SECTION-I

INTRODUCTION TO OPERATING SYSTEM & COMPUTER NETWORK

- **Digital video or audio composition** - Audio or video composition and editing have been made much easier by computers. It no longer costs thousands of dollars of equipment to compose music or make a film. Graphics engineers can use computers to generate short or full-length films or even to create 3D models.
- **Medicine** - You can diagnose diseases. You can learn the cures. Software is used in magnetic resonance imaging to examine the internal organs of the human body. Software is used for performing surgery.
- **Mathematical Calculations** - Thanks to computers, which have computing speeds of over a million calculations per second we can perform the biggest of mathematical calculations.
- **Banks** - All financial transactions are done by computer software. They provide security, speed and convenience.
- **Travel** - One can book air tickets or railway tickets and make hotel reservations online.
- **Defense** - There is software embedded in almost every weapon. Software is used for controlling the flight and targeting in ballistic missiles. Software is used to control access to atomic bombs.
- **E-Learning** - Instead of a book it is easier to learn from an E-learning software.
- **Examinations** - You can give online exams and get instant results. You can check your examination results online.
- **Business** - Shops and supermarkets use software, which calculate the bills. Taxes can be calculated and paid online. Accounting is done using computers. One can predict future trends of business using artificial intelligence software. Software is used in major stock markets. One can do trading online. There are fully automated factories running on software.
- **An ATM machine -** The computer software authenticates the user and dispenses cash.
- **News** - There are many websites through which you can read the latest or old news.
- **Planning and Scheduling** - Software can be used to store contact information, generating plans, scheduling appointments and deadlines.
- **Sports** - Software is used for making umpiring decisions. There is simulation software using which a sportsperson can practice his skills. Computers are also used to identify flaws in technique.

- **Weather analysis** - Supercomputers are used to analyze and predict weather.
- **Word Processing** - Word Processing software automatically corrects spelling and grammar mistakes. If the content of a document repeats, you don't have to type it each time. You can use the copy and paste features. You can print documents and make several copies. It is easier to read a word-processed document than a handwritten one. You can add images to your document.
- **Internet** - It is a network of almost all the computers in the world. You can browse through much more information than you could do in a library. That is because computers can store enormous amounts of information. You also have very fast and convenient access to information. Through E-Mail, you can communicate with a person sitting thousands of miles away in a few seconds. Chat software enables one to chat with another on a real-time basis. Video conferencing tools are becoming readily available to the common man.

1.3 COMPUTER COMPONENTS

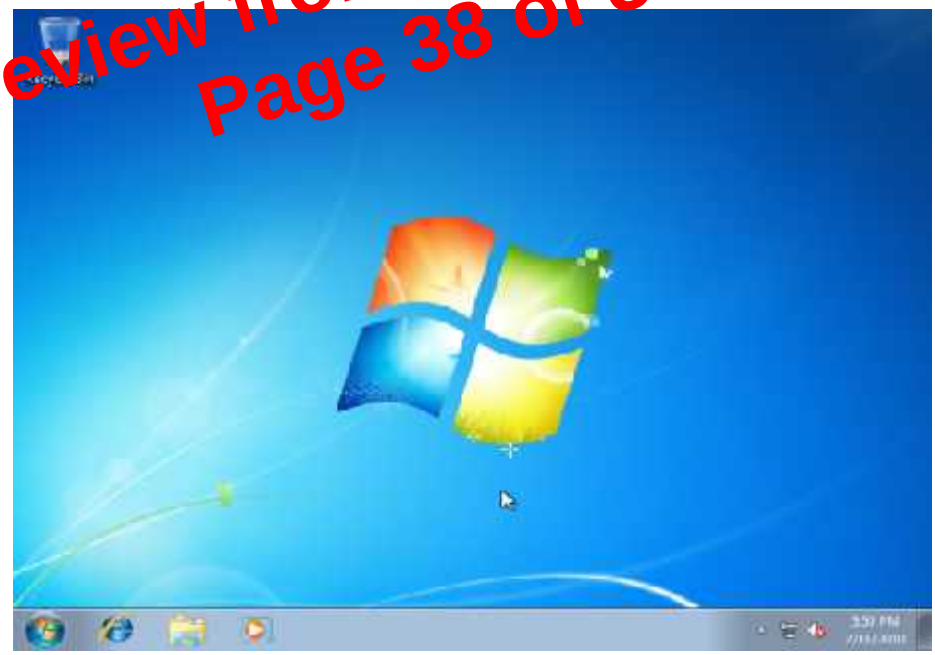
Basically computer components come into a following particular category.

- **Hardware**: Hardware is a comprehensive term for all of the physical parts of a computer, as distinguished from the data it contains or operates on, and the software that provides instructions for the hardware to accomplish tasks. A typical computer contains in a desktop or tower case the following parts:

- Motherboard which holds the CPU, main memory and other parts, and has slots for expansion cards
- Power supply - a case that holds a transformer, voltage control and fan
- Storage controllers, of IDE, SCSI or other type, that control hard disk , floppy disk, CD-ROM and other drives; the controllers sit directly on the motherboard (on-board) or on expansion cards.
- Graphics controller that produces the output for the monitor
- Hard disk, floppy disk and other drives for mass storage
- Interface controllers (parallel, serial, USB) to connect the computer to external peripheral devices such as printers or scanners

Select your network location type. This setting can be changed later, but do note that choosing a profile will have effect on the Windows Firewall and sharing settings. Click on "Next".

Windows will finalize the settings and your desktop will appear.



This concludes the Windows 7 installation. Next, you would probably want to update your computer with the latest hot fixes and/or patches from Microsoft.

Types of IPV4 Address

The Internet standards define the following types of IPv4 addresses:

- ***Unicast.*** Assigned to a single network interface located on a specific subnet on the network and used for one-to-one communications.
- ***Multicast.*** Assigned to one or more network interfaces located on various subnets on the network and used for one-to-many communications.
- ***Broadcast***. Assigned to all network interfaces located on a subnet on the network and used for one-to-everyone-on-a-subnet communications.

❖ INTERNET PROTOCOL (IP V.6)

An IPv6 address consists of 128 bits, therefore allowing an astronomical number of machines. This is equivalent to the value of 2 raised to the power of 128, a number with nearly 40 trailing zeros.

➢ **IPv6 features include:**

- Supports source and destination addresses that are 128 bits (16 bytes) long.
- Requires IPSec support.
- Uses Flow Label field to identify packet flow for QoS handling by router.
- Allows the host to send fragments packets but not routers.
- Doesn't include a checksum in the header.
- Uses a link-local scope all-nodes multicast address.
- Does not require manual configuration or DHCP.
- Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.
- Supports a 1280-byte packet size (without fragmentation).
- Uses Multicast Neighbor Solicitation messages to resolve IP addresses to link-layer addresses.
- Moves optional data to IPv6 extension headers.

➢ **IPv6 Address Format**

IPv6 uses **16-byte hexadecimal** number fields separated by **colons (:)** to represent the **128-bit addressing** format that makes the address

To determine the desired subnetting scheme, start with an existing network ID to be subnetted. The network ID to be subnetted can be a class-based network ID, a subnetted network ID, or a supernet. The existing network ID contains a series of network ID bits that are fixed and a series of host ID bits that are variable. Based on your requirements for the number of subnets and the number of hosts per subnet, choose a specific number of host bits to be used for the subnetting.

Step 2: Enumerating Subnetted Network IDs: Based on the number of host bits you use for your subnetting, you must list the new subnetted network IDs. There are two main approaches:

- Binary—List all possible combinations of the host bits chosen for subnetting and convert each combination to dotted decimal notation.
- Decimal— Add a calculated increment value to each successive subnetted network ID and convert to dotted decimal notation.

Either method produces the same result: the enumerated list of subnetted network IDs.

Note

There are a variety of documented shortcut techniques for subnetting. However, they only work under a specific set of constraints (for example, only up to 8 bits of a class-based network ID). The following methods described are designed to work for any subnetting situation (class-based, more than 8 bits, supernetting, variable length subnetting).

To create the enumerated list of subnetted network IDs using the binary method

o Based on n, the number of host bits chosen for subnetting, create a three-column table with 2 n entries. The first column is the subnet number (starting with 1), the second column is the binary representation of the subnetted network ID, and the third column is the dotted decimal representation of the subnetted network ID.

For each binary representation, the bits of the network ID being subnetted are fixed to their appropriate values and the remaining host bits are set to all 0's. The host bits chosen for subnetting vary.

o In the first table entry, set the subnet bits to all 0's and convert to dot decimal notation. The original network ID is subnetted with its new subnet mask.

- In the next table entry, increase the value within the subnet bits.
- Convert the binary result to dotted decimal notation.
- Repeat steps 3 and 4 until the table is complete.

For example, create a 3-bit subnet of the private network ID 192.168.0.0. The subnet mask for the new subnetted network IDs is 255.255.224.0 or /19. Based on *n* = 3, construct a table with 8 (= 2 3) entries.

The entry for subnet 1 is the all 0's subnet. Additional entries in the table are successive increments of the subnet bits, as shown in Table 1.19. The host bits used for subnetting are underlined.

Subnet	Binary Presentation	Subnetted Network ID
1	11000000.10101000.***000***00000.00000000	192.168.0.0/19
2	11000000.10101000.***001***00000.00000000	192.168.32.0/19
3	11000000.10101000.***010*** 0000.00000000	192.168.64.0/19
4	11000000.10101000.***011*** 0000.00000000	192.168.96.0/19
5	11000000.10101000.***100*** 0000.00000000	192.168.128.0/19
6	11000000.10101000.***101*** 0000.00000000	192.168.160.0/19
7	11000000.10101000.***110*** 0000.00000000	192.168.192.0/19
8	11000000.10101000.***111*** 0000.00000000	192.168.224.0/19

Step 3: Enumerating IP Addresses for Each Subnetted Network ID

Based on the enumeration of the subnetted network IDs, you must now list the valid IP addresses for new subnetted network IDs. To list each IP address individually would be too tedious.

Instead, enumerate the IP addresses for each subnetted network ID by defining the range of IP addresses (the first and the last) for each subnetted network ID.

There are two main approaches:

- Binary—Write down the first and last IP address for each subnetted network ID and convert to dotted decimal notation.
- Decimal—Add values incrementally, corresponding to the first and last IP addresses for each subnetted network ID and convert to dotted decimal notation.

Either method produces the same result: the range of IP addresses for each subnetted network ID.[14]

[14] http://technet.microsoft.com/en-us/library/cc958834.aspx

NIC carry out several important **function**s are as follows:-

- Monitoring activity on the communication medium
- Providing each workstation/server with a unique identification Address (MAC)
- Creating (building) the frames needed to transmit data on the Communication medium
- Controlling LAN transmission speed
- Transmission error detection and recovery
- Recognizing and receiving data transmitted to the computer

ii) Repeaters

Repeater is a device that increases the strength of the data signals sent across the network. It obtains a weak signal from the network, amplifies it and passes it on to the next network segment so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable which runs longer than 100 meters.

Repeaters work on the Physical Layer of the OSI model. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row.

iv) Bridges

A **network bridge** connects multiple network segments at the data link layer (layer 2) of the OSI model. Bridges do not promiscuously copy traffic to all ports, as hubs do, but learn which MAC addresses are reachable through specific ports. Once the bridge associates a port and an address, it will send traffic for that address only to that port. Bridges do send broadcasts to all ports except the one on which the broadcast was received.[16]

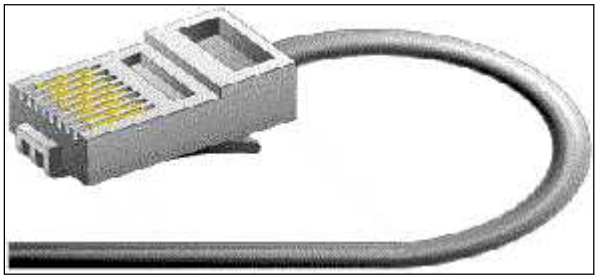
17

Bridge carries out several important **functions** including

- It is a layer-2 device and can operate in both the physical and data link layers of the OSI model.
- They are usually used to connect networks with similar architecture.
- Bridges are used to break up a bigger LAN into small manageable segments; hence network performance can be improved.
- Network security and reliability is also improved due to smaller LAN segments.
- Bridges forward frames (after extracting destination MAC address from frame header) between various LAN segments.
- Keeps the traffic on each segment separate thereby controls congestion, isolates LAN segments.
- Bridges perform Error checking on Frame.

[16] http://networkschool.wordpress.com/
[17] http://rosilaabdullah.blogspot.in/2009/10/basic-hardware-components.html

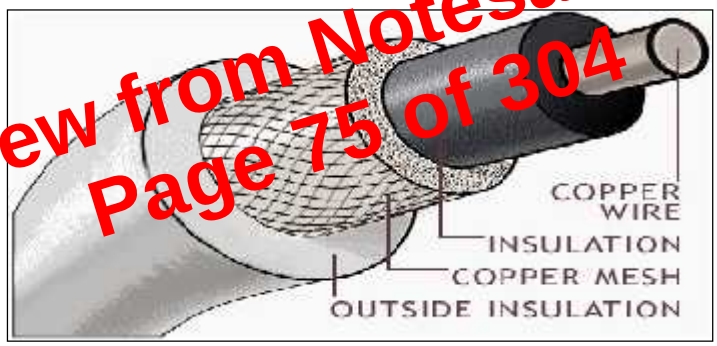
borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.



RJ-45 connector

Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield. The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.



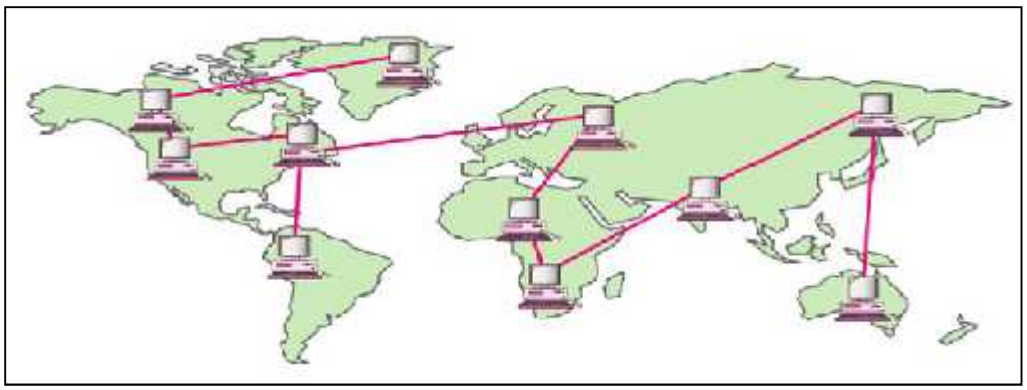
Coaxial cable

The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable has been popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the

respectively. The largest and most well-known example of a WAN is the Internet. A WAN is a data communications network that covers a relatively broad geographic area.



VI) WLAN (Wireless Local Area Network)

Wireless Local Area Networks are much like LAN networks, except they do not require network cables to connect each other. Radio and infrared signals are used to communicate between machines whilst using a wireless local area network. Wireless Local Area Networks allow for small amounts of mobility whilst being connected to the internet.

Wireless Local Area Networks work according to the IEEE 802.11 standards.

Wireless Area Networks are commonly seen being used by a WiFi internet connection. Wireless LAN connections offer a surprising amount of

Registered Jack 45 (RJ45)

The cable connector that is found on almost all UTP and STP cable s is a Registered Jack 45 which is mostly commonly referred to as RJ45. This type of connector resembles the older RJ11 connectors that most people are familiar with from wired telephones. Figure 5 below shows an example of a RJ45 connector:

Straight Tip (ST)

The Straight Tip (ST) connector is often seen on the end of a multi-mode cable; it has been commonly seen along with the SC connector for the last 20 years but is being slowly replaced by multi-fiber connectors (LC and MTP). Figure 6 below shows an example of a ST connector:

Subscriber Connector (SC)

The Subscriber Connector (SC) can be seen commonly on MMF or SMF; as with SC connectors, the ST connector is slowly being replaced by multi-fiber connectors. Figure 7 below shows an example of an SC connector:

Lucent Connector (LC)

The Lucent Connector (LC) was developed for high-density deployments where multiple fibers would be terminated within a confined space. Unlike the SC and ST connectors, the LC connector is always duplex connecting a pair of fibers at a time. Figure 8 below shows an example of a LC connector:

Multi-fiber Push On (MPO)

The Multi-fiber Push On (MPO) connector is another duplex connector that offers an easy options for connection. As the name suggests, it was designed to be able to be connected multiple times without the creation of any potential connector issues. It is often also referred to as Multi-fiber Termination Push-on (MTP); the MTP connector is a brand name (US Conec). Figure 9 below shows an example of an MPO connector:

CASE STUDY I:

Universal Bank has its registered office at Delhi. It has branches at Mumbai, Chennai, Hyderabad and Bangalore. The operating departments in the bank are Finance, Insurance, Loan, IT, Marketing, Customer Service and HR. Universal Bank uses LAN as their computer network for each department. All the branches of the bank from different cities are connected through WAN. The bank is expanding and decided to open its branches at different locations in the city.
Determine which type of network to be used within a city
Use LAN computer network for each department in the new branch. MAN can be used for connecting the different branches of the bank within the city

CASE STUDY II:

The Customer Service department of Universal bank provides online services to the customers. At Hyderabad branch, the Customer Service department network is not functioning properly. So the bank has decided to build an alternative network for that department.
Selecting the network criteria
Decide network type and configuration, number of users, speed of the network, hardware to be used, operating system to be installed and anti-virus software

CASE STUDYIII:

Pune branch of the Universal bank has built an insurance department in such a way that each device is connected to one another. This department consists of seven agents. It is required that agents should handle only

4.4 DESCRIPTION OF OSI LAYERS[31]

The OSI model divides the complex task of computer-to-computer communications, traditionally called ***internetworking*****,** into a series of stages known as *layers*. Layers in the OSI model are ordered from lowest level to highest. Together, these layers comprise the OSI stack. The stack contains seven layers in two groups:

Upper layers:-			
7. Application	6.Presentation	5. Session	
Lower layers:-			
4. Transport	3. Network	2. Data link	1. Physical

The Open Systems Interconnect (OSI) model has seven layers. This article describes and explains them, beginning with the 'lowest' in the hierarchy (the physical) and proceeding to the 'highest' (the application). The layers are stacked this way:

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

PHYSICAL LAYER

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

- **Data encoding**: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It

[31] https://support.microsoft.com/kb/103884

- Logical-physical address mapping: translates logical addresses, or names, into physical addresses.

ARP matches a MAC Address to an IP address and Routers make forwarding decisions based on IP addresses. If an attacker wants to cause problems when they are physically located within the network then they can ARP cache poison, but what if they are outside of the network? They can use routers. Port scanning is often an attacker's first probe of your network.[33]

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

- Message segmentation: accepts a message from the session layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
- Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.
- Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.
- Port Addressing
- Error control
- Flow Control

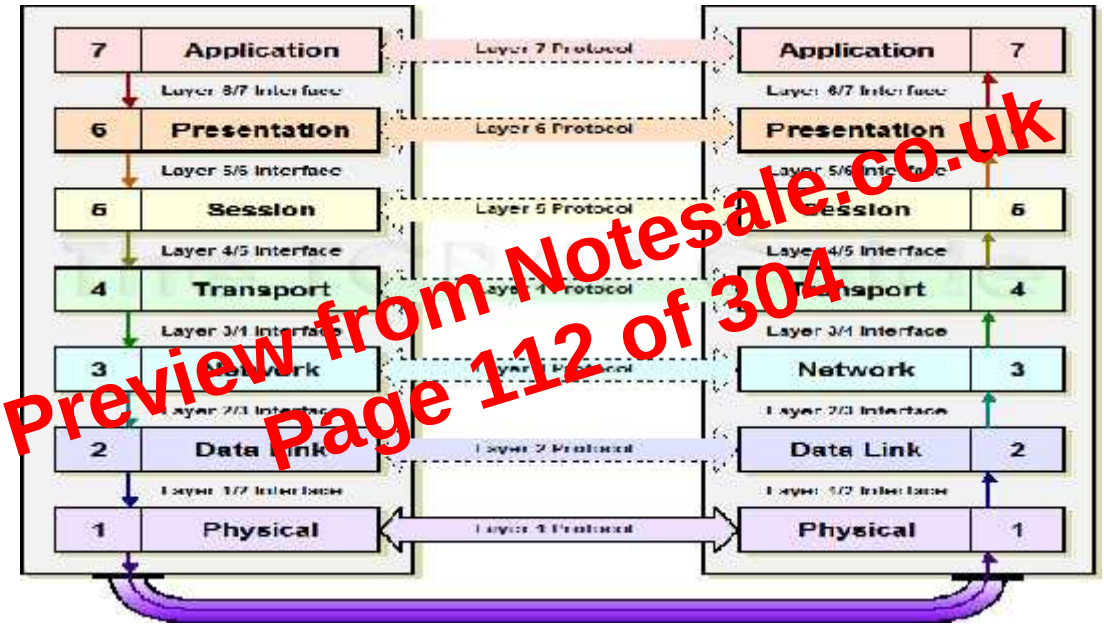
The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries.

Port scanning is often an attacker's first probe of your network.

APPLICATION LAYER

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

- Resource sharing and device redirection
- Remote file access
- Remote printer access
- Inter-process communication
- Network management
- Directory services
- Electronic messaging (such as mail)



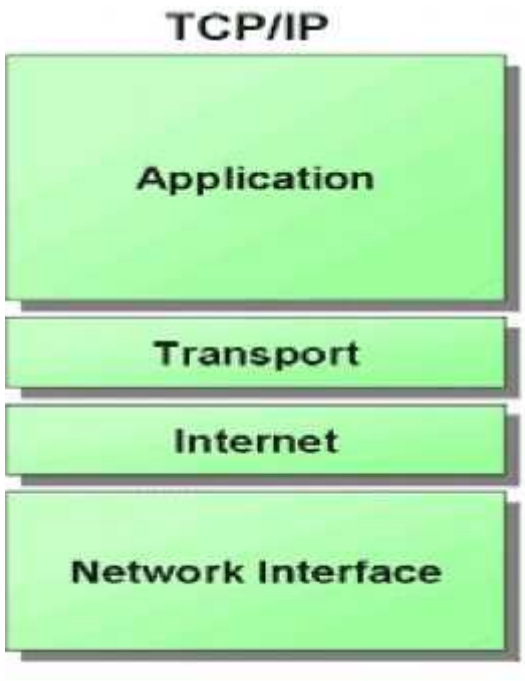
Communication between sender and receiver

Protocols used in Each Layer

Protocols are the communication standards, agreed upon ways and the language, which two computers understand in order to send and receive the data.

Layer 2: Data Link Layer protocol

- ARP : Address Resolution Protocol
- L2TP : Layer 2 Tunnelling Protocol
- SLIP : Serial Line Internet Protocol



iii

1. **Application Layer***:* Provide services to the application software running on a computer. Application layer provides an interface between software running on a computer and the network itself. Example for TCP/IP application is web browser. Example protocols are HTTP, POP3, and SMTP etc.
2. **Transport Layer***:* Consists of mainly two protocol options. Transmission control protocol (TCP) and User datagram protocol (UDP). Each layer provides a service to the layer above it. In same layer interaction on different computers, the two computers use protocol to communicate with the same layer on another computer. The protocol defined by each layer uses a header that is transmitted between the computers, to communicate what each computer wants to do. While In Adjacent layer interaction on the same computer, one layer provides a service to a higher layer. The software or hardware that implements the higher layer requests that the next lower layer perform the needed function.
3. **Internetwork Layer**: Internet protocol (IP), works much like the postal service. IP defines logical addressing so that each host computer can have a different IP address. Similarly, IP defines the process of routing so that routers can choose where to send data correctly.
4. **Network Interface Layer:** Defines the protocols and hardware required to deliver data across some physical network. The term network interface refers to the fact that this layer defines how to connect the host computer, which is not part of the network, to the network. It is the interface between the computer and network. Ethernet is one example protocol at the TCP/IP network interface layer. Ethernet

The well known ports are internet services that have been assigned a specific port. For example, SMTP is assigned 25 and HTTP is assigned 80. Services listen on the network for the request at well known ports.

Ports are used in the TCP [RFC793] to name the ends of logical connections, which carry long-term conversations. For providing services to unknown callers, a service contact port is defined. This list specifies the port used by the server process as its contact port. The contact port is sometimes called the "well-known port".

The Well Known Ports are those from 0 to 1023. Use by the application end points that communicate using the Internet's Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP). Each kind of application has a designated port number. For example, a remote job entry application has the port number of 5; the Hypertext Transfer Protocol (HTTP) application has the port number of 80; and the Post Office Protocol Version 3 (POP3) application, commonly used for e-mail delivery, has the port number of 110. When one application communicates with another application at another host computer on the Internet, it specifies that application in each data transmission by using its port number.

b) Registered ports: 1024–49151

The registered Ports are those from 1024 to 49151. Many applications need to use TCP/IP but are not specified in RFCs, or are not so universally used that they warrant a worldwide well-known port number. To ensure that these various applications do not conflict with each other, IANA uses the bulk of the overall port number range for registered port numbers. Anyone who creates a viable TCP/IP server application can request to reserve one of these port numbers, and if approved, the IANA will register that port number and assign it to the application.

These port numbers are generally accessible by any user on a system and are therefore sometimes called user port numbers. This is temporary ports, usually used by clients, and will vary each time a service is used. It is also called ephemeral ports, because they last for only a brief time. The port is then abandoned and can be used by other services.

Examples of applications with registered port numbers include Sun's NEO Object Request Broker (port numbers 1047 and 1048) and

CHAPTER 5

SERVERS

Objective

5.1 DNS
5.2 DHCP
5.3 File Server
5.4 Mail Server
5.5 Email Functioning Protocol
5.6 Email Header

5.1 Domain Name Server (DNS)

If we had to remember the IP addresses of all of the Web sites then visiting site every day is not as much possible, Human beings just are not that good at remembering strings of numbers. We are good at remembering words, however, and that is where domain names come in. You probably have hundreds of domain names stored in your head. All servers on the Internet also have human-readable names, called domain names. www.networksecurity.com is a human-readable name. It is easier for most of us to remember www.networksecurity.com than it is to remember 209.116.69.66.

The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Domain Name System: A system for converting host names and domain names into IP addresses on the Internet or on local networks that use the TCP/IP protocol. DNS uses port number 53.

The name www.networksecurity.com actually has three parts:

1. The host name ("www")
2. The domain name ("networksecurity ")
3. The top-level domain name ("com")

DNS servers are installed and maintained by private businesses and Internet governing bodies around the world. For the Internet, 13 root name servers support the hundreds of Internet top-level domains.

When your computer is connected to the Internet, the ISP (Internet Service Provider) automatically allocates primary and secondary DNS server addresses to your desktop. DNS server is a kind of telephone directory for the Internet that interprets hostname of the computer into IP address. DNS servers of ISP cannot handle traffic during major times, which results in the slow speed of the Internet or sometimes server down trouble. This problem is modified in the Free Public DNS Servers that can handle any amount of traffic at any time. There are multiple servers, if one breaks down; other is ready to operate for you. The lists of Top 5 Free Public DNS Servers are given below:

1. Google Public DNS Server
2. Open DNS
3. Norton DNS Server
4. Comodo Secure DNS
5. DNS Advantage[vii]

CASE STUDY I: Hackers Exploiting SNMP Clients Using Google's Public DNS Server Spoofed IP (8.8.8.8)

On 15th September 2014, SANS ISC reported that hackers are using Google's Public DNS Server IP (8.8.8.8) to launch SNMP amplification DDoS attack against vulnerable devices available on the Internet. These packets actually do not originate from Google's server but these are crafted or spoofed packets where the source IP is changed or translated to Google's IP to make it look authentic as 8.8.8.8 is a widely used Public DNS server and even network experts will mistakenly consider it as genuine traffic. [viii]

CASE STUDY II: DoS Attack Knocks out Microsoft Sites Hackers Geared DoS Attack to Target DNS Switch.

January 25, 2001 - Microsoft's Web site was brought down by a powerful Denial of Service (DoS) attack. The DoS attack began in the morning and extended through the afternoon, making the company's Web page intermittently unavailable to customers. Due to the magnitude and security issues, the FBI was brought in to take care of the case.
In the past, DoS attacks did not have enough power to take down the Domain Name Service (DNS) servers of a huge company such as Microsoft.

Security Tip

Basic **VoIP architecture** elements such as phones, servers, and PBXs rely heavily on your supporting **network infrastructure** (DHCP, DNS, TFTP, and so on). If one of those support elements is attacked or taken offline, a side effect may be that VoIP applications are crippled or severely limited in usability.
Many VoIP phones are configured, by default, to request an IP address dynamically every time they are turned on or rebooted. If the **DHCP server** is **unavailable** at the time they boot up, or the maximum number of IP addresses have already been allocated by that DHCP server, then the phone might not be **usable on the network**.[41]

There are two types of DHCP attack; they are **DHCP starvation Attack** and **DHCP rogue attack**. In DHCP starvation attack, a malicious user sends numerous DHCP request with spoofed MAC address. This causes a Denial of Service at DHCP server, thus not allowing an authentic user from using the network. It can be avoided by limiting the number of MAC address.

In DHCP rouge attack, a malicious user acts as if he is a DHCP server and provides a reliable user with Wrong gateway, Wrong DNS and Wrong IP. The user will experience numerous problems ranging from connection problem to communication problems with other host. This can be avoided by using a multilayer switch which got a capability to drop the packets.[42]

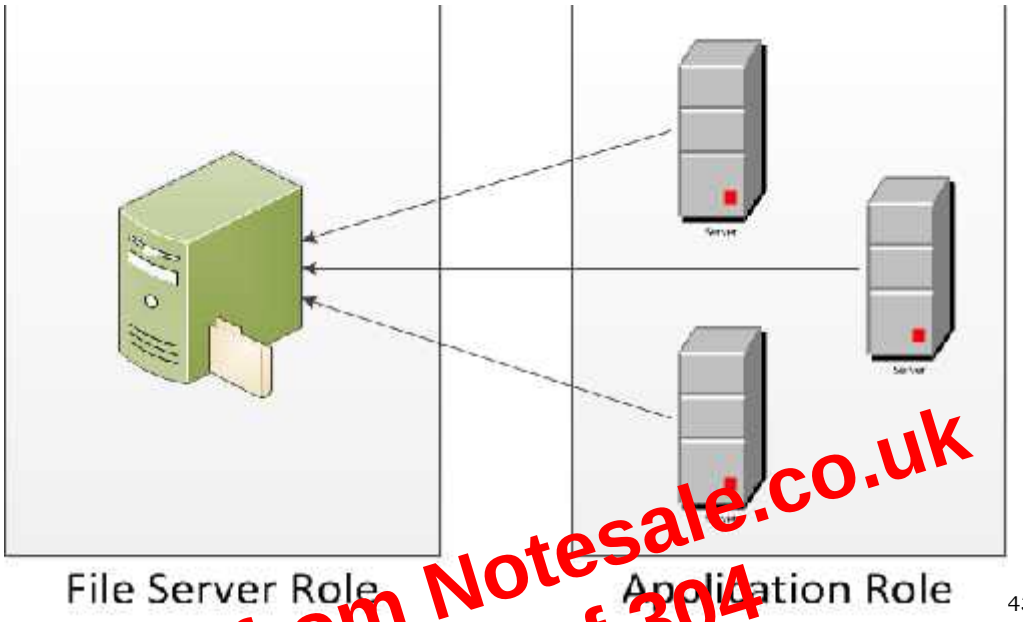
5.3 FILE SERVER

File server is a computer attached to a network that has the primary purpose of providing a location for the shared storage of computer files such as documents, sound files, photographs, movies, images, databases, etc. that can be accessed by the workstations that are attached to the computer network.

In the client/server model, a file server is a computer responsible for the central storage and management of data files so that other computers on the same network can access the files. A file server allows users to share information over a network without having to physically

[41] http://flylib.com/books/en/2.351.1.36/1/
[42] http://resources.infosecinstitute.com/vlan-hacking/

transfer files by floppy diskette or some other external storage device. Any computer can be configured to be a host and act as a file server. In its simplest form, a file server may be an ordinary PC that handles requests for files and sends them over the network.



[43]

In a more sophisticated network, a file server might be a dedicated network-attached storage (NAS) device that also serves as a remote hard disk drive for other computers, allowing anyone on the network to store files on it as if to their own hard drive. A program or mechanism that enables the required processes for file sharing can also be called a file server. On the Internet, such programs often use the File Transfer Protocol (FTP).

The administrator can configure the machine to be a dedicated fileserver; which would mean that the machine will only be used as a fileserver. Also, a non-dedicated fileserver; which would allow the fileserver to be used simultaneously as a workstation. File servers provide the ability to back up data with ease as everything is stored on one computer. Quotas can be set so that each user will have a certain amount of space on which he/she can save data.

[43] https://encryptedtbn2.gstatic.com/images?q=tbn:ANd9GcQJ40JURxf3MEf6wtsqdiODzZfSMyQl30AtRHhKGYVo0Ga4FA-tTA

5.4 MAIL SERVER

Email is one of the best known and most widely used services across the Internet. It allows users to send text messages, files, pictures, music, videos and other media to anyone else who has an email address no matter where they're located in the world. Email is usually a bundled feature with many Internet service providers or web-hosting domains.

A mail server is an application that receives incoming e-mail from local users and remote senders and forwards outgoing e-mail for delivery. A computer dedicated to running such applications is also called a mail server. Microsoft Exchange, qmail, Exim and sendmail are among the more common mail server programs.

EMAIL FUNCTIONING PROTOCOL

Mail servers can be broken down into main categories: **Web Based** Email, **POP3** Email Servers, **SMTP** Mail Servers, **IMAP4** Email servers. Outgoing mail servers are known as SMTP, or Simple Mail Transfer Protocol, servers. Incoming mail servers come in two main varieties. POP3, or Post Office Protocol version 3, servers are best known for storing sent and received messages on PCs. The SMTP server listens on well-known port number 25, POP3 listens on port 110 and IMAP uses port 143.

- **Web-Based Email**

This may be the type of email that most users are familiar with. Many free email providers host their servers as web-based email. This allows users to log into the **email server** through the use of an **Internet browser** to send and receive their mail. It is useful for people on the go since they can check their email anywhere they have access to the Internet.

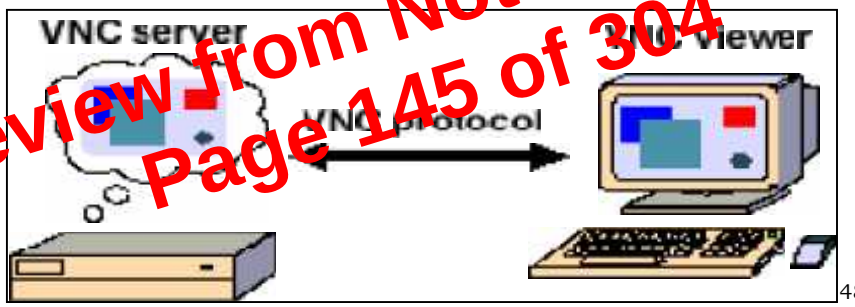
Given that you have an e-mail client on your machine, you are ready to send and receive e-mail. All that you need is an e-mail server for the client to connect. Let us imagine what the simplest possible e-mail server would look like in order to get a basic understanding of the process.

applications, however, are generally regarded as slower and offering fewer features and security options than Windows Remote Desktop.[46]

VNC works on a **client/server** model. A VNC viewer (or client) is installed on the local computer and connects to the server component, which must be installed on the remote computer. The server transmits a duplicate of the remote computer's display screen to the viewer. It also interprets commands coming from the viewer and carries them out on the remote computer. It is based on the concept of a **Remote Frame Buffer** or *RFB*.

The protocol simply allows a server to update the frame buffer displayed on a viewer. Because it works at the frame buffer level, it is potentially applicable to all operating systems, windowing systems and applications. This includes X/Unix, Windows 3.1/95/NT and Macintosh, but might also include PDAs, and indeed any device with some form of communications link. The protocol will operate over any reliable transport such as TCP/IP.

VNC is platform independent and is compatible with any operating system. Computers must be networked with TCP/IP and have open ports allowing traffic from the IP addresses of devices that may need to connect. [47]



[48]

This is truly a "**thin-client**" protocol; it has been designed to make very few requirements of the viewer. In this way, clients can run on the widest range of hardware, and the task of implementing a client is made as simple as possible. [49]

VNC was created as an open source research project in the late 1990s. Since that time, several mainstream remote desktop solutions have been created based on VNC. The original development team produces the Real VNC package. Other popular derivatives are explained as follows:

[46] http://compnetworking.about.com/od/softwareapplicationstools/g/bldef_vnc.htm
[47] http://searchnetworking.techtarget.com/definition/virtual-network-computing
[48] http://ayesha.phys.virginia.edu/~bryan/vnc/clientserver.gif
[49] http://www.hep.phy.cam.ac.uk/vnc_docs/howitworks.html

Remote Assistance is designed to have an **expert** user provide assistance to a **novice** user. The 'expert' and 'novice' terms are used to describe assistor (expert) and assisted (novice). When assisting a novice user, the expert can used text- based chat built into Remote Assistance. The expert can also take control of a novice user's desktop (with permission).

There are **two ways** to get help by using Windows Remote Assistance. If both you and your helper are running Windows 7, Windows 8, or Windows RT on your computers, you can use **Easy Connect**. Otherwise, use an **invitation file**.[58]

CASE STUDY III: Custom Manufacturer of Stone Products Improves Productivity by 30 Percent

Lido Stone Works, a custom manufacturer of stone products, wanted a more automated production environment, so it asked to a well-known machinery manufacturer, for help. Lido decided to implement an intelligent system from Breton and Microsoft that connects manufacturing equipment with central servers. The solution includes ASEM Ubiquity software based on Windows Embedded. As a result, Lido has increased revenue by 70 percent and productivity by 30 percent while Breton has cut travel costs by approximately €400,000 (US$524,000) by assisting customers remotely. Most importantly, the solution is helping Lido realize its potential for innovation.[59]

[58] http://blogs.msdn.com/b/securitytipstalk/archive/2013/09/26/remote-assistance-101.aspx
[59] http://www.microsoft.com/casestudies/Case_Study_Detail.aspx?CaseStudyID=710000002834

Other **P2P file-sharing** programs are:

- FrostWire
- BearShare
- eMule

➢ Email

For decades, files have been transferred from person to person over a network using email software. Emails can travel across the Internet or within a company's intranet. Like FTP systems, email systems use a client/server model. The **sender and receiver** may use different **email software** programs, but the sender must know the recipient's email address, and that address must be configured to allow the incoming mail.

Email systems are designed for **transferring small amounts** of **data** and generally limit the size of individual files that can be shared. These are some common Email file-sharing programs are as below:

- sendgrid
- WetTransfer
- Dropsend
- Binfer

➢ Online Sharing Services

Finally, numerous Web sites built for personal and/or community file sharing exist on the Internet. Members post or upload their files to the site using a Web browser, and others can then download copies of these files using their browser. Some community file sharing sites charge member fees, while others are free (advertising supported). Providers often tout the cloud storage technology advantages of these services, although available storage space tends to be limited, and having too much personal data in the cloud is a concern for some consumers.[62]

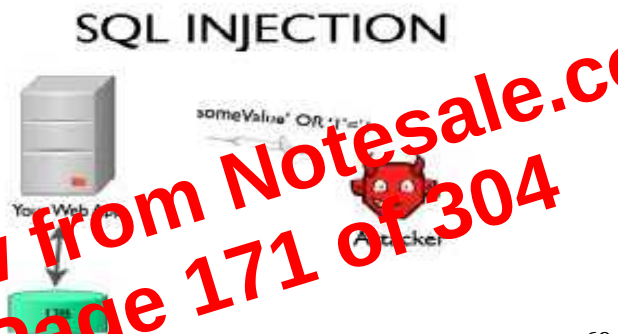
- Streamfile
- Wikisend
- PipeBytes

[62] http://compnetworking.about.com/od/basicnetworkingconcepts/a/file_sharing.htm

3. SQL Injection:

A SQL injection attack consists of **insertion or "injection"** of a SQL query via the input data from the client to the application. A successful SQL injection **exploit** can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system.

SQL injection is a code injection technique that exploits a security vulnerability occurring in the database **layer of an application**. The vulnerability is present when **user input** is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.



[69]

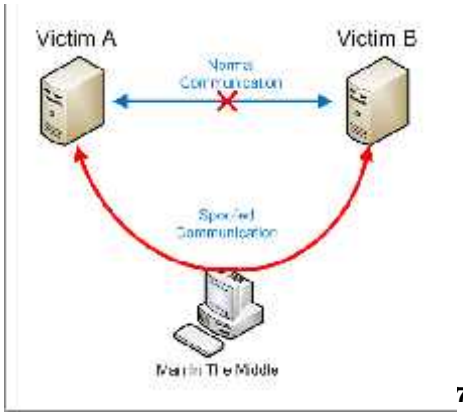
Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker. The primary form of SQL injection consists of direct insertion of code into user-input variables that are concatenated with SQL commands and executed.

4. DNS poisoning:

This is an attack where DNS information is falsified. The attacker will send **incorrect DNS information** which can cause traffic to be diverted. The DNS information can be falsified since name servers do not verify the source of a DNS reply. When a DNS request is sent, an attacker can send a false DNS reply with additional bogus information which the requesting DNS server may cache. This attack can be used to

[69] http://blog.hostonnet.com/wp-content/uploads/2014/08/sql-injection.jpg

- **MITM:**



[73]

In **eavesdropping**, an attacker simply listens to a set of transmissions to and from different hosts even though the attacker's computer isn't party to the transaction.

Many relate this type of attack to a leak, in which sensitive information could be disclosed to a third party without the legitimate users' knowledge. Manipulation attacks build on the capability of eavesdropping by taking this unauthorized receipt of a data stream and changing its contents to suit a certain purpose of the attacker perhaps spoofing an IP address, changing a MAC address to emulate another host, or some other type of modification.

To prevent an eavesdropping attack, one must encrypt the contents of a data transmission at several levels, preferably using SSH, SSL, or IPSec.

Otherwise, large amounts of traffic containing private information are passed through thin air, just waiting for an attacker to listen in and collect the frames for further illegitimate analysis.

[73] http://www.valencynetworks.com/images/mitm-attack1.png

8.4. HARDWARE LEVEL ATTACK

Hardware hacking and **reverse engineering** techniques commonly used against electronic products and embedded systems.

The risk of acquiring **hardware components** with a **backdoor** is concrete. Asian governments aren't exclusively accused of stealthily designing backdoors. Recently, **Edward Snowden revealed** that the NSA requested that the US manufacture to plant a backdoors in exported products.

Malicious hardware modifications from insiders represent a serious threat. System complexity, the large number of designers and engineers involved in every project and the delocalization of production in risky countries due to low cost poses a security threat.

A malicious individual could alter a small component in the overall system for **espionage** or **sabotage**. Such attacks can be especially devastating in security-critical industries, such as the military.

The introduction of hardware Trojans could happen in each phase of the supply chain, depending on the methods adopted by attackers and on the technology used for hacking.

Common hardware attacks include:

- Manufacturing backdoors, for malware or other penetrative purposes; backdoors aren't limited to software and hardware, but they also affect embedded radio-frequency identification (RFID) chips and memory.
- Eavesdropping by gaining access to protected memory without opening other hardware inducing faults, causing the interruption of normal behavior.
- Hardware modification tampering with invasive operations; hardware or jail broken software.
- Backdoor creation; the presence of hidden methods for bypassing normal computer authentication systems.
- Counterfeiting product assets that can produce extraordinary operations and those made to gain malicious access to systems.

CHAPTER 9

COMMON NETWORK SECURITY SOLUTION

Objective

9.1 Firewall
9.2 IDS/IPS
9.3 DMZ
9.4 Proxy Server
9.5 Honey Net
9.6 Antivirus
9.7 Windows Defender
9.8 Biometric Devices

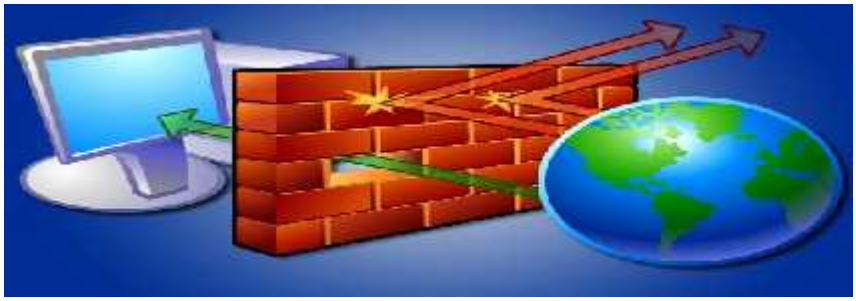
9.1 FIREWALL

Introduction to firewall

Basically, a **firewall** is a barrier to keep destructive forces away from your property. A firewall is a part of a computer system or network that is designed to **block unauthorized** access while permitting outward communication.

It is also a device or set of devices configured to **permit**, **deny**, **encrypt**, **decrypt**, or **proxy** all computer traffic between different security domains based upon a set of rules and other criteria. Firewalls can be implemented in both **hardware** and **software**, or a combination of both.

A firewall is a term used to describe a device or application that will control and restrict data transfers between a computer system and internet connection. [74]



[74] en.wikibooks.org/wiki/Network_Plus.../**Devices**/Common_**Devices**

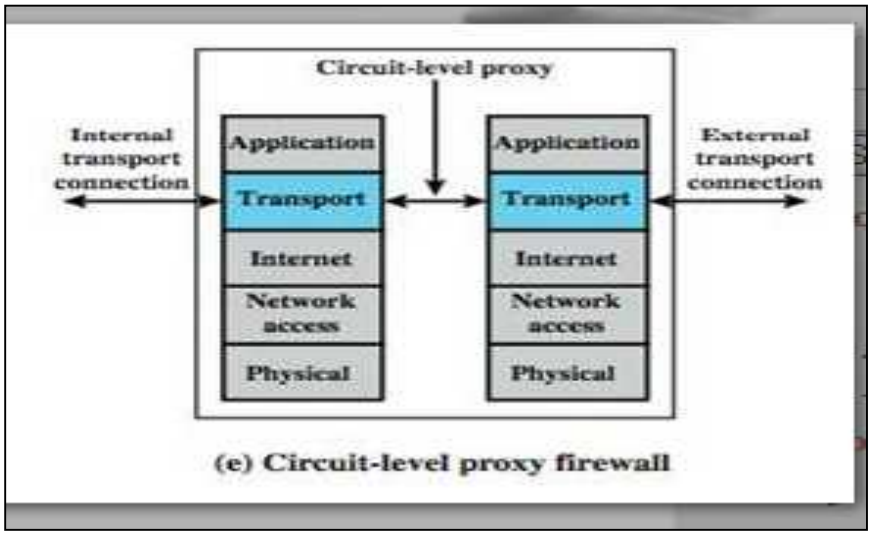
As it works on the application layer, it may inspect the contents of the traffic, blocking what the firewall administrator views as inappropriate content, such as certain websites, viruses, and attempts to exploit known logical flaws in client software, and so forth. An application layer firewall does not route traffic on the network layer. All traffic stops at the firewall which may initiate its own connections if the traffic satisfies the rules.

iv) Circuit Gateways

Also called a "Circuit Level Gateway," this is a firewall approach that validates connections before allowing data to be exchanged.

What this means is that the firewall doesn't simply allow or disallow packets but also determines whether the connection between both ends is valid according to configurable rules, then opens a session and permits traffic only from the allowed source and possibly only for a limited period of time. Whether a connection is valid may for examples be based upon:

- destination IP address and/or port
- source IP address and/or port
- time of day
- protocol
- user
- password



(e) Circuit-level proxy firewall

method in which companies can save significant sums over traditional ways of connecting remote offices and workers.

iv. Allow content filtering

Content Filtering can help organizations increase productivity and reduce legal and privacy risks by automatically enforcing acceptable Internet use policies at the Internet gateway. Businesses requiring Internet use policies can implement them on a firewall with content filtering capability.

vi) Network protection

Connecting any computer to the Internet can be extremely dangerous. If the operating system is not configured correctly, have vulnerabilities. Given the rapid increase in the number of 'always on' and broadband Internet connections, the need for enhanced network security has increased dramatically. A router running Network Address Translation (NAT) is a good option to provide some security, but not in all circumstances. For enhanced protection, particularly where NAT cannot be used implementing a firewall is vital.

vii) Preventing attacks

The fundamental purpose of a firewall is to protect against attacks from the Internet. There are many different ways of attacking a network such as: Hacker/Cracker attacks whereby a remote Internet user attempts to gain access to a network, usually with the intention to destroy or copy data. There is also Denial of Service (DoS) and distributed DoS attacks resulting in loss of services such as email, Internet connectivity or causing servers to run almost at a standstill. A correctly configured firewall will prevent most attacks and may use a combination of the following processes to offer protection:

- Stealth the network. This is a process whereby the firewall effectively 'hides' the protected network so that it does not appear on the Internet.
- Stateful Packet Inspection. Stateful packet inspection technology analyses each packet as it travels through the firewall to make sure it is legitimate and that the source and destination of each packet are valid.

firewall can do nothing about this. It's really a people-management problem, not a technical problem.

iii) A firewall can't protect against completely new threats

A firewall is designed to protect against known threats. A well-designed one may also protect against new threats. (For example, by denying any but a few trusted services, a firewall will prevent people from setting up new and insecure services.) However, no firewall can automatically defend against every new threat that arises. Periodically people discover new ways to attack, using previously trustworthy services, or using attacks that simply hadn't occurred to anyone before. You can't set up a firewall once, and expect it to protect you forever.

iv) A firewall can't protect against viruses

Firewalls can't keep PC and Macintosh viruses out of a network. Although many firewalls scan all incoming traffic to determine whether it is allowed to pass through to the internal network, the scanning is mostly for source and destination addresses and port numbers, not for the details of the data. Even with sophisticated packet filtering or proxying software, virus protection in a firewall is not very practical. There are simply too many types of viruses and too many ways a virus can hide within data.

Detecting a virus in a random packet of data passing through a firewall is very difficult; it requires:

- Recognizing that the packet is part of a program
- Determining what the program should look like
- Determining that the change is because of a virus

The most practical way to address the virus problem is through host based virus protection software, and user education concerning the dangers of viruses and precautions to take against them.

Services in DMZ

Any service that is being provided to users on the external network can be placed in the DMZ. The most common of these services are:

- Web servers
- Mail servers
- FTP servers
- VoIP servers

Web servers that communicate with an internal database require access to a database server, which may not be publicly accessible and may contain sensitive information. The web servers can communicate with database servers either directly or through an application firewall for security reasons.

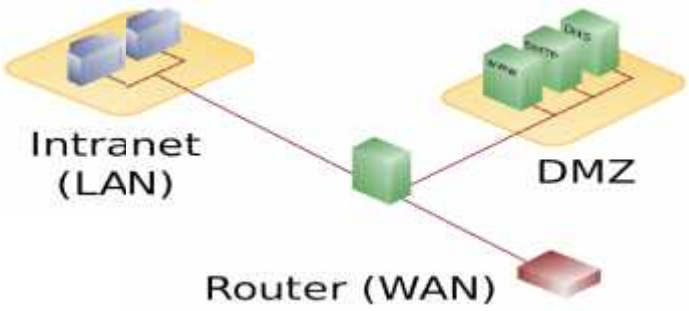
E-mail messages and particularly the user database are confidential, so they are typically stored on servers that cannot be accessed from the Internet (at least not in an insecure manner), but can be accessed from email servers that are exposed to the Internet.

The mail server inside the DMZ passes incoming mail to the secured/internal mail servers. It also handles outgoing mail.

Architecture

There are many different ways to design a network with a DMZ. Two of the most basic methods are with a single firewall, also known as the three legged model, and with dual firewalls. These architectures can be expanded to create very complex architectures depending on the network requirements.

Single firewall



- Never send your password via email or other unsecured channel
- Yes, write your password down but don't leave the paper lying around, lock the paper away somewhere, preferably off-site and definitely under lock and key.
- Be very careful when entering your password with somebody else in the same room.

PASSWORD POLICY

The best practices approach for the password you have to set the account policy. Some useful option of password policy explained as below

- **Enforce password history**

This policy setting determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows XP is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the **Minimum password age** setting to prevent users from repeatedly changing their password.

- **Maximum password age**

Values for this policy setting range from 1 to 999 days. (You may also set the value to 0 to specify that passwords never expire.) This policy setting defines how long a user can use their password before it expires. The default value for this policy setting is 42 days. Most passwords can be cracked; therefore, the more frequently the password is changed the less opportunity an attacker has to use a cracked password. However, the lower this value is set, the higher the potential for an increase in calls to help desk support.

- **Minimum password age**

This policy setting determines the number of days that a password must be used before a user may change it. The range of values for this policy setting is between 1 and 998 days. (You may also set the value to 0 to allow immediate password changes.) The default value for this policy setting is 0 days.

and a second factor to corroborate identity. The second factor could be an access code, a PIN or even a biometric reading.

In computer systems, an access control list contains a list of permissions and the users to whom these permissions apply. Such data can be viewed by certain people and not by other people and is controlled by access control. This allows an administrator to secure information and set privileges as to what information can be accessed, who can access it and at what time it can be accessed.[91]

Data Access: Protecting Your Data

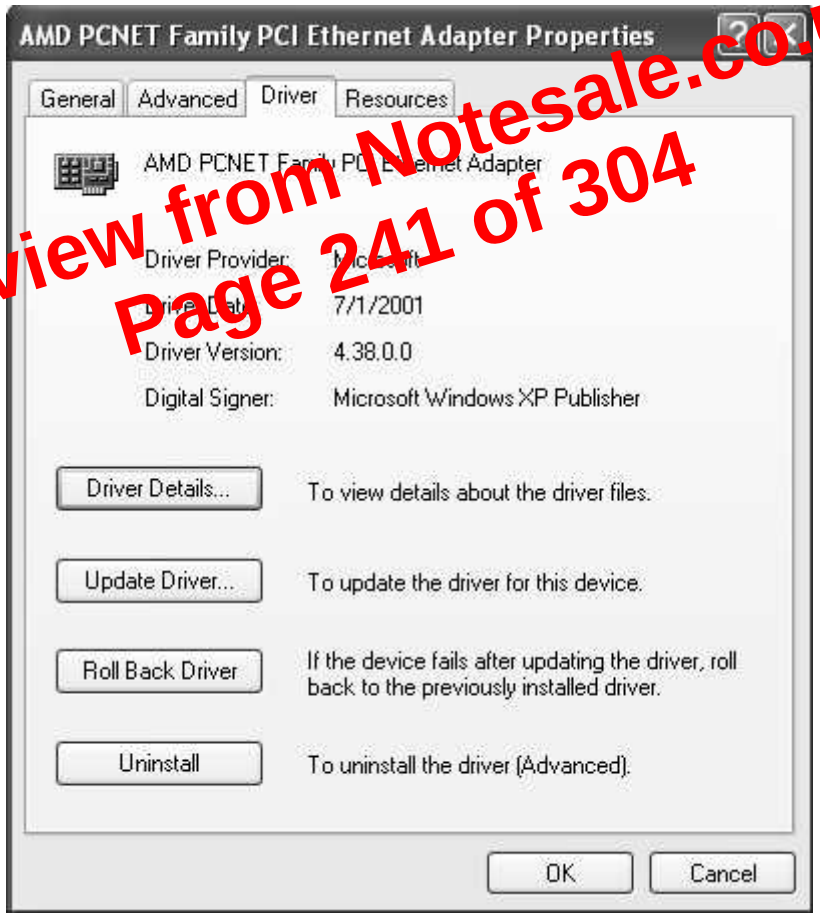
The second important way in which a system provides computer security is by controlling access to the data stored in a system: Who can read your files? Who can change your files? Can you decide to share your data with other users? How does the system make decisions about access control? If you work alone on a PC, you don't need to worry about access controls. You own all of your files and you can read and write them as you wish. If you want to share a file with someone, you can copy it onto a diskette and hand it over. With shared computers, it isn't as easy. As soon as you begin to work on a system that supports multiple users, you'll have to start worrying about data protection and access controls. You may not want every user in the system to be able to read your files. You certainly won't want them to change your files.

There are two basic types of access controls that provide different levels of protection to the files in your system: discretionary access control and mandatory access control. With **discretionary access control** (DAC) you decide how you want to protect your files, and whether to share your data. With the more complex **mandatory access control** (MAC) the system protects your files. Discretionary access control (DAC) is an access policy that restricts access to files (and other system objects such as directories and devices) based on the identity of users and/or the groups to which they belong. In contrast to mandatory access control, in which the system controls access, DAC is applied at your own discretion. With DAC, you can choose to give away your data; with MAC, you can't.

[91] http://www.techopedia.com/definition/5831/access-control

You can also use the Update Driver option to reinstall drivers for a device that has ceased to function correctly because of a driver problem. If updating the drivers does not successfully restore device functionality, consider removing the device by using Device Manager and then restarting the computer. If the device supports Plug and Play, Windows will recognize the device when the computer restarts. Non–Plug and Play devices require manual reinstallation.

- Revert to a previous version of a driver by clicking the Roll Back Driver button. This feature restores the last device driver that was functioning before the current driver was installed. Windows supports driver rollback for all devices except printers. In addition, driver rollback is available only on devices that have had new drivers installed. When a driver is updated, the previous version is stored in the %systemroot%\system32\reinstall backup's folder.

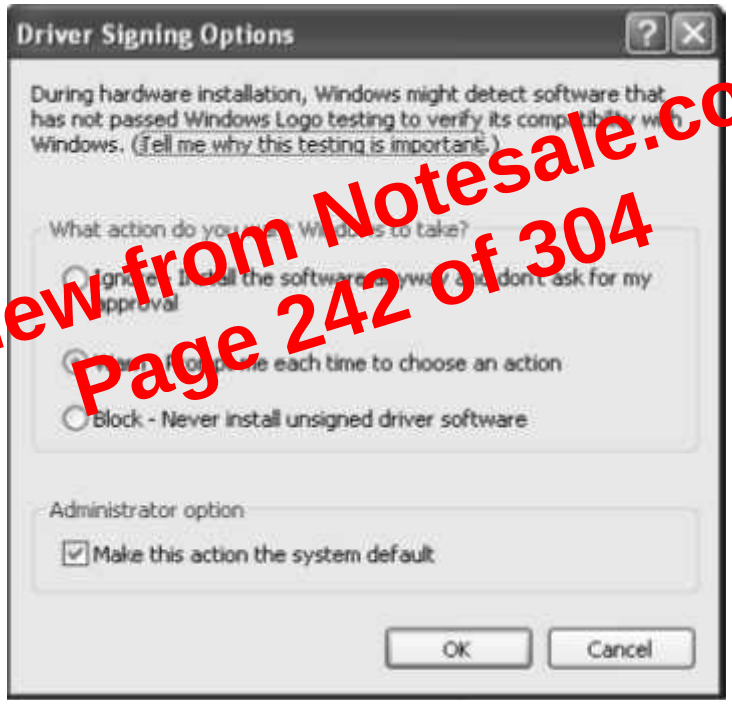


- Remove the device from the computer by clicking the Uninstall button.

How to Configure and Monitor Driver Signing?

Hardware drivers can often cause a computer running Windows to become unstable or to fail entirely. Windows implements driver signing as a method to reduce the likelihood of such problems. Driver signing allows Windows XP to identify drivers that have passed all Windows Hardware Quality Labs (WHQL) tests, and have not been altered or overwritten by any program's installation process.

To configure how the system responds to unsigned files, click System in the Performance and Maintenance window in Control Panel. In the System Properties dialog box, on the Hardware tab, click Driver Signing to open the Driver Signing Options dialog



You can configure the following three driver signing settings:

- Ignore This option allows any files to be installed regardless of their digital signature or the lack thereof.
- Warn This option, the default, displays a warning message before allowing the installation of an unsigned file.
- Block this option prevents the installation of unsigned files.

Manager. At this point, you can continue the download otherwise the download is cancelled and removed automatically.

- **In Private Browsing**

Sometimes we don‘t want to leave a trace of their web browsing activity on their computers. Whether it‘s shopping for a gift on a shared computer or checking email at an Internet café, there are times when you don‘t want to leave any evidence of your browsing or search history for others to see.

Microsoft InPrivate Browsing helps prevent browsing history, temporary Internet files, form data, cookies, usernames, and passwords from being retained by the browser. You can start InPrivate Browsing from the New Tab page, from the Internet Explorer Jump List, or by selecting InPrivate Browsing from the Safety menu. Internet Explorer will launch a new browser session that won‘t record any information including web pages that you visit and searches that you perform. Closing the browser window ends the InPrivate Browsing session.

2. MOZILLA FIREFOX

Mozilla Firefox is one of the best browsers out there on the market, and it's free. Through the unique development methods of Open Source, the Mozilla Foundation and contributors are able to make a product with impressive speed and fewer bugs than programs developed by traditional methods. Mozilla Firefox has a number of unique features, and it is overall a good product.

SECURITY FEATURES OF FIREFOX

- **Browse with Security**

Whether it's buying a gift, paying your bills or simply signing in to Facebook, it's important keep your personal info out of the hands of any online bad guys who might be snooping around. Fortunately, Firefox is packed with advanced security features to help you stay safe.

- **Instant website ID**

The Site Identity Button is a Firefox security feature that gives you more information about the sites you visit. Using the Site Identity Button, you can find out if the website you are viewing is encrypted, if it is verified, who owns the website, and who verified it. This should help you avoid malicious websites that are trying to get you to provide important information. The Site Identity Button is in the Location bar to the left of the web address.

When viewing a website, the Site Identity Button will display in one of three colours - gray, blue, or green. Clicking on the Site Identity Button will display security information about the website, with a matching gray, blue, or green "**Passport Officer**" icon.

- Gray - No identity information
- Blue - Basic identity information
- Green - Complete identity information

- **Do-Not track**

  Firefox has a Do-not-track feature that lets you tell websites you don't want your browsing behaviour tracked.

- **Securing website connections**

  Firefox keeps attackers from intercepting your sensitive data by automatically establishing secure connections to websites that offer secure https servers.

3. GOOGLE CHROME

Google Chrome has been steadily gaining in the browser market share since its launch 3 years ago. It's not without its flaws but it definitely falls in the "kind a cool" category.

Chrome has a lot of obscure features which could immensely enhance one's browsing productivity if he were to know about them. This post intends to do reveal exactly those features.

SOME OF THE IMPORTANT SECURITY FEATURES OF CHROME

õ **Incognito mode**

For times when you want to browse in stealth mode, Google Chrome offers the incognito browsing mode.

WebPages that you open and files downloaded while you are incognito aren't recorded in your browsing and download histories. All new cookies are deleted after you close all incognito windows that you've opened. Changes made to your Google Chrome bookmarks and general settings while in incognito mode are always saved.

- **Pop-ups** are blocked by default from appearing automatically and cluttering your screen.
- **Location requests**: Google Chrome alerts you by default whenever a site wants to use your location information
- **Notifications**: Some websites, such as Google Calendar, can show notifications on your computer desktop. Google Chrome alerts you by default whenever a site wants permission to automatically show notifications.

Click **Manage exceptions** in any section to customize how resources for specific websites should be handled. Want to add a site to the exceptions list? You can enter hostnames and IP addresses, as well as specific domain masks (e.g. enter [*.]Google.com to match everything from google.com and www.google.com, but not othergoogle.com).

õ **UNDERSTANDING OTHER DATA SENT BY THE BROWSER**

It only communicates with Google services where absolutely necessary to deliver features and functionality. You can disable features that require this kind of communication in Chrome's options so you are in control of what is sent to Google when you use Chrome.

- **Safe browsing**

Chrome will show you a warning message before you visit a site that is suspected of containing malware or phishing.

- **Advanced security settings**

Google Chrome has security measures in place to help protect you as you browse the web. Follow these steps to adjust these settings:

i) Click the wrench icon  on the browser toolbar.
ii) Select Settings.

Feature of Digital Signature

Sender

- Calculates Message Digest.
- Encrypts digest with own Secret Key.
- Appends it to message.

Receiver

- Calculates Message Digest.
- Decrypts encrypted digest with Senders Public Key.
- Compares with calculated value.

Authenticity and Confidentiality

- A signs message with his own private key.
- A then encodes the resulting message with B's Public key.
- B decodes the message with his own Private Key.
- B applies A's Public key on the digital signature.

Authenticity and Integrity

- B needs to know that A and only A sent the message.
- B uses A's public key on the signature.
- Only A's public key can decode the message.
- A cannot repudiate his signature.
- Digital signature cannot be reproduced from the message.
- No one can alter a ciphered message without changing the result of the decoding operation.

11.5 HASH FUNCTIONS

A hash function H is a transformation that takes a variable-size input m and returns a fixed-size string, which is called the hash value h (that is, h = H(m)). Hash functions with just this property have a variety of general computational uses, but when employed in cryptography the hash functions are usually chosen to have some additional properties.[100]

The basic requirements for a cryptographic hash function are:

- the input can be of any length,
- the output has a fixed length,
- H(x) is relatively easy to compute for any given x ,
- H(x) is one-way,
- H(x) is collision-free.

A hash function H is said to be one-way if it is hard to invert, where "hard to invert" means that given a hash value h, it is computationally infeasible to find some input x such that H(x) = h.

If given a message x, it is computationally infeasible to find a message y not equal to x such that H(x) = H(y) then H is said to be a weakly collision-free hash function.

A strongly collision-free hash function H is one for which it is computationally infeasible to find any two messages x and y such that H(x) = H(y).

The hash value represents concisely the longer message or document from which it was computed; one can think of a message digest as a "digital fingerprint" of the larger document.

Perhaps the main role of a cryptographic hash function is in the provision of digital signatures. Since hash functions are generally faster than digital signature algorithms, it is typical to compute the digital signature to some document by computing the signature on the document's hash value, which is small compared to the document

[100] http://www-it.fmi.uni-sofia.bg/courses/business/flash/crypto/functions/HashFunct.htm

RedHat for servers and SuSE for workstations. However, the differences are likely to be very superficial. The best strategy is to test a couple of distributions; unfortunately not everybody has the time for this.

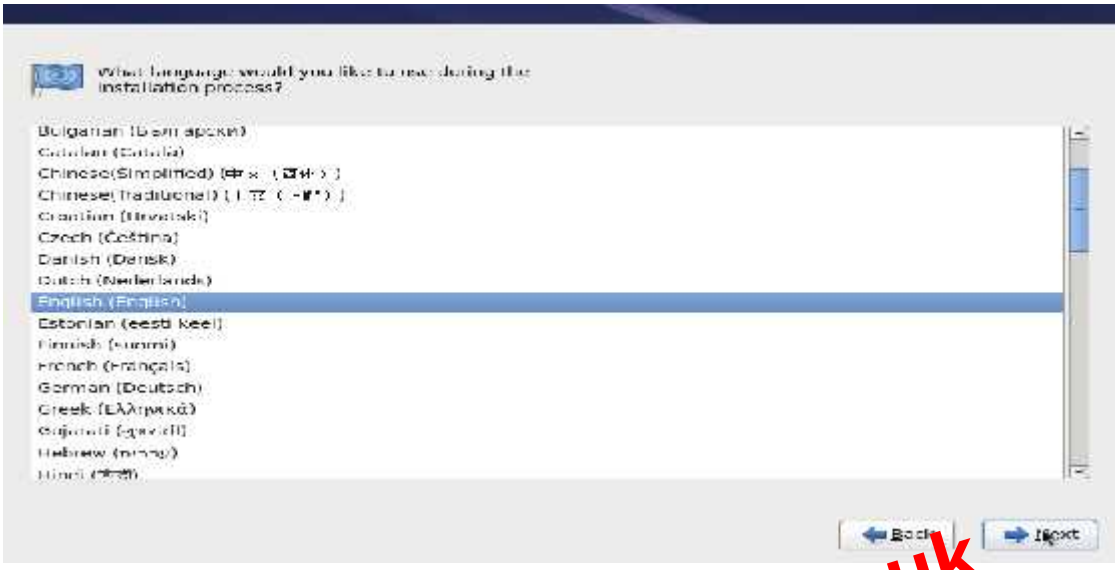
Linux is not very user friendly and confusing for beginners:

It must be said that Linux, at least the core system, is less user friendly to use than MS Windows and certainly more difficult than MacOS, but... In light of its popularity, considerable effort has been made to make Linux even easier to use, especially for new users. More information is being released daily, such as this guide, to help fill the gap for documentation available to users at all levels.

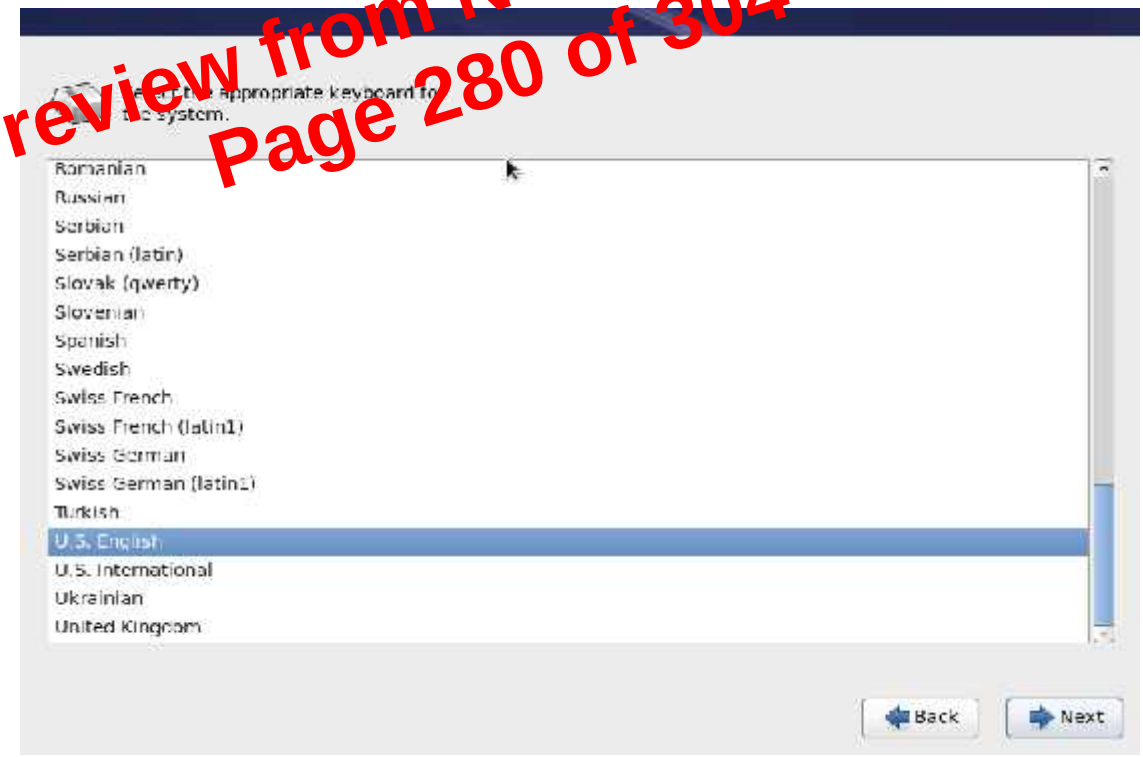
Is an Open Source product trustworthy?

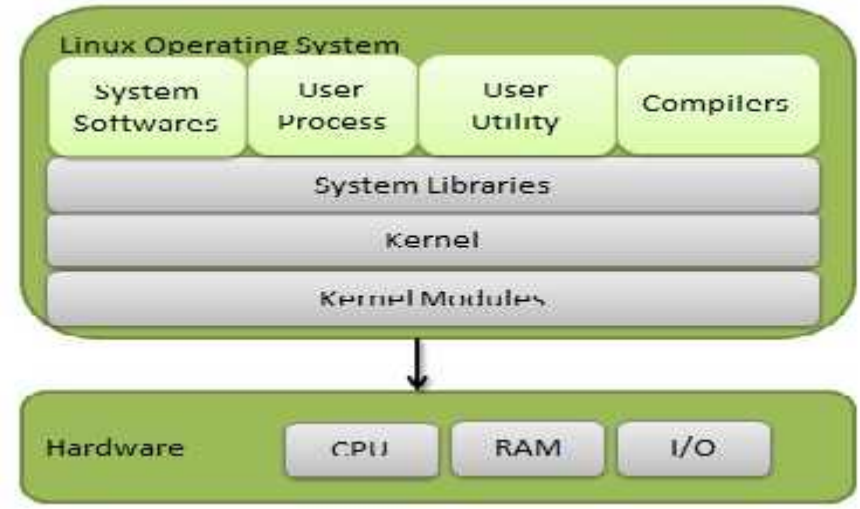
How can something that is free also be reliable? Linux users have the choice whether to use Linux or not, which gives them an enormous advantage compared to users of proprietary software, who don't have that kind of freedom. After long periods of testing, most Linux users come to the conclusion that Linux is not only as good, but in many cases better and faster that the traditional solutions. If Linux were not trustworthy, it would have been long gone, never knowing the popularity it has now, with millions of users. Now users can influence their systems and share their remarks with the community, so the system gets better and better every day. It is a project that is never finished, that is true, but in an ever changing environment, Linux is also a project that continues to strive for perfection.

Step 3- Next, we need to select the language- English or any other language as per your preference, and then press 'Next'.



Step 4- In this step, the RHEL installer would ask you about the appropriate type of keyboard for the system. We take the 'US English' keyboard; you can pick any other option depending on the type of your keyboard. Then press 'Next'.





Kernel Mode Vs User Mode

Kernel component code executes in a special **privileged** mode called **kernel mode** with full access to all resources of the **computer**. This code represents a single process, executes in single address space and do not require any context switch and hence is very efficient and fast. Kernel runs each **processes** and provides system services to processes, provides protected access to hardware to processes.

Support code which is not required to run in kernel mode is in System **Library**. User programs and other system programs works in **User Mode** which has **no access** to system hardware and kernel code. User programs/ utilities use System libraries to access Kernel functions to get system's low level tasks.

BASIC FEATURES

Following are some of the important features of Linux Operating System.

- **Portable** - Portability means **software's** can works on different types of hardware's in same way. Linux kernel and application programs support their installation on any kind of hardware platform.
- **Open Source** - Linux source code is freely available and it is **community based development** project. Multiple teams' works in collaboration to enhance the capability of Linux operating system and it is continuously evolving.

14. **ls** - lists files and directories
    a. ls / - lists the contents of the '/' mount point
    b. ls -l - lists the contents of a directory in long format:
    Includes: permissions, links, ownership, size, date, name
    c. ls -ld /etc - lists properties of the directory '/etc', NOT the contents of '/etc'
    d. ls -ltr - sorts chronologically from older to newer (bottom)
    e. ls --help - returns possible usage information
    f. ls -a - reveals hidden files. e.g. '.bash_history'

Note: files/directories prefixed with '.' are hidden. e.g. '.bash_history'

15. **cat** - catenates files
    a. cat 123.txt - dumps the contents of '123.txt' to STDOUT
    b. cat 123.txt 456.txt dumps both files to STDOUT
    c. cat 123.txt 456.txt > 123456.txt - creates new catenated file

16. **mkdir** - creates a new directory
    a. mkdir testRH5 - creates a 'testRH5' directory

17. **cp** - copies files
    a. cp 123.txt testRH5/
    By default, 'cp' does NOT preserve the original modification time

    b. cp -v 456.txt testRH5/

18. **mv** - moves files
    a. mv 123456.txt testRH5/ - moves the file, preserving timestamp

19. **rm** - removes files/directories
    a. rm 123.txt
    b. rm -rf 456.txt - removes recursively and enforces

20. **touch** - creates blank file/updates timestamp
    a. touch test.txt - will create a zero-byte file, if it doesn't exist
    b. touch 123456.txt - will update the timestamp
    c. touch -t 200801091530 123456.txt - changes timestamp

21. **stat** - reveals statistics of files
    a. stat 123456.txt - reveals full attributes of the file

22. **find** - finds files using search patterns
    a. find / -name 'fstab'

Note: 'find' can search for fields returned by the 'stat' command

	rebooted.	cannot match the reliability of Linux.
Software	Linux has a large variety of available software programs, utilities, and games. However, Windows has a much larger selection of available software.	Because of the large amount of Microsoft Windows users, there is a much larger selection of available software programs, utilities, and games for Windows.
Software Cost	Many of the available software programs, utilities, and games available on Linux are freeware or open source. Even such complex programs such as Gimp, OpenOffice, StarOffice, and wine are available for free or at a low cost.	Although Windows does have software programs, utilities, and games for free, the majority of the programs will cost anywhere between $20.00 - $200.00+ US dollars per copy.
Hardware	Although hardware manufacturers have made great advancements in supporting Linux it still will not support most hardware devices. However, for the hardware devices that have driver support they usually work in all versions of Linux.	Because of the amount of Microsoft Windows users and the broader driver support, Windows has a much larger support for hardware devices and almost all hardware manufacturers will support their products in Microsoft Windows.
Security	Linux is and has always been a very secure operating system. Although it still can be attacked when compared to Windows, it much more secures.	Although Microsoft has made great improvements over the years with security on their operating system, their operating system continues to

		be the most vulnerable to viruses and other attacks.
Open Source	Many of the Linux variants and many Linux programs are open source and enable users to customize or modify the code however they want to.	Microsoft Windows is not open source and the majority of Windows programs are not open source.
Support	Although it may be more difficult to find users familiar with all Linux variants, there are vast amounts of available online documentation and help, available books, and support available for Linux.	Microsoft Windows includes its own help section, has vast amount of available online documentation and help, as well as books on each of the versions of Windows.