Explain difference between baseband and broadband transmission.

Explain redirector.

Explain the HELLO protocol used for.

Explain a DNS resource record.

Explain External Data Representation.

Explain a pseudo tty.

Explain a Management Information Base (MIB).

Explain the difference between an unspecified passive open and a fully specified passive open.

What is the difference between POP3 and IMAP Mail Server?

What is ERD(Emergency Repair Disk)?

What are the Advantages and Disadvantages of DHCP?

What is Recovery Console?

What is a different between switch and Hub?

Explain traffic shaping.

Explain Project 802.

What do you meant by "triple X" in Networks?

Explain the minimum and maximum length of the header in the TCP segment and IP datagram

What is frame relay, in which layer it comes?

What is RAID?

What is attenuation?

Difference between bit rate and baud rate?

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

What is Gateway-to-Gateway protocol?

What is a Multi-homed Host?

What is SLIP (Serial Line Internet Protocol)?

What is RIP (Routing Information Protocol)?

What is Interior Gateway Protocol ?

Why EIGRP is more efficient in operation than IGRP ?

Name the four key technologies that are used by EIGRP ?

What is Enhanced Interior Gateway Routing Protocol ?

What is Banyan VINES ?

What is Data-Link Switching ?

Where is SMDS Interface Protocol used ?

What is Switched Multimegabit Data Service ?

What is the basic difference between transparent bridges and source-route bridges relative to the forwarding processes ?

What is Transparent Bridge ?

What is source-route bridging algorithm ?

Which are the three types of routing tables ?

What protocol is used by DNS name servers ?

BOOTP helps a diskless workstation boot. How does it get a message to the network looking for its IP address and the location of its operating system boot files ?

What are 10Base2, 10Base5 and 10BaseT Ethernet LANs ?

What is the difference between interior and exterior neighbor gateways?

What is External Data Representation?

What is a pseudo tty?

What is the Network Time Protocol?

What is anonymous FTP and why would you use it?

What does the Mount protocol do ?

What are TCP Ports?

What is Automatic Private IP Addressing (APIPA)?

What are private IP addresses?

What is DHCP?

What is an Ethernet MAC address?

What is ICMP?

Where can we find assigned port numbers?

How do applications coexist over TCP and UDP?

How does TCP try to avoid network meltdown?

What is the 6bone?

Why dont we have IPv5?

What is IPv6?

What is ARP?

Does IP Protect Data On The Network?

What is IP?

What is TCP/IP?

What is IPsec?

Difference between TCP\IP and UDP?

What is Domain Name Server ?

What is Domain Naming Service(DNS)?

What is URL?

What is Inet address?

Can you be able to identify between Straight- through and Cross- over cable wiring?

Explain the layered aspect of a UNIX system. What are the layers? What does it mean to say they are layers?

What is a router? What is a gateway?

What is UTPHow do cryptography-based keys ensure the validity of data transferred across the network?

What is binding order?

What is data link layer in the OSI reference model responsible for?

What's the meaning of ARP in TCP/IP?

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.

Answer : Redirector is software that intercepts file or prints I/O requests and translates t **Answer :** The HELLO protocol uses time instead of distance to determine optimal routing. It is an alternative to the Routing Information Protocol.

Answer :

A resource record is an entry in a name server's database. There are several types of resource records used, including name-to-address resolution information. Resource records are maintained as ASCII files.

Answer :

External Data Representation is a method of encoding data within an RPC message, used to ensure that the data is not system-dependent.

Answer :

A pseudo tty or false terminal enables external machines to connect through Telnet or rlogin. Without a pseudo tty, no connection can take place.

Answer :

Anonymous FTP enables users to connect to a host without using a valid login and password. Usually, anonymous FTP uses a login called anonymous or guest, with the password usually requesting the user's ID for tracking purposes only. Anonymous FTP is used to enable a large number of users to access files on the host without having to go to the trouble of setting up logins for them all. Anonymous FTP systems usually have strict controls over the areas an anonymous user can access.

Answer :

A Management Information Base is part of every SNMP-managed device. Each SNMP agent has the MIB database that contains information about the device's status, its performance, connections, and configuration. The MIB is queried by SNMP.

Answer :

An unspecified passive open has the server waiting for a connection request from a client. A fully specified passive open has the server waiting for a connection from a specific client.

Answer :

The using of IMAP to access your mailbox has advantages over POP3 and the difference of their working mechanism.

Mechanism of POP3
•Since email needs to be downloaded into desktop PC before being displayed, you may have the following problems for POP3 access:
You need to download all email again when using another desktop PC to check your email.
May get confused if you need to check email both in the office and at home.
The downloaded email may be deleted from the server depending on the setting of your email client.
•All messages as well as their attachments will be downloaded into desktop PC during the 'check new email' process.
•Mailboxes can only be created on desktop PC. There is only one mailbox (INBOX) exists on the server.
•Filters can transfer incoming/outgoing messages only to local mailboxes.
•Outgoing email is stored only locally on the desktop PC.
•Messages are deleted on the desktop PC. Comparatively, it is inconvenient to clean up your mailbox on the server.
•Messages may be reloaded onto desktop PC several times due to the corruption of system files.

Mechanism of IMAP
•Since email is kept on server, it would gain the following benefits for IMAP access:
No need to download all email when using other desktop PC to check your email.
Easier to identify the unread email.
•A whole message will be downloaded only when it is opened for display from its content.
•Multiple mailboxes can be created on the desktop PC as well as on the server.
•Filters can transfer incoming/outgoing messages to other mailboxes no matter where the mailboxes locate (on the server or the PC).
•Outgoing email can be filtered to a mailbox on server for accessibility from other machine.
•Messages can be deleted directly on the server to make it more convenient to clean up your mailbox on the server.
•The occurrence of reloading messages from the server to PC is much less when compared to POP3.

Answer :

To create an ERD:
1. Click Start, point to Programs, point to Accessories, point to System Tools, and then click Backup.
2. On the Tools menu, click Create an Emergency Repair Disk.
You can use the ERD for the following repair functions:
• Inspect and repair the startup environment.
• Verify the Windows 2000 system files and replace missing or damaged files.
• Inspect and repair the boot sector.
When you attempt to repair Windows 2000, it asks if you have an ERD diskette, if you do not have the diskett, press L and the computer attempts to locate your Windows 2000 installation to perform repairs. This process looks for the Boot.ini file on your computer partition and reads the ARC paths to your operating system(s). The computer then attempts to load the following hive for each ARC path:
%systemroot%\System32\Config\Software
This attempt finds which installation versions matches the installation CDROM used to do the repair.
If the Boot.ini file cannot be read, or the software hive is corrupt, the repair is not able to proceed. At this time, you must have a ERD diskette containing a valid Setup.log file for that computer before repairs are possible.
The registry hives saved during setup are in the following folder:
%systemroot%\repair
The registry hives are used during a FAST repair only, otherwise you need to use Recovery Console to manually copy a more recent registry hive saved by NTbackup in the following folder:
%systemroot%\repair\regback

Answer :

DHCP (Dynamic Host Configuration Protocol) allows your computer to automatically obtain a fully functional IP address from the central RPI DHCP server. Every time you boot up your computer, your operating system retrieves a new IP address. DHCP is the default network configuration for most operating systems. If however you need

to set up DHCP again, follow the instructions on the various Network Configurations webpages for your specific operating system. Static IP is a manual way of obtaining an IP address for your computer. The IP address is predetermined and always the same. A static IP address can be obtained for free from the VCC Help Desk by filling out a short form. There are a few advantages and disadvantages to using a static IP.
Advantages:
Your IP address remains the same so that you can run Internet services that require your IP address to remain the same in order for them to work properly (ie. Web Server, FTP Server).
If, for some reason, the RPI DHCP server is having difficulties handing out IP address, you will still be able to access the web, since your IP is predetermined.
Disadvantages:
You will only be able to effectively use your static IP address from your place of residence. You will be unable to use the web from other places on campus.
Configuring the network settings on your computer is more difficult for static IP than for DHCP, since DHCP is automatic and static IP is manual.

Answer :

The Recovery Console is a feature of the Windows 2000 and Windows XP operating systems. It provides the means for administrators to perform a limited range of tasks using a textual user interface. As its name suggests, its primary function is to enable administrators to recover from situations where Windows does not boot as far as presenting its graphical user interface

.
Answer :

Although hubs and switches both glue the PCs in a network together, a switch is more expensive and a network built with switches is generally considered faster than one built with hubs. When a hub receives a packet (chunk) of data (a frame in Ethernet lingo) at one of its ports from a PC on the network, it transmits (repeats) the packet to all of its ports and, thus, to all of the other PCs on the network. If two or more PCs on the network try to send packets at the same time a collision is said to occur. When that happens all of the PCs have to go though a routine to resolve the conflict. The process is prescribed in the Ethernet Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol. Each Ethernet Adapter has both a receiver and a transmitter. If the adapters didn't have to listen with their receivers for collisions they would be able to send data at the same time they are receiving it (full duplex). Because they have to operate at half duplex (data flows one way at a time) and a hub retransmits data from one PC to all of the PCs, the maximum bandwidth is 100 Mhz and that bandwidth is shared by all of the PC's connected to the hub. The result is when a person using a computer on a hub downloads a large file or group of files from another computer the network becomes congested. In a 10 Mhz 10Base-T network the affect is to slow the network to nearly a crawl. The affect on a small, 100 Mbps (million bits per scond), 5-port network is not as significant.
An Ethernet switch automatically divides the network into multiple segments, acts as a high-speed, selective bridge between the segments, and supports simultaneous connections of multiple pairs of computers which don't compete with other pairs of computers for network bandwidth. It accomplishes this by maintaining a table of

each destination address and its port. When the switch receives a packet, it reads the destination address from the header information in the packet, establishes a temporary connection between the source and destination ports, sends the packet on its way, and then terminates the connection. Picture a switch as making multiple temporary crossover cable connections between pairs of computers (the cables are actually straight-thru cables; the crossover function is done inside the switch). High-speed electronics in the switch automatically connect the end of one cable (source port) from a sending computer to the end of another cable (destination port) going to the receiving computer on a per packet basis. Multiple connections like this can occur simultaneously. It's as simple as that. And like a crossover cable between two PCs, PC's on an Ethernet switch do not share the transmission media, do not experience collisions or have to listen for them, can operate in a full-duplex mode, have bandwidth as high as 200 Mbps, 100 Mbps each way, and do not share this bandwidth with other PCs on the switch. In short, a switch is "more better."

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.

Answer :

It is a project started by IEEE to set standards that 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.

Answer :

The function of PAD (Packet Assembler Disassembler) is described in a document known as X.3. The standard protocol has been defined between the terminal and the PAD, called X.28; another standard protocol exists between hte PAD and the network, called X.29. Together, these three recommendations are often called "triple X"

Answer :

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

Answer :

Frame relay is a packet switching technology. It will operate in the data link layer. Because the protocol assumes it is functioning over a private connection, Frame Relay does not monitor whether the frame is error-free. A Frame Relay node can start switching traffic out onto a new line as soon as it has read the first two bytes of addressing information at the beginning of the frame. This lets a frame pass through several switches and arrive at its destination with only a few bytes' delay. Because the delays are relatively small, network latency is not much different from leased line connections, but costs are lower because the network is shared though the service provider. Frame Relay packets are routed through one or more virtual circuits known as DLCIs (Data Link Connection Identifiers). These are permanent virtual circuits that the service provider sets at subscription time. At this time the ISP also sets the CIR (Committed Information Rate), which specifies the amount of guaranteed bandwidth. If you send data frames faster than this rate, the network will flag the excess frames with a DE (Discard Eligibility) bit. The marked frames may still get to their destination, but they may also be discarded if the network is congested. When a company purchases a Frame Relay service, it can specify its desired CIR level. The higher the level set, the higher the cost. However, companies often set the CIR level to low or zero, thus saving money but also setting themselves up for potential data loss. On the other hand, because data is sent over a private line, it is less vulnerable to eavesdropping or alteration by malicious individuals.

Answer :

RAID (Redundant Array of Independent Disks) is a set of technology standards for teaming disk drives to improve fault tolerance and performance. Each RAID level represents a set of trade-offs between performance, redundancy, and cost.
RAID 0 — Optimized for Performance
RAID 0 uses striping to write data across multiple drives simultaneously. This means that when you write a 5GB file across 5 drives, 1GB of data is written to each drive. Parallel reading of data from multiple drives can have a significant positive impact on performance. The trade-off with RAID 0 is that if one of those drives fail, all of your data is lost and you must retore from backup.RAID 0 is an excellent choice for cache servers, where the actual data being stored is of little value, but performance is very important.
RAID 1 — Optimized for Redundancy
RAID 1 uses mirroring to write data to multiple drives. This means that when you write a file, the file is actually written to two disks. If one of the disks fails, you simply replace it and rebuild the mirror. The tradeoff with RAID 1 is cost. With RAID 1, you must purchase double the amount of storage space that your data requires.
RAID 5 — A Good Compromise
RAID 5 stripes data across multiple disks. RAID 5, however, adds a parity check bit to the data. This slightly reduces available disk capacity, but it also means that the RAID array continues to function if a single disk fails. In the event of a disk failure, you simply replace the failed disk and keep going. The tradeoffs with RAID 5 are a

small performance penalty in write operations and a slight decrease in usabable storage space.
RAID 0+1 — Optimize for Performance and Redundancy
RAID 0+1 combines the performance of RAID 0 with the redundancy of RAID 1. To build a RAID 0+1 array, you first build a set of RAID 1 mirrored disks and you then combine these disk sets in a RAID 0 striped array. A RAID 0+1 array can survive the loss of one disk from each mirrored pair. RAID 0+1 cannot survive the loss of two disks in the same mirrored pair.

Answer :

Attenuation is a general term that refers to any reduction in the strength of a signal. Attenuation occurs with any type of signal, whether digital or analog. Sometimes called loss, attenuation is a natural consequence of signal transmission over long distances. The extent of attenuation is usually expressed in units called decibels (dBs).

Answer :
Baud (pronounced /b??d/, unit symbol "Bd"), is a measure of the symbol rate, that is, the number of distinct symbol changes (signalling events) made to the transmission medium per second in a digitally modulated signal. The term baud rate is also commonly used to refer to the symbol rate. Bitrate (sometimes written bit rate, data rate or as a variable Rbit) is the number of bits that are conveyed or processed per unit of time. Bit rate is often used as synonym to the terms connection speed, transfer rate, channel capacity, maximum throughput and digital bandwidth capacity of a communication system.
"Bitrate" is sometimes used interchangeably with "baud rate", which is correct only when each modulation transition of a data transmission system carries exactly one bit of data.
Answer :
The default IP Maximum Datagram Size is 576. The default TCP Maximum Segment Size is 536.

Answer : GGP is a "min-hop" algorithm, i.e., its length measure is simply the number of network hops between gateway pairs. It implements a distributed shortest-path algorithm, which requires global convergence of the routing tables after a change in topology or connectivity. Each gateway sends a GGP routing update only to its neighbors, but each update includes an entry for every known network, where each entry contains the hop count from the gateway sending the update.

Answer :

A computer that is connected to more than one physical data link, these data links may or may not be attached to the same network. The host may send and receive data over any of the links but will not route traffic for other nodes. Multi-homed hosts are becoming increasingly common, making it possible to connect a host to more than one subnet simultaneously. This type of configuration provides a number of advantages including better throughput, reduced routing overhead and (possibly) secure communication between sensative networks through a trusted host. However,

although the connection of a multi-homed host might be quite innocent and with the best intentions, it can lead (and has been observed at SLAC) to disasterous results for the network as a whole if it is configured incorrectly. In particular a multihomed host acting as a router has the potential to cause unwanted traffic possibly denying service to many users.

Answer :

The Serial Line Internet Protocol (SLIP) is a mostly obsolete encapsulation of the Internet Protocol designed to work over serial ports and modem connections. It is documented in RFC 1055. On PCs, SLIP has been largely replaced by the Point-to-Point Protocol (PPP), which is better engineered, has more features and does not require its IP address configuration to be set before it is established.It is a very simple layer two protocol that provides only basic framing for IP. SLIP is used for communication between two machines that are previously configured for communication with each other. For example, your Internet server provider may provide you with a SLIP connection so that the providers server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you.

Answer :

The Routing Information Protocol, or RIP, as it is more commonly called, is one of the most enduring of all routing protocols. RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send.

Answer :

IGRP is a distance vector Interior Gateway Protocol (IGP). Distance vector routing protocols mathematically compare routes using some measurement of distance. This measurement is known as the distance vector. Routers using a distance vector protocol must send all or a portion of their routing table in a routing-update message at regular intervals to each of their neighboring routers. As routing information proliferates through the network, routers can identify new destinations as they are added to the network, learn of failures in the network, and, most importantly, calculate distances to all known destinations.

Answer :

Unlike most other distance vector routing protocols, EIGRP does not mandate a periodic update of routing tables between neighboring routers. Instead, it employs a neighbor discovery/recovery mechanism to ensure that neighbors remain aware of each other's accessibility. As long as a router receives periodic hello packets from its neighbors, it can assume that those neighbors remain functional. More importantly, it can assume that all of its routes that rely upon passage through those neighbors remain usable. Thus, EIGRP is much more efficient than conventional distance vector routing protocols because it imposes much less overhead on routers and transmission facilities during normal operation.

Answer :

EIGRP employs four key technologies, including neighbor discover/recovery, Reliable Transport Protocol (RTP), Diffusing Update ALgorithm (DUAL) finite-state machine, and a modular architecture that enables support for new protocols to be easily added to an existing network.

Answer :
The Enhanced Interior Gateway Routing Protocol (EIGRP) represents an evolution from its predecessor IGRP. This evolution resulted from changes in networking and the demands of diverse, large-scale internetworks. EIGRP integrates the capabilities of link-state protocols into distance vector protocols. Additionally, EIGRP contains several important protocols that greatly increase its operational efficiency relative to other routing protocols. One of these protocols is the Diffusing update algorithm (DUAL). DUAL enables EIGRP routers to determine whether a path advertised by a neighbor is looped or loop-free, and allows a router running EIGRP to find alternate paths without waiting on updates from other routers. EIGRP provides compatibility and seamless interoperation with IGRP routers. An automatic-redistribution mechanism allows IGRP routes to be imported into EIGRP, and vice versa, so it is possible to add EIGRP gradually into an existing IGRP network. Because the metrics for both protocols are directly translatable, they are as easily comparable as if they were routes that originated in their own autonomous systems (ASs). In addition, EIGRP treats IGRP routes as external routes and provides a way for the network administrator to customize them.
Answer :

Banyan Virtual Integrated Network Service (VINES) implements a distributed network operating system based on a proprietary protocol family derived from the Xerox Corporation's Xerox Network Systems (XNS) protocols. VINES uses a client/server architecture in which clients request certain services, such as file and printer access, from servers.

Answer :

Data-link switching (DLSw) provides a means of transporting IBM Systems Network Architecture (SNA) and network basic input/output system (NetBIOS) traffic over an IP network. It serves as an alternative to source-route bridging (SRB), a protocol for transporting SNA and NetBIOS traffic in Token Ring environments that was widely deployed before the introduction of DLSw. In general, DLSw addresses some of the shortcomings of SRB for certain communication requirements—particularly in WAN implementations. This chapter contrasts DLSw with SRB, summarizes underlying protocols, and provides a synopsis of normal protocol operations. The three primary functions of DLSw are :

•The Switch-to-Switch Protocol (SSP) is the protocol maintained between two DLSw nodes or routers.

•The termination of SNA data-link control (DLC) connections helps to reduce the likelihood of link layer timeouts across WANs.

•The local mapping of DLC connections to a DLSw circuit.

Answer :

The SMDS Interface Protocol (SIP) is used for communications between CPE (Customer premises equipment) and SMDS (Switched Multimegabit Data Service) carrier equipment. SIP provides connectionless service across the subscriber network interface (SNI), allowing the CPE to access the SMDS network.

Answer :

Switched Multimegabit Data Service (SMDS) is a high-speed, packet-switched, datagram-based WAN networking technology used for communication over public data networks (PDNs). SMDS can use fiber- or copper-based media. SMDS networks consist of several underlying devices to provide high-speed data service. These include customer premises equipment (CPE), carrier equipment, and the subscriber network interface (SNI). CPE is terminal equipment typically owned and maintained by the customer. CPE includes end devices, such as terminals and personal computers, and intermediate nodes, such as routers, modems, and multiplexers. Intermediate nodes, however, sometimes are provided by the SMDS carrier. Carrier equipment generally consists of high-speed WAN switches that must conform to certain network equipment specifications. These specifications define network operations, the interface between a local carrier network and a long-distance carrier network, and the interface between two switches inside a single carrier network.

Answer :

In a transparent bridged environment, bridges determine whether a frame needs to be forwarded, and through what path based upon local bridge tables. In an SRB network, the source device prescribes the route to the destination and indicates the desired path in the RIF.

Answer :

Transparent bridges were first developed at Digital Equipment Corporation (Digital) in

the early 1980s. Transparent bridges are so named because their presence and operation are transparent to network hosts. When transparent bridges are powered on, they learn the workstation locations by analyzing the source address of incoming frames from all attached networks. For example, if a bridge sees a frame arrive on port 1 from Host A, the bridge concludes that Host A can be reached through the segment connected to port 1. Through this process, transparent bridges build a table. The bridge uses its table as the basis for traffic forwarding. When a frame is received on one of the bridge's interfaces, the bridge looks up the frame's destination address in its internal table. If the table contains an association between the destination address and any of the bridge's ports aside from the one on which the frame was received, the frame is forwarded out the indicated port. If no association is found, the frame is flooded to all ports except the inbound port. Broadcasts and multicasts also are flooded in this way. Transparent bridges successfully isolate intrasegment traffic, thereby reducing the traffic seen on each individual segment. This is called filtering and occurs when the source and destination MAC addresses reside on the same bridge interface. Filtering usually improves network response times, as seen by the user. The extent to which traffic is reduced and response times are improved depends on the volume of intersegment traffic relative to the total traffic, as well as the volume of broadcast and multicast traffic.

Answer :

The source-route bridging (SRB) algorithm was developed by IBM and was proposed to the IEEE 802.5 committee as the means to bridge between all LANs. SRBs are so named because they assume that the complete source-to-destination route is placed in all inter-LAN frames sent by the source. SRBs store and forward the frames as indicated by the route appearing in the appropriate frame field. Assume that Host X wants to send a frame to Host Y. Initially, Host X does not know whether Host Y resides on the same LAN or a different LAN. To determine this, Host X sends out a test frame. If that frame returns to Host X without a positive indication that Host Y has seen it, Host X assumes that Host Y is on a remote segment. To determine the exact remote location of Host Y, Host X sends an explorer frame. Each bridge receiving the explorer frame copies the frame onto all outbound ports. Route information is added to the explorer frames as they travel through the internetwork. When Host X's explorer frames reach Host Y, Host Y replies to each individually, using the accumulated route information. Upon receipt of all response frames, Host X chooses a path based on some predetermined criteria. Host X must select one of these two routes. The IEEE 802.5 specification does not mandate the criteria that Host X should use in choosing a route, but it does make several suggestions, including the following:
•First frame received
•Response with the minimum number of hops
•Response with the largest allowed frame size
•Various combinations of the preceding criteria
In most cases, the path contained in the first frame received is used.

Answer :

The three types of routing tables are fixed, dynamic, and fixed central. The fixed table must be manually modified every time there is a change. A dynamic table changes its

information based on network traffic, reducing the amount of manual maintenance. A fixed central table lets a manager modify only one table, which is then read by other devices. The fixed central table reduces the need to update each machine's table, as with the fixed table. Usually a dynamic table causes the fewest problems for a network administrator, although the table's contents can change without the administrator being aware of the change.

Answer :

DNS uses UDP for communication between servers. It is a better choice than TCP because of the improved speed a connectionless protocol offers. Of course, transmission reliability suffers with UDP.

Answer :

BOOTP sends a UDP message with a subnetwork broadcast address and waits for a reply from a server that gives it the IP address. The same message might contain the name of the machine that has the boot files on it. If the boot image location is not specified, the workstation sends another UDP message to query the server

Answer :

10Base2—An Ethernet term meaning a maximum transfer rate of 10 Megabits per second that uses baseband
signaling, with a contiguous cable segment length of 100
meters and a maximum of 2 segments.
10Base5—An Ethernet term meaning a maximum transfer rate of 10 Megabits per second that uses baseband
signaling, with 5 continuous segments not exceeding 100
meters per segment.
10BaseT—An Ethernet term meaning a maximum transfer rate of 10 Megabits per second that uses baseband
signaling and twisted pair cabling.

Answer :

Interior gateways connect LANs of one organization, whereas exterior gateways connect the organization to the outside world.

Answer :

eXternal Data Representation (XDR) is an IETF standard from 1995 of the presentation layer in the OSI model. XDR allows data to be wrapped in an architecture independent manner so data can be transferred between heterogeneous computer systems. Converting from the local representation to XDR is called encoding. Converting from XDR to the local representation is called decoding. XDR is implemented as a software library of functions that is portable between different operating systems and is also independent of the transport layer.

Answer :

In Unix, a pseudo terminal is a pseudo-device pair that provides a text terminal interface without associated virtual console, computer terminal or serial port hardware. Instead, a process replaces the role of the underlying hardware for the pseudo terminal session.For each pseudo terminal, the operating system kernel provides two character devices: a master device and a slave device.The master and slave devices, in their most common deployment, form an association between a Unix shell and a terminal emulation program or some sort of network server.The slave device file, which generally has a nomenclature of /dev/ttyp*, has the appearance and supported system calls of any text terminal. Thus it has the understanding of a login session and session leader process (which is typically the shell program).The master device file, which generally has a nomenclature of /dev/ptyp*, is the endpoint for communication with the terminal emulator. It receives the control requests and information from the other party over this interface and responds accordingly.

Answer :

The Network Time Protocol is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NTP uses UDP port 123 as its transport layer. It is designed particularly to resist the effects of variable latency (Jitter).NTP is one of the oldest Internet protocols still in use (since before 1985).

Answer :

Anonymous FTP enables users to connect to a host without using a valid login and password. Usually, anonymous FTP uses a login called anonymous or guest, with the password usually requesting the user's ID for tracking purposes only. Anonymous FTP is used to enable a large number of users to access files on the host without having to go to the trouble of setting up logins for them all. Anonymous FTP systems usually have strict controls over the areas an anonymous user can access.

Answer :

The Mount protocol returns a file handle and the name of the file system in which a requested file resides. The message is sent to the client from the server after reception of a client's request.

Answer :

Data transmitted over a network using the Transport Control Protocol/Internet Protocol (TCP/IP), such as the Internet, includes address information that identifies the computer (32-bit IP address) and a port. Ports number (16-bit number) the ends of logical connections used for long-term data transfers between applications. For example port 80 is the standard File Transfer Protocol (FTP) port used by HyperText Transfer Protocol (HTTP) to send and retrieve web pages. Service contact ports or "well-known ports" are used to provide services to unknown callers. Port numbers are divided into three categories and ranges:

Well Known Ports are those from 0 through 1023
Registered Ports are those from 1024 through 49151
Dynamic and/or Private Ports are those from 49152 through 65535

Answer :

Windows 98, 98 SE, Me, and 2000 have an Automatic Private IP Addressing (APIPA) feature that will automatically assign an Internet Protocol address to a computer on which it installed. This occurs when the TCP/IP protocol is installed, set to obtain it's IP address automatically from a Dynamic Host Configuration Protocol server, and when there is no DHCP server present or the DHCP server is not available.After the network adapter has been assigned an automatic IP address, a computer can communicate with any other computers on the local network that are also configured by APIPA or have static IP address manually set to the 169.254.x.y (where x.y is the client's unique identifier) address range with a subnet mask of 255.255.0.0.

Answer :

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets (local networks):
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

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.

Answer :
MAC stands for 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. **Answer :**

Internet Control Message Protocol (ICMP) defines a small number of messages used for diagnostic and management purposes. ICMP depends on IP to move packets around the network on its behalf. ICMP is basically IP's internal network management protocol and is not intended for use by applications. Two well known exceptions are the ping and traceroute diagnostic utilities:
Ping sends and receives ICMP "ECHO" packets, where the response packet can be taken as evidence that the target host is at least minimally active on the network.
Traceroute sends UDP packets and infers the route taken to the target from ICMP "TIME-TO-LIVE EXCEEDED" or "PORT UNREACHABLE" packets returned by the network. (Microsoft's TRACERT sends ICMP "ECHO" packets rather than UDP packets, and so receives ICMP "TIME-TO-LIVE EXCEEDED" or "ECHO RESPONSE" packets in return.)

Answer :

The IANA(Internet Assigned Numbers Authority) allocates and keeps track of all kinds of arbitrary numbers used by TCP/IP, including well-known port numbers. The entire collection is published periodically in an RFC called the Assigned Numbers RFC, each of which supersedes the previous one in the series.

Answer :

Each application running over TCP or UDP distinguishes itself from other applications using the service by reserving and using a 16-bit port number. Destination and source port numbers are placed in the UDP and TCP headers by the originator of the packet before it is given to IP, and the destination port number allows the packet to be delivered to the intended recipient at the destination system.
So, a system may have a Telnet server listening for packets on TCP port 23 while an FTP server listens for packets on TCP port 21 and a DNS server listens for packets on port 53. TCP examines the port number in each received frame and uses it to figure out which server gets the data. UDP has its own similar set of port numbers.
Many servers, like the ones in this example, always listen on the same well-known port number. The actual port number is arbitrary, but is fixed by tradition and by an official allocation or "assignment" of the number by the Internet Assigned Numbers Authority (IANA).

Answer :

TCP includes several mechanisms that attempt to sustain good data transfer rates while avoiding placing excessive load on the network. Some of the TCP algorithm are "Slow Start", "Congestion Avoidance", "Fast Retransmit" and "Fast Recovery". TCP also mandates an algorithm that avoids "Silly Window Syndrome" (SWS), an undesirable condition that results in very small chunks of data being transferred between sender and receiver.

Answer :

The 6bone is the experimental IPv6 backbone being developed using IPv6-in-IPv4 tunnels. This is intended for early experimentation with IPv6 and is not a production service.

Answer :

IPv5 never existed. The version number "5″ in the IP header was assigned to identify packets carrying an experimental non-IP real-time stream protocol called ST. ST was never widely used, but since the version number 5 had already been allocated the new version of IP was given its own unique identifying number, 6.

Answer :
IP Version 6 (IPv6) is the newest version of IP, sometimes called IPng for "IP, Next Generation". IPv6 is fairly well defined but is not yet widely deployed. The main differences between IPv6 and the current widely-deployed version of IP (which is IPv4) are:
IPv6 uses larger addresses (128 bits instead of 32 bits in IPv4) and so can support many more devices on the network.
IPv6 includes features like authentication and multicasting that had been bolted on to IPv4 in a piecemeal fashion over the year **Answer :**

Address Resolution Protocol (ARP) is a mechanism that can be used by IP to find the link-layer station address that corresponds to a particular IP address. It defines a method that is used to ask, and answer, the question "what MAC address corresponds to a given IP address?". ARP sends broadcast frames to obtain this information dynamically, so it can only be used on media that support broadcast frames. Most LAN's (including Ethernet, FDDI, and Token Ring) have a broadcast capability and ARP is used when IP is running on those media.

s. **Answer :**

IP itself does not guarantee to deliver data correctly. It leaves all issues of data protection to the transport protocol. Both TCP and UDP have mechanisms that guarantee that the data they deliver to an application is correct. IP does try to protect the packet's IP header, the relatively small part of each packet that controls how the packet is moved through the network. It does this by calculating a checksum on the header fields and including that checksum in the transmitted packet. The receiver verifies the IP header checksum before processing the packet. Packets whose checksums no longer match have been damaged in some way and are simply discarded.

Answer :

Internet Protocol (IP) is the central, unifying protocol in the TCP/IP suite. It provides the basic delivery mechanism for packets of data sent between all systems on an internet, regardless of whether the systems are in the same room or on opposite sides of the world. All other protocols in the TCP/IP suite depend on IP to carry out the fundamental function of moving packets across the internet. In terms of the OSI networking model, IP provides a Connectionless Unacknowledged Network Service, which means that its attitude to data packets can be characterised as "send and

forget". IP does not guarantee to actually deliver the data to the destination, nor does it guarantee that the data will be delivered undamaged, nor does it guarantee that data packets will be delivered to the destination in the order in which they were sent by the source, nor does it guarantee that only one copy of the data will be delivered to the destination.

Answer :

TCP/IP is a name given to the collection (or suite) of networking protocols that have been used to construct the global Internet.The TCP/IP name is taken from two of the fundamental protocols in the collection, IP (Inernet Protocol) and TCP. These protocols work together to provide a basic networking framework that is used by many different application protocols, each tuned to achieving a particular goal. TCP/IP protocols are not used only on the Internet. They are also widely used to build private networks, called internets (spelled with a small 'i'), that may or may not be connected to the global Internet (spelled with a capital 'I'). An internet that is used exclusively by one organization is sometimes called an intranet.

Answer :

IPsec stands for "IP Security". The IPsec working group of the IETF is developing standards for cryptographic authentication and for encryption within IP.

Answer :

The primary difference between UDP and TCP lies in their respective implementations of reliable messaging. TCP includes support for guaranteed delivery , meaning that the recipient automatically acknowledges the sender when a message is received, and the sender waits and retries in cases where the receiver does not respond in a timely way. UDP, on the other hand, does not implement guaranteed message delivery. A UDP datagram can get "lost" on the way from sender to receiver, and the protocol itself does nothing to detect or report this condition. UDP is sometimes called an unreliable transport for this reason.
Another way in which UDP works unreliably is in the receipt of a burst of multiple datagrams. Unlike TCP, UDP provides no guarantees that the order of delivery is preserved. For example, a client application might send the following four datagrams to a server

D1

D22

D333

D4444

but UDP may present the datagrams to the server-side application in this order instead:

D333

D1

D4444

D22

In practice, UDP datagrams arrive out-of-order relatively infrequently — generally only under heavy traffic conditions.

Answer :

This is a server that matches up the URL of a website (eg www.kyapoocha.com) with its proper numeric IP address - it translates www.kyapoocha.com into the unique numeric IP address (69.72.210.210). Whenever you request a web page the web browser must consult the domain name server to find out what the numeric translation of the URL is. This is necessary because computers only understand the numeric IP address, whereas we humans prefer to use meaningful and more memorable text.

Answer :

It is very difficult to remember a set of numbers(IP address) to connect to the Internet. The Domain Naming Service(DNS) is used to overcome this problem. It maps one particular IP address to a string of characters.

Answer :

URL stands for Uniform Resource Locator and it points to resource files on the Internet. URL has four components: http://www. address. com:80/index.html, where http - protocol name, address - IP address or host name, 80 - port number and index.html - file path.

Answer : Every computer connected to a network has an IP address. An IP address is a number that uniquely identifies each computer on the Net. An IP address is a 32-bit number. Top of Form

Answer :

Straight-through is type of wiring that is one to to one connection Cross- over is type of wiring which those wires are got switchedWe use Straight-through cable when we connect between NIC Adapter and Hub. Using Cross-over cable when connect between two NIC Adapters or sometime between two hubs.

Answer :

A UNIX system has essentially three main layers:

. The hardware

. The operating system kernel

. The user-level programs

The kernel hides the system's hardware underneath an abstract, high-level programming interface. It is responsible for implementing many of the facilities that users and user-level programs take for granted.

The kernel assembles all of the following UNIX concepts from lower-level hardware features:

. Processes (time-sharing, protected address space)

. Signals and semaphores

. Virtual Memory (swapping, paging, and mapping)

. The filesystem (files, directories, namespace)

. Pipes and network connections (inter-process communication)

Answer :

Semaphore is a synchronization tool to solve critical-section problem, can be used to control access to the critical section for a process or thread. The main disadvantage (same of mutual-exclusion) is require busy waiting. It will create problems in a multiprogramming system, where a single CPU is shared among many processes. Busy waiting wastes CPU cycles.
Deadlock is a situation when two or more processes are waiting indefinitely for an event that can be caused by only one of the waiting processes. The implementation of a semaphore with a waiting queue may result in this situation.

Answer :

Routers are machines that direct a packet through the maze of networks that stand between its source and destination. Normally a router is used for internal networks while a gateway acts a door for the packet to reach the 'outside' of the internal network

Answer :

UTP — Unshielded twisted pair 10BASE-T is the preferred Ethernet medium of the 90s. It is based on a star topology and provides a number of advantages over coaxial media.
It uses inexpensive, readily available copper phone wire. UTP wire is much easier to install and debug than coax. UTP uses RG-45 connectors, which are cheap and reliable.

Answer :

Each IP packet is assigned a checksum, so if the checksums do not match on both receiving and transmitting ends, the data was modified or corrupted.

Answer :

The order by which the network protocols are used for client-server communications. The most frequently used protocols should be at the top.

Answer :

Data link layer is located above the physical layer, but below the network layer. Taking raw data bits and packaging them into frames. The network layer will be responsible for addressing the frames, while the physical layer is reponsible for retrieving and sending raw data bits.

Answer :

The “ARP” stands for Address Resolution Protocol. The ARP standard defines two basic message types: a request and a response. a request message contains an IP address and requests the corresponding hardware address; a replay contains both the IP address, sent in the request, and the hardware address.