CISCO **CCNA** Certification knowledge to pass the exam
(Taken from the **CISCO** WEB site)

Knowledge of OSI Reference Model

(1) Identify and describe the functions of each of the seven layers of the **OSI** reference model.

Open Systems Interconnection (OSI)
OSI consists of two environments; the OSI environment, which is made up of seven layers of OSI protocols and the local system environment, which is the end computer system. The reason for dividing the environment in this way was to avoid interfering with the innovation of the design and implementation of computer systems. OSI facilitates a vehicle to communicate between dissimilar or similar computer based systems. The local computer system environment has a closed operating system and performs its designed functions within these bounds. All application processes that do not require communicating with other systems to complete its tasks, will provide, the end result with out any problems. However when an application process needs to communicate with another application process located in a remote system, both systems must become open to the OSI environment Many operations and concepts are involved in this process. There is interaction between peer entities within a layer and interaction between layers.

Important concepts to understand OSI Layering are:

- Each layer performs unique and specific task
- A layer only has knowledge of its immediately adjacent layers
- A layer uses services of the layer below
- A layer performs functions and provides services to the layer above
- A layer service is independent of the implementation

The Application layer is unique among the seven layers in that, it has no layer above. The application consists of 'Service Elements' that are incorporated within the application process when it needs to become a part of the OSI environment.

CONCEPT OF A LAYER

Each layer contains a logical groupings of functions that provide specific services for facilitating a communication. A function, or a group of functions, making up a functional unit is a logical entity that accepts one or more inputs (arguments) and produces a single output (value) determined by the nature of the function. Functions can be grouped in a collective unit, which is then defined as (N) layer having (N+1) layer an upper layer boundary and (N-1) layer as a lower boundary. The N layer receives services from N-1 layer and provides services to N+1 layer.

SEVEN LAYERS OF THE OSI MODEL AND THEIR FUNCTIONS

- Layer 7 is the APPLICATION layer: provides services directly to applications. Responsible for identifying and establishing the availability of the intended partner, and required resources. It is also responsible for determining if there exist sufficient communication resources to reach the remote partner.

- Layer 6 is the PRESENTATION layer: Data encryption, decryption, compression and decompression are functions of this layer. It does this by using Abstract Syntax Notation 1 (ASN.1) ASN.1 standardization allows differing computer architectures to exchange data that are from differing computer architectures.

- Layer 5 is the SESSION layer: facilitates a dialog between communicating systems and controls the dialog. Offers three different dialogs, simplex, half-duplex and full duplex. Session is set up by connection establishment, data transfer and connection release.

- Layer 4 is the TRANSPORT layer: Segments data and also reassembles data from upper layers. Delivers data in a connection and connection less modes. Includes simplex (one way) half duplex (both ways one at a time) full duplex (both ways simultaneously). Also flow control and error recovery.

- Layer 3 is the NETWORK layer: Establishes a connection between two nodes by physical and logical addressing. Includes routing and relaying data through internetworks. This layer's primary function is to deliver packets from the source network to the destination network.

- Layer 2 is the DATA LINK layer: Ensures hardware addressing of the device, and delivery to the correct device. Translates data messages from upper layers to frames, enabling hardware to transmit upper layer messages as a bit stream. Provides flow control to the layer 2. Also carries a Frame Check Sequence to make sure the frame received is identical to the one transmitted.

- Logical Link Control (LLC) Sublayer of the Data Link Control layer provides flexibility to Network Layer and the Media Access Control (MAC) layer. It runs between Network Layer and the MAC sublayer of the data Link Layer.

- Media Access Control (MAC) Sub Layer of the Data Link Layer is responsible for framing. It builds frames from the 1s and 0s that the Physical Layer picks up from the wire.

- Layer 1 is the PHYSICAL layer: Which transmits the raw bit stream and includes electrical signaling and hardware interface.

(2) Describe connection orientated network service and connection less network service. Identify the key difference between them.

Department of Defense (DOD) model is analogous to the OSI model and is the model used in the TCP/IP protocol suite. Following are the layers of the DOD model:

DOD Model	Analogous to	OSI Model
• Process/Application		Application Presentation Session
• Host to Host		Transport
• Internet		Network
• Network Access		Data Link Physical

At the transport layer of OSI and the Host to Host layer of DOD, there is a connection establishment process with the end system. This is a very impotent process where the

sending system decides whether to use a reliable link, which is connection orientated, resource intensive or to use an unreliable link, connection less access to the end system with very much less resource utilization.

The two protocols involved in the connection establishment of the end system is Transmission Control Protocol (TCP) for reliable connection and User Datagram Protocol UDP for unreliable connection.

TCP is defined in the RFC 793 and defines a reliable, connection orientated full duplex byte stream for a user process. TCP creates a CONNECTION orientated service by contacting the end system and establishing a set of guidelines both can support. Such agreements as how much data segments can be transferred before an acknowledgement is received. TCP takes large blocks of data coming from upper layers and segments them. Then it adds numbers to the segments so the end system can sequence them at arrival and assemble the original block before sending it to the upper layer. When TCP creates a connection between two end systems, it is called a VIRTUAL CIRCUIT. This virtual circuit is created at the time the one system needs to send a data stream to the end system and takes it down when the data transfer is completed.

The three phases of the TCP are CONNECTION ESTABLISHMENT, CONNECTION MAINTENANCE and CONNECTION TIREDOWN.

UDP is defined in RFC 768. It is the protocol that does not consume system resources as much as TCP but it unreliable and transfers data to the destination system with out establishing a connection and hence, connectionless protocol. UDP sends data to the destination system in numbered segments same as TCP but it can not retransmit erred segments if they get lost or damaged.

- Key differences between connection orientated network service and connection less network service.

Packet header:	Connection orientated service	Connection less service
	Source Port, Destination Port	Source Port, Destination Port
	Sequence number	No Sequence Number
	Acknowledgement Number	No Acknowledgement number
	Data offset	No data offset
	Length of data	Variable length of data
	Flags	No flags
	Window	No window
	Check sum	Check sum
	Urgent pointer	No Urgent pointer
	Options and Padding	No Options and Padding

Both TCP and UDP use the concept of ports and sockets to identify a connection between two communicating computers. A connection-orientated service is mainly used for secure and reliable data transfer, where the requirement is also transfer of data in timely manner. If the underlying network, drops data packets because the network is congested or the end system buffers overflow, a connection orientated service can recover, but the connection less service cannot recover from such faults because, once the data frame leaves the sending systems buffer, it is cleared by the sending system and there are no acknowledgement sent to the sending system. To get the high reliability with the connection orientated system, large amount of system resources has to be allocated for buffers and CPU time. As for the connection less service it is analogous to mailing a letter and is not resource intensive. The buffers can be much smaller because the frame that is transmitted does not have to wait for an acknowledgment before been discarded. CPU utilization is much less for connectionless service because of the absence windowing mechanism.

(3) Describe Data Link addresses and Network Address, and identify the key differences.

Data Link addresses are the source address and the destination address of the 48 bit BIA of the hardware NIC card. At each interface these addresses change because, on route to the destination a frame has to pass may INC cards. Address Resolution Protocol (ARP) finds the MAC address when it moves to a different segment. Network layer address has a source and a destination address, which are end points of the transmitting and receiving systems. It provides routing and relaying functions to achieve it goal. It provides a transparent path to the transport layer for a best end to end packet delivery service.

(4) Identify at least three reasons why industry uses a layered model

Layered model avoids interfering with the innovation of design and implementation of computer systems
Facilitates communication between dissimilar systems
Allow changes to one layer with out changing other layers
Facilitate systematic network trouble shooting
Reduce the complexity of networking into more manageable layers and sub layers

(5) Define and explain the five conversion steps of data encapculation

- User information is converted to data
- Data is converted to segments
- Segments are converted to packets or datagrams
- Packets or datagrams are converted to frames
-
- Frames are converted to bits (1s and 0s)

(6) Define Flow Control and describe the three basic methods used in networkig

Flow control stops a sending station from flooding the receiver station buffers, if it has no resources to match the speed of data arriving from the receiving station. Once the buffers are emptied at the receiver, it sends a message to the transmitter to start sending again. It is called windowing and controls how much data is transmitted from one end to the other.

Has a fixed window say 7, the transmitting station sends seven packets before waiting for an acknowledgement packet. Once the acknowledgement is received at the receiver, it sends another seven packets.

Window size of one. Every packet sent to the receiver has to be acknowledged before the transmitter can send the next packet.
Variable window, if the receiving station for some reason finds difficult to catch up with buffer emptying, it then tells receiver to reduce the window size and the sender does so.

(6) List the key internetworking functions of the OSI network layer and how they are performed in a router.

Network layer of the OSI seven layer model conations many protocols that a router use to evaluate the best route it should take and it is updated regularly so the best route is available for the packet to be transported. Network layers primary function is to send packets from the originating network to destination network. After the router has decided the best path from source to the destination network, the router switches the packet to it. This is known as packet switching. Essentially, this is forwarding the packet received by the router on one network interface (NIC card), or port to the port that connects to the best path through the network cloud. An internetwork must continually designate all paths of its media connections. All routers in the internetwork cloud are connected by media (cables), each line connecting a router to another is numbered. Routers use these numbers as network addresses. These addresses posses and convey important information about the path of the media connections. They are used by routing protocols to pass packets from a source onward towards to its destination. The network layer creates a composite "network map" and a communication strategy model by combining information about the sets of links into an internetwork with path discrimination, path switching and route processing functions. It can also use these addresses to provide relay capability and to interconnect independent networks. Routers using network layer protocols streamline network performance by not letting unnecessary broadcasts get into the internetwok cloud.

Knowledge of WAN protocols

(8) Differentiate between the following WAN services: FRAME RELAY, ISDN/LAPD, HDLC and PPP

Frame relay is used to connect large number of sites in the network because it is relatively inexpensive to do so. The service provider gives you a frame relay circuit and is charged for the amount of data and the bandwidth you use as oppose to T1 circuit that charges with a flat monthly rate whether you use partial bandwidth or the full bandwidth regardless. Frame relay is a high performance WAN protocol that operates at the Data Link layer and the Physical layer of the OSI model.

Integrated Services Digital Network (ISDN) is designed to run over existing telephone networks. It can deliver end to end digital service carrying voice and data. ISDN operates at OSI model, physical layer, data link layer and network layer. It can carry multimedia and graphics with all other voice, data services. ISDN supports all upper layer protocols

and you can choose PPP, HDLC or LAPD as your encapsulation protocol. It has two offerings, Primary rate which is 23B+D channels. 23, 64 kbps and one 64kbps mainly used for signaling. The other is the Basic Rate which has 2B+D channels two 64kbps and one 16kbps.

At data link layer ISDN supports two protocols; LAPB and LAPD. LAPB is used to mainly transfer data from upper layers and has three types of frames. I-Frames carry upper layer information and carries out sequencing, flow control, error detection and recovery. S- Frames carry control information for the I-frame. LAPD provides an additional multiplexing function to the upper layers enabling number of network entities to operate over a single physical access. Each individual link procedure acts independently of others. The multiplex procedure combines and distributes the data link channels according to the address information of the frame. Each link is associated with a specific Service Access Point (SAP), which is identified in the part of the address field.

High Level Data Link Control (HDLC) is a bit oriented data link layer frame protocol that has many versions similar to LAP, LAPB, and LAPD. CISCO routers default encapsulation is HDLC, but it is proprietary to CISCO.

Point to Point Protocol (PPP) is a Data Link Layer protocol that can be used over ether asynchronous (dial up) or synchronous (ISDN) lines. It uses Link Control Protocol (LCP) to build and maintain data link connections. Included in PPP is the authentication protocols, PAP and CHAP, and data compression. It supports IP, IPX, AppleTalk, DECnet and OSI/CLNS.

(9) Recognize key Frame Relay terms and features

Frame Relay is a high performance WAN protocol that operates at the physical and data link layer of the OSI reference model. It was originally designed to operate on ISDN circuits, but today it is used on variety of network interfaces. To configure Frame Relay on a CISCO router, we have to specify it as an encapsulation on a serial interface. There are only two encapsulation methods are available, CISCO, the default and the type IETF. A frame Relay connection between CISCO devices the type: CISCO is used and between a CISCO device and a non CISCO device type IETF is used.

#encapsulation frame relay cisco or #encapsulation frame relay ietf

Frame Relay virtual circuits are identified by Data Link Connection Identifiers (DLCI). DLCIs are issued by the Frame Relay service provider. It is used to map IP addresses at each end of the virtual circuit. Local Management Interface (LMI) was developed by CISCO and others to enhance the CCITT-ITU standard with protocol features that allowed internetworking devices communicate easily with a Frame Relay network. LMI messages provide current DLCI values, global or local significance of the DLCI values and the status of virtual circuits. CISCO supports three types of LMIs: CISCO which is the default, ANSI and Q933A.

(10) List commands to configure, maps and subinterfaces

To configure DLCI (config-if) #frame-relay interface-dlci 16
Any number from 0 to 4292967295 can be as the DLCI number.
To configure LMI (config-if)#frame-relay lim-type q933a

Subinterfaces can have multiple virtual circuits on a single serial interface and treat each virtual circuit as a separate interface. The advantage of using subinterfaces is that you can assign different network layer characteristics each subinterface and virtual circuit, such as IP routing on one virtual circuit and IPX routing on another.
(config)# int s0.16 The serial interface s0 configured with a subinterface 16
There are two types of subinterfaces, point to point and multipoint. Point to point is used when a single virtual circuit connect one router to another. Multipoint is used when the router is in the middle of star virtual circuits.

Map command is used to map IP devices address at the end of the virtual circuits to DLCIs so that they can communicate. There are two types of mapping: Use Frame Relay map command and use inverse-arp function. Example of Frame Relay map command:
#int s).16
#encap frame relay ietf
#no inverse-arp
#ip address 172.16.30.1 255.255.255.0
#frame relay map ip 172.16.30.17 30 cisco broadcast

Example of Frame Relay inverse-arp command:
#int s0.16
#encap frame-relay ietf
#ip address 172.16.30.1 255.255.255.0

(11) List commands to monitor Frame Relay operation on the router

In the user mode key in the following:
Router>sho frame ?
ip show frame relay IP statics
lmi show frame relay lmi statics
map show frame relay map table
pvc show frame relay pvc statics
route show frame relay route
traffic show frame relay protocol statics

(12) Identify PPP operations to encapsulate WAN data on CISCO routers

Point to Point Protocol (PPP) is a data link protocol that can be used on asynchronous (dial up) or synchronous ISDN circuits. It uses Link Control Protocol (LCP) to build and

maintain data link connections. Some features included in PPP are: Password Authentication Protocol (PAP) and Challenge Handshake Password Authentication Protocol (CHAP). Data compression and multiprotocols such as IP, IPX , AppleTalk DECnet and OSI/CLNS are supported. Encapsulate PPP on the router
#int s0
#encapsulate ppp

(13) State a relevant use and context for ISDN networking

Integrated Services Digital Network (ISDN) can run on existing telephones lines to provide an end to end digital service for both domestic and business uses. ISDN can carry, in addition to voice and data, multimedia as well. ISDN can used as a backup circuit for high speed network links. CISCO routers can be configured to automatically dial up on an ISDN link when the main network link goes down.

(14) Identify ISDN protocols, function groups, reference points and channels

ISDN protocols were defined by CCITT (now ITU-T), and there are three protocols that define the complex transmission issues:

- Protocol specifications beginning with latter **E,** specify ISDN on the existing telephone network, ie; Analog lines.

- Protocol specifications beginning with letter **I,** specify concepts, terminology and services.

- Protocol specifications beginning with letter **Q,** specify trunk switching and signaling.

(15) Describe CISCO's Implementation of ISDN BRI

ISDN Basic Rate Interface (BRI), service provides two B channels and D channel, which is also known as 2B+D. B channels operate at 64 kbps and carries user information where D channel operates at 16 kbps and usually carry control and signaling information. D channel signaling protocol spans the OSI reference model's, Physical layer, Data link layer and the Network layer. The two 64 kbps lines can be used as a single 128 kbps channel. To place a call on ISDN is similar to placing a call on Plain Old Telephones (POTS). For ISDN network to identify a call placed on its network, you must use directory numbers and Service Profile Identifiers (SPID)s. These two items are given to you by the service provider. Directory number is a telephone number you will use when you call. The SPID is a number the telephone uses to identify equipment on your ISDN connection. Majority of switches in US are either AT&T 5ESS, 4ESS or Northern Telcom DMS 100. Attaching a CISCO router to ISDN needs either a Network

Termination 1 or an ISDN modem. If router has a BRI interface, (called Terminal End Point 1) then it is ready to be connected to the ISDN network.

```
Router#config t
Router(config)#isdn switch-type basic-dms100
Router(config)#int bri0
Router(config-if)#encap ppp
Router(config-if)#isdn spid 775456721
Router(config-if)#ppp authentication chap
```

IOS

(16) Log in to a router in user and privilege mode

CISCO IOS software has a command interpreter called Exec. Exec has two levels of access: User mode and privilege mode. These two levels serve as for access into the different levels of commands. In user mode one can only do: Check router status, connecting to remote devices, making temporary changes to terminal settings and viewing basic system information. In the privilege mode you can change the configuration of the router and get detail reports of router status. Test and run debug operations. Access global configuration modes.

When you first log into a router, press ENTER and you will be in the Exec mode. At the prompt it will ask if you need a password. **Router>** This is the User mode as stated above very little can be done at this level. When you type in Enable: Router>**Enable** and press return it will ask for the password. Once you key in the correct password, your in the privilege mode. Now the prompt will show you **Router#.**

(17) Use the context-sensitive help facility

One can receive help on any command by typing ? after the command. In the following example: Router# clock ? you typed in clock a space and the question mark, and pressed enter. Reply was as follows: set Set the time and date. Now you want to know what format to enter. So you put another question after the set as follows: Router# clock set ?. Now you will get the format in the reply as follows: hh:mm:ss: Current Time (hh:mm:ss)

(18) Use the command history and editing features

The user interface comes in with an editing feature to help you type in repetitive commands. One can turn off editing by typing **terminal no editing** and again turn it on by typing **terminal editing.**

The router keeps the last ten commands you entered during your console or terminal session, in a special memory buffer called command history. One can recall commands from the command history buffer and reuse them or modify slightly to save on typing. To see all the commands type the following at the command prompt Router#show history

and press enter. All commands you typed in will be shown. To increase the size of the command history buffer you type the following: Router#terminal history size 100. This will increase the size to 100 lines from the default value. VT 100 terminal emulation gives use of up down and side arrows in addition to the other keys as shown below:

- CTRL+A Move to the beginning of the command line
- CTRL+E Move to the end of the command line
- CTRL+F (or right arrow) Move one character forward
- CTRL+B (or left arrow) Move one character backward
- CTRL+P (or up arrow) Repeat previous command entry
- CTRL+N (or down arrow) Most recent command recall
- ESC+B Move backward one word
- ESC+F Move forward one word

(19) Examine router elements (**RAM,ROM,CDP,show**)

CISCO routers use the following type of memory:

- Random Access Memory (RAM) stores the running configuration when the router is running and it is cleared when switched off. Also provides cashing, routing tables and packet buffering. The IOS operates from RAM

- Flash Memory is an electrically erasable, re-programmable ROM that holds the operating system image and microcode. This facilitates the upgrades to the operating system with out replacing the chips on the motherboard.

- Read Only Memory (ROM) is used by the router to store bootstrap program, operation system software and Power On Self Test (POST). The ROM chips are installed in sockets on the router's motherboard, so that they can be replaced or upgraded. ROM holds the smaller version of IOS and is loaded during power up so the router can boot up.

- Nonvolatile RAM (NVRAM) This memory does not loose its information when the router is powered down. Stores the systems start up configuration file and the virtual configuration register.

Cisco Discovery Protocol (CDP) is CISCO's proprietary protocol that allows you to access configuration on other routers with a single command. By running Sub Network Access Protocol (SNAP) at the data link layer, two devices running different Network Layer protocols can communicate and learn about each other. These devices include all LAN and some WANs. CDP starts by default on any router version 1.3 earlier and discovers neighboring CISCO routers running CDP by doing a Data Link broadcasts. It does not matter what protocol is running at the network layer. Once CDP has disproved a router, it can then display information about the upper layer protocols, such as IP and IPX. The router caches the information it receives from its CDP neighbors. Any time a router receives up dated information that a CDP neighbor has changed, it discards the old information in favor of the broadcast.

There are many show commands available for the administrator to manage the router. They can be found by typing at the command prompt Router#sh ?.

(20) Manage configuration files from the privilege exec mode.

When the router is powered up, it does a self-test, then a loads the IOS image, and finds the configuration file and loads it. Startup configuration is in NVRAM and the operating system places it on to the RAM. To manage configuration files you must be in privilege mode. At start up you will be in user mode. To get to the privilege mode do the following: Router>enable, if passwords are enabled then enter them when asked. Now your in privilege mode. Router#. By typing **config t** you can modify configuration files. Following are commands for starting and saving configurations:

- Show startup-config — Shows the configuration that will loaded when the router boots.
- Show running-config — Show the configuration that is currently loaded to RAM and is running
- Erase startup-config — This command will erase the configuration in NVRAM and put you in to the initial configuration dialog
- Reload — This command will reload the startup-config to Memory
- Setup — This command starts the initial configuration dialog

Software version 10.3 and earlier should run the following router commands:

- Show config — Same as show startup-config

- Write term — Same as show running-config
- Write erase — Same as erase startup-config
- Write mem — Same as copy running-config startup config

(21) Control router password, identification and banner

There are five different passwords that is used to secure CISCO routers and they are as follows:

Enable secret is a cryptographic password used in version 10.3 and up. It has precedence over the enable password when it exists. One can configure this password, ether during the setup mode or by typing the following:
Router#config t
Router(config)#enable secret kit (kit is the password you entered)

Enable password is used when there is no enable secret and when you are using older software, and some older images. The administrator manually encrypts it. One can set this password during the setup process or by typing the following:

Router#config t
Router(config)#enable password athul (athul is the password)
If both passwords are present, both passwords can not be the same.

Virtual Terminal Password is used for Telnet sessions with the router. You can change the password at any time , but it must be specified or you will not be able to telnet in to the router. The password can be set up as follows:

Router#config t
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password kit (kit is the password)
Line vty 0 4 specifies the number of telnet sessions allowed in router. One can also setup a different password each line by typing line vty [port number]

Auxiliary Password is used to setup a password for the auxiliary port. This port is used to connect a modem to the router for remote console connection. It is set as follows:
Router#config t
Router(congfig)#line aux 0
Router(config-line)#login
Router(config-line) #password kit (kit is the password)

Console Password is used to setup a password for the console port. It can be set up as follows:

Router#config t
Router(config)$line con 0
Router(config-line)#login
Router(config-line)#password kit (kit is the password)

Entering a Banner
The banner added will be displayed when ever any one logs in to the CISCO router. The command to enter is banner #.motd. Message of the day (motd) has to start with a delimiting character. Type as follows: Router(config)#banner motd k (k is the delimiter) Now enter the text message and end with the character 'k'. So we enter the following: If you are not authorized log out immediately
K(and press enter)
Router(config)#end

(22) Identify the main CISCO IOS commands for router startup.

Router's configuration files contain the configuration of the router. There are two basic configuration files for each router: startup and running. Startup configuration is held in NVRAM and is accessed when router is started. The startup configuration is placed in RAM for the router to run. Following command will display the startup configuration.
Router#sh star

(23) Enter the initial configuration using the setup command

Setup command facility is an interactive facility that allows you to perform first time configuration and other basic configuration procedure on the router. The command parser allows you to make detail changes to your configuration. However, some major configuration changes do not require granularity provided by the command parser. In this case you can use the setup command facility to make major enhancements to the configuration. Set up can make add a protocol suite, to make major addressing schemes changes, or configure a newly installed interface. Setup command facility provides you with a high level view of the configuration and guides you through the configuration change process. If you are not familiar with CISCO products and the command parser, the setup command facility is a particularly valuable tool, because it asks you questions required to make configuration changes. To start setup, key in the following:
Router#setup and press enter.

(24) Copy and manipulate configuration files

Binary executable IOS image is held in flash memory. IOS image is the binary program that parses and executes the configuration, while IOS configuration tells the device its current configuration. You can copy the content of the flash to a TFTP server by entering the following command Router#copy flash tftp
One can copy TFTP server to flash memory by typing Router#copy tftp flash. An interactive dialog begins and asks whether to erase the entire content of the flash before copying the file. Content of the flash memory can be displayed by the command Router>sh flash

One can copy the current configuration from a router to a TFTP server by typing Router#copy run tftp.

Or telnet to the router, copy a TFTP configuration file to running conflagration by typing the following command: Router#copy run

(25) List the commands to load CISCO IOS software from: flash memory, TFTP server, or ROM.

One can specify where the router should look for the CISCO IOS software to create a fall back in case one configuration does not load or one needs to load from a TFTP server. To load the CISCO IOS from a TFTP server, use the following command string:
Boot system TFTP ios_filename TFTP_ipaddress. There are three places that the CISCO router can look for the a valid IOS: flash, TFTP server or ROM. Following commands will load the IOS from flash and ROM
Router(config)#boot flash
Router(config)#boot rom

(26) Prepare to backup, upgrade and load a backup CISCO IOS image

Use the TFTP server to backup the IOS image. Type the following command at the command prompt: Router(config) copy flash tftp. Flash memory can be used to upgrade the IOS without physically changing the EEPROM. To load a backup image can be carried out from TFTP server, flash and ROM. Typing the following command will cause the router to try the other alternatives if the flash configuration does not come up.
boot system flash ios_filename
boot system TFTP ios_filename
boot system rom

(27) Prepare the initial configuration of your router and enable IP

When you power up the router, it does a POST and finds and loads the IOS image, the operation system for the router. Before the router can function, as you want it to, it needs to finds its configuration and apply it. If the router does not find a configuration file and it

is not configured to find one on the network, it will begin the setup dialog. The setup is menu driven and all you have to do is to answer the questions. Setup dialog will let you get the router up and running with a very basic configuration. It will allow you to give a host name, set both password and secret password, enable any network layer protocols assign appropriate addresses to router interfaces and enable dynamic routing protocols.

Every CISCO router has a 16 bit configuration register, which is stored in a secial memory location in NVRAM. This register controls number of functions and some of which are listed below:

- Force the system in to the bootstrap program
- Select a boot source and default boot file name
- Enable or disable the console Break function
- Set the console terminal baud rate
- Load operating software from ROM
- Enable booting from a TFTP server

The configuration register boot field is the portion of the configuration register that determines whether the router loads an IOS image, and if so where to get it from. The least significant four bits, 0 through 3, make up the boot field. If the boot field is 0x0 (all four bits set to zeros) then the router will enter ROM monitor mode. If the boot field value is set to 0x1 (binary 0001) the router will boot from the image in ROM. If the boot field value is 0x2 through 0xF (binary 0000 through 1111) then the router will follow the normal boot sequence and will look for the boot system commands in the configuration file on the NVRAM.. Type Router# sh ver, will display the configuration register value currently in effect and the value that will be used at the next reload. Display line in the discussion is displayed on the screen is as follows:
Configuration register is 0x142 (will be 0x102 at next reload)

You can place special commands in the router's configuration file that will instruct it where to find the IOS image. If you do not specify a file name, the router will load the first valid file it finds in the flash memory. Following are the boot commands:

Router(config)#boot system flash Boots from flash
Router(config)#boot system tftp 172.16.1.150 Boots from a TFTP server with ip address 172.16.1.150
Router(config)#boot system ROM Boots from ROM (this is last resort if nothing works and should be changed after the flash is corrected)

Network Protocols

(28) Monitor Novell IPX operation on the router

Once you have IPX configured and running, following show commands can be used to verify and track router is communicating correctly:
Router#sh ipx servers.This command will show the content of the SAP table. Server name, IPX address, port, route, hops and interface.

Router#sh ipx route This command will display the IPX routing table entries that the router knows about. The router reports networks to which is connected to directly and also the networks that it has learned since coming on line.

If you were to up parallel IPX paths between routers, by default, the CISCO routers will not learn about these paths. The router will learn a single path to the destination and discard alternative parallel, equal cost paths. If you need more than one parallel path to a destination then the router has to be configured Router(config)#ipx maximum paths 2 (up to 512).

Router#sh ipx traffic. This command will display a summary of the number of IPX packets received and transmitted by the router. Summary will show IPX, RIP and SAP update packets.

Router#sh ipx int e0

The debug IPX command will display IPX packets as its running through your internetwork
Router#debug ipx routing can have two commands, debug routing activity or debug routing events. Since debug IPX command is CPU intensive, it should be switched off as soon as monitoring process is over as shown: Router#undebug ipx routing act

(29) Describe two parts of network addressing, then identify the parts in specific protocol address examples.

The 32 bit structure of the IP address is comprised of a network address and host address. Number of bits assigned to each of these components varies with the address class.
IP addressing is analogues to the address of a letter. Street address is analogues to the network address and the house number is analogues to the host address. The concept of subnetting allows the network portion of the address to be subdivided in to number of logical sections; subnets. With subnetting the two part IP address becomes a three part address, a network address, subnetwork address and a host address.

In Class A address, the most significant bit of the first octet is set to 0 and first octet is set for the network address, leaving 24 bits for the host address. This corresponds to possible network addresses of 0 to 127. The reserved values are 0 and 127, leaving 1 to 126 for network addressing in class A.

In Class B address, the most significant bit and one after it is set to 10 leaving 16 bits for the network address and 16 bits for the host address. This corresponds to possible network address of 128 to 191.

In Classes C address, the most significant bit and two bits after are set to 110 leaving 24 bits for network address and 8 bits for host address. This corresponds to possible network address of 192 to 223.

Class D and Class E is not required for the CCNA examination.

(30) Create different classes of IP addresses (and subnetting)

For the subnet address scheme to work, every host on the network must know which part of the host address will be used as the subnet address. This is accomplished by assigning a subnet mask to each host. Following are the subnet masks for each Class

• Class A	net.node.node.node	default subnet mask	255.0.0.0
• Class B	net.net.node.node	default subnet mask	255.255.0.0
• Class C	net.net,net,node	default sunet mask	255.255.255.0

(31) Configure IP addresses

Following commands will configure the IP address for the Ethernet interface 0
Router#config t
Router(config)#int e0
Router(config-if)#ip address 172.16.50.10 255.255.255.0
Router(config-if)#no shut

(32) Verify IP addresses

Router#sh ip int e0 will display the following:
Ethernet0 is up, line protocol is up
Internet address is 172.16.50.10 255.255.255.0
Broadcast address is 255.255.255.255
Also many other interface details

(33) List required IPX addresses and encapsulation type

IPX performs functions at layer 3 and 4 of the OSI model. It controls the assignment of IPX addresses (software addressing) on individual nodes, governs packet delivery across networks, and make routing decisions based on information provided by routing protocols, RIP or NLS. IPX is a connectionless protocol and it does not require an acknowledgement from the destination node. To communicate with upper layer protocols, IPX uses sockets. These are similar to TCP/IP ports, in that they are used to address, multiple independent applications running on the same machine.

Sequence Packet eXchange (SPX) is a connection-orientated protocol as oppose to IPX. Through it upper layers can be assured that the data was delivered from the source to the destination. SPX works by creating virtual circuits or connections between machines, with each connection having a specific connection ID, included in the SPX header.

Routing Information Protocol (RIP) is a distance vector routing protocol used to discover IPX routes through internetworks. It employs ticks (1/8 th of a second) and the hop count (number of routers between nodes) as metric for determine preferred routes.

Service Advertising Protocol (SAP) allows servers to advertise the services they provide on the network. There are three types of SAP packets defined: Periodic updates, service quires and service response.

Netware Link Services Protocol (NLSP) is an advanced link state routing protocol, intended to replace Novell RIP and SAP.

Netware Core Protocol (NCP) provides clients with server resources such as file access, security and printing.

IPX addressing is somewhat different from IP addressing. The administrator assigns the network part of the address and the node part is automatically assigned. IPX address has 80 bits or 10 bytes. It is divided in to network address, which is 4 bytes and the node address which is the remaining 6 bytes. An example of an IPX address is as follows: 0000.7C80.0000.8609.33E9. The first 8 hex digits (0000.7C80) represents the network part of the address, next 8 hex digits (0000.8609) represents the node part of the address and the last 4 hex digits (33E9) represents the socket.

Encapsulation or framing is the process of taking packets from upper layer protocols and building frames to transmit across the network. Encapsulation takes IPX datagarms from Layer 3 and builds frames at layer 2 to transmit on one of the supported media.

Encapsulation on following media is as follows:

• Ethernet		Cisco Keyword
Netware Frame:	Ethernet_802.3	novell-ether (default Netware 3.11)
	Ethernet_802.2	sap
	Ethernet_II	arpa
	Ethernet_snap	snap
• Token Ring		
Netware Frame:	Token-Ring	sap (default)
	Token-Ring_snap	snap

- FDDI

Netware Frame:	fddi_snap	snap (default)
	Fddi_802.2	sap
	Fddi_raw	novell-fddi

(34) Enable the Novell IPX protocol and configure interfaces

First you enable IPX routing and after you enable IPX protocol on each interface as follows:

Router(config)#ipx routing
Router(config)#int e0
Router(config-in)#ipx network 2100

You can add multiple frame types to the same interfaces follows: using the old way
Router(config)#int so
Router(config-in)#ipx netwok 3200 encap hdlc sec

Next is to use the current method:
Router(config)#int e0.100
Router(config-subif)#ipx network 2300 sap

(35) Identify functions of the TCP/IP Transport layer

The Transport layer protocol equivalent to the layer in the DOD model is the Host to Host protocol. Its main purpose is to shield the upper layer applications from the complexities of the network. Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) operate at this layer. TCP is a connection-orientated protocol, which means that it first establishes a connection on a virtual circuit between source and destination, before sending user data. UDP is a connection less protocol, which means the source is not concerned whether the datagram it sent to the destination, did arrive there or not. TCP and UDP both receive large chunks of data form the upper layers and they break them down to manageable segments so that they can be transmitted to their destinations. Each segment is numbered so that at the destination they can be reassembled. Only TCP keeps tract of this reassembly process, by requesting the missing segment from the source. If a segment is missing from a UDP transmission, the destination does not have a mechanism request it from the source. Therefore UDP is a unreliable protocol. TCP carries out error checking, and requests a retransmission, also through a windowing mechanism it controls the data flow so that receiver buffers are not

flooded by the source. TCP is a full duplex, connection orientated, reliable and accurate protocol.

(36) Identify the functions of the TCP/IP network layer protocol.

At network layer, the TCP/IP protocol suit has the Internet Protocol (IP) in operation. The function of IP includes, packet routing and providing a single network interface to the upper layers. The lower layers do not carry out any routing and routing occurs at the IP internet layer. To route, IP looks at each packet's IP address, then using a routing table it decides where a packet is to be sent next, choosing the best path. All hosts on a network has an IP address and it contains the required routing information to enabling the packet to travel to the destination. IP receive data segments from the next upper layer, which is the Host to Host layer and fragments them to datagrams or packets. Each datagram is assigned an IP address of the sender and the IP address of the recipient. Each machine that receives the datagram makes a routing decision based upon the packet's destination IP address. The IP packet has a header and in it there is a field which carries an IP type number. This number indicate the socket number that the IP datagram should use to pass the data to upper layer which is the Host to Host layer. Data travelling on the internet layer is, either a TCP datagrma or a UDP datagram.

(37) Identify Functions performed by ICMP

Internet Control Message Protocol (ICMP)is a management protocol and a messaging service provider for IP. Its messages are carried as IP datagrams. RFC 1256 ICMP Router Discovery Messages is an annex to ICMP, which affords hosts extend capability in discovering routes to gateways. Periodically, router advertisements are announced over the network, reporting IP addresses for its network interfaces. Hosts listens for these network infomercials to acquire route information. A router solicitation is a request for immediate advertisement and may be sent by a host when it starts up. Following are some common events and messages that ICMP relates to:

- Destination Unreachable: If a router cannot send an IP address any further, it uses ICMP to send a message back to the sender advertising it of the situation. For example if the router receives a packet destined to a network that the router does not know about, it will send an ICMP Destination Unreachable message back to the sending station.

- Buffer full: If a router's memory buffer for receiving in coming datagrams is full, it will use ICMP to send out this message.

- Hops: Each IP datagram is allotted a certain number of routers that it may go through, called Hops. If it reaches its limit of hops before arriving at its destination, the last router to receive that datagram deletes it. The executioner

router then uses ICMP to send an message to the originator that the datagram is dead.

- Ping: Packet Internet Groper uses ICMP echo message to check the physical connectivity of machines on an internetwork.

(38) Configure IPX access lists and SAP filters to control basic Novell traffic

Similar to IP access lists IPX has two types of access lists: Standard IPX Access Lists and Extended IPX Access lists.

Standard IPX access lists allow or deny packets based on source and destination IPX addresses. Template to enter standard IPX access lists is as follows:

Access-list (number from 800 to 899) (permit or deny) (source network IPX number) (destination network IPX number)

Following example will show how the access list will permit or deny access to IPX packets.

```
Router#config t
Router(config)#access-list 810 permit 30 10
Router(config)#int e0
Router(config-if)#ipx access-group 810 out
```

810 correspond to the 800 to 899 range. This access-list mean that any network other than 30 will be denied access network 10. If we wanted to allow access all networks to 10 other than 50 the access-list entry will be as follows:
Router(config)#access-list 810 deny 50 10
Once we configure the access-list we must apply it to the interface, and it applied as follows:
Router(config)#int e0
Router(config-if)#ipx access-group 810 out
Which means that the above restriction is applied to the interface Ethernet 0, IPX outgoing packets from the router to the network.

Extended IPX access lists can filter based on the following: Source network, source node, destination network, destination node, IPX protocol (SAP, SPX etc) and IPX sockets.

Template to enter the extended IPX access list is as follows:
access-list (number, 900 to 999) permit or deny (protocol) (source IPX network number) (source socket) (destination IPX network number) (destination socket)

Following example will show how the extended access list will permit or deny IPX network access using extended access lists

Router(config)#access-list 910 deny –1 50 0 10 0

This means that the access is denied to any IPX protocol type from IPX network 50 on all sockets to enter IPX network 10 on all sockets.
If you want to let any network access any network, any protocol and on any socket the entry will be as follows:

Router(config)#access-list 910 permit –1 –1 0 –1 0
Again once the access list is configured it has to be applied the interface as follows:
Router(config)int e0
Router(config-if)#access-group 910 out

IPX SAP filters are used to control access IPX devices. The template for implementing IPX SAP filters are as follows: access-list (number 1000 to 1099) (permit or deny) (source network.node address of the server) (service type)

Source address here is the IXP internal address for example 0000.7c80.0000.8609.33e9
Router(config)#access-list 1010 permit 0000.7c80.0000.33e9 0
Access list 1010 is in the range, 1000 to 1099 reserved for IPX SAP filters. This IPX SAP filter will allow packets from 0000.7c80.0000.8609.33e9 to enter the Ethernet interface and be included in SAP updates across the network. The last entry is the service type and we entered 0, which means all services should be allowed.

Now that we created the SAP filter, lets apply it to the interface for it to be operational. We apply it to the interface as follows:
Router(config)#int e0
Router(config-if)#ipx input–sap-filter 1010

Routing

(39) Add the RIP routing protocol to your configuration

Route Information Protocol (RIP) is a distance vector routing protocol that practices classfull routing, which is used to discover the cost of a given route in terms of hops and stores that information on a routing table.

The router can then consult the table to select the least costly most efficient route to a destination. It gathers information by watching for routing table broadcasts by other routers and updating its own table in the event that a change occurs. RIP routing tables has following minimum entries: IP destination address, A metric (1 to 15) indicative of the total cost in hops, of a particular route to a destination, IP address of a the next router that a datagram would reach , on the path to its destination, A maker signaling recent changes to a route, Timers, which are used to regulate performance, Flags, which indicate whether the information about the routers has recently changed, Hold-downs used to prevent regular update messages from reinstating a route that is no longer functional,

Split horizon used to prevent routing loops. A poison reverse updates used to prevent routing loops. RIP sends out routing updates at regular intervals and whenever a network topology changes occurs. And uses the following timers to regulate its performance.

Routing table update timer typically 30 seconds
Route invalid timer 90 seconds
Route flush timer 240 seconds
To add RIP routing to a router type in the following:
Router#config t
Router(config)#router rip
Router(config-router)#network 172.16.0.0
Router(config-router)#^Z
Router#wr mem (write to the running configration)

(40) Add the IGRP routing protocol to your configuration

Interior Gateway Routing Protocol (IGRP) is a CISCO proprietary, distance vector interior routing protocol that was designed by CISCO to overcome the limitations presented by RIP. IGRP hop count is 255 as oppose to RIP's limited 15 hop count.

IGRP advertises three types of routes:
Interior: These are routes between subnets. If a network is not subnetted then IGRP will not advertise the interior routes.

System: These are routes to networks within an Autonomous System. They are derived from directly connected interfaces, other IGRP routes, or access servers. They do not include subnet information.

Exterior: These are routes to networks out side of the Autonomous System. They are considered when identifying a gateway of last resort. The gateway of last resort is chosen from the list of exterior routes that IGRP provides.

Type in the following to add IGRP routing
Router(config)#router igrp 10 (10 is the Autonomous System number it can be any number from 1 to 65535)
Router(config-router)#network 172.16.0.0
Router(config-router)#^Z
Router#wt mem

(41) Explain the services of separate and integrated multiprotocol routing

A separate protocol routing is when the routing device, eg: a switch uses a routing table based on MAC address, and can accommodate only one encapsulation type. This type of routing is carried out at the data link, MAC sublayer.

Multiprotocol routing is carried out mostly by routers and similar devices because, the routing decisions are made at network layer and the routing tables are at network layer. At network layer there can exist, many different protocols and with them comes their own associated routing tables. So a router can have a IP routing table, IPX routing table and a Apple Talk routing table.

A bridge or a switch connects two or more physical networks into a single logical network, where as routers connects two or more logical networks and routes between them using information that is built by routing protocols and kept in routing tables. The advantage of a router as compared to a bridge or a switch is that it physically and logically breaks a network in to multiple manageable pieces, allows for control of routed packets, and routes network layer protocols at the same time.

(42) List problems that each routing type encounters when dealing with topology changes and describe techniques to reduce the number of these problems.

(43) Describe the benefits of network segmentation with routers

Routers filter by both the hardware and network addresses. Routers only forward packets to the network segment that the packet is destined for. The benefits of network segmentation could be summarized as follows:

Manageability: Multiple routing protocols give the flexibility of designing for optimum requirements of the network.

Increased functionality: CISCO routers addresses the issues of flow control, error control congestion control and fragmentation, Also efficient control over packet lifetime.

Multiple active paths: Using the protocols DSAPs, SSAPs and path metrics, routers can make informed routing decisions as well as interpret the next layer protocol. CISCO routers can have more than on active link between routers.

Network Security

(44) Configure standard and extended access lists to filter IP

Access lists are used to control access via a router to the network or from the network to another network or to a device attached to the router. Packet filtering is performed by the access lists, to either, entering packets to the router, or exiting packets from the router. Apart from providing security to the network, access lists provide valuable static on packet flow.

Access lists are a list of conditions that the network designer can enforce to get total control of access to the network and exit from the network. When you apply the access list to the router interface, it has the total control of packets entering and leaving the interface. Configuring the Standard IP access list and applying to the interface is as follows: First you configure the access list then you apply it to the interface.
Configure access list as follows using the template:
Access-list (number) (permit or deny) (source address)
Router(configt)#access-list 10 permit 172.16.30.2
Access list number for standard IP access list is any number from 1 to 99
Now we apply it to the interface as follows:
Router(config)#int e0
Router(config-if)#access-group 10 out
out at the end of the command means that the restriction is for the packets going out of the e0 interface.

(45) Monitor and verify selected access lists

Router#sh access –1 Will show all the access lists running on the router. Following example will show the output;
Extended access list 110
Permit tcp 172.16.50.2 host 172.16.10.2 eq 8080 (34 matches)
What the above two lines show is as follows: first line gives the access number, which is 110 an extended IP access list (any number from 100 to 199). The second line shows the number of packets that matched.

Router#sh ip access-list Will show only the IP access lists as shown below
Extended IP access list 110
Permit tcp host 172.16.50.2 host 172.16.10.2 eq 8080 (15 matches)

If the log command was used on the access list the console will then display the following:
Access list number, Source address, Source port, Destination address Destination address, Number of packets.

When monitoring access lists it is important to find out which interface an access list applied to. The two commands to display this information is
Router#sh int e0 and Router#sh run

LAN Switching

(46) Describe the advantage of LAN segmentation

A single Ethernet LAN will work well for a limited number of users attached to the Ethernet. As time goes by and the number of users attached to the Ethernet increases and the number of people want to get on the network at the same time also increases.

Congestion begins to creep in and the user access to the network begins to slow down. The remedy for this situation is to segment the LAN in to manageable parts so that each part or segment has a amount of users attached to it so that it will get congested even if all the users access simultaneously. There are many ways to do this segmentation.

(47) Describe LAN segmentation using Bridges

Physical segmentation: You can segment by bridges and routers. Bridges segment at the MAC address of the Data Link layer. A bridge will first look at a routing table and match the packet to a segment and forwards it.

(48) Describe LAN segmentation using Routers

Routers use the network layer to segment the network with network layer address and the MAC address of the interface. The routing table will give the MAC address and the network layer addressing protocol address. eg IP address, IPX address or apple Talk address.

(49) Describe LAN segmentation using Switches

LAN switches uses at line speed by using the destination MAC address. In order to ensure that the packet is forwarded to the correct port, cut through switching is used. Cut through looks at the in coming frame FCS has passed it as error free, it looks at the destination MAC address and starts to forward before the full packet is received. Cut through switching greatly improves the throughput.

(50) Name and describe two switching methods

The two switching methods or modes are Store and Forward, and Cut Through.

With Store and Forward switching method, the LAN router copies the entire frame in to its buffer and checks the following and discards the frame if they are not correct:
A CRC error, if the frame is runt (less than 64 bytes including the CRC) or a giant (more than 1518 bytes including CRC). The frame has no errors then the router looks up the routing table and sends to the correct interface for transmission down the line. Latency due to this error checking varies with the length of the frame.

Cut Through switching, the LAN switch copies only the destination address to its buffers (six bytes after the preamble). It then looks at the destination address on the switching table, determines the outgoing interface and submits it to the correct interface for transmission down the line. Cut through switching reduce latency because, first it does not copy the complete frame to the buffer and secondly it starts to transmitting the frame as soon as it locate the destination address from the routing table.

(51) Describe full and half duplex Ethernet operation

Full duplex can transmit and receive simultaneously, but to do so one needs a CISCO switch that has a full duplex interface. The end user needs a full duplex NIC card so that it can be connected to the switch full duplex switch interface. Full duplex Ethernet uses point to point connections and it is collusion free transmission. This is because it does not share bandwidth with any other device. The frames sent by two nodes can not collide because they are on physically separate transmit and receive circuits. If you have a full duplex 10 Mbps Ethernet operating on the same switch port it can theoretically have a throughput of 20 Mbps.

Half duplex will send and receive, one at a time. When the transmitter is transmitting his receiving circuit is in active. Same with the receiver, when his receiving circuit is active his transmitting circuit is inactive.

(52) Describe the congestion problem in Ethernetworks

Ethernet device gets access to the network by listening to the signals on the cable. If no one is transmitting then the device starts to transmit. If two devices start to transmit at the same time a collusion will occur and each station will back off and retransmit the frame later. This is good for a small number of devices attached to the network but when there are too many devices gets attached, the collisions become more frequent and delays occur.

(53) Describe the benefits of network segmentation with bridges

Bridges segment the network by the MAC address of the data link layer. By segmenting a logical network in to multiple physical segments, it ensures network reliability, availability, scalability and manageability.

(54) Describe the benefits of network segmentation with switches.

Just like bridges LAN switches use destination MAC address in order to ensure that the packet gets to the right out going port. Switches are similar to bridges with more ports attached to it.

(55) Describe the features and benefits of fast Ethernet

Fast Ethernet is the IEEE 802.3u standard also known as 100 Base T. It is 10 times faster because the bit rate is 100 Mbps instead of 10 Mbps for 10 Base T. This standard defines the physical layer and the data link layer, and uses the same CSMA/CD transmission technology as 10 Base T. The other standards associated with Fast Ethernet are as

follows: 100 Base FX which is 100 Mbps two strand multi mode 50/125 or 62.5/125-micron fiber optic cable. 100 Base T4 can use CAT 3,4,or 5 cabling with RJ 45 connector. 100 Base TX can use CAT 5 or 100 ohm two pair shielded twisted pair or type 1 cable.

Benefits of fast Ethernet can listed as follows:

- 100 Base T is 10 times faster as 10 Base T
- Existing cabling and network equipment can be used
- 10 Mbps and 100 Mbps can exist on the same cable media
- It uses tried and tested CSMA/CD
- Migration to 100 Mbps from 10 Mbps does not create any problems

(56) Describe the guide lines and distance limitations of Fast Ethernet

To exist on the same cable media, 10 Base T and 100 Base T, the time slots should be the same. Standard defined round trip is shorter for 100 Base T. Therefore maximum distance between transmitter and receiver is shorter for 100 Base T. Maximum distance between end nodes for 100 Base TX is 100 meters and for 100 Base FX is 412 meters

(57) Distinguish between Cut Through and Store and Forward LAN switching

Cut through switching, the LAN switching device copies destination address to its in put buffer and looks at the destination switching table for the destination address. As soon as it finds the destination address, it starts to transmit the frame to the destination. This reducers the latency associated with store and forward

Store and forward switching, the LAN switching device copies the entire frame to its in put buffer and does a CRC check, runt check and a giant check on the frame. If any of them checks gives errors then the frame is dropped, if not it looks at the routing table and locates the destination address and sends the frame to the appropriate interface to transmit it down the line. All these checks take time and latency time increases for store and forward switching.

(58) Describe the operation of Spanning Tree Protocol and its benefits

IEEE 802.1d standard defines the Spanning Tree Protocol and was developed to prevent routing loops in a network. If a router, a switch or a hub has more than one path to the same destination, then a routing loop problem could occur. To prevent this, the spanning tree protocol is executed between devices to detect and logically block redundant paths on the network. For fault networks there should be redundant links between devices, and to be loop free it should also execute the spanning tree protocol.

(59) Describe the benefits of virtual LANs

Virtual LAN (VLAN) is a logical group of end users and resources connected to defined ports on a switch. This logical group communicates at layer 2 and layer 3 to establish the Virtual LAN. Most beneficial asset in implementing is the functional group. It is secure because on out side of the VLAN group can get access to the group and the members of the group can not go out side of the group. Next item is that if a member of the VLAN group is moved from one floor to another, no set ups are required because the member can go to the next floor be connected to a different switch with a port that is in the same VLAN group. Because VLAN operates at layer 2 and 3, broadcasts can be controlled.

Following are the primary benefits of VLAN: Broadcast control, Functional groups and Security.

(60) Define and describe the function of the MAC address

Media Access Control (MAC) address is the hardware address of the interface and it is burned in to the NIC card. This is a unique number issued by IEEE to the manufacturer. It is 6 bytes long and the first 24 bits represents the vendor and next 24 bits represents the serial number of the NIC card. This hardware address is used by the MAC layer of the Data Link layer to identify uniquely, the LAN device, to the network layer.