CS610 - Computer Network FAQs By www.virtualians.pk

Question: What is Broadcast?

Answer: Broadcast means to sent to more than one recipient. In communications and on networks, a broadcast message is one distributed to all stations. For example, as in television or radio networks, there is one transmitter and many listeners

Question: I can't understand it. " Instead of how a specific protocol handles congestion, we should concentrate on what congestion is and why it must be handled."

Answer: It is very simple english and it means that for now we do not need to go into details that how the congestion (overloading) is handles, but we are more to focus on what is congestion and why it is needed to be controlled.

Question: I can't understand the basic concept of "Fixed networks". Plz explain the term individually and also with respect to the mobile networks

Answer: Fixed Network includes the example of your lab network with laid network lines and are not moved usually. On the other side mobile networks include example of your Mobile phones which can also be said as wireless networks.

Question: “Multiple technologies exist that are used to connect different networks” So my question is what are these different technologies? Kindly list them and also list the features of these technologies and why we don't have any single standard for connecting networks?.

Answer: You do not need to go into details of the multiple networks provided by different companies.

Some of the examples of the networking technologies are: Ethernet, Fast Ethernet, Myrinet, ATM, SCRAMNet, Fibre Channel, FDDI. If you need to learn about the features of these technologies for your own knowledge, you should search for them over the internet as a vast information exists about these technologies over the internet.

Different companies develop their own technology for their sale and publicity to compete with other companies as well as they provide with some enhance idea with the existing technology that is then considered as more improved version or given different name.

Question: Explain about routers and how different networks are connected by routers?

Answer: Router is an agent device on a communications network that speeds up message delivery. On a single network linking many computers through a mesh of possible connections, a router receives transmitted messages and forwards them to their correct destinations over the most efficient available route. On an interconnected set of local area networks (LANs) using the same communications protocols, a router serves the somewhat different function of acting as a link between LANs, enabling messages to be sent from one to another. You will read in detail about routers in later lectures.

Question: Explain the term Latency.

Answer: Latency is the time required for a signal to travel from one point on a network to another.

Question: How models are either so simple are either so cpmplex how can we exlpain by giving any exmple?

Answer: These conceptual models complexity or simplicity depends on the information provided on the provider side or the understanding gathered on the learner (client) side. It can be easily understood with your own example. As it is written in very clear words in handouts that the complexity depends if the information provided is not prior to details or they are so simple that sometimes it is hard to distinguish between the details. But you have not understood it, so you have taken it as the complex form and don't find it that the information provided is enough to your understanding.

Question: I want you to explain the concept of PING command.

Answer: PING stands for Packet Internet Groper. It is a protocol for testing whether a particular computer is connected to the Internet by sending a packet to its IP address and waiting for a response. In any windows system , 95, 98 , XP or 2000 or any other, go to the windows command prompt and type "ping/?", press enter and you will know if it is working in the windows and also how can you use different options of PING command.

Question: How can we disable a pinging request (for secority purpose)?

Answer: PING is an internal command which cannot be disabled. Also , there is no security issue in it that it is needed to be disabled. It only provies the networking information and IP information which is open to the clients.

Question: 'traceroute' does not work in the LAN when sitting on a client computer, what could be the possible causes and how can be resolved?

Answer: Trace Route works on all the systems on the network. You should see if you are not making any typing mistake or if you are using Wrindows XP then you need to type "tracert" command for trace routing.

Question: PING command is only used to know the existence of a site or is there any other use/advantage too of PING command.

Answer: It is a protocol for testing whether a particular computer is connected to the Internet/LAN by sending a packet to its IP address and waiting for a response.

Question: What factor determines how much byte data packed is send from the host computer. In one of the example in Lecture 2 you determines 32 byte and in other it was 56? What this difference means?

Answer: It is an internal feature of the ping command that it by default work with 32 data bytes. You simply try the ping command and you will learn its working , ping with different servers. In any windows system , 95, 98 , XP or 2000 or any other, go to the windows command prompt and type "ping/?", press enter and you will know if it is working in the windows and also how can you use different options of PING command.

Question: What is the difference b/w "PING and Trace Route Probing Tools".

Answer: PING stands for Packet Internet Groper. It is a protocol for testing whether a particular computer is connected to the Internet by sending a packet to its IP address and waiting for a response. In any windows system , 95, 98 , XP or 2000 or any other, go to the windows command prompt and type "ping/?", press enter and you will know if it is working in the windows and also how can you use different options of PING command.

Traceroute shows all the computers in the defined network path, it shows all the computers which comes in the way of source and the destination computers. Type "tracert/?" in command prompt in Windown XP and you will see its different functionalities.

Question: As ping tells us about the connectivity of the host or other computer, is it uses any resources of the local computer or not?

Answer: Yes, it does use resources of the computer. It is an internal command and use the network resources.

Question: What is is the difference between computational power and resources?

Answer: Computational power can be defined as the act of processing of the computer. Resource is any part of a computer system or a network, such as a disk drive, printer, or memory, that can be allotted to a program or a process while it is running.

Question: I tried ping and tracert both with different sites but when I do it with VU website it does not respond and messages come out to be request time out. Why is it so? As VU website is alive, is that because of any security reason or there is some other problem?

Answer: It is not any security reason. Any site which is outside the secure link responds to ping and tracert commands. The problem is the network traffic over the VU sites or the internet speed you are having. As VU sites holds a lots of users and these commands need a free way for information. I can tell you as an example, if i use ping or tracert commands for vu sites they work very correctly and efficiently without any time out, but while using any other site, such as google.com or msn.com, i have tried to use tracert command on both sites with an interval of half an hour, and i have come up with the result that when i used the command earlier it was working ok and just gave a timeout once , but the other time it is not responding at all.

Question: Why Some networks or computers reject the ping packets ?

Answer: It may be due to the complexity of the network connections. Also it can be due to the fact that the server is too busy and not been able to respond all the clients. This may happen mostly in internet probing.

Question: Is this ping & tacing a route tools only use in XP window or other windows like 98 or 95 etc.?

Answer: In any windows system , 95, 98 , XP or 2000 or any other, go to the windows command prompt and type "ping/?", press enter and you will know if it is working in the windows and also how can you use different options of PING command.

Question: Kindly explain briefly the basics of Data Stuffing?

Answer: Data Stuffing basically involves bit stuffing and byte stuffing: Bit stuffing is the practice of adding bits to a stream of data. Bit stuffing is required by many network and communications protocols for the following reasons: To prevent data being interpreted as control information. For protocols that require a fixed-size frame, bits are sometimes inserted to make the frame size equal to this set size.

For protocols that required a continuous stream of data, zero bits are sometimes inserted to ensure that the stream is not broken.

Byte Stuffing , also referred to as Character Stuffing.

Question: What is CSMA ? What is the concept of LAN hardware?

Answer: CSMA is short for Carrier Sense Multiple Access / Collision Detection, a set of rules determining how network devices respond when two devices attempt to use a data channel simultaneously (called a collision). Standard Ethernet networks use CSMA/CD to physically monitor the traffic on the line at participating stations. If no transmission is taking place at the time, the particular station can transmit. If two stations attempt to transmit simultaneously, this causes a collision, which is detected by all participating stations. After a random time interval, the stations that collided attempt to transmit again. If another collision occurs, the time intervals from which the random waiting time is selected are increased step by step. This is known as exponential back off.

CSMA/CD is a type of contention protocol. Networks using the CSMA/CD procedure are simple to implement but do not have deterministic transmission characteristics.

LAN hardware includes the network adapter and the wires used to connect these adaptors in all computers. This is the simplest definition of LAN hardware. What do you not understand about it, specify your confusion.

Question: What is the basic function of trace routing and ping.?

Answer: PING stands for Packet Internet Groper. It is a protocol for testing whether a particular computer is connected to the Internet by sending a packet to its IP address and waiting for a response. In any windows system , 95, 98 , XP or 2000 or any other, go to the windows command prompt and type "ping/?", press enter and you will know if it is working in the windows and also how can you use different options of PING command.

Traceroute shows all the computers in the defined network path, it shows all the computers which comes in the way of source and the destination computers. Type "tracert/?" in command prompt in Windown XP and you will see its different functionalities.

Question: Please breifly explain "binary exponential backoff".

Answer: If two stations attempt to transmit simultaneously, this causes a collision, which is detected by all participating stations. After a random time interval, the stations that collided attempt to transmit again. If another collision occurs, the time intervals from which the random waiting time is selected are increased step by step. This is known as exponential back off.

Question: Broadcast Address must be "all 1s" Pls tell me that what are the total no.of 1s in a broadcast address. and how it can be send to other computers on the LAN?

Answer: A broadcast message is addressed to all stations on the network. The destination address in a broadcast message consists of all 1s (0xFFFFFFFF). All stations automatically receive frames with this address. Normally, broadcast messages are sent for network management and diagnostic purposes.

On IP networks, the IP address 255.255.255.255 (in binary, all 1s) is the general broadcast address. You can't use this address to broadcast a message to every user on the Internet because routers block it, so all you end up doing is broadcasting it to all hosts on your own network. The broadcast address for a specific network includes all 1s in the host portion of the IP address. For example, on the class C network 192.168.1.0, the last byte indicates the host address (a 0 in this position doesn't refer to any host, but provides a way to refer to the entire network). The value 255 in this position fills it with all 1s, which indicates the network broadcast address, so packets sent to 192.168.1.255 are sent to all hosts on the network. So the boradcast address contains 8 number of 1's.

Question: In CSMA/CD why we use a random time from 0-d. Why we not assign a specific but different wait time for all the machines.

Answer: Standard Ethernet networks use CSMA/CD to physically monitor the traffic on the line at participating stations. If no transmission is taking place at the time, the particular station can transmit. If two stations attempt to transmit simultaneously, this causes a collision, which is detected by all participating stations. After a random time interval, the stations that

collided attempt to transmit again. If another collision occurs, the time intervals from which the random waiting time is selected are increased step by step. That is why we use random time.

Question: Is CRC detects balance errors or not. If not then is there any technique that can detect balance error ?

Answer: CRC can detect balance errors. CRC error checking uses a complex calculation to generate a number based on the data transmitted which is same as balance errors.

Question: What does Spatial and Temporal Locality Principles mean? Does it mean that we are having LANs for in LANS computer are located in a close contact with eath other, and to eastablish a connection with nearby computer is a lot more easier than with the computers residing far away?

Answer: Spatial Locality pattern refers to the communication which is carried out between computers in a network which are located very near to each other.

Temporal Locality pattern means that the communicaion is carried out between same computers again and again.

It may cause difference in peer to peer connection speed, but when it comes to LANs with servers then the speed is controlled by the server.

Question: How can perform shift register?

Answer: Shift registers are a type of sequential logic circuit, mainly for storage of digital data. They are a group of flip-flops connected in a chain so that the output from one flip-flop becomes the input of the next flip-flop. Most of the registers possess no characteristic internal sequence of states. All the flip-flops are driven by a common clock, and all are set or reset simultaneously.

Revise your CS302 course to remember Shift Registers.

Question: What is IPV4 and IPV6?

What is the difference between "ping" and "ping6" and "tracert" and "tracert6"?

Answer: The core protocol used on the Internet is called the Internet Protocol or simply IP. The current version of this protocol is version 4 (IPv4). This version of the protocol was designed over 20 years ago. Since that time, a great deal about networking has been learned and much more still has changed. The original design has proven to work well, but in hindsight, a number of shortcomings with the design have been exposed. A new version of the protocol, version 6, is being deployed by the Internet community (version 5 was used for testing and never widely implemented). Most systems now have IPv6 support built in and many network operators are beginning trials and building production networks based on the newer version of IP.

IPv4 Internet addresses are unique 32-bit identifiers used to address hosts on the Internet.

IPv6 is backward compatible with IPv4, provided that special techniques are used. For example, to enable communication between far distances of IPv6 devices connected by IPv4 networks, tunneling may be employed. To support IPv4/IPv6 compatibility, a scheme was developed to allow IPv4 addresses to be embedded within the IPv6 address structure. This method takes regular IPv4 addresses and puts them in a special IPv6 format so they are recognized as being IPv4 addresses by certain IPv6 devices.

ping6 is the IPv6 version ping.

To trace a full IPv6 network path, you can use the tracert6 command.

Question: What are the pros and cons of TCP /IP network?

Answer: TCP/IP (Transmission Control Protocol/Internet Protocol) allows computers to communicate with one another over a network. Some of the advantages of TCP/IP include:

- Computers on the same network can communicate

- Computers on different networks can communicate

- Different types of computers can send messages to one another.

- Platform independent

- The protocol of the internet

TCP/IP is really a standard which computer manufacturers have agreed will be used to allow computers to exchange data. TCP/IP is not just one protocol, but is actually a collection of several. TCP and IP are the two major components, although there are several other components included in the entire procedure.

Question: Please explan the term " TDM" . What is it ?

Answer: TDM stands for Time Division Multiplexing. It is a type of multiplexing where two or more channels of information are transmitted over the same link by allocating a different time interval ("slot" or "slice") for the transmission of each channel. I.e. the channels take turns to use the link. Some kind of periodic synchronising signal or distinguishing identifier is usually required so that the receiver can tell which channel is which. TDM becomes inefficient when traffic is intermittent because the time slot is still allocated even when the channel has no data to transmit.

Question: As the concept of packets if we want to send a big file in Mb's so we have to break it into packets as first turn into Kb's then we can send the file if we want to send it quickly?

Answer: If for example you are required to send a 5MB file over a network. If you send the whole file as one file, it will first break into packets and then will be sent and these packets will reunite to for the original file. If you break it into file of size 1MB each or 500KB each then it will again be broken down in packets and same procedure will be carried out. But the packets in case of whole 5MB file, there will be many packets and so it will take a little more time while creating and reuniting packets as compared to the less number of packets in case of 1MB or 500KB files, which will take a little less time.

Question: Computer Networks or individual servers are connect to form THE INTERNET via Routers. When we use "trace route" command to find the path from source to destination, are these IP's belong to routers, or servers or both because router must also have some address to be uniquely identified. If both routers and server machines have some IP address then how could we distinguish between these IP's?

Answer: Routers do not have any IP address. They are the electronic devices. Routers are an intermediary device on a communications network that expedites message delivery. On a single network linking many computers through a mesh of possible connections, a router receives transmitted messages and forwards them to their correct destinations over the most efficient available route. On an interconnected set of local area networks (LANs) using the same communications protocols, a router serves the somewhat different function of acting as a link

between LANs, enabling messages to be sent from one to another. Therefore you only need one IP address. i,e., of server.

Question: What is the diffrence between Transponder and repeaters?

Answer: Transponders are devices that receives a signal from and retransmits it on a different frequency to one or more other destinations.

Repeaters are devices used on communications circuits that decreases distortion by amplifying or regenerating a signal so that it can be transmitted onward in its original strength and form. On a network, a repeater connects two networks or two network segments at the physical layer and regenerates the signal.

Question: Plz explain what is difference between character based machines and bit orianted machines?

Answer: Bit Oriented Machines are based on Bit Stiffing Techniques.

Bit stuffing is the practice of adding bits to a stream of data. Bit stuffing is required by many network and communications protocols for the following reasons:

To prevent data being interpreted as control information.

For protocols that require a fixed-size frame, bits are sometimes inserted to make the frame size equal to this set size.

For protocols that required a continuous stream of data, zero bits are sometimes inserted to ensure that the stream is not broken.

Character Oriented Machines are based on Byte Stiffing techniques. See handouts for byte stuffing detials.

Question: What is the diffrence between LAN user IP and a Modem user IP ? Most of the LAN IP's of diffrent LANs are same for example 192.168.0.43 many diffrent LAN users have this IP so how can i acess this IP of diffrent LAN network user which have the same IP ? Is this poosible the modem IP are also same of diffrent users ?

Answer: LAN IP is the IP address given to a network (to every individual computer). This IP address which you have mentioned is the standard of any LAN IP network address. Modem IP is is the IP given at the time when you are connected to the ISP (Internet Service Provider) which gives a different IP to all its users when they are connected. IP is basically managed by the servers. In a LAN configuration, each computer has a different IP address. It may be so if you visit two different labs, you may find same IP address on some computer in these two labs, but these labs will not be interconnected to each other. Similarly the modem IP's are never the same. In simple words IP addresses are not same on similar networks.

Question: I want to know what is parity checking ? When we will CRC ?

Answer: Parity Checking is the prodecure of using parity bit to check the accuracy of transmitted data.

CRC (cyclic redundancy check) is a procedure used in checking for errors in data transmission. CRC error checking uses a complex calculation to generate a number based on the data transmitted. The sending device performs the calculation before transmission and sends its result to the receiving device. The receiving device repeats the same calculation after transmission. If both devices obtain the same result, it is assumed that the transmission was error-free. The procedure is known as a redundancy check because each transmission includes not only data but extra (redundant) error-checking values.

Question: Please explan the two term "Byte Stuffing" & "Bit Stuffing". What is different between Byte Stuffing and Bit Sutffing ?

Answer: Bit stuffing is the practice of adding bits to a stream of data. Bit stuffing is required by many network and communications protocols for the following reasons:

To prevent data being interpreted as control information.

For protocols that require a fixed-size frame, bits are sometimes inserted to make the frame size equal to this set size.

For protocols that required a continuous stream of data, zero bits are sometimes inserted to ensure that the stream is not broken.

Byte Stuffing , also referred to as Character Stuffing.

Question: What is meant by impairment?

Answer: Impairment means to cause a damage or lost of some network connection.

Question: How CRC hardware actually work with data ?

Answer: CRC (cyclical redundancy check) is a procedure used in checking for errors in data transmission. CRC error checking uses a complex calculation to generate a number based on the data transmitted. The sending device performs the calculation before transmission and sends its result to the receiving device. The receiving device repeats the same calculation after transmission. If both devices obtain the same result, it is assumed that the transmission was error-free. The procedure is known as a redundancy check because each transmission includes not only data but extra (redundant) error-checking values.

Question: Which is the better option for comunicating (point to point) like star topology or the other one?

Answer: It depends on the network you are using. All topologies have their advantages and disadvantages depending on the usage. Star topology is mostly used in general networks.

Question: What is the meaning of Mobile Network and Semi Persistent connections ?

Answer: Mobile Networks are a kind of wireless networking in which there is no physical or direct link through wires as in your lab network. Example of mobile networks are the mobile phones.

Semi persistent connections means those connections which are with intervals. For example, you might have noticed that sometimes your mobile phoes just reply to some network even when you are not receiving or dialing any number, it is because the network keeps on cheking the devices in range not all the time but after several intervals.

Question: What is firewall restriction from ISP?

Answer: A firewall is installed to prevent computers in the network from communicating directly with computers external to the network and vice versa. Instead, all communication is routed through a proxy server outside of the network, and the proxy server decides whether it is safe to let a particular message or file pass through to that network. ISPs usually restrict the

protocol which allows the IP address to travel along the path to keep safe from any kind of access to their network not allowing to travel through their proxy.

Question: What is hardware fault? where it occur and why?

Answer: Hardware fault can occur if the system crashes, its physical components cause errors due to any reason like system halt, over heating, component failure damage. There can be many reasons of its occurance. Please contact your operating systems instructor for more details.

Question: What are the two types of transmission technology available?

Answer: (i) Broadcast and (ii) point-to-point

Question: What is subnet?

Answer: A generic term for section of a large networks usually separated by a bridge or router.

Question: Difference between the communication and transmission.

Answer: Transmission is a physical movement of information and concern issues like bit polarity, synchronisation, clock etc. Communication means the meaning full exchange of information between two communication media.

Question: What are the possible ways of data exchange?

Answer: (i) Simplex (ii) Half-duplex (iii) Full-duplex.

Question: What is SAP?

Answer: Series of interface points that allow other computers to communicate with the other layers of network protocol stack.

Question: What is NETBIOS and NETBEUI?

Answer: NETBIOS is a programming interface that allows I/O requests to be sent to and received from a remote computer and it hides the networking hardware from applications. NETBEUI is NetBIOS extended user interface. A transport protocol designed by microsoft and IBM for the use on small subnets.

Question: What is RAID?

Answer: A method for providing fault tolerance by using multiple hard disk drives.

Question: What is passive topology?

Answer: When the computers on the network simply listen and receive the signal, they are referred to as passive because they don't amplify the signal in any way. Example for passive topology - linear bus.

Question: What is Brouter?

Answer: Hybrid devices that combine the features of both bridges and routers.

Question: What is cladding?

Answer: A layer of a glass surrounding the center fiber of glass inside a fiber-optic cable.

Question: How Gateway is different from Routers?

Answer: A gateway operates at the upper levels of the OSI model and translates information between two completely different network architectures or data formats

Question: What is attenuation?

Answer: The degeneration of a signal over distance on a network cable is called attenuation.

Question: What is MAC address?

Answer: The address for a device as it is identified at the Media Access Control (MAC) layer in the network architecture. MAC address is usually stored in ROM on the network adapter card and is unique.

Question: Difference between bit rate and baud rate.

Answer: Bit rate is the number of bits transmitted during one second whereas baud rate refers to the number of signal units per second that are required to represent those bits. baud rate = bit rate / N where N is no-of-bits represented by each signal shift

Question: What are the types of Transmission media?

Answer: Signals are usually transmitted over some transmission media that are broadly classified in to two categories.

Question: Guided Media:

Answer: These are those that provide a conduit from one device to another that include twisted-pair, coaxial cable and fiber-optic cable. A signal traveling along any of these media is directed and is contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic that accept and transport signals in the form of electrical current. Optical fiber is a glass or plastic cable that accepts and transports signals in the form of light.

Question: Unguided Media:

Answer: This is the wireless media that transport electromagnetic waves without using a physical conductor. Signals are broadcast either through air. This is done through radio communication, satellite communication and cellular telephony.

Question: What is Project 802?

Answer: It is a project started by IEEE to set standards to enable intercommunication between equipment from a variety of manufacturers. It is a way for specifying functions of the physical layer, the data link layer and to some extent the network layer to allow for interconnectivity of major LAN protocols. It consists of the following: 802.1 is an internetworking standard for compatibility of different LANs and MANs across protocols. 802.2 Logical link control (LLC) is the upper sublayer of the data link layer which is non-architecture-specific, that is remains the same for all IEEE-defined LANs. Media access control (MAC) is the lower sublayer of the data link layer that contains some distinct modules each carrying proprietary information specific to the LAN product being used. The modules are Ethernet LAN (802.3), Token ring LAN (802.4), Token bus LAN (802.5). 802.6 is distributed queue dual bus (DQDB) designed to be used in MANs.

Question: What are the different type of networking / internetworking devices?

Answer: Repeater: Also called a regenerator, it is an electronic device that operates only at physical layer. It receives the signal in the network before it becomes weak, regenerates the original bit pattern and puts the refreshed copy back in to the link. Bridges: These operate both in the physical and data link layers of LANs of same type. They divide a larger network in to smaller segments. They contain logic that allow them to keep the traffic for each segment separate and thus are repeaters that relay a frame only the side of the segment containing the intended recipent and control congestion. Routers: They relay packets among multiple interconnected networks (i.e. LANs of different type). They operate in the physical, data link and network layers. They contain software that enable them to determine which of the several

possible paths is the best for a particular transmission. Gateways: They relay packets among networks that have different protocols (e.g. between a LAN and a WAN). They accept a packet formatted for one protocol and convert it to a packet formatted for another protocol before forwarding it. They operate in all seven layers of the OSI model.

Question: What are the data units at different layers of the TCP / IP protocol suite?

Answer: The data unit created at the application layer is called a message, at the transport layer the data unit created is called either a segment or an user datagram, at the network layer the data unit created is called the datagram, at the data link layer the datagram is encapsulated in to a frame and finally transmitted as signals along the transmission media.

Question: What is difference between ARP and RARP?

Answer: The address resolution protocol (ARP) is used to associate the 32 bit IP address with the 48 bit physical address, used by a host or a router to find the physical address of another host on its network by sending a ARP query packet that includes the IP address of the receiver. The reverse address resolution protocol (RARP) allows a host to discover its Internet address when it knows only its physical address.

Question: What is the minimum and maximum length of the header in the TCP segment and IP datagram?

Answer: The header should have a minimum length of 20 bytes and can have a maximum length of 60 bytes.

Question: What is the range of addresses in the classes of internet addresses?

Answer: Class A 0.0.0.0 - 127.255.255.255 Class B 128.0.0.0 - 191.255.255.255 Class C 192.0.0.0 - 223.255.255.255 Class D 224.0.0.0 - 239.255.255.255 Class E 240.0.0.0 - 247.255.255.255

Question: What are major types of networks and explain?

Answer: Peer-to-peer network, computers can act as both servers sharing resources and as clients using the resources. Server-based networks provide centralized control of network resources and rely on server computers to provide security and network administration

Question: What are the important topologies for networks?

Answer: BUS topology: In this each computer is directly connected to primary network cable in a single line. Advantages: Inexpensive, easy to install, simple to understand, easy to extend. STAR topology: In this all computers are connected using a central hub. Advantages: Can be inexpensive, easy to install and reconfigure and easy to trouble shoot physical problems. RING topology: In this all computers are connected in loop. Advantages: All computers have equal access to network media, installation can be simple, and signal does not degrade as much as in other topologies because each computer regenerates it.

Question: What is mesh network?

Answer: A network in which there are multiple network links between computers to provide multiple paths for data to travel.

Question: What is difference between baseband and broadband transmission?

Answer: In a baseband transmission, the entire bandwidth of the cable is consumed by a single signal. In broadband transmission, signals are sent on multiple frequencies, allowing multiple signals to be sent simultaneously.

Question: Explain 5-4-3 rule?

Answer: In a Ethernet network, between any two points on the network ,there can be no more than five network segments or four repeaters, and of those five segments only three of segments can be populated.

Question: What is the difference between routable and non- routable protocols?

Answer: Routable protocols can work with a router and can be used to build large networks. Non-Routable protocols are designed to work on small, local networks and cannot be used with a router

Question: Why should you care about the OSI Reference Model?

Answer: It provides a framework for discussing network operations and design.

Question: What is logical link control?

Answer: One of two sublayers of the data link layer of OSI reference model, as defined by the IEEE 802 standard. This sublayer is responsible for maintaining the link between computers when they are sending data across the physical network connection.

Question: What is virtual channel?

Answer: Virtual channel is normally a connection from one source to one destination, although multicast connections are also permitted. The other name for virtual channel is virtual circuit.

Question: What is traffic shaping?

Answer: One of the main causes of congestion is that traffic is often busy. If hosts could be made to transmit at a uniform rate, congestion would be less common. Another open loop method to help manage congestion is forcing the packet to be transmitted at a more predictable rate. This is called traffic shaping.

Question: What is multicast routing?

Answer: Sending a message to a group is called multicasting, and its routing algorithm is called multicast routing.

Question: What is region?

Answer: When hierarchical routing is used, the routers are divided into what we will call regions, with each router knowing all the details about how to route packets to destinations within its own region, but knowing nothing about the internal structure of other regions.

Question: What is silly window syndrome?

Answer: It is a problem that can ruin TCP performance. This problem occurs when data are passed to the sending TCP entity in large blocks, but an interactive application on the receiving side reads 1 byte at a time.

Question: What is Mail Gateway?

Answer: It is a system that performs a protocol translation between different electronic mail delivery protocols.

Question: What is IGP (Interior Gateway Protocol)?

Answer: It is any routing protocol used within an autonomous system.

Question: What is EGP (Exterior Gateway Protocol)?

Answer: It is the protocol the routers in neighboring autonomous systems use to identify the set of networks that can be reached within or via each autonomous system.

Question: What is autonomous system?

Answer: It is a collection of routers under the control of a single administrative authority and that uses a common Interior Gateway Protocol.

Question: What is BGP (Border Gateway Protocol)?

Answer: It is a protocol used to advertise the set of networks that can be reached with in an autonomous system. BGP enables this information to be shared with the autonomous system. This is newer than EGP (Exterior Gateway Protocol).

Question: What is Gateway-to-Gateway protocol?

Answer: It is a protocol formerly used to exchange routing information between Internet core routers.

Question: What is NVT (Network Virtual Terminal)?

Answer: It is a set of rules defining a very simple virtual terminal interaction. The NVT is used in the start of a Telnet session.

Question: What is a Multi-homed Host?

Answer: It is a host that has a multiple network interfaces and that requires multiple IP addresses is called as a Multi-homed Host.

Question: What is OSPF?

Answer: It is an Internet routing protocol that scales well, can route traffic along multiple paths, and uses knowledge of an Internet's topology to make accurate routing decisions.

Question: What is Proxy ARP?

Answer: It is using a router to answer ARP requests. This will be done when the originating host believes that a destination is local, when in fact is lies beyond router.

Question: What is RIP (Routing Information Protocol)?

Answer: It is a simple protocol used to exchange information between the routers.

Question: LAN, MAN, CAN, and WAN: What are the differences? What is each one used for?

Answer: LAN, MAN, CAN, and WAN are all different types of networks used when connecting to the internet and/or other computers. LAN is a local area network used in small areas such as homes or offices. LANs offer quick data transferring due to its small area and transfer area. Additionally, LANs don't need an external telecom device in order to be accessed. MANs are metropolitan area networks, so they are used for larger areas, such as entire cities. CANs are a type of MAN meaning campus area network. As the name implies, they are commonly used on academic campuses, but can also be used in most any moderate area. WAN is a wide area network and is good for a larger area. WAN are often compared to LAN connections. They have a slower data transfer due to the wide range. WANs are commonly used in large organizations due to their extensive area.

Question: What is a network firewall?

Answer: A firewall is a system or group of systems that enforces an access control policy between two or more networks. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic. Probably the most important thing to recognize about a firewall is that it implements an access control policy. If you don't have a good idea of what kind of access you want to allow or to deny, a firewall really won't help you. It's also important to recognize that the firewall's configuration, because it is a mechanism for enforcing policy, imposes its policy on everything behind it. Administrators for firewalls managing the connectivity for a large number of hosts therefore have a heavy responsibility.

Question: Why would I want a firewall?

Answer: The Internet, like any other society, is plagued with the kind of jerks who enjoy the electronic equivalent of writing on other people's walls with spraypaint, tearing their mailboxes off, or just sitting in the street blowing their car horns. Some people try to get real work done over the Internet, and others have sensitive or proprietary data they must protect. Usually, a firewall's purpose is to keep the jerks out of your network while still letting you get your job done. Many traditional-style corporations and data centers have computing security policies and practices that must be followed. In a case where a company's policies dictate how data must be protected, a firewall is very important, since it is the embodiment of the corporate policy. Frequently, the hardest part of hooking to the Internet, if you're a large company, is not

justifying the expense or effort, but convincing management that it's safe to do so. A firewall provides not only real security--it often plays an important role as a security blanket for management.

Question: What can a firewall protect against?

Answer: Some firewalls permit only email traffic through them, thereby protecting the network against any attacks other than attacks against the email service. Other firewalls provide less strict protections, and block services that are known to be problems. Generally, firewalls are configured to protect against unauthenticated interactive logins from the ``outside'' world. This, more than anything, helps prevent vandals from logging into machines on your network. More elaborate firewalls block traffic from the outside to the inside, but permit users on the inside to communicate freely with the outside. The firewall can protect you against any type of network-borne attack if you unplug it. Firewalls are also important since they can provide a single ``choke point'' where security and audit can be imposed. Unlike in a situation where a computer system is being attacked by someone dialing in with a modem, the firewall can act as an effective ``phone tap'' and tracing tool. Firewalls provide an important logging and auditing function; often they provide summaries to the administrator about what kinds and amount of traffic passed through it, how many attempts there were to break into it, etc. Because of this, firewall logs are critically important data. They can be used as evidence in a court of law in most countries. You should safeguard, analyze and protect yoru firewall logs accordingly. This is an important point: providing this ``choke point'' can serve the same purpose on your network as a guarded gate can for your site's physical premises. That means anytime you have a change in ``zones'' or levels of sensitivity, such a checkpoint is appropriate. A company rarely has only an outside gate and no receptionist or security staff to check badges on the way in. If there are layers of security on your site, it's reasonable to expect layers of security on your network.

Question: What can't a firewall protect against?

Answer: Firewalls can't protect against attacks that don't go through the firewall. Many corporations that connect to the Internet are very concerned about proprietary data leaking out of the company through that route. Unfortunately for those concerned, a magnetic tape, compact disc, DVD, or USB flash drives can just as effectively be used to export data. Many organizations that are terrified (at a management level) of Internet connections have no coherent policy about how dial-in access via modems should be protected. It's silly to build a six-foot thick steel door when you live in a wooden house, but there are a lot of organizations out there buying expensive firewalls and neglecting the numerous other back-doors into their network. For a firewall to work, it must be a part of a consistent overall organizational security architecture.

Firewall policies must be realistic and reflect the level of security in the entire network. For example, a site with top secret or classified data doesn't need a firewall at all: they shouldn't be hooking up to the Internet in the first place, or the systems with the really secret data should be isolated from the rest of the corporate network. Lost or stolen PDAs, laptops, cell phones, USB keys, external hard drives, CDs, DVDs, etc. For protection against this type of data loss, you will need a good policy, encryption, and some sort of enterprise auditing/enforcement. Places that really care about Intellectual Property (IP) and data loss prevention use USB firewalling technology on their desktops and systems in public areas. The details are outside the scope of this FAQ. Badly written, pooly thought out, or non-existent organizational policy. A firewall is the end extension of an organization's security policy. If that policy is ill-informed, pooly formed, or not formed at all, then the state of the firewall is likely to be similar. Executive buy-in is key to good security practice, as is the complete and unbiased enforcement of your policies. Firewalls can't protect against political exceptions to the policy, so these must be documented and kept at a miniumum. Another thing a firewall can't really protect you against is traitors or idiots inside your network. While an industrial spy might export information through your firewall, he's just as likely to export it through a telephone, FAX machine, or Compact Disc. CDs are a far more likely means for information to leak from your organization than a firewall. Firewalls also cannot protect you against stupidity. Users who reveal sensitive information over the telephone are good targets for social engineering; an attacker may be able to break into your network by completely bypassing your firewall, if he can find a ``helpful" employee inside who can be fooled into giving access to a modem pool or desktop through a "remote support" type portal. Before deciding this isn't a problem in your organization, ask yourself how much trouble a contractor has getting logged into the network or how much difficulty a user who forgot his password has getting it reset. If the people on the help desk believe that every call is internal, you have a problem that can't be fixed by tightening controls on the firewalls. Firewalls can't protect against tunneling over most application protocols to trojaned or poorly written clients. There are no magic bullets and a firewall is not an excuse to not implement software controls on internal networks or ignore host security on servers. Tunneling ``bad" things over HTTP, SMTP, and other protocols is quite simple and trivially demonstrated. Security isn't ``fire and forget". Lastly, firewalls can't protect against bad things being allowed through them. For instance, many Trojan Horses use the Internet Relay Chat (IRC) protocol to allow an attacker to control a compromised internal host from a public IRC server. If you allow any internal system to connect to any external system, then your firewall will provide no protection from this vector of attack.

Question: How is Network Performance Measured?

Answer: The performance or "speed" of a computer network is normally measured in units of bits per second (bps). This quantity can represent either an actual data rate or a theoretical limit to available network bandwidth. The related units of Kbps, Mbps, Gbps represent increasingly larger multiples of bps.

Question: What Is a Network Name?

Answer: A network name is a string that computing devices use to identify a specific computer network. Network names are typically different from names of individual computers or the addresses computers use to identify each other.

Question: What is an intranet?

Answer: Intranet is the generic term for a collection of private computer networks within an organization. An intranet uses network technologies as a tool to facilitate communication between people or workgroups to improve the data sharing capability and overall knowledge base of an organization's employees.

Question: How fast can a normal Null Modem cable transfer files?

Answer: A null modem cable connects to two standard serial ports for networking two computers together. Null modem cables enable direct data transfer with a minimum of setup required. A null modem cable differs from ordinary serial cables the same way as Ethernet crossover cables differ from ordinary Ethernet cables. Null modem cables reverse the transmit and receive lines on end to enable direct two-way communication. A null modem cable for PCs ordinarily follows the RS-232 standard and uses the same serial ports as RS-232 cables. An RS-232 null modem cable transfers data at the rate of 115 Kbps. The fastest null modem cable, based on RS-422, supports up to 450 Kbps. Today, null modem cables are used primarily by engineers. USB keys, Ethernet crossover cables, and general purpose network routers have effectively made the null modem cable obsolete.

Question: Who invented the IP - the Internet Protocol?

Answer: No single person or organization created the modern Internet, including Al Gore, Lyndon Johnson, or any other individual. Instead, multiple people developed the key technologies that later grew to become the Internet: Email - Long before the World Wide Web, email was the dominant communication method on the Internet. Ray Tomlinson developed in 1971 the first email system that worked over the early Internet. Ethernet - The physical communication technology underlying the Internet, Ethernet was created by Robert Metcalfe and

David Boggs in 1973. TCP/IP - In May, 1974, the Institute of Electrical and Electronic Engineers (IEEE) published a paper titled "A Protocol for Packet Network Interconnection." The paper's authors - Vinton Cerf and Robert Kahn - described a protocol called TCP that incorporated both connection-oriented and datagram services. This protocol later

Question: How did the Internet get started?

Answer: (A) A 1969 U.S. Department of Defense study lead to the deployment of an experimental packet-switched network (the ARPANET) that eventually evolved into the Internet. The military theorized that a distributed data network would be more fault-tolerant than a telephone network, which could be disabled simply by attacking its central office

Question: I have two or more computers. How do I connect them to share files and printers?

Answer: Popular Network Types Ethernet: 10/100Mbps Home PNA 2.0 (Phone Line): 10Mbps Wireless 802.11b: 11 Mbps Wireless HomeRF 2.0: 10Mbps When choosing a network type (topology) for your home four things should be considered. Cost, Expandability, Location of Your PC's and speed. This article does not explain every networking type available, but each of the following network types offer a solution that is suitable for the home, has wide industry support and offers a good value for the money. Ethernet: The most popular network type for both home and business is Ethernet. Ethernet is fastest of the network types and can be the least expensive. Ethernet networks are very stable and your network speed will never fluctuate or be prone to interference like other network types are. Ethernet requires special cables running from each computer. These cables are plugged into a central 'ethernet hub' or 'switch'. If your computers are far apart, running cable in an existing home may be difficult. Pre-made ethernet cables come in sizes ranging from 3 feet to 50 feet. Ethernet adapters come in many shapes and sizes, but PCI Ethernet cards are both the fastest and least expensive. Ethernet can operate at 10Mbps or 100Mbps. When shopping for ethernet equipment, be sure to look for 100Mbps or 10/100Mbps equipment. 10Mbps equipment is older and slower than the 10/100Mbps equipment and the price difference has become nigligible. Note, older 10Mbps equipment will work just fine on 10/100Mbps networks. If only two computers are being connected, a single CROSSOVER cable can be used instead of the standard cables + switch method.

Question: How can one disable or enable Simple File Sharing in Windows XP?

Answer: Simple File Sharing permits controlling both sharing and NTFS permissions at the folder level. Network access is through a guest account. Windows XP Home Edition always has Simple File Sharing enabled. By default, it is turned off in Windows Professional when it

joins a workgroup. Classic file sharing is used when Windows XP Pro joins a domain. Windows XP Home cannot join a domain. Simple File Sharing can be disabled in Windows XP Pro when it is a member of a workgroup. When it is disabled security can be controlled for individual user accounts. To disable Simple File Sharing, click start, double-click My Computer, Tools, Folder Options, View tab, at the bottom of the list uncheck Use simple file sharing (Recommended).

Question: How do I check my network IP address in Windows XP (and in Windows 2000/NT)?

Answer: Open a DOS windows in Windows XP (Start, All Programs, Accessories, Command Prompt). Enter at the command prompt enter ipconfig, e.g... C:\Documents and Settings\Larry F. Byard>ipconfig Windows IP Configuration Ethernet adapter Local Area Connection: Connection-specific DNS Suffix . : IP Address. . . . . : 192.168.123.197 Subnet Mask . . . . . : 255.255.255.0 Default Gateway . . . . . : 192.168.123.254 To obtain the syntax for ipconfig, enter ipconfig /?. C:\Documents and Settings\Larry F. Byard>ipconfig /? USAGE: ipconfig [/? | /all | /renew [adapter] | /release [adapter] | /flushdns | /displaydns | /registerdns | /showclassid adapter | /setclassid adapter [classid]] where adapter Connection name (wildcard characters * and ? allowed, see examples) Options: /? Display this help message /all Display full configuration information. /release Release the IP address for the specified adapter. /renew Renew the IP address for the specified adapter. /flushdns Purges the DNS Resolver cache. /registerdns Refreshes all DHCP leases and re-registers DNS names /displaydns Display the contents of the DNS Resolver Cache. /showclassid Displays all the dhcp class IDs allowed for adapter. /setclassid Modifies the dhcp class id. The default is to display only the IP address, subnet mask and default gateway for each adapter bound to TCP/IP. For Release and Renew, if no adapter name is specified, then the IP address leases for all adapters bound to TCP/IP will be released or renewed. For Setclassid, if no ClassId is specified, then the ClassId is removed. Examples: > ipconfig ... Show information. > ipconfig /all ... Show detailed information > ipconfig /renew ... renew all adapters > ipconfig /renew EL* ... renew any connection that has its name starting with EL > ipconfig /release *Con* ... release all matching connections, eg. "Local Area Connection 1" or "Local Area Connection 2" If your PC is connected to the a device such as broadband router or cable MODEM with a DHCP server, you are using automatic IP addresses, and you want to test it, config /release and ipconfig /renew to release and renew the IP address lease. You should see it change, however, the new IP address may be the same as the old one.

Question: What is DHCP?

Answer: DHCP = Dynamic Host Configuration Protocol is an Internet protocol. It resides in a DHCP server and clients that use the server. Simply put, a DHCP server supplies Internet Protocol (IP) addresses when requested by client computers on a TCP/IP network that have TCP/IP configured to obtain their IP addresses automatically. A DHCP server is configured to use a range of IP addresses known as its scope. It automatically and dynamically manages the allocation of IP addresses within its scope. IP addresses are assigned to clients under a lease arrangement that can be set for to expire after a given time.

Question: When you have a cable MODEM from an ISP is the DHCP sitting at the ISP site?

Answer: Yes, one of them is. A DOCSIS (Data Over Cable Service Interface Specification) cable MODEM also has a DHCP server which supplies a local IP address that is used to connect to the ISP DHCP server top obtain an IP for the Internet. Is DHCP part part of the Windows 2000 Server the operating system? A DHCP server is included as a service with Windows NT/2000 Server. Windows 2000, 98 SE/Me, etc. Internet Connection Server (ICS) software includes a DHCP server.

Question: Can a Cat 6 modular plug be plugged into Cat 5 and 5e RJ-45 Jacks?

Answer: Yes. The physical dimensions of Cat 6 RJ-45 plugs and jacks are identical to Cat 5 and 5e plugs and jacks. They are backward compatible with Cat 3, Cat 5, and Cat 5e plugs and jacks.

Question: What is an Ethernet MAC address?

Answer: MAC = Media Access Control. Each and every Ethernet device interface to the network media (e.g., network adapter, port on a hub) has a unique MAC address, which is "burned" into the hardware when it is manufactured. MAC addresses uniquely identify each node in a network at the Media Access Control layer, the lowest network layer, the one that directly interfaces with the media, such as the actual wires in a twisted-pair Ethernet. In modern Ethernets the MAC address consists of six bytes which are usually displayed in hexadecimal; e.g., 00-0A-CC-32-FO-FD The first three bytes (e.g., 00-0A-CC) are the manufacturer's code and can be used to identify the manufacturer. The last three are the unique station ID or serial number for the interface. One can determine the MAC address of an operating Network Interface Card (NIC or network adapter) in Windows 9X/Me with Start, Run, enter winipcfg, and select the adapter. In Windows NT, 2000, and XP it can be determined by opening a DOS Window/Prompt (Start, Programs, Accessories...) and typing: C:\>ipconfig /all The MAC

address/station ID may be printed on the NIC. Many broadband routers can clone a NIC MAC address. That is, make the Wide Area Network (WAN) Ethernet interface going to a cable or DSL MODEM look like a NIC in a PC. This is useful in that many MODEMs marry themselves to a specific MAC address when they are first installed and it can be rather difficult to get them to marry themselves to a new MAC address. The WAN port MAC address on some routers can be manually changed (e.g., the SMC7004ABR).