Difference between the communication and transmission.

The differences between the communication and transmission are:

Physical movement of information and concerning about bit priority, synchronization, clock etc is referred as transmission, where as full exchange of information among media of communication is referred as communication.

Transmission is all about transmitting of data to the destination, where as the dialogue between the source and destination is all about communication.

What is the difference between TFTP and FTP application layer protocols?

The differences between FTP and TFTP: *File Transfer Protocol* (*FTP*) is a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet.

Trivial File Transfer Protocol (**TFTP**) is a file transfer protocol notable for its simplicity.[*citation needed*] It is generally used for automated transfer of configuration or boot files between machines in a local environment. Compared to FTP, TFTP is extremely limited, providing no authentication, and is rarely used interactively by a user

FTP is connection oriented, where as TFTP is not.
TFTP uses error checking and flow control, where as TFTP does not cause error checking.

FTP uses TCP as transport protocol, where as TFTP uses UDP as transport protocol.
Authentication is mandatory in FTP, where as authentication is not needed in TFTP.

Just getting and putting application effectively is the design concern of TFTP, where as FTP provides more control and data connection aspects.

Difference between bit rate and baud rate.

The differences between bit rate and baud rate:

Bit rate is measured as number of data bits transmitted / second in communication channel.

Baud rate is measured as number of times a signal state is changed in a communication channel.

One change of state can transmit one bit or less than one bit which depends on modulation technique used. The bit and baud rate have the connection:

bps = baud / second x the number of bits / per baud

What are NETBIOS and NETBEUI?

Network Basic Input Output System provides session layer of OSI model related services which allows the applications on different computers for communicating over a LAN. NetBIOS runs over TCP/IP through NetBIOS over

TCP/IP (NBT) protocol. This process results in every computer in the network with NetBIOS name and an IP address that corresponds to a host name.

NetBIOS Extended User Interface is an extended version of NetBIOS. It is a program that allows computers to communicate within a local area network. NetBEUI forms the frame format which was not a specification of NetBIOS. NetBEUI is the best choice for performing communication within a LAN.

Difference between ARP and RARP.

The differences between ARP and RARP:

Address Resolution Protocol is utilized for mapping IP network address to the hardware address that uses data link protocol.

Reverse Address Resolution Protocol is a protocol using which a physical machine in a LAN could request to find its IP address from ARP table or cache from a gateway server.

IP address of destination to physical address conversion is done by ARP, by broadcasting in LAN.

Physical address of source to IP address conversion is done by RARP.

ARP associates 32 bit IP address with 48 bit physical address.

Allowing a host to disco

POP3:

All emails are to be downloaded again if used by another desktop PC for checking the email.
May leads to confusion if used for checking email in office and at home pc.
Attachments will be down loaded into desktop while the ‘check new email’ process is in progress.
Mailboxes can be created only on desktop and one mail box exists on the server.

IMAP:

There is no need for downloading all email while using another desktop PC for checking email.
Unread mail identification is easier.
Message downloading is possible only when opened for display from its contents.
Multiple mailboxes creation is possible on the desktop PC and also on the server.

What is a Transaction server?

A transaction server is software that is used for implementing transactions.
A transaction comprises of multiple steps that must automatically be completed. A transaction server consists of a safety providing system and environment where the programs can be written for making use of the features of guaranteed transactions.

What is Message Oriented Middleware (MOM)?

An infrastructure focuses on sending and receiving messages to increment interoperability, flexibility and flexibility of an application. MOM performs this by allowing an application to be distributed over platforms of different kind. MOM reduces the application development complexity which spans multiple operating systems and network protocols. This process insulates the application developer from the operating systems details and network interfaces. Various APIs across diverse platforms and networks are provided by MOM.

What is Groupware server?

Groupware server is software that allows the collaboration of users, irrespective of location through the internet or intranet to work together in an atmosphere which is virtual.

What are TP-Lite and TP-Heavy Monitors?

TP-Lite Monitor: The integration of TP monitors functions in a database engines is called as TP-Lite monitor.

TP-Heavy Monitor: A TP monitor that supports the client/server architecture and allows PC for initiating very complex multiserver transaction from the desktop.

What is LAN?

LAN is a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide-area network (WAN). Most LANs connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU with which it executes programs, but it also is able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions.

Define the term Protocol.

Protocol is a standard way of communicating across a network. A protocol is the "language" of the network. It is a method by which two dissimilar systems can communicate. TCP is a protocol which runs over a network.

Define File Transfer Protocol.

File Transfer Protocol (FTP), a standard Internet protocol, is the simplest way to exchange files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol

(SMTP), which transfers e-mail, FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It's also commonly used to download programs and other files to your computer from other servers.

Networking - What is FTP (File Transfer Protocol)? - Jan 28, 2009, 17:00 pm by Rajmeet Ghai

What is FTP (File Transfer Protocol)?

FTP is File Transfer Protocol. It used to exchange files on the internet. To enable the data transfer FTP uses TCP/IP, FTP is most commonly used to upload and download files from the internet. FTP can be invoked from the command prompt or some graphical user interface. FTP also allows to update (delete, rename, move, and copy) files at a server. It uses a reserved port no 2

Explain the 7 Layers of OSI.

Layer 1: Physical layer
It represents all the electrical and physical specifications for devices.

Layer 2: Data link layer
It provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical layer.

Layer 3: Network layer
The Network layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks.

Layer 4: Transport layer
It provides transparent transfer of data between end users.

Layer 5: Session layer
It controls the sessions between computers. It connects, manages and terminates the connections between the local and remote application.

Layer 6: Presentation layer
It transforms data to provide a standard interface for the Application layer.

Layer 7: Application layer
It provides a means for the user to access information on the network through an application.

What is a network? What are the different kinds of network? Explain them

A network is a group of computers or nodes connected together. They are connected with each other by communication paths.

Types of Networks:

LAN – Local Area Network connects a group of nodes covering a small physical area. LAN's are most commonly seen in offices, building etc. LAN's enable higher transfer rate of data, smaller coverage of area and hence less wiring.

WAN – Wide Area Network connects a group of nodes covering a wide area. WAN typically connects and allow communication between regions or national boundaries. The most common example of WAN is internet.

VPN – Virtual Private Network connects or links nodes in some larger area by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. It is used for secure communication through the public internet. VPN alone may not support explicit security features, such as authentication or content encryption.

Intranet – It is a set of networks under the control of a single administrative person. It can be considered as an internal network of an organization. If it is large, web servers are used to provide information to the users.

Extranet – It is a network that restricts itself within a single organization. It can be categorized as WAN, MAN etc. however; it cannot have a single LAN. It must have a connection (at least one) with external network.

What are network topologies? Explain Ring, Bus and Star topology.

A network topology describes the layout of a network. It describes how different nodes and elements are connected to each other. Different types of topology:

a. Ring:-

- All nodes connected with another in a loop.
- Each device is connected to one or more another device on either side.

b. Bus

- All nodes connected to a central and a common cable called as a back bone.
- In bus topology, the server is at one end and the clients are connected at different positions across the network.
- Easy to manage and install.
- If the backbone fails, the entire communication fails.

c. Star

- All nodes connected to a central hub.

- The communication between the nodes is through the hub.
- Relative requires more cables as compared to BUS. However if any node fails, it wont affect the entire LAN.

Explain IP, TCP and UDP.

TCP – Transmission control Protocol is used to establish communication between nodes or networks and exchange data packets. It guarantees delivery of data packets in the order they were sent. Hence it is most commonly used in all applications that require guaranteed delivery of data. It can handle both timeouts (if packets were delayed) and retransmission (if packets were lost). The stream of data is transmitted in segments. The segment header is 32 bit. it is a connectionless communication protocol at the third level (network) of the OSI model.

IP – Internet protocol is used for transmission of data over the internet. IP uses IP addresses to identity each machine uniquely. Message is sent using small packets. The packet contains both the sender and receivers address. IP does not guarantee the delivery in the same order as sent. This is because the packets are sent via different routes. It is a connectionless communication protocol at the third level (network) of the OSI model.

UDP – User Data Protocol is a communication protocol. It is normally used as an alternative for TCP/IP. However there are a number of differences between them. UDP does not divide data into packets. Also, UDP does not send data packets in sequence. Hence, the application program must ensure the sequencing. UDP uses port numbers to distinguish user requests. It also has a checksum capability to verify the data.

How would you define IP address?

IP address or Internet Protocol address is the address of a device attached to an IP network (TCP/IP network). It is a must for every client, server and network device to have a unique IP address for each network connection (network interface). Every IP packet contains a source IP address and a destination IP address. As a device moves from one network to another, its IP address changes.

Networking - How would you define IP address? - Jan 28, 2009 at 22:10 PM by Rajmeet Ghai

Computers using the TCP/IP for communication are uniquely identified by a 32 bit address called as an IP address. The routers use the IP address information to forward the packet to the destination computer.

IP addresses are categorized as:

Private address: these IP addresses are used exclusively within a private network and not for public to see.

Public Address: these are registered IP addresses used for public.

Each IP address has a network address and a host address. IP addresses are expressed in four sets of three numbers, separated with dots. Each set is called as an octet because when converted to binary; it denotes eight binary.

Explain the functionality of PING.

Ping Is particularly used to check if the system is in network or not. It also gives packet lost information. In windows ping command is written as ping ip_address. The output returns the data packets information. The number of packets sent, received and lost is returned by PING.

What is multicasting?

Multicasting allows a single message to be sent to a group of recipients. Emailing, teleconferencing, are examples of multicasting. It uses the network infrastructure and standards to send messages.

Explain the core naming mechanism, Domain Name System (DNS).

A Domain Name system is used to convert the names of the website on the internet to IP addresses. The domain names for each IP addresses are stored in a database that is distributed across different servers. A domain name space consists of a tree of domain names. The tree has zones. Zones consist of a collection of connected nodes. These nodes are served by a name server. A domain name is usually in the form of mydomain.com. Here, .com is the top level domain. Where as mydomain is the sub domain or subdivision. A host name is a domain name that has one or more IP addresses associated with it.

Comment on Data Encryption Standard (DES) weakness and strength.

The Data Encryption Standard (DES) is a symmetric key block cipher which takes 64-bit plaintext and 56-bit key as an input and produces 64-bit cipher text as output. The DES function is made up of P and S-boxes. P-boxes transpose bits and S-boxes substitute bits to generate a cipher.

Strength- The strength of DES lies on two facts:

- The use of 56-bit keys: 56-bit key is used in encryption, there are 256 possible keys. A brute force attack on such number of keys is impractical.
- The nature of algorithm: Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness.

Weakness- Weakness has been found in the design of the cipher:

- Two chosen input to an S-box can create the same output.
- The purpose of initial and final permutation is not clear.

If you are a victim of Denial of Service (Dos) then what you do?

The function of a denial of service attack is to flood its target machine with too much traffic and prevents it from being accessible to any other requests or providing services.

- To prevent DoS attacks firewall can be configured as a relay; in this approach the firewall responds on behalf of the internal host. During the attack, the firewall responds to the SYN sent by the attacker; since the ACK never arrives, the firewall terminates the connection.
- By Keeping protocols and Antivirus software up-to-date, we can prevent to be a victim of DoS. A regular scanning of the machine is also necessary in order to detect any "anomalous" behavior.

What are Brute Force Attacks?

Brute forcing is a mechanism which is used by an attacker to break the encryption of data by applying a set of various key. Cryptanalyst has a set of number of keys and apply them one by one to the encryption algorithm until he get the right key.

Example: http://www.xxxxx.com/online/Displaymsg.asp?msgID=78961

In this example a cryptanalyst may apply bruteforcing to the value of msgID and read the user's data.
In this the browser requesting for Displaymsg.asp page and sending msgID 78961 to the web server.

What are Brute Force Attacks?

Brute forcing is a mechanism which is used by an attacker to break the encryption of data by applying a set of various key. Cryptanalyst has a set of number of keys and apply them one by one to the encryption algorithm until he get the right key.

Example: http://www.xxxxx.com/online/Displaymsg.asp?msgID=78961

In this example a cryptanalyst may apply bruteforcing to the value of msgID and read the user's data.
In this the browser requesting for Displaymsg.asp page and sending msgID 78961 to the web server

How do you use RSA for both authentication and secrecy?

RSA is a public key encryption algorithm. The RSA algorithms are based on the mathematical part that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product.

For authentication: One can encrypt the hash (MD4/SHA) of the data with a private key. This is known as digital signature.

For Secrecy: Secrecy/confidentiality is achieved by encrypting the data with public key and decrypting with private key.

Can you differentiate among encoding, encryption and hashing?

Encoding: Basically encoding is used to protect the integrity of data as it crosses through communication network to keep its original message upon arriving. It is primarily an insecure function because it is easily reversible.

Encryption: Encryption is basically designed for confidentiality and data integrity and reversible only if you have the appropriate key.

Hashing: With hashing the operation is one-way i.e. non-reversible. It takes an input (or 'message') and returns a fixed-size string, which is called the hash value.

If you have to generate a hash function then what characteristics are needed in a secure hash function?

A secure hash function should have the following characteristics:

i. The output generated by a hash function should be of a fixed length.

ii. It should be very easy to find out a hash function for a given message.

iii. If a hash value is given of a message than it is almost impossible to get that message.

iv. The two different messages should not have the same hash value; it is against the hash function property.

What is digital signature? Differentiate between Physical and Digital Signature

A digital signature is an electronic analogue of a written signature; the digital signature can be used to provide assurance that the claimed signatory signed the information. Digital signature is used to detect the integrity of signed data. We can differentiate between physical and digital signature as:

i. Physical signature is just writing on paper but digital signature includes crucial parameters of identification.

ii. Physical signature can be coped but it is impossible to copy a digital signature.

iii. Physical signature does not give any privacy to content but digital signature enables encryption and thus privacy.

What is PIX firewall security? How does it differ from a firewall?

PIX (Private Internet Exchange)

It is a popular IP firewall and NAT (Network Address Translation) appliance.

PIX firewall security is developed by Cisco Systems.

PIX firewall is used to protect your network with a stateful packet filtering firewall.

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications.

What are Malware? Explain different types of Malware

Malware is a software program which is developed to destroy a computer system. These programs runs in victim's computer without any information to the victim, i.e. victim do not know that someone hacked his system.

Different types of malware are: worm, Trojans Horse, Rootkits.

Worm: Worm is a computer program which makes its copy again and again in the victim's computer. They damage the network by using a lot bandwidth.

Trojan Horses: Trojan horse consists of two parts, server and client. Server is an executable file which runs on victim's computer and attacker may take the full control of the victim's computer.

Rootkits: Rootkits are used to hide the malicious processes from active process

Networking - Services provided by IP (Internet Protocol) - July 31, 2009 at 17:00 pm by Vidya Sagar

Explain the services provided by IP (Internet Protocol) - Addressing, Fragmentation, Packet timeouts and options

1. Addressing: For the purpose of delivering datagram packets, IP needs to know about the address of the destination. By including the host addressing, this task is carried out by IP. As IP operates in an internet, its systems are designed to accept the addressing of devices which are unique.

2. Fragmenting: The datagram packets are sent to the data link layer for the purpose of transmission on the network. The physical network frame size that uses IP may be different. To resolve this, IP fragments the datagram into certain pieces. So that, each piece can be carried on the network. The receiving systems use these pieces and reassemble the whole IP datagram again.

3. Packet timeouts: A timeout packet is the time for waiting next instruction from the command station. If the command is not sent by the station, it shuts down

What is Network Mask?

A network mask is used for determination of what subnet an IP address belongs to. An IP address has network address and the host address. The first two numbers represents the network address and the second two numbers represents the host of the network.

Explain the classes of IP address

IP addresses are organized into classes. For convenience of humans, IP addresses are expressed in the decimal format. Every number in each class is represented as binary to computers.

The four numbers in an IP address are known as 'octets'. Each of them has eight bit positions. The octets are divided into two sections: Net and Host. The first octet represents Net for identifying the network and the Host contains the last octet. There are five IP classes.

Class A: The class A is used for very large networks. There are 1 to 126 are part of this class. That means there are 126 Class A networks. Class A networks accounts for half of the total available IP addresses.

Class B: It is used for medium size networks. The IP address with a first octet from 128 to 191 is part of this class. Class B networks have a first bit value of 1 and a second bit value of 0 in the first octet.

Class C: Class C is used for small to middle size networks. IP address with a first octet starts from 192-223. Class C networks have a first bit value of 1, second bit value of 1 and a third bit value of 0 in the first octet.

Class D: It has first, second and third bit value as 1 and the fourth bit as 0. The other 28 bits are used for identifying the group of computers which is intended for multicast messages.

Class E: Class E is used for identification purpose. The four bits value is 1. The other 28 bits are used for identifying the group of computers which is intended for multicast messages.

<<Previous Next>>

Define Broadcast, Unicast and Multicast.

Unicast: A term used in communication to describe a piece of information to send from one point to another. There are only sender and receiver. All LANs support unicast transfer mode and most applications that employ TCP transport protocol uses unicast messaging.

Broadcast: A term used for describing communication that is sent a piece of information from one point to all other points. There is one sender and multiple receivers. All LANs support broadcast transmission.

Multicast: A term described in communicating a piece of information sent from one or more points to a set of other points. The senders and receivers are one or more.

What is Network Mask?

A network mask is used for determination of what subnet an IP address belongs to. An IP address has network address and the host address. The first two numbers represents the network address and the second two numbers represents the host of the network.

What is the Domain Name System (DNS)? What are the advantages of it?

A hierarchical naming system for computer systems, services or for that matter any resource participating in the internet. Various information with domain names is assigned to each of the participants. DNS translates the names of domain into meaningful to humans into binary identifiers that are associated with the equipment of network to locate and address these devices.

Advantages:

More Reliable: Delivers messages to the users with zero downtime.

Faster: DNS are connected well at intersections of internet. Any cast technology enables requests are answered to the next closest node in the case of maintenance or downtime.

Smarter: Automatic corrections of typo

Explain the use of Internet Control Message Protocol (ICMP).

Internet Control Message Protocol is one of the important protocols in the Internet Protocol suite. It is mainly used in operating system of networked computers, for the purpose of sending error messages, for example, a requested service is unavailable or the host could not be reached. It is not directed by the network applications. ICMPs are utilized by routers, hosts for communicating the updates or error information to other routers.

What are the differences between a domain and a workgroup?

In a domain, one or more computer can be a server to manage the network. On the other hand in a workgroup all computers are peers having no control on each other. In a domain, user doesn't need an account to logon on a specific computer if an account is available on the domain. In a work group user needs to have an account for every computer.
In a domain, Computers can be on different local networks. In a work group all computers needs to be a part of the same local network.

What is PPP protocol? Explain PPP packet format.

Point to Point protocol helps communication between 2 computers over a serial cable, phone line or other fiber optic lines. E.g. Connection between an Internet Service Provider and a host. PPP also provides authentication. PPP operates by sending Request packets and waiting for Acknowledge packets that accept, reject or try to change the request. The protocol is also used to negotiate on network address or compression options between the nodes.

Packet format:-

Flag field: 1 byte: - Indicates frames beginning or end
Address field: 1 byte: - Used for broadcast address (destination address)
Control field: 1 byte: - Used as a control byte
Protocol field: - 1 or 2 bytes: - Setting of protocol in information field (of datagram)
Information: - 0 or more bytes: - Datagram (whether it contains data or control information)

Padding: - 0 or more bytes: - optional padding
FCS: - 2 or more bytes: - error check sum

What are switches? Explain the concepts of Layer-3 switches.

It is a device that connects multiple network segments.
A switch analyzes the MAC address and then determines where to send the data.
So a file addressed to a computer reaches only that computer through the use of a switch.
The term 'switch' commonly refers to a Network bridge that processes and routes data at the Data link layer (layer 2) of the OSI model.

Switches that additionally process data at the Network Layer are often referred to as Layer 3 switches or Multilayer switches.

What is Router? Explain components of Routers.

The way switches connect multiple computers, a router connects multiple networks. Routers comprise of data consisting of large tables of networks and addresses. Routers use algorithms to determine the shortest route to an address in a network.

Routers - August 20, 2008, 17:00 pm by Rajmeet Ghai

What are the basic components of routers?

Answer

Components of Router

Internal components:

- ROM:- Used to store the routers bootstrap details, operating system software.
- Flash memory: - holds the operating systems images. The content is retained when the router is restarted.
- RAM: - Used to store the Routing tables, configuration files, caching and buffering details. Content is lost when lost router is switched off or restarted.
- NVRAM:- Stores the routers startup config files. Data is non volatile.
- Network interfaces to connect router to network.

External components:

- Virtual terminals: For accessing routers
- Network management stations.

Explain the concept and capabilities of Unicast IP Addresses

It is an IP address that uniquely identifies a host in a network.
The datagram with a unicast IP address is received and processed by only a single host.

What is IP Multicasting?

It is an IP address that identifies a particular group of hosts in network.
This group of hosts is called a multicast group.

Explain the classes of IP addresses. Why do we need them?

Class A:
Range: from 0.0.0.0 to 127.255.255.255.
Leftmost bit: 0.
First 8 bits: netid.
Remaining 24 bits: hostid.

Class B:
Range: from 128.0.0.0 to 191.255.255.255.
Leftmost 2 bits: 10
First 16 bits: netid
Last 16 bits: the hostid

Class C:
Range: from 192.0.0.0 to 223.255.255.255.
Class C networks use the first 24 bits to determine the netid.
Leftmost 3 bits: 110
The next 21 bits define network.
8 bits define the hostid.

Class D:
First 4 bits: 1110
The remaining 28 bits define multicast addresses.
No netid or hostid in a class D address.
Addresses is used for multicasting.

Class E:
First 4 bits: 1111
Addresses reserved for special use on the Internet.
There is no netid or hostid in a class E address.

What is Superneting? Explain the concept of custom Subneting.

Supernetting or Classless Inter-Domain Routing (CIDR)

- It is a way to aggregate multiple Internet addresses of the same class.
- The adjacent network address (eg:192.168.2.0/24 and an address 192.168.3.0/24) can be merged (into 192.168.2.0/23) using supernetting.
- Supernetting is the basis for most routing protocols currently used on the Internet.
- It is mostly used to combine Class C network addresses.

Subneting- October 24, 2008 at 18:10 pm by Rajmeet Ghai

Describe the concept of Subneting.

Subneting is a process of breaking the network into smaller units. These units care called as subnets. Here a subnet could be several machines in a single LAN. Networks using IP can create sub networks of logical addresses. With every IP address there some of the bits in the machine can be used to identify a specific subnet. The IP address then contains three parts: the network number, the subnet number, and the machine number.

Subneting- October 24, 2008 at 18:10 pm by Rajmeet Ghai

What is custom Subneting?

Subnets that can be customized; i.e. modifying the dividing point between subnet ID and host ID to suit the needs of our network. The subnet mask that we use when creating a customized subnet is, called a custom subnet mask. This custom subnet mask is used to find the customization..

What is Subneting? Explain the advantages of using Subneting.

Subneting is dividing a network into several subnets.
This is usually done for the following purposes:

- Reducing network traffic by decreasing the number of broadcasts
- Exceeding the limitations in a local area network
- Enabling people to connect to the network remotely without opening the entire network

Subneting- October 24, 2008 at 18:10 pm by Rajmeet Ghai

Explain the advantages of using Subneting.

Advantages of using Subneting:-

- Easier network management and trouble shooting
- Routing table's size is reduced which means faster network transfers
- Solves network congestion problems:- Since the complete network is divided into smaller networks

- Network addresses can be decentralized e.g. the administrator of the network can monitor the subnet.

What is MAC address?

Media Access Control address is an identifier for assigned to most network adapters or Network Interface Cards by the manufacturer for the purpose of identification. MAC address is used in MAC protocol sub layer. MAC address is usually encodes the registered identification number that is registered by the manufacturer. The numbering spaces managed by the IEEE, which are common for formulating a MAC address: MAC-48, EUI-48 and EUI-64.

Define DNS

The DNS translates Internet domain and host names to IP addresses. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites. DNS implements a distributed database to store this name and address information for all public hosts on the Internet.

What is Application layer?

The application layer is located at the top of the TCP/IP protocol layers. This one contains the network applications which make it possible to communicate using the lower layers. The software in this layer therefore communicates using one of the two protocols of the layer below (the transport layer), i.e. TCP or UDP. In computer networking, an application layer firewall is a firewall operating at the application layer of a protocol stack.[1] Generally it is a host using various forms of proxy servers to proxy traffic instead of routing it. 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.

Define Telnet

Telnet is the main Internet protocol for creating a connection to a remote server.

Define SMTP.

SMTP - Short for Simple Mail Transfer Protocol, a protocol for sending e-mail messages between servers.

MAC vs. IP Addressing

Whereas MAC addressing works at the data link layer, IP addressing functions at the network layer (layer 3). It's a slight oversimplification, but one can think of IP addressing as supporting the software implementation and MAC addresses as supporting the hardware implementation of the network stack. The MAC address generally remains fixed and follows the network device, but the IP address changes as the network device moves from one network to another.

What is VPN?

A VPN is a service that offers secure, reliable connectivity over a shared public network infrastructure such as the Internet. VPNs maintain the same security and management policies as a private network. They are the most cost effective method of establishing a virtual point-to-point connection between remote users and an enterprise customer's network.

VPN - August 20, 2008, 17:00 pm by Rajmeet Ghai

What is VPN?

Virtual Private network is a network that used the public telecommunication infrastructure. This means that it used public wires to connect the nodes. E.g. Internet. VPN supports remote access to computers and allow data to be transmitted over this public network. Even though the data is transmitted over a public network, encryption and decrypting data to ensure security.

<<Previous Next>> The **Dynamic Host Configuration Protocol** (**DHCP**) is a network configuration protocol for hosts on Internet Protocol (IP) networks. Computers that are connected to IP networks must be configured before they can communicate with other hosts. The most essential information needed is an IP address, and a default route and routing prefix. DHCP eliminates the manual task by a network administrator. It also provides a central database of devices that are connected to the network and eliminates duplicate resource assignments.

Difference between Static and Dynamic IP.

Static IP is also called as permanent address assigned to each device in a network, whereas Dynamic IP, a temporary address assigned to the device via DHCP software. IP address assigned to your service by your cable or DSL Internet provider is typically dynamic IP. In routers and operating systems, the default configuration for clients is dynamic IP

What is the difference between public and private IP?

A public IP address allows equipment accessible to everyone on the internet. A private IP address is for private use within the network and allows many more PCs to be connected. If you are using a private IP and wants VOIP, you need to change to a public IP address.

<<Previous Next>>

What is Network Address Translation?

Network Address Translation acts as an agent between the Internet and a local network. It is a dynamic method which is used to minimize Internet connectivity needs. Network address translation describes the rewriting of the Internet Protocol (IP) addresses of data packets so that multiple transmissions require only one IP address.

Define IP multicast.

IP multicast technology reduces traffic by sending stream of information to many recipients at one go. Video conferencing, stock quotas are the examples based on IP multicast.

Define Address Resolution Protocol.

Address Resolution Protocol ARP, is responsible for mapping an IP address to its corresponding physical network address. It is mostly seen on Ethernet network.

What is Routing Protocol? Explain its purposes.

Routing protocol specifies how the routers communicate, disseminating the information which enables the routers to be selected between two nodes in a network.

Routing protocol interacts and informs the hardware that is needed to transmit the data between transmitter and the receiver for transmission over network.

How would you define IP address?

IP address or Internet Protocol address is the address of a device attached to an IP network (TCP/IP network). It is a must for every client, server and network device to have a unique IP address for each network connection (network interface). Every IP packet contains a source IP address and a destination IP address. As a device moves from one network to another, its IP address changes.

Networking - How would you define IP address? - Jan 28, 2009 at 22:10 PM by Rajmeet Ghai

Computers using the TCP/IP for communication are uniquely identified by a 32 bit address called as an IP address. The routers use the IP address information to forward the packet to the destination computer.

IP addresses are categorized as:

Private address: these IP addresses are used exclusively within a private network and not for public to see.

Public Address: these are registered IP addresses used for public.

Each IP address has a network address and a host address. IP addresses are expressed in four sets of three numbers, separated with dots. Each set is called as an octet because when converted to binary; it denotes eight binary.

Define broadcast domain.

It is a logical area in a computer network where any computer connected to the network can directly transmit to any other computer in the domain without having to go through a routing device.

Define gateway

A gateway is a network point that provides entrance into another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within your company's network or at your local Internet service provider (ISP) are gateway nodes.

What is firewall?

A firewall is a hardware or software installed to provide security to the private networks connected to the internet. They can be implemented in both hardware and software, or a combination of both. All data entering or leaving the Intranet passes through the firewall which allows only the data meeting the administrators' rules to pass through it

What is Data encryption?

Data encryption ensures data safety and very important for confidential or critical data. It protect data from being read, altered or forged while transmission.

Define Digital Signatures.

Digital signature is an attachment to an electronic message used for security purpose. It is used to verify the authenticity of the sender.

<<Previous Next>>

What is the Public Key Encryption?

Public key encryption use public and private key for encryption and decryption. In this mechanism, public key is used to encrypt messages and only the corresponding private key can be used to decrypt them. To encrypt a message, a sender has to know recipient's public key.

What is CSMA and CD concept?

In CSDA (carrier sense multiple access), presence of any digital signal in a network is checked before transmission. Data transmission occurs only when no signal is sensed.

CD, Collision detection is responsible for monitoring carrier in order to avoid signal jam.

<<Previous Next>> **Explain token ring technology.**

In this technology, all the devices are arranged in a circle. A token moves around the circular network. A device waits for the token before it sends its frame. Once it receives token, it initiates transmission of its frame.

Explain the use of network interface card, NIC.

NIC is used to connect computer to an Ethernet network.

What is Ethernet technology?

Ethernet technology is a high speed broadcast bus technology. In this type, all the station shares a single ether channel and receives every single transmitted signal.

What is TCP / IP protocol?

Transmission Control Protocol / Internet Protocol: - It is a family of protocols used for communication and connection between hosts on the internet. It is the most widely used standard for transmitting data over the internet. The four layers in the protocol are (from bottom to top):- Physical layer, Data link layer, Network layer, transport layer and application layer, also called as the OSI model. In TCP/IP , IP is responsible for forwarding packets while TCP ensures the correct delivery of data from client to server. TCP detects loss of data as well.

Define File Transfer Protocol.

File Transfer Protocol (FTP), a standard Internet protocol, is the simplest way to exchange files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol

(SMTP), which transfers e-mail, FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It's also commonly used to download programs and other files to your computer from other servers.

Networking - What is FTP (File Transfer Protocol)? - Jan 28, 2009, 17:00 pm by Rajmeet Ghai

What is FTP (File Transfer Protocol)?

FTP is File Transfer Protocol. It used to exchange files on the internet. To enable the data transfer FTP uses TCP/IP, FTP is most commonly used to upload and download files from the internet. FTP can be invoked from the command prompt or some graphical user interface. FTP also allows to update (delete, rename, move, and copy) files at a server. It uses a reserved port no 21.

What is NetBIOS protocol?

NetBIOS (Network Basic Input/Output System) Protocol allows applications on separate computers to communicate over a LAN. It runs over TCP/IP giving each computer in the network a NetBIOS name and IP address. E.g. It can be used for computers running Windows 2000 (or before) to join a computer network running Windows 2000 (or later).

What is PPP protocol? Explain PPP packet format.

Point to Point protocol helps communication between 2 computers over a serial cable, phone line or other fiber optic lines. E.g. Connection between an Internet Service Provider and a host. PPP also provides authentication. PPP operates by sending Request packets and waiting for Acknowledge packets that accept, reject or try to change the request. The protocol is also used to negotiate on network address or compression options between the nodes.

Packet format:-

Flag field: 1 byte: - Indicates frames beginning or end
Address field: 1 byte: - Used for broadcast address (destination address)
Control field: 1 byte: - Used as a control byte
Protocol field: - 1 or 2 bytes: - Setting of protocol in information field (of datagram)
Information: - 0 or more bytes: - Datagram (whether it contains data or control information)
Padding: - 0 or more bytes: - optional padding
FCS: - 2 or more bytes: - error check sum

What is NNTP (Network News Transfer Protocol)?

NNTP or Network News Transfer Protocol is used to manage the notes posted on Unset newsgroup (a collection of posted notes on a subject posted by different users). NNTP servers

are responsible for managing Usenet newsgroup collected globally. A NTTP client is a part of the web browser also called as a news reader. It uses a reserver port no 119.

Define SMTP.

SMTP - Short for Simple Mail Transfer Protocol, a protocol for sending e-mail messages between servers.

What is POP3 (Post Office Protocol 3)?

POP3 or Post Office Box 3 is used fro receiving emails. It is a client server protocol which holds the email. Once the email is downloaded from the server, POP3 deletes it from the server. Ordinal numbers are used to identify specific messages.

What is SNMP (Simple Network Management Protocol)?

SNMP or Simple Network Management Protocol is typically used for managing the network. Managing the network includes managing the nodes present in the network. These nodes may be server, routers, bridges and hubs. SNMP agents are used to achieve this. Managing the network is essential because it helps to monitor network performance, detect network faults or failures, audit network usage etc. the SNMP messages like TRAP, GET or SET may be invoked by network elements or network management system.

What is Routing Protocol? Explain its purposes.

Routing protocol specifies how the routers communicate, disseminating the information which enables the routers to be selected between two nodes in a network.

Routing protocol interacts and informs the hardware that is needed to transmit the data between transmitter and the receiver for transmission over network.

Next question>>

What is Routing Protocols?

Routing protocols are used to assist in achieving the basic purpose of routing. They specify the routers the method to communicate with each other. They help the routers select the best possible path between nodes. There are different types of protocols such as link-state routing protocols, path vector protocols and distance vector routing protocols. These protocols prevent routing loops to form or break if formed already. They help to decide preferred routes from a sequence of hop costs..

<<Previous Next>>

What is UDP protocol?

User Data Protocol is a communication protocol. It is normally used as an alternative for TCP/IP. However there are a number of differences between them. UDP does not divide data into packets. Also, UDP does not send data packets in sequence. Hence, the application program must ensure the sequencing. UDP uses port numbers to distinguish user requests. It also has a checksum capability to verify the data.

TCP and UDP - Jan 28, 2009, 17:00 pm by Rajmeet Ghai

TCP vs. UDP.

TCP guarantees the delivery of data. UDP on the other hand, does not guarantee delivery of data. TCP delivers messages in the order they were sent. UDP has no ordering mechanisms. In TCP data is sent as a stream while UDP sends data as individual packets. UDP is faster than TCP. TCP is a connection oriented protocol while UDP is connectionless.

<<Previous Next>>

What is UDP protocol?

User Data Protocol is a communication protocol. It is normally used as an alternative for TCP/IP. However there are a number of differences between them. UDP does not divide data into packets. Also, UDP does not send data packets in sequence. Hence, the application program must ensure the sequencing. UDP uses port numbers to distinguish user requests. It also has a checksum capability to verify the data.

TCP and UDP - Jan 28, 2009, 17:00 pm by Rajmeet Ghai

TCP vs. UDP.

TCP guarantees the delivery of data. UDP on the other hand, does not guarantee delivery of data. TCP delivers messages in the order they were sent. UDP has no ordering mechanisms. In TCP data is sent as a stream while UDP sends data as individual packets. UDP is faster than TCP. TCP is a connection oriented protocol while UDP is connectionless.

What is Tunneling?

Tunneling is a mechanism provided to transfer data securely between two networks. The data is split into smaller packets and passed through the tunnel. The data passing through the tunnel has 3 layers of encryption. The data is encapsulated. Tunneling can be approached by Point to Point tunneling protocol

What are voluntary and compulsory tunnels?

Voluntary Tunneling
Users computer is an end point of the tunnel and acts as tunnel client. Here the client or user issues a request to configure and create a voluntary tunnel. They require a dial up or LAN connection. Example of dial up connection is internet at home where a call is made to the ISP and connection is obtained.

Compulsory tunneling
In compulsory tunneling, instead of the user a vpn remote access server configures and creates a tunnel. Hence, the end point is the Remote sever not the user.

<<Previous Next>>

Explain static and dynamic tunnels.

Tunnels that are created manually are static tunnels. Tunnels that are auto discovered are dynamic tunnels. In dynamic tunneling, tcp connections can be checked dynamically. If no connections exist that are routed through the tunnel, a check for more suitable gateway can be done. Static tunneling may at times require dedicated equipments

Explain the use of RTP and RTCP protocols.

Use of RTP and RTCP:-

1. RTP can be used to transfer Real time data like voice packets.
2. RTP can be used with RTCP which makes it possible to monitor data.
3. Packet loss can be detected by RTP using Sequence number

RTCP provides Qos feedback :- Packets lost, round trip time.

What is a stream socket?

A stream socket provides two way communications between a client and server. This communication is reliable and sequenced. Stream sockets are above TCP to run across any networks. They provide unduplicated flow of data and have well established mechanism for creating and destroying connections and for detecting errors.

Datagram vs. stream.

Stream can be considered as a pipe that allows full duplex connection. A datagram or a packet on the other hand, has a source and a destination. There is no connection. Stream is like a communication channel while datagram is completely self contained. Streams provide a reliable

and sequenced communication. Datagram's on the other hand are unreliable and no sequence maintained

What is a socket?

A socket is used to connect an application to a network protocol. A socket enables communication between a client and a server. The communication is started when the client is assigned a local port number, and binds a socket to it. The client writes on the socket and gets information from server by reading it.

Networking - What is a socket? - March 08, 2008 at 19:10 pm by Rajmeet Ghai

What are Sockets? How do Sockets Work?

A socket is used to connect an application to a network protocol. A socket enables communication between a client and a server. The communication is started when the client is assigned a local port number, and binds a socket to it. The client writes on the socket and gets information from server by reading it. The Socket class is used to communicate. It provides rich set of methods for both asynchronous and synchronous data transfer. ConnectAsynch is used to start an asynchronous connection. SendAsynch and ReceiveAsynch are used to send and receive data. Shutdown and close methods are used to shutdown and close the sockets.