetworking)-** It connects local networks, thus establishing internetworking. The internet layer has the task of exchanging datagrams across network boundaries. It is therefore also referred to as the layer that establishes internetworking, indeed, it defines and establishes the Internet. This layer defines the addressing and routing structures used for the TCP/IP protocol suite. The primary protocol in this scope is the Internet Protocol, which defines IP addresses. Its function in routing is to transport datagrams to the next IP router that has the connectivity to a network closer to the final data destination.
- ✓ **Link layer-** The link layer (commonly Ethernet) contains communication technologies for a local network. This layer defines the networking methods within the scope of the local network link on which hosts communicate without intervening routers. This layer describes the protocols used to describe the local network topology and the interfaces needed to affect transmission of Internet layer datagrams to next-neighbor hosts.

Application Layer

It contains all protocols and methods of process-to-process communications across an Internet Protocol (IP) network. Its methods use the underlying transport layer protocols to establish host-to-host connections. Both TCP/IP and the OSI model specify a group of protocols and methods identified by the name application layer. The following protocols are described in the application layer of the Internet protocol suite.

- ✓ Remote login - Telnet
- ✓ File transfer - FTP, TFTP
- ✓ Electronic mail - SMTP,IMAP, POP
- ✓ Support services - DNS, RARP, BOOTP, SNMP

Transport Layer

The transport layer or layer 4 provides end-to-end communication services for applications by providing services like connection-oriented data stream support, reliability, flow control, and multiplexing. It is contained in the TCP/IP as TCP and in the OSI model as transport layer.

The Transmission Control Protocol (TCP) is used for connection-oriented transmissions, whereas the connectionless User Datagram Protocol (UDP) is used for simpler messaging transmissions. TCP has stateful design for reliable transmission and data stream services. Various services provided by a transport-layer protocol include

- ✓ Connection-oriented communication- Interpreting the connection as a data stream provides benefits to applications.
- ✓ Byte orientation- It is easier to process data stream as a sequence of bytes helping various underlying message formats.

- ✓ Same order delivery- The network layer doesn't guarantee data packet arrival in the same order that they were sent, hence segment numbering is used, with the receiver passing them to the application in order.
- ✓ Reliability- Packets may be lost due to network congestion hence, an error detection code like checksum checks data corruption, and verify correct receipt by sending an ACK or NACK message to sender. Automatic repeat request retransmits lost or corrupted data.
- ✓ Flow control- The rate of data transmission between two nodes is managed to prevent a fast sender for more data. It also improves efficiency by reducing buffer under run.
- ✓ Congestion avoidance- It controls traffic entry into a network by avoiding oversubscription of link capabilities of intermediate nodes and networks by reducing rate of sending packets.
- ✓ Multiplexing- Ports provide multiple endpoints on a single PC like the name on a postal address is a multiplexing, and differs between different recipients at same location. Computer applications each listen for information on their own ports, which enables the use of more than one network service at the same time.

Internet Layer or IP Layer

It is a group of internetworking methods, protocols, and specifications used to transport datagrams (packets) from the originating host across network, to destination host specified by a network address (IP address). It facilitates internetworking or connecting multiple networks by gateways.

Internet-layer protocols use IP-based packets and have three functions, for outgoing packets, select the next-hop host (gateway) and transmit the packet to this host by passing it to the appropriate link layer implementation; for incoming packets, capture packets and pass the packet payload up to the appropriate transport-layer protocol, if appropriate. In addition it provides error detection and diagnostic capability. The Version 4 of the IP (IPv4), IP is capable of automatic fragmentation or de-fragmentation of packets, based on the maximum transmission unit (MTU) of link elements.

It is not responsible for reliable transmission and offers "best effort" delivery hence, no proper arrival making network resilient and assigning reliability provision to higher level protocols. In IPv4 (not IPv6), a checksum is used to protect the header of each datagram.

Network Access Layer

It is the lowest layer which provides the means for the system to deliver data to the other devices on a directly attached network. It defines how to use the network to transmit data and thus, must know the details of the underlying network to correctly format the data being transmitted to comply with the network constraints. The TCP/IP Network Access Layer has the functions of all three lower layers of OSI (Network, Data Link, and Physical).

Functions performed at this level include encapsulation of IP datagrams into the frames transmitted by the network, and mapping of IP addresses to the physical addresses used by the network. One of TCP/IP's strengths is its universal addressing scheme. The IP address must be converted into an address appropriate for physical network over which the datagram is transmitted.

Devices at different layers

Devices at different layers of TCP/P network model are

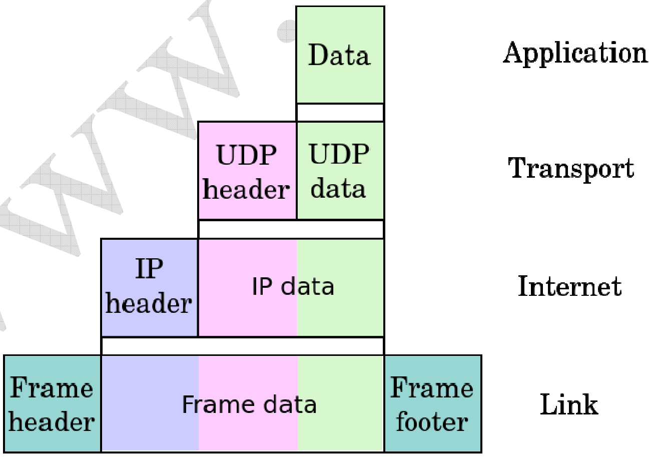
- ✓ Layer 1- It is the physical layer. Media converters operate at Layer 1 to convert electrical signals and physical media without doing anything to data coming through the link. Media converters have two ports—one in, one out— to convert the incoming electrical signal from one cable type and then transmit it over another type.

- ✓ Layer 2- It is the data-link layer. Switch and media converter operate at Layer 2 to sort packets using physical network addresses or MAC addresses. All network hardware is permanently assigned this number during its manufacture. Both switches and media converters can be Layer 2 devices. A switch has more ports than a media converter. Devices are fast, but aren't smart as they don't look at data packets closely.
- ✓ Layer 3- It is the Network Layer and layer 3 switches use network or IP addresses to identify locations on the network. Layer 3 switches are smarter due to routing functions to find the best way to send a packet to its destination.
- ✓ Network Router - A router routes data packets between two networks by reading the destination information in each packet so, for an immediate network it has access to, it will strip the outer packet, readdress the packet to the proper Ethernet address, and transmit it but, for another network destination it is sent to another router, re-package outer packet to receive by next router and send it to next router.

Data Encapsulation

It is a method for communication protocols to logically separate functions in the network and abstracts it from their underlying structures by inclusion or information hiding within higher level objects. Link encapsulation by the physical layer allows local area networking by higher layers and IP provides global addressing of individual computers; UDP adds application or process selection, i.e., the port specifies the service such as a Web or TFTP server.

The more abstract layer is called the upper layer protocol while the more specific layer is called the lower layer protocol. Encapsulation is a characteristic feature of most networking models, including the OSI Model and TCP/IP suite of protocols. An image of encapsulation of application data descending through the layers



Internet Protocol

The OSI physical layer and data link layer do not define how to deliver data between devices interconnected with multiple devices. The OSI network layer provides the end-to-end delivery of data between endpoints with any type of physical network in between. The network layer specifies data routing. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering datagrams from the source host to the destination host solely based on the addresses. For this purpose, IP defines datagram structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram source and destination. OSI network layer has following functions which include

- ✓ **Logical addressing -** Sending the data packet from one network to another network requires logical addressing. It helps to distinguish source and destination systems. Network layer adds header to data coming from upper layers and include logical address of sender and receiver. Every host in the network must have a unique address that determines where it is. This address is normally assigned from a hierarchical system.
- ✓ **Routing -** As networks are divided into subnetworks and connect to other networks for wide-area communications, networks use gateways or routers to route packets to their final destination. It is also called as the process of forwarding packets (Layer 3 PDUs)
- ✓ **Routing protocol -** A protocol used by routers to learn dynamically about addresses in a network, for decision making during routing or forwarding process.

IP Routing

Data packet is routed from source to destination by passing through one or more routers and networks. The IP Routing protocols enable routers to build up a forwarding table to relate an final destination address with next hop addresses. Various protocols used in routing are BGP (Border Gateway Protocol), IS-IS (Intermediate System - Intermediate System), OSPF (Open Shortest Path First) and RIP (Routing Information Protocol).

IP routing is done on a hop-by-hop basis. IP does not know the complete route to any destination (except directly connected). IP routing provides the IP address of the next-hop router to which the data is sent and the next-hop router is assumed to be closer to destination. IP routing performs the following actions

- ✓ Search the routing table for an entry that matches the complete destination IP address (matching network ID and host ID). If found, send the packet to the indicated next-hop router or to the directly connected interface.
- ✓ Search the routing table for an entry that matches just the destination network ID. If found, send the packet to the indicated next-hop router or to the directly connected interface. All the hosts on the destination network can be handled with this single routing table entry.
- ✓ Search the routing table for an entry labeled "default." If found, send the packet to the indicated next-hop router.

If none of the steps works, the datagram is undeliverable. If the undeliverable datagram was generated on this host, a "host unreachable" or "network unreachable" error is normally returned to the application that generated the datagram. Each entry in routing table has

- ✓ Specification of which network interface the datagram should be passed to for transmission.
- ✓ Destination IP address. It is either a host address or network address, as specified by the flag field. A host address with a nonzero host ID identifies one particular host, while a network address has a host ID of 0 and identifies all the hosts on that network.
- ✓ IP address of a next-hop router or directly connected network. The next-hop router is not the final destination, but it forwards data to the final destination.

- ✓ Flags. One flag specifies whether the destination IP address is the address of a network or the address of a host. Another flag says whether the next-hop router field is really a next-hop router or a directly connected interface.

IP routing protocols load routing tables with valid, loop-free routes and involves functions as

- ✓ Placing the best route, if more than one route to a subnet is available.
- ✓ Removing invalid routes from the routing table.
- ✓ Dynamically learn and load routing table for a route to all subnets in the network.
- ✓ Replace lost routes, quickly with best available route, also called convergence time.
- ✓ Preventing routing loops.

Every routing protocols publicizes it's routes as

- ✓ Add a route for each subnet directly connected to it.
- ✓ Update neighbor router about all directly connected and learned routes.
- ✓ Add new routes from neighbors

IP Addressing

An IP address is a 32 bit binary number, looks like the following

00000100 10000000 00000011 00000001

It is divided into four 8-bit chunks, called octet, and represented into decimal number for humans to understand like 4.128.3.1 An IP address consists of two parts

- ✓ The leftmost bits specify the network address component, called network ID.
- ✓ The rightmost bits specify the host address components, called host ID.

Hosts on a network can communicate with devices in the same network by MAC address but for different networks, a router to move data is needed. Each LAN has a unique network ID and all hosts on that network have same network ID but different host ID. A network ID enables a router to put a packet onto the correct network segment. To decide which network is correct, the router looks up a routing table, which is a table contains entries for network addresses (network ID + all host bits set to 0). Each network interface uses a unique IP address.

IP addresses are broken into classes to accommodate different sizes of networks as

- ✓ Class A (1-126)- It supports extremely large networks and uses only first octet for the network address and rest three octets for host addresses. The first bit of a Class A address is always 0 but, the lowest number represented is 00000000 (decimal 0), and highest number is 01111111 (decimal 127) both are reserved and cannot be used as a network address. Any address start with 127 is reserved for loopback.
- ✓ Class B (128-191)- It supports middle-sized and large-sized networks with first two octets for network address and rest two octets for host addresses. The first two bits of a Class B address is binary number 10; thus, the lowest number represented is 10000000 (decimal 128) and highest number is 1011111 (decimal 191).
- ✓ Class C (192-223)- It supports small-sized networks with first three octets for network address and remaining one octet for host addresses. The first three bits of a Class C address is binary number 110 thus, lowest number represented is 11000000 (decimal 192), and the highest number is 11011111 (decimal 223).

- ✓ Class D- 224-239 is reserved for multicasting, for a single station to simultaneously transmit a datagrams to multiple recipients. It's first four bits is binary number 1110.
- ✓ Class E- 240-255 is experimental addresses, reserved by the IETF for its research.

The block at the beginning and end of each class is called network address and broadcast address, respectively. These two special IP addresses are reserved and detailed as

- ✓ Network address- It has all host bits set to 0 to identify the network itself and cannot be assigned like 46.0.0.0 is the network address of the network containing the host 46.4.64.21.
- ✓ Broadcast address- It has all host bits set to 1 and used to send data to all the devices on a network like 46.255.255.255 is the broadcast address of network with host 46.4.64.21. Routers will forward broadcast packets on all interfaces but usually routers disable broadcast-forwarding.

The list of the Class A, B, C, D, E IP address is summarized as

Class	Leading bits	Start	End	Network Bits	Host Bits
A		0.0.0.0	127.255.255.255	8	24
B	10	128.0.0.0	191.255.255.255	16	16
C	110	192.0.0.0	223.255.255.255	24	8
D	1110	224.0.0.0	239.255.255.255		

The Internet Corporation for Assigned Network Numbers (ICANN, www.icann.org) is in charge for universal IP address assignment and ICANN, assigns regional authority to other cooperating organizations.

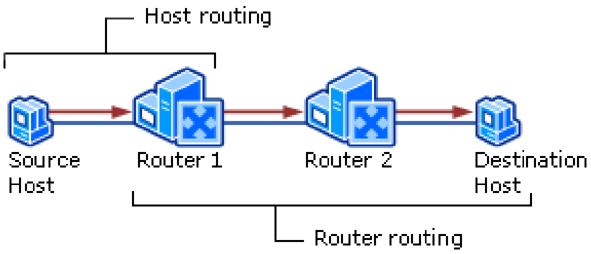
Host & Router Routing

Host Routing - Hosts actually use some simple routing logic when choosing where to send a packet. This two-step logic is as follows

- ✓ If destination IP address is in same subnet, send the packet directly to that destination host.
- ✓ If destination IP address is not in same subnet, send the packet to default gateway.

Router Routing - When a router gets a packet that is not destined for it, the router deliver it to either the destination host or to another router, as per the logic

- ✓ If destination network matches a router attached network, router forwards packet to destination by destination host's physical address.
- ✓ If destination network is not directly attached, the router forwards packet to an intermediate router's physical address chosen as per optimal route in the routing table.



DNS

It is an Internet service to translate domain names into IP addresses as, domain names are alphabetic, they're easy to remember but internet is based on IP addresses. A DNS service translates the name into the corresponding IP address like, the domain name www.example.com might translate to 198.105.232.4. The DNS system is an network as, if one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

A DNS lookup can be bypassed by giving IP address instead of domain name. DNS works in an complex and hierarchical manner. After connecting the PC or network node to Internet service provider (ISP) or WiFi network, the modem or router assigns a network address to node and sends network configuration about one or more DNS servers to use.

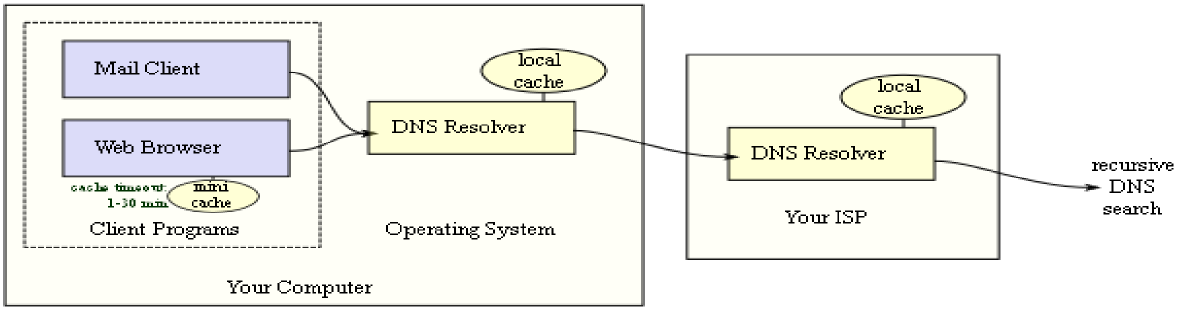
DNS identifies by domain names that are organized as a tree or in hierarchical manner according to organizational or administrative boundaries. Each node of the tree, called a domain, is given a label. The domain name of the node is the concatenation of all the labels on the path from the node to the root node like network.support.vskills.in

- ✓ support.vskills.in is the domain name.
- ✓ . is the root domain
- ✓ in is the top level domain
- ✓ vskills is the second-level domain
- ✓ support is a subdomain of microsoft
- ✓ network is the hostname

For administrative purpose, domain name space is divided into DNS zones, each starting at a node and extending down to the leaf node or to nodes where other zones start. A DNS zone is a portion of the global DNS name space for which administrative responsibility has been delegated. The data for each zone is stored in a name server, which answers queries about the zone using the DNS protocol. A zone and a domain are different as a zone consists of discrete or contiguous portion of the domain tree, which can map exactly to a single domain or include only part of a domain. On the other hand, every node in the DNS tree is a domain, even if it has no subdomains. Any computer registered to join the Domain Name System can act as a DNS server. A DNS server contains a database of network names and address for other Internet hosts. DNS servers are organized in a hierarchy structure. At its top level, the root zone or root domain "." is administered by a set of 13 root nameserver clusters distributed throughout the world. DNS protocol use both TCP and UDP ports – port 53/tcp and port 53/udp.

The Name Resolution process is done as

- ✓ Upon receiving query from client, the local nameserver will check if it has the authority for the required domain name. If it has, the local nameserver returns the IP address sought. Otherwise, go to step 2.
- ✓ Query one of the root nameservers to find the server authoritative for the next level down.
- ✓ Querying this second nameserver for the address of a DNS server with detailed knowledge of the second-level domain.
- ✓ Repeating the previous step to progress down the name, until the final step which would, rather than generating the address of the next DNS server, return the final address sought.



DHCP

Dynamic Host Configuration Protocol (DHCP) is a network protocol to automatically assign an IP address and other network configuration to a computer from a defined range of numbers (i.e., a scope) configured for a given network. DHCP assigns an IP address when a system is started as

- ✓ A user turns on a computer with a DHCP client.
- ✓ The client computer sends a broadcast request (called a DISCOVER or DHCPDISCOVER), looking for a DHCP server to answer.
- ✓ The router directs the DISCOVER packet to the correct DHCP server.
- ✓ The server receives the DISCOVER packet. Based on availability and usage policies set on the server, the server determines an appropriate address (if any) to give to the client. The server then temporarily reserves that address for the client and sends back to the client an OFFER (or DHCPOFFER) packet, with that address information. The server also configures the client's DNS servers, WINS servers, NTP servers, and sometimes other services as well.
- ✓ The client sends a REQUEST (or DHCPREQUEST) packet, letting the server know that it intends to use the address.
- ✓ The server sends an ACK (or DHCPACK) packet, confirming that the client has a been given a lease on the address for a server-specified period of time.

A computer is manually configured to use specified IP address but it can result in error or inattention to detail resulting in IP address conflict hence, DHCP is used. DHCP server uses three methods for allocating IP-addresses as

- ✓ Dynamic allocation- A range of IP addresses is assigned to DHCP server and each client requests an IP address from DHCP server for a lease with a controllable time period, allowing the DHCP server to reclaim (and then reallocate) IP addresses that are not renewed.
- ✓ Automatic allocation- The DHCP server permanently assigns a IP address to a requesting client from the range defined. But DHCP server keeps a table of past IP address assignments, so that it can preferentially assign to a client the same IP address that the client previously had.
- ✓ Static allocation- The DHCP server allocates an IP address based on a table with MAC address/IP address pairs, which are manually filled by administrator. It is not supported by all DHCP servers.

DHCP uses two ports destination UDP port 67 for sending data to the server, and UDP port 68 for data to the client. DHCP communications are connectionless in nature. DHCP clients and servers on the same subnet communicate via UDP broadcasts else for different subnets, a DHCP Helper or DHCP Relay Agent is used.

Internet

The World Wide Web (also called WWW or the Web), is a system of interlinked hypertext documents accessed via the Internet. With a web browser, user can view web pages with text, images, videos and other multimedia content, and navigate between them via hyperlinks. Hence, user can jump from one document to another simply by clicking on hot spots or hyperlinks. There are several applications called Web browsers that make it easy to access the World Wide Web like Mozilla Firefox, Google chrome and Microsoft's Internet Explorer.

Web servers are computer systems with web server software running on them and having web sites or information in the form of web pages, which is accessible over internet.

User locates the server, the specific web page, and the protocol to get data from server by using DNS (getting server's IP address from the server's name) and HTTP (used for web page reply and request and hyper linking).

HTTP (Hyper Text Transfer Protocol), HTTPS & SSL

HyperText Transfer Protocol or HTTP is the protocol used by the World Wide Web and defined by RFC 2616. It specify message formatting and transmission with actions Web servers and browsers should take in response to various commands.

An HTTP session is a sequence of network request-response transactions. An HTTP client or user sends a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a server (port 80). An HTTP server listening on that port waits for a client's request message. Upon receiving the request, the server sends back a status line, such as "HTTP/1.1 200 OK", and a message of its own. The body of this message is typically the requested resource, although an error message or other information may also be returned.

HTTP defines several commands and responses and the most frequent the HTTP GET request with the filename, is sent from client to get a file from a web server. Server confirms by sending an HTTP GET response with a return code of 200 (meaning "OK") and the file's contents. HTML specifies Web pages formatting and display. HTTP is a stateless protocol. A stateless protocol does not require the HTTP server to retain information or status about each user for the duration of multiple requests. However, some web applications implement states or server side sessions using one or more of the following methods

- ✓ HTTP cookies.
- ✓ Query string parameters, for example, /index.php?session_id=some_unique_session_code.
- ✓ Hidden variables within web forms.

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is used for secure communication on Internet. It is layering addition of the HTTP on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications. HTTPS provides authentication of the web site and associated web server communicating with. It provides bidirectional encryption of communications between a client and server. HTTPS encrypts the HTTP protocol including the request URL, query parameters, headers, and cookies.

Internet Terms (Hypertext, URL, Domain Name)

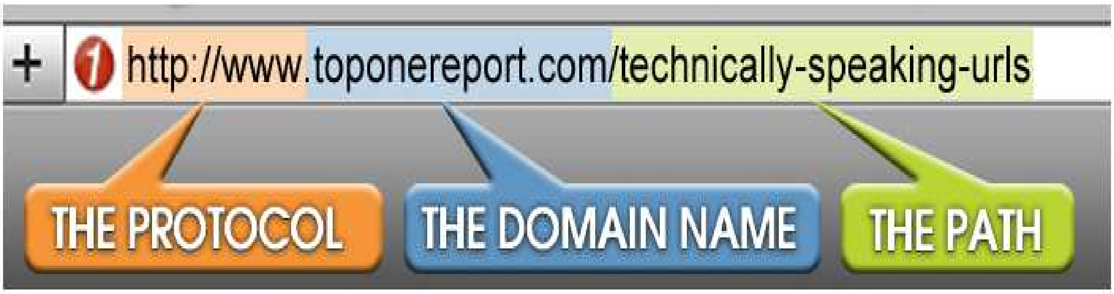
The World Wide Web (WWW) is a subset of the Net--a collection of interlinked documents that work together using a specific Internet protocol called Hypertext Transfer Protocol (HTTP). Web pages are written in Hypertext Markup Language (HTML), which tells the Web browser what to display. The significant feature of the Web is its ability to link pages to one another. Just click a link, and you're at a Web site on the other side of the world hence, this moving around by clicking is called as 'Surfing'.

Hypertext

Hypertext is text which contains links to other texts. Linking to objects whether text, pictures, music, programs, and so on can be creatively linked to each other. The hypertext pages are activated by a mouse click, key press sequence or by touching the screen.

URL

Uniform Resource Locator (URL) is the global address of documents and other resources on the World Wide Web. On the web, each web page has the URL which is in the address bar of browser as illustrated



Some key parts to the URL are the protocol, the domain name and the file path.

Protocol - It is usually the "http", followed by "://", though it can be "https", "ftp", or other things. It is the method to get the information from a server. Web pages use the Hypertext Transfer Protocol (HTTP). It is the method how the information is given.

Hostname or Domain Name This is usually everything after "://" but before the next "/", if there is one. It is usually the domain name. A hostname like "www.example.com" can be further broken down into the top-level domain ("com"), the domain name ("example.com"), and the sub domain ("www"). It is also called the host address and can also be a number called an IP address. All computers on Internet have an IP address which is a set of 12 digits separated by a period. A domain name is converted into IP address for getting the web page by a domain name server (DNS), which has directory of domain names and the corresponding IP addresses.

An organization can register for a domain name, selecting one of the top-level specifications mentioned above that describes it best, and then preceding it with a recognizable version of its name. For example, the ABC Software Systems company will have a domain name like abc.com. From there, it can divide itself into sub domains, extending the organization chart to department levels, or it can just give all of its computers names in the abc.com domain.

File Path – It is anything that appears after the "/" or after the hostname, but before a possible "?". An example would be "games/images/display.html". It can be quite long. It can have a filename ("display.html" in the previous example), or just be one or more directories ("games/images/" in that example). This denotes what file to display at that site. It always begins with a forward slash character and may consist of one or more directory names. It usually correspond to the directory structure of the web site

Every file on the Web has its URL to be accessed by web server and if a file has no URL, the web server will then

- ✓ Look for a default file and return that like index.html.
- ✓ Show a error message saying that the page cannot be found or a 404 message.

ISP (Internet Service Provider)

An ISP (Internet Service Provider) is a company which provides internet access to other companies or individuals. An ISP maintains connections to other networks and ISPs, acting as a router for internet traffic between a customer's computer and any other machine also connected to the internet anywhere else in the world.

Web Browser

It is application software, which is used to locate, retrieve and also display content on the World Wide Web, including Web pages, images, video and other files. As a client/server model, the browser is the client run on a computer that contacts the Web server and requests information. The Web server sends the information back to the Web browser which displays the results on the computer or other Internet-enabled device that supports a browser.

Today's browsers are fully-functional software which interpret and display HTML and HTML 5 Web pages, applications, JavaScript, AJAX and other content hosted on Web servers. Many browsers offer plug-ins which extends the capabilities of a browser like the flash plug-in.

Commonly used browsers are Mozilla Firefox from Mozilla Foundation with the latest release is version 21 and Internet Explorer from Microsoft and the latest release is version 11. Other major browsers include Google Chrome, Apple Safari and Opera.
A number of browsers are used to access the Web on a mobile device. These mobile browsers (also called as "Microbrowser") are optimized to display Web content on smaller mobile device screens and to also perform using less computing power and memory capacity compared to a desktop or laptop computers. Mobile browsers are typically "stripped down" versions of Web browsers and offer fewer features in order to run well on mobile devices.

1.2. Website

A website, also written as web site, or simply site, is a set of related web pages typically served from a single web domain. A website is hosted on at least one web server, accessible via a network such as the Internet or a private local area network through an Internet address known as a uniform resource locator (URL). All publicly accessible websites collectively constitute the World Wide Web.

Web pages, which are the building blocks of websites, are documents, typically written in plain text interspersed with formatting instructions of Hypertext Markup Language (HTML, XHTML). They may incorporate elements from other websites with suitable markup anchors. Webpages are accessed and transported with the Hypertext Transfer Protocol (HTTP), which may optionally employ encryption (HTTP Secure, HTTPS) to provide security and privacy for the user of the webpage content. The user's application, often a web browser, renders the page content according to its HTML markup instructions onto a display terminal.

The pages of a website can usually be accessed from a simple Uniform Resource Locator (URL) called the web address. The URLs of the pages organize them into a hierarchy, although hyperlinking between them conveys the reader's perceived site structure and guides the reader's navigation of the site which generally includes a home page with most of the links to the site's web content, and a supplementary about, contact and link page.

Some websites require a subscription to access some or all of their content. Examples of subscription websites include many business sites, parts of news websites, academic journal websites, gaming websites, file-sharing websites, message boards, web-based email, social networking websites, websites providing real-time stock market data, and websites providing various other services (e.g., websites offering storing and/or sharing of images, files and so forth).

Types of Websites

Type of Website	Description	Examples
Affiliate	A site, typically few in pages, whose purpose is to sell a third party's product. The seller receives a commission for facilitating the sale.	
Affiliate Agency	Enabled portal that renders not only its custom CMS but also syndicated content from other content providers for an agreed fee. There are usually three relationship tiers.	Commission Junction, advertisers like eBay, or a consumer like Yahoo!.
Archive site	Used to preserve valuable electronic content threatened with extinction. Two examples are: Internet Archive, which since 1996 has preserved billions of old (and new) web pages; and Google Groups, which in early 2005 was archiving over 845,000,000 messages posted to Usenet news/discussion groups.	Internet Archive, Google Groups
Attack site	A site created specifically to attack visitors' computers on their first visit to a website by downloading a file (usually a trojan horse). These websites rely on unsuspecting users with poor anti-virus protection in their computers.	
Blog (web log)	Sites generally used to post online diaries which may include discussion forums (e.g., Blogger, Xanga). Many bloggers use blogs like an editorial section of a newspaper to express their ideas on anything ranging from politics to religion to video games to parenting,	WordPress

Type of Website	Description	Examples
	along with anything in between. Some bloggers are professional bloggers and they are paid to blog about a certain subject, and they are usually found on news sites.	
Brand-building site	A site with the purpose of creating an experience of a brand online. These sites usually do not sell anything, but focus on building the brand. Brand building sites are most common for low-value, high-volume fast moving consumer goods (FMCG).	
Celebrity website	A website the information in which revolves around a celebrity. These sites can be official (endorsed by the celebrity) or fan-made (run by a fan or fans of the celebrity without implicit endorsement).	jimcarrey.com
Crowdfunding website	Platform to fund projects by the pre-purchase of products.	
Click-to-donate site	A website that allows the visitor to donate to charity simply by clicking on a button or answering a question correctly. An advertiser usually donates to the charity for each correct answer generated.	The Hunger Site, Freerice, Ripple (charitable organisation)
Community site	A site where persons with similar interests communicate with each other, usually by chat or message boards.	Myspace, Facebook, orkut
Content site	A site the business of which is the creation and distribution of original content	Slate, About.com
Classified ads site	A site publishing classified advertisements	gumtree.com, Craigslist
Corporate website	Used to provide background information about a business, organization, or service.	
Dating website	A site where users can find other single people looking for long range relationships, dating, or just friends. Many of them are pay per services, but there are many free or partially free dating sites. Most dating sites today have the functionality of social networking websites.	eHarmony, Match.com
Electronic commerce (e-commerce) site	A site offering goods and services for online sale and enabling online transactions for such sales.	Amazon.com
Forum website	A site where people discuss various topics.	
Gallery website	A website designed specifically for use as a Gallery; these may be an art gallery or photo gallery and of commercial or non-commercial nature.	
Government site	A website made by the local, state, department or national government of a country. Usually these sites also operate websites that are intended to inform tourists or support tourism.	For example, Richmond.com is the geodomain for Richmond, Virginia
Gripe site	A site devoted to the criticism of a person, place,	

Type of Website	Description	Examples
	corporation, government, or institution.	
Gaming website	A site that lets users play online games. Some enable people to gamble online.	
Gambling website		
Humor site	Satirizes, parodies or otherwise exists solely to amuse.	
Information site	Most websites fit in this category to some extent. They do not necessarily have commercial purposes.	RateMyProfessors.com, Free Internet Lexicon and Encyclopedia. Most government, educational and nonprofit institutions have an informational site.
Media-sharing site	A site that enables users to upload and view media such as pictures, music, and videos	Flickr, YouTube, Google Videos
Mirror site	A website that is the replication of another website. This type of website is used as a response to spikes in user visitors. Mirror sites are most commonly used to provide multiple sources of the same information, and are of particular value as a way of providing reliable access to large downloads.	
Microblog site	A short and simple form of blogging. Microblogs are limited to certain amounts of characters and works similar to a status update on Facebook.	Twitter
News site	Similar to an information site, but dedicated to dispensing news, politics, and commentary.	cnn.com
Personal website	Websites about an individual or a small group (such as a family) that contains information or any content that the individual wishes to include. Such a personal website is different from a Celebrity website, which can be very expensive and run by a publicist or agency.	
Phishing site	a website created to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business (such as Social Security Administration, PayPal) in an electronic communication (see Phishing).	
p2p/Torrents website	Websites that index torrent files. This type of website is different from a Bit torrent client which is usually a stand-alone software.	Mininova, The Pirate Bay, IsoHunt
Political site	A site on which people may voice political views, show political humor, campaigning for elections, or show information about a certain political party or ideology.	
Porn site	A site that shows sexually explicit content for	

Type of Website	Description	Examples
	enjoyment and relaxation. They can be similar to a personal website	
	when it's a website of a porn actor/actress or a media sharing website where user can upload from their own sexually explicit material to movies made by adult studios.	
Question and Answer (Q&A) site	Answer site is a site where people can ask questions & get answers.	Quora, Yahoo! Answers, Stack Exchange Network (including Stack Overflow)
Religious site	A site in which people may advertise a place of worship, or provide inspiration or seek to encourage the faith of a follower of that religion.	
Review site	A site on which people can post reviews for products or services.	Yelp, Rotten Tomatoes
School site	a site on which teachers, students, or administrators can post information about current events at or involving their school. U.S. elementary-high school websites generally use k12 in the URL	
Scraper site	a site which largely duplicates without permission the content of another site, without actually pretending to be that site, in order to capture some of that site's traffic (especially from search engines) and profit from advertising revenue or in other ways.	
Search engine site	A website that indexes material on the Internet or an intranet (and lately on traditional media such as books and newspapers) and provides links to information as a response to a query.	Google Search, Bing, GoodSearch, DuckDuckGo
Shock site	Includes images or other material that is intended to be offensive to most viewers	Goatse.cx, rotten.com
Showcase site	Web portals used by individuals and organisations to showcase things of interest or value	
Social bookmarking site	A site where users share other content from the Internet and rate and comment on the content.	StumbleUpon, Digg, Total Knowledge
Social networking site	A site where users could communicate with one another and share media, such as pictures, videos, music, blogs, etc. with other users. These may include games and web applications	Facebook, Orkut, Google+
Warez	A site designed to host or link to materials such as music, movies and software for the user to download.	
Webmail	A site that provides a webmail service.	Hotmail, Gmail, Yahoo!
Web portal	A site that provides a starting point or a gateway to other resources on the Internet or an intranet.	msn.com, msnbc.com, yahoo
Wiki site	A site in which users collaboratively edit its content.	Wikipedia, WikiHow, Wikia

1.3. Web Hosting

A web hosting service is a type of Internet hosting service that allows individuals and organizations to make their website accessible via the World Wide Web. Web hosts are companies that provide space on a server owned or leased for use by clients, as well as providing Internet connectivity, typically in a data center. Web hosts can also provide data center space and connectivity to the Internet for other servers located in their data center, called collocation, also known as Housing in Latin America or France.

The scope of web hosting services varies greatly. The most basic is web page and small-scale file hosting, where files can be uploaded via File Transfer Protocol (FTP) or a Web interface. The files are usually delivered to the Web "as is" or with minimal processing. Many Internet service providers (ISPs) offer this service free to subscribers. Individuals and organizations may also obtain Web page hosting from alternative service providers. Personal web site hosting is typically free, advertisement-sponsored, or inexpensive. Business web site hosting often has a higher expense depending upon the size and type of the site.

Single page hosting is generally sufficient for personal web pages. A complex site calls for a more comprehensive package that provides database support and application development platforms (e.g. PHP, Java, Ruby on Rails, ColdFusion, or ASP.NET). These facilities allow customers to write or install scripts for applications like forums and content management. Also, Secure Sockets Layer (SSL) is typically used for e-commerce.

The host may also provide an interface or control panel for managing the Web server and installing scripts, as well as other modules and service applications like e-mail. Some hosts specialize in certain software or services (e.g. e-commerce), which are commonly used by larger companies that outsource network infrastructure.

Internet hosting services can run Web servers. Many large companies that are not internet service providers need to be permanently connected to the web to send email, files, etc. to other sites. The company may use the computer as a website host to provide details of their goods and services and facilities for online orders.

- ✓ Free web hosting service: offered by different companies with limited services, sometimes supported by advertisements, and often limited when compared to paid hosting.
- ✓ Shared web hosting service: one's website is placed on the same server as many other sites, ranging from a few to hundreds or thousands. Typically, all domains may share a common pool of server resources, such as RAM and the CPU. The features available with this type of service can be quite basic and not flexible in terms of software and updates. Resellers often sell shared web hosting and web companies often have reseller accounts to provide hosting for clients.
- ✓ Reseller web hosting: allows clients to become web hosts themselves. Resellers could function, for individual domains, under any combination of these listed types of hosting, depending on who they are affiliated with as a reseller. Resellers' accounts may vary tremendously in size: they may have their own virtual dedicated server to a colocated server. Many resellers provide a nearly identical service to their provider's shared hosting plan and provide the technical support themselves.

- ✓ Virtual Dedicated Server: also known as a Virtual Private Server (VPS), divides server resources into virtual servers, where resources can be allocated in a way that does not directly reflect the underlying hardware. VPS will often be allocated resources based on a one server to many VPSs relationship, however virtualisation may be done for a number of reasons, including the ability to move a VPS container between servers. The users may have root access to their own virtual space. Customers are sometimes responsible for patching and maintaining the server.
- ✓ Dedicated hosting service: the user gets his or her own Web server and gains full control over it (user has root access for Linux/administrator access for Windows); however, the user typically does not own the server. One type of dedicated hosting is self-managed or unmanaged. This is usually the least expensive for dedicated plans. The user has full administrative access to the server, which means the client is responsible for the security and maintenance of his own dedicated server.
- ✓ Managed hosting service: the user gets his or her own Web server but is not allowed full control over it (user is denied root access for Linux/administrator access for Windows); however, they are allowed to manage their data via FTP or other remote management tools. The user is disallowed full control so that the provider can guarantee quality of service by not allowing the user to modify the server or potentially create configuration problems. The user typically does not own the server. The server is leased to the client.
- ✓ Colocation web hosting service: similar to the dedicated web hosting service, but the user owns the colo server; the hosting company provides physical space that the server takes up and takes care of the server. This is the most powerful and expensive type of web hosting service. In most cases, the colocation provider may provide little to no support directly for their client's machine, providing only the electrical, Internet access, and storage facilities for the server. In most cases for colo, the client would have his own administrator visit the data center on site to do any hardware upgrades or changes. Formerly, many colocation providers would accept any system configuration for hosting, even ones housed in desktop-style minitower cases, but most hosts now require rack mount enclosures and standard system configurations.
- ✓ Cloud hosting: is a new type of hosting platform that allows customers powerful, scalable and reliable hosting based on clustered load-balanced servers and utility billing. A cloud hosted website may be more reliable than alternatives since other computers in the cloud can compensate when a single piece of hardware goes down. Also, local power disruptions or even natural disasters are less problematic for cloud hosted sites, as cloud hosting is decentralized. Cloud hosting also allows providers to charge users only for resources consumed by the user, rather than a flat fee for the amount the user expects they will use, or a fixed cost upfront hardware investment. Alternatively, the lack of centralization may give users less control on where their data is located which could be a problem for users with data security or privacy concerns.
- ✓ Clustered hosting: having multiple servers hosting the same content for better resource utilization. Clustered servers are a perfect solution for high-availability dedicated hosting, or creating a scalable web hosting solution. A cluster may separate web serving from database hosting capability. (Usually web hosts use clustered hosting for their shared hosting plans, as there are multiple benefits to the mass managing of clients).
- ✓ Grid hosting: this form of distributed hosting is when a server cluster acts like a grid and is composed of multiple nodes.
- ✓ Home server: usually a single machine placed in a private residence can be used to host one or more web sites from a usually consumer-grade broadband connection. These can be purpose-built machines or more commonly old PCs. Some ISPs actively attempt to block home servers

by disallowing incoming requests to TCP port 80 of the user's connection and by refusing to provide static IP addresses. A common way to attain a reliable DNS host name is by creating an account with a dynamic DNS service. A dynamic DNS service will automatically change the IP address that a URL points to when the IP address changes.

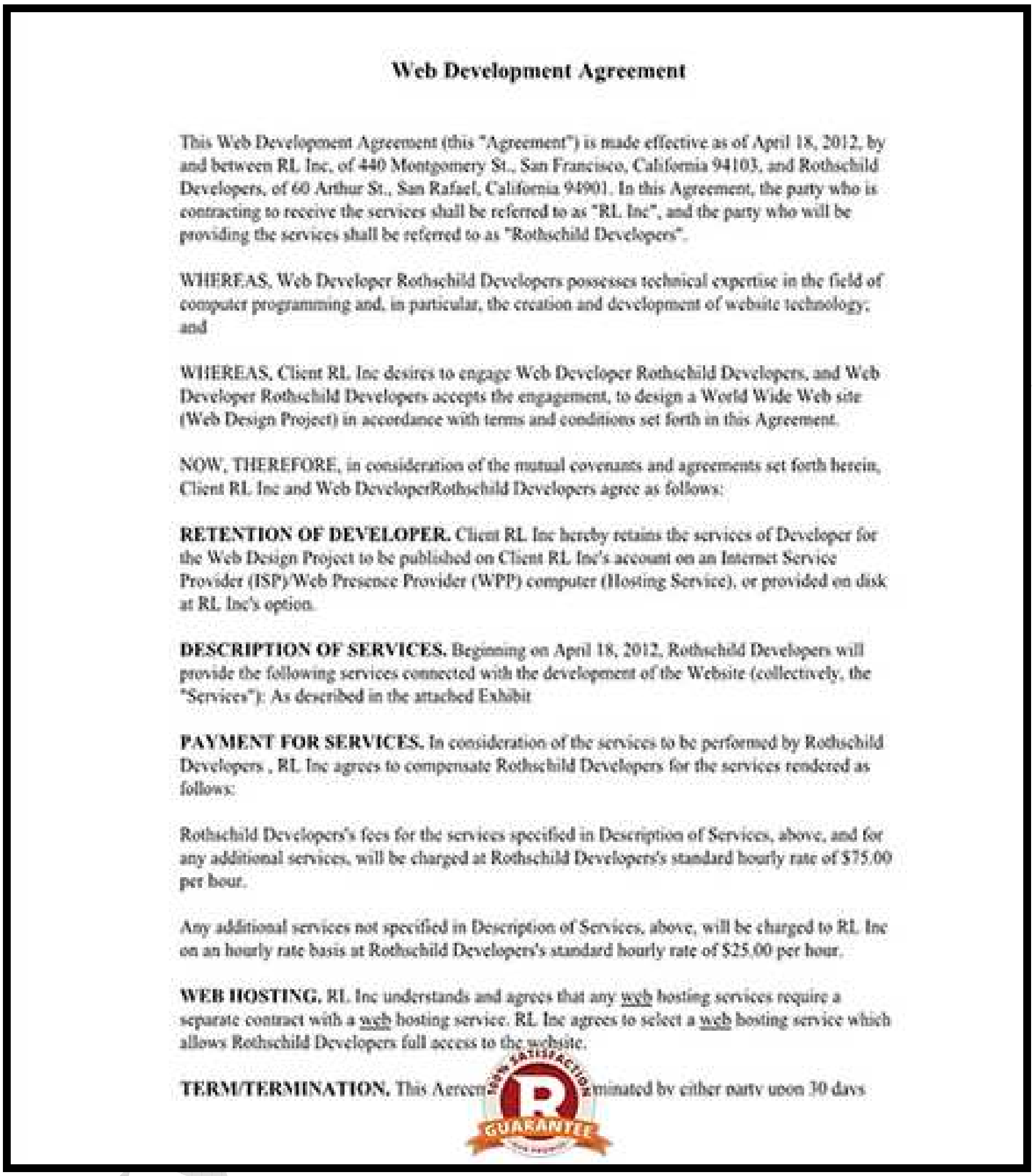
Some specific types of hosting provided by web host service providers

- ✓ File hosting service: hosts files, not web pages
- ✓ Image hosting service
- ✓ Video hosting service
- ✓ Blog hosting service
- ✓ Paste bin
- ✓ Shopping cart software
- ✓ E-mail hosting service

Web Development and Hosting Agreements

Web Development Agreements: A Web Development Agreement is a contract between a web developer and the individual or business in need of a new or redesigned website

A sample web development agreement is shown below:



Web Development Agreement

This Web Development Agreement (this "Agreement") is made effective as of April 18, 2012, by and between RL Inc, of 440 Montgomery St., San Francisco, California 94103, and Rothschild Developers, of 60 Arthur St., San Rafael, California 94901. In this Agreement, the party who is contracting to receive the services shall be referred to as "RL Inc", and the party who will be providing the services shall be referred to as "Rothschild Developers".

WHEREAS, Web Developer Rothschild Developers possesses technical expertise in the field of computer programming and, in particular, the creation and development of website technology; and

WHEREAS, Client RL Inc desires to engage Web Developer Rothschild Developers, and Web Developer Rothschild Developers accepts the engagement, to design a World Wide Web site (Web Design Project) in accordance with terms and conditions set forth in this Agreement.

NOW, THEREFORE, in consideration of the mutual covenants and agreements set forth herein, Client RL Inc and Web DeveloperRothschild Developers agree as follows:

RETENTION OF DEVELOPER. Client RL Inc hereby retains the services of Developer for the Web Design Project to be published on Client RL Inc's account on an Internet Service Provider (ISP)/Web Presence Provider (WPP) computer (Hosting Service), or provided on disk at RL Inc's option.

DESCRIPTION OF SERVICES. Beginning on April 18, 2012, Rothschild Developers will provide the following services connected with the development of the Website (collectively, the "Services"): As described in the attached Exhibit

PAYMENT FOR SERVICES. In consideration of the services to be performed by Rothschild Developers , RL Inc agrees to compensate Rothschild Developers for the services rendered as follows:

Rothschild Developers's fees for the services specified in Description of Services, above, and for any additional services, will be charged at Rothschild Developers's standard hourly rate of $75.00 per hour.

Any additional services not specified in Description of Services, above, will be charged to RL Inc on an hourly rate basis at Rothschild Developers's standard hourly rate of $25.00 per hour.

WEB HOSTING. RL Inc understands and agrees that any web hosting services require a separate contract with a web hosting service. RL Inc agrees to select a web hosting service which allows Rothschild Developers full access to the website.

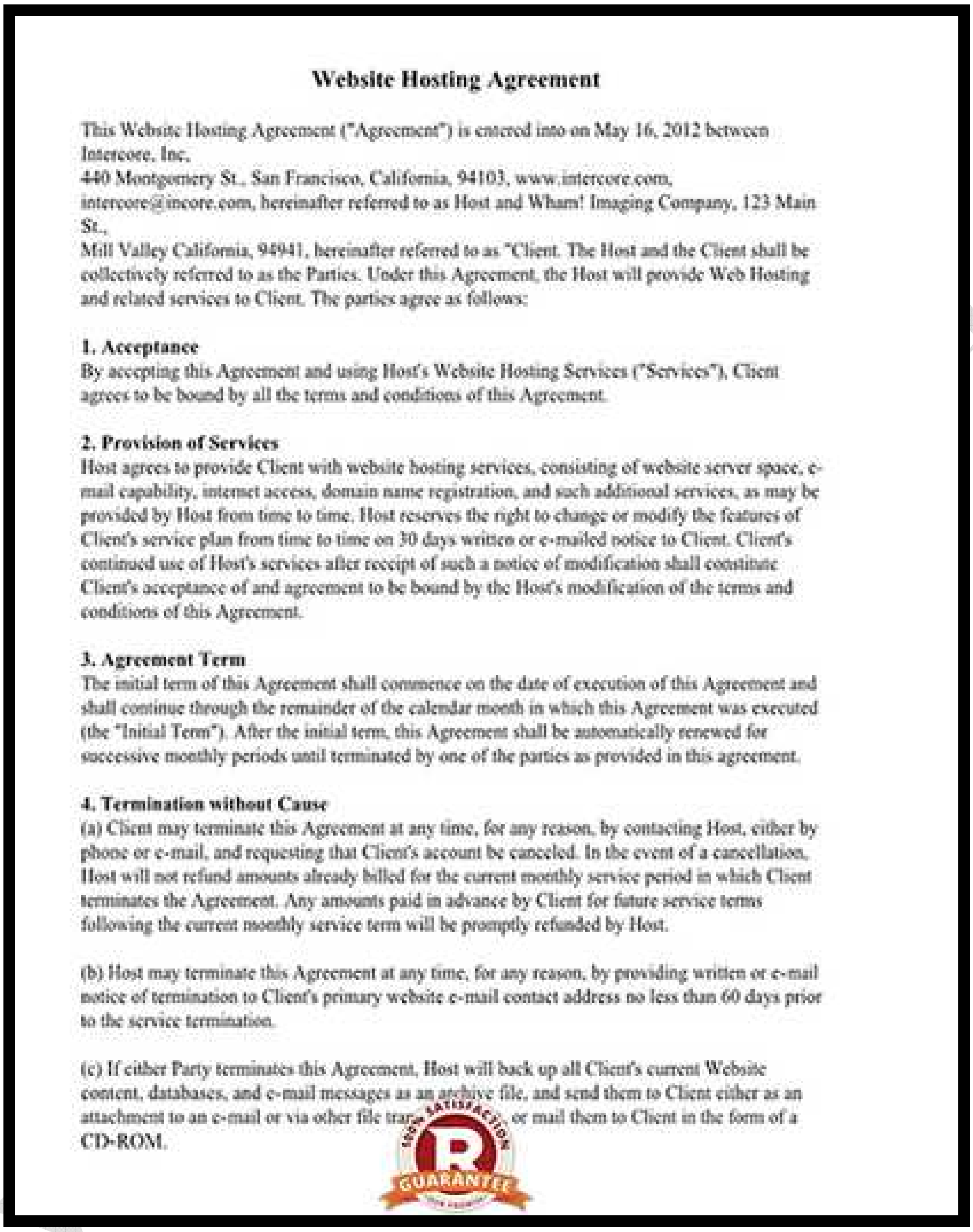
TERM/TERMINATION. This Agreem minated by either party upon 30 days

Web Hosting Agreement

A web hosting agreement is needed by a Web Hosting company offering web hosting services to other companies or if one would like to hire a web hosting service to manage a website.

A web hosting agreement helps to clarify existing agreements with clients as well as actively look for new clients. Most of the time one cannot depend on an email chain as proof of an agreement. A formal web hosting agreement is always needed to make it official.

A sample web hosting agreement can be seen below



Website Hosting Agreement

This Website Hosting Agreement ("Agreement") is entered into on May 16, 2012 between
Intercore, Inc,
440 Montgomery St., San Francisco, California, 94103, www.intercore.com,
intercore@incore.com, hereinafter referred to as Host and Wham! Imaging Company, 123 Main
St.,
Mill Valley California, 94941, hereinafter referred to as "Client. The Host and the Client shall be collectively referred to as the Parties. Under this Agreement, the Host will provide Web Hosting and related services to Client. The parties agree as follows:

1. Acceptance
By accepting this Agreement and using Host's Website Hosting Services ("Services"), Client agrees to be bound by all the terms and conditions of this Agreement.

2. Provision of Services
Host agrees to provide Client with website hosting services, consisting of website server space, e-mail capability, internet access, domain name registration, and such additional services, as may be provided by Host from time to time. Host reserves the right to change or modify the features of Client's service plan from time to time on 30 days written or e-mailed notice to Client. Client's continued use of Host's services after receipt of such a notice of modification shall constitute Client's acceptance of and agreement to be bound by the Host's modification of the terms and conditions of this Agreement.

3. Agreement Term
The initial term of this Agreement shall commence on the date of execution of this Agreement and shall continue through the remainder of the calendar month in which this Agreement was executed (the "Initial Term"). After the initial term, this Agreement shall be automatically renewed for successive monthly periods until terminated by one of the parties as provided in this agreement.

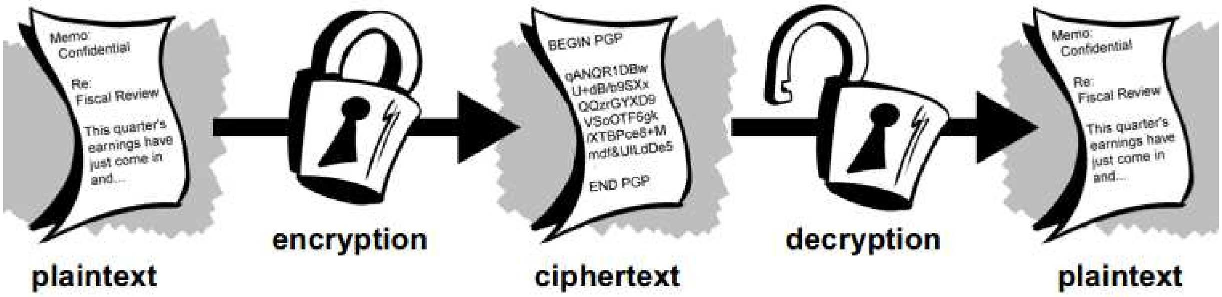
4. Termination without Cause
(a) Client may terminate this Agreement at any time, for any reason, by contacting Host, either by phone or e-mail, and requesting that Client's account be canceled. In the event of a cancellation, Host will not refund amounts already billed for the current monthly service period in which Client terminates the Agreement. Any amounts paid in advance by Client for future service terms following the current monthly service term will be promptly refunded by Host.

(b) Host may terminate this Agreement at any time, for any reason, by providing written or e-mail notice of termination to Client's primary website e-mail contact address no less than 60 days prior to the service termination.

(c) If either Party terminates this Agreement, Host will back up all Client's current Website content, databases, and e-mail messages as an archive file, and send them to Client either as an attachment to an e-mail or via other file tra[illegible] or mail them to Client in the form of a CD-ROM.

1.4. Cryptography

Data that can be read and understood without any special measures is called plaintext or cleartext. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption.



Cryptographic Algorithms Types

There are several ways of classifying cryptographic algorithms like categorization based on the number of keys that are employed for encryption and decryption, defined by their application and use. The three types of algorithms that are usually classified into are

- ✓ Secret Key Cryptography (SKC) - Uses a single key for both encryption and decryption
- ✓ Public Key Cryptography (PKC) - Uses one key for encryption and another for decryption
- ✓ Hash Functions - Uses a mathematical transformation to irreversibly "encrypt" information

Symmetric and Asymmetric key Cryptography

The two primary types of encryption are symmetric and asymmetric key encryption.

Symmetric Key Encryption - It means both sender and receiver use the same secret key to encrypt and decrypt the data. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet.

As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key. The drawback to symmetric key encryption is there is no secure way to share the key between multiple systems. Systems that use symmetric key encryption need to use an offline method to transfer the keys from one system to another. This is not practical in a large environment such as the Internet, where the clients and servers are not located in the same physical place. The strength of symmetric key encryption is fast, bulk encryption. Weaknesses of symmetric key encryption are key distribution, scalability, limited security (confidentiality only) and The fact that it does not provide non-repudiation, meaning the sender's identity can be proven.

Examples of symmetric algorithms are DES (data encryption standard), 3DES, AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm), Twofish, RC4 (Rivest Cipher 4)

Asymmetric (or public) key cryptography – It was created to address the weaknesses of symmetric key management and distribution. But there's a problem with secret keys: how can they be exchanged securely over an inherently insecure network such as the Internet?

Anyone who knows the secret key can decrypt the message, so it is important to keep the secret key secure. Asymmetric encryption uses two related keys known as a key pair. A public key is made available to anyone who might want to send you an encrypted message. A second, private key is kept secret, so that only you know it. Any messages (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key. This means that you do not have to worry about passing public keys over the Internet as they are by nature available to anyone. A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

The relationship between the two keys in asymmetric key encryption is based on complex mathematical formulas. One method of creating the key pair is to use factorization of prime numbers. Another is to use discrete logarithms. Asymmetric encryption systems are based on one-way functions that act as a trapdoor. Essentially the encryption is one-way in that the same key cannot decrypt messages it encrypted. The associated private key provides information to make decryption feasible. The information about the function is included in the public key, whereas information about the trapdoor is in the private key.

Anyone who has the private key knows the trapdoor function and can compute the public key. To use asymmetric encryption, there needs to be a method for transferring public keys. The typical technique is to use X.509 digital certificates (also known simply as certificates). A certificate is a file of information that identifies a user or a server, and contains the organization name, the organization that issued the certificate, and the user's email address, country, and public key.
When a server and a client require a secure encrypted communication, they send a query over the network to the other party, which sends back a copy of the certificate. The other party's public key can be extracted from the certificate. A certificate can also be used to uniquely identify the holder. Asymmetric encryption can be used for Data encryption and Digital signatures

Asymmetric encryption can provide Confidentiality, Authentication and Non-repudiation. Strengths of asymmetric key encryption include Key distribution, Scalability and confidentiality, authentication, and non-repudiation. The weakness of asymmetric key encryption is that the process is slow and typically requires a significantly longer key. It's only suitable for small amounts of data due to its slow operation.

Private and Public Key Exchange

Key exchange also called as key establishment, is method to exchange cryptographic keys between users, using a cryptographic algorithm. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other's public key.

Prior to any secured communication, users must set up the details of the cryptography. In some instances this may require exchanging identical keys (in the case of a symmetric key system). In others it may require possessing the other party's public key. While public keys can be openly exchanged (their corresponding private key is kept secret), symmetric keys must be exchanged over a secure communication channel.

Formerly, exchange of such a key was extremely troublesome, and was greatly eased by access to secure channels such as a diplomatic bag. Clear text exchange of symmetric keys would enable any interceptor to immediately learn the key, and any encrypted data.

The advance of public key cryptography in the 1970s has made the exchange of keys less troublesome. Since the Diffie-Hellman key exchange protocol was published in 1975, it has become possible to exchange a key over an insecure communications channel, which has substantially reduced the risk of key disclosure during distribution. It is possible, using something akin to a book code, to include key indicators as clear text attached to an encrypted message. The encryption technique used by Richard Sorge's code clerk was of this type, referring to a page in a statistical manual, though it was in fact a code. The German Army Enigma symmetric encryption key was a mixed type early in its use; the key was a combination of secretly distributed key schedules and a user chosen session key component for each message.

In more modern systems, such as OpenPGP compatible systems, a session key for a symmetric key algorithm is distributed encrypted by an asymmetric key algorithm. This approach avoids even the necessity for using a key exchange protocol like Diffie-Hellman key exchange.

Another method of key exchange involves encapsulating one key within another. Typically a master key is generated and exchanged using some secure method. This method is usually cumbersome or expensive (breaking a master key into multiple parts and sending each with a trusted courier for example) and not suitable for use on a larger scale. Once the master key has been securely exchanged, it can then be used to securely exchange subsequent keys with ease. This technique is usually termed Key Wrap. A common technique uses Block ciphers and cryptographic hash functions.

A related method is to exchange a master key (sometimes termed a root key) and derive subsidiary keys as needed from that key and some other data (often referred to as diversification data). The most common use for this method is probably in SmartCard based cryptosystems, such as those found in banking cards. The bank or credit network embeds their secret key into the card's secure key storage during card production at a secured production facility. Then at the Point of sale the card and card reader are both able to derive a common set of session keys based on the shared secret key and card-specific data (such as the card serial number). This method can also be used when keys must be related to each other (i.e., departmental keys are tied to divisional keys, and individual keys tied to departmental keys). However, tying keys to each other in this way increases the damage which may result from a security breach as attackers will learn something about more than one key. This reduces entropy, with regard to an attacker, for each key involved.

Two of the most common key exchange algorithms are

- ✓ Diffie-Hellman Key Agreement algorithm
- ✓ RSA key exchange process

Both methods provide for highly secure key exchange between communicating parties. An intruder who intercepts network communications cannot easily guess or decode the secret key that is required to decrypt communications. The exact mechanisms and algorithms that are used for key exchange varies for each security technology. In general, the Diffie-Hellman Key Agreement algorithm provides better performance than the RSA key exchange algorithm.

1.5. Public Key Infrastructure

Public-key cryptography (also called asymmetric-key cryptography) uses a key pair to encrypt and decrypt content. The key pair consists of one public and one private key that are mathematically related. An individual who intends to communicate securely with others can distribute the public key but must keep the private key secret. Content encrypted by using one of the keys can be decrypted by using the other. Assume, for example, that Bob wants to send a secure email message to Alice. This can be accomplished in the following manner

- ✓ Both Bob and Alice have their own key pairs. They have kept their private keys securely to themselves and have sent their public keys directly to each other.
- ✓ Bob uses Alice's public key to encrypt the message and sends it to her.
- ✓ Alice uses her private key to decrypt the message.

This simplified example highlights at least one obvious concern Bob must have about the public key he used to encrypt the message. That is, he cannot know with certainty that the key he used for encryption actually belonged to Alice. It is possible that another party monitoring the communication channel between Bob and Alice substituted a different key.

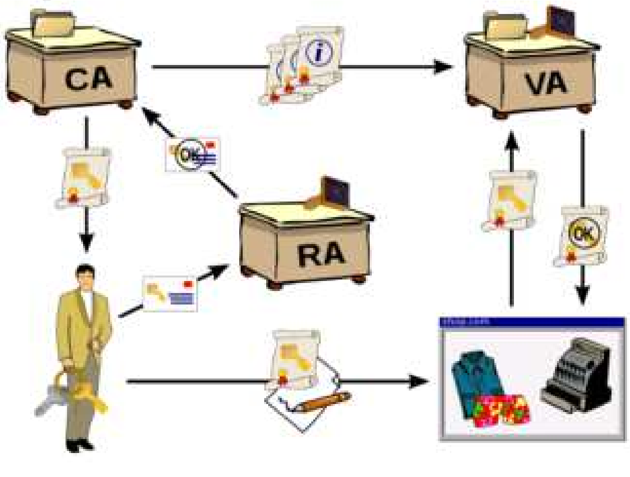
The public key infrastructure concept has evolved to help address this problem and others. A public key infrastructure (PKI) consists of software and hardware elements that a trusted third party can use to establish the integrity and ownership of a public key. The trusted party, called a certification authority (CA), typically accomplishes this by issuing signed (encrypted) binary certificates that affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate. The CA signs the certificate by using its private key. It issues the corresponding public key to all interested parties in a self-signed CA certificate. When a CA is used, the preceding example can be modified in the following manner

- ✓ Assume that the CA has issued a signed digital certificate that contains its public key. The CA self-signs this certificate by using the private key that corresponds to the public key in the certificate.
- ✓ Alice and Bob agree to use the CA to verify their identities.
- ✓ Alice requests a public key certificate from the CA.
- ✓ The CA verifies her identity, computes a hash of the content that will make up her certificate, signs the hash by using the private key that corresponds to the public key in the published CA certificate, creates a new certificate by concatenating the certificate content and the signed hash, and makes the new certificate publicly available.
- ✓ Bob retrieves the certificate, decrypts the signed hash by using the public key of the CA, computes a new hash of the certificate content, and compares the two hashes. If the hashes match, the signature is verified and Bob can assume that the public key in the certificate does indeed belong to Alice.
- ✓ Bob uses Alice's verified public key to encrypt a message to her.
- ✓ Alice uses her private key to decrypt the message from Bob.

In summary, the certificate signing process enables Bob to verify that the public key was not tampered with or corrupted during transit. Before issuing a certificate, the CA hashes the contents, signs (encrypts) the hash by using its own private key, and includes the encrypted hash in the issued certificate. Bob verifies the certificate contents by decrypting the hash with the CA public key, performing a separate hash of the certificate contents, and comparing the two hashes. If they match, Bob can be reasonably certain that the certificate and the public key it contains have not been altered. A typical PKI consists of the following elements.

Element	Description
Certification Authority	Acts as the root of trust in a public key infrastructure and provides services that authenticate the identity of individuals, computers, and other entities in a network.
Registration Authority	Is certified by a root CA to issue certificates for specific uses permitted by the root. In a Microsoft PKI, a registration authority (RA) is usually called a subordinate CA.
Certificate Database	Saves certificate requests and issued and revoked certificates and certificate requests on the CA or RA.
Certificate Store	Saves issued certificates and pending or rejected certificate requests on the local computer.
Key Archival Server	Saves encrypted private keys in the certificate database for recovery after loss.

PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique within each CA domain. The third-party validation authority (VA) can provide this information on behalf of CA. The binding is established through the registration and issuance process, which, depending on the assurance level of the binding, may be carried out by software at a CA or under human supervision. The PKI role that assures this binding is called the registration authority (RA), which ensures that the public key is bound to the individual to which it is assigned in a way that ensures non-repudiation.



1.6. Electronic Signature

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a electronic document (e-mail, spreadsheet, text file, etc.) thus, ensuring that the original content of the electronic document is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

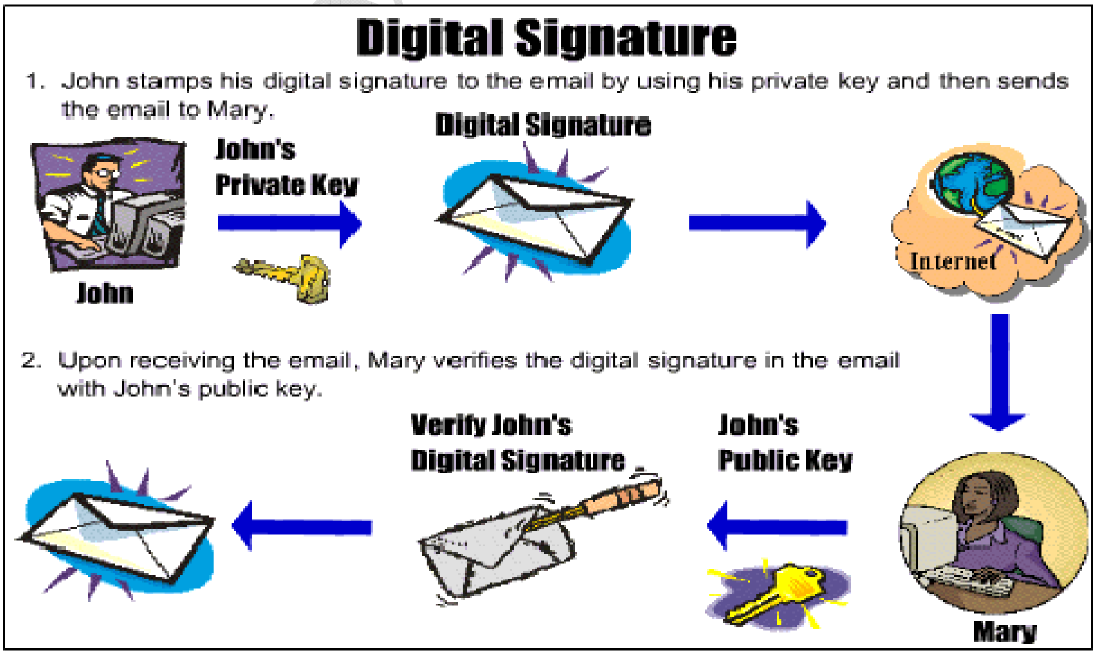
Digital Signature Working

Assume John need to send a contract to Mary in another town. John wants to give Mary the assurance that it was unchanged from what John sent and that it is really from John.

- ✓ John copy-and-paste the contract (it's a short one!) into an e-mail note.
- ✓ Using special software, John obtains a message hash (mathematical summary) of the contract.
- ✓ John then use a private key that John have previously obtained from a public-private key authority to encrypt the hash.
- ✓ The encrypted hash becomes John digital signature of the message. (Note that it will be different each time John sends a message.)

At the other end, Mary receives the message.

- ✓ To make sure it's intact and from John, Mary makes a hash of the received message.
- ✓ Mary then uses John's public key to decrypt the message hash or summary.
- ✓ If the hashes match, the received message is valid.


Digital Signature
1. John stamps his digital signature to the email by using his private key and then sends the email to Mary.
John's Private Key
Digital Signature
John
Internet
2. Upon receiving the email, Mary verifies the digital signature in the email with John's public key.
Verify John's Digital Signature
John's Public Key
Mary

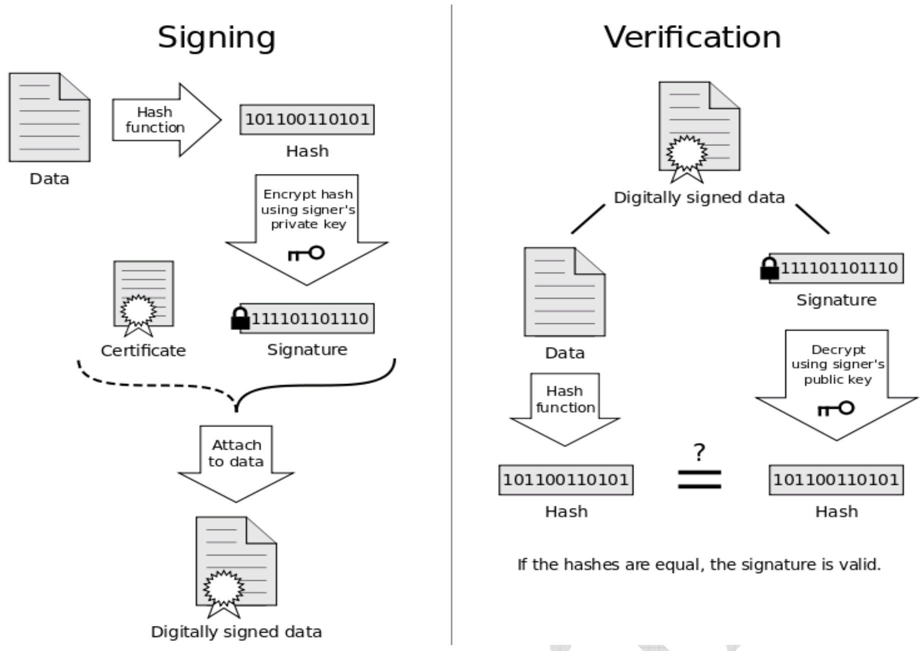
A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Digital signatures are often used to implement electronic signatures, but not all electronic signatures use digital signatures. In some countries, including the United States, India, Brazil, and members of the European Union, electronic signatures have legal significance.

Digital signatures employ a type of asymmetric cryptography. For messages sent through a non-secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes, in the sense used here, are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything represented as a string of bits like electronic mail, contracts, or a message sent via some other cryptographic protocol. A digital signature scheme typically consists of three algorithms

- ✓ A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- ✓ A signing algorithm that, given a message and a private key, produces a signature.
- ✓ A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key.



Authentication of Digital Signature and Electronic Records

There are three critical elements to data security. Confidentiality, integrity, and authentication are known as the CIA triad Data encryption provides confidentiality, message hashing provides integrity and message digital signatures provide authentication. Cryptography offers the following four basic elements

- ✓ Confidentiality – It is assurance that only authorized users can read or use confidential information.
- ✓ Authentication – It is the verification of the identity of the entities that communicate over the network.
- ✓ Integrity – It is the verification that the original contents of information have not been altered or corrupted.
- ✓ Non-repudiation - It is the assurance that a party in a communication cannot falsely deny that a part of the actual communication occurred.

Below are some common reasons for applying a digital signature to communications:

Authentication

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

Integrity

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

Non-repudiation

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Note that this authentication, non-repudiation etc. properties rely on the secret key not having been revoked prior to its usage. Public revocation of a key-pair is a required ability, else leaked secret keys would continue to implicate the claimed owner of the key-pair. Checking revocation status requires an "online" check, e.g. checking a "Certificate Revocation List" or via the "Online Certificate Status Protocol". Very roughly this is analogous to a vendor who receives credit-cards first checking online with the credit-card issuer to find if a given card has been reported lost or stolen. Of course, with stolen key pairs, the theft is often discovered only after the secret key's use, e.g., to sign a bogus certificate for espionage purposes.